some of

CRYPTOCURRENCY

گرداورنده : مصطفی جلیلیانفر

نسخه صفر (فروردین ۱۳۹۸)

فهرست

پیشگفتار

این کتاب مجموعه ای از مقالات و مطالب گرداوری شده از سایت های پارسی از اینترنت می باشد . تعدادی از مقالات دارای ایراداتی هستند و برای تعدادی از عناوین، مطلب یا مقاله ای یافت نشد یا مقاله ای بدرخور وجود نداشت و یا گردآورنده موفق به یافتن آن نشد. بنا به دلایل ذکر شده کتاب فاقد یکپارچگی کلامی است . امید آن است که در نسخه بعدی با ترجمه مقالات انگلیسی و یا افزودن مقالات فارسی مناسب همه عناوین تکمیل گردند.

ارز دیجیتال Cryptocurrency

واژه ارز دیجیتال برگردان پارسی واژه انگلیسیcryptocurrency است. این واژه از دو عبارت crypto به معنای رمز و currency به معنای ارز تشکیل شده است. به همین دلیل گاهی از معادل رمزارز، ارز رمزگذاری شده یا ارز رمزینه برای این مفهوم نیز استفاده می‌شود. ارز دیجیتال در واقع یک شکل الکترونیکی از پول است که به صورت رمزنگاری شده در اینترنت از یک آدرس به آدرس دیگر انتقال داده می‌شود .

اطلاعات مربوط به مالکیت ارز دیجیتال و تراکنش‌ها بر روی دفترکل توزیع شده یا Distributed ledger قرار دارد .این شبکه اطلاعات مذکور را در اختیار عموم قرار می‌دهد و همه کاربران می‌توانند سابقه تراکنش‌ها را ببینند.

تاریخچه ارزهای دیجیتال

ریشه‌های ارز دیجیتال به ایجاد شرکت دیجی‌کش در اواخر دهه ۹۰ میلادی توسط دیوید چاوم برمی‌گردد. دیجی‌کش که در آن از علم رمزنگاری استفاده شده بود، بستری برای بانک‌ها فراهم می‌کرد تا به وسیله آن قابلیت انتقال ارزش به صورت الکترونیکی فراهم شود.

یکی از اولین ها ای-گلد با پشتوانه طلا در سال ۱۹۹۶ ایجاد شد. یکی از پول‌های دیجیتال مطرح دیگر Liberty Reserve بود که در سال ۲۰۰۶ به‌وجود آمد. این سرویس به کاربران اجازه می‌داد تا پول دلار یا یوروی خود را به Liberty Reserve تبدیل کرده و بتوانند آن را آزادانه با دستمزد ۱٪ بین یکدیگر رد و بدل کنند. هر دوی این سرویس‌ها متمرکز بوده و برای استفاده در پول‌شویی شهرت داشتند. همین امر سبب شد تا دولت آمریکا هر دو سرویس را تعطیل کند. گسترش تازه ارز رمزی علاقه به استفاده مجدد از پول‌های دیجیتال را افزایش داده است. این امر با معرفی بیت‌کوین در سال ۲۰۰۹ همراه بود که آن را به بزرگ‌ترین و موردِ قبول‌ترین پول دیجیتال تبدیل کرد. نقطه قوت بیت‌کوین در برابر سایر نمونه‌های پیشین استفاده از فناوری دفتر کل توزیع شده بود.

در چند سال گذشته ارزهای دیجیتال زیادی معرفی و عرضه شده اند. در حال حاضر بیش از ۳۰۰۰ ارز دیجیتال خصوصی و عمومی در بازارهای جهانی تجارت می شود.

تفاوت ارزهای فیات و ارزهای دیجیتال

ارزهای فیات (مانند ریال و دلار و ...) توسط بانک مرکزی هر کشور منتشر می‌شود. پشتوانه این پولها معمولا اقتصاد آن کشور و در گذشته ذخایر طلای آن کشور بوده است. اما ارز دیجیتال این گونه نیست و بیشتر آنها بدون هر نوع پشتوانه فیزیکی منتشر می‌شوند. البته استثناهایی وجود دارد که پشتوانه آنها دلار، یورو، طلا و ... می باشد (مانند tether که پشتوانه آن دلار آمریکاست).

دومین تفاوت پول فیات با ارز دیجیتال به ساختار تراکنش آنها مربوط می‌شود. در تراکنش‌های آنلاین بین دو نفر، یک واسطه (معمولا) بانک وجود دارد که بر آن نظارت می‌کند. اما نقل‌وانتقال ارز دیجیتال بین دو نفر به صورت همتا به همتا صورت می‌گیرد. به جای وجود یک نهاد واسطه مرکزی. درستی تراکنش در ارز دیجیتال توسط شبکه‌ای از کاربران که بر روی شبکه آن ارز حضور دارند تایید می‌شود.

بازگشت ناپذیری تراکنش‌های ارز دیجیتال سومین تفاوت است. در حالت عادی و در خریدهای آنلاین، در صورت بروز مشکل و یا اعتراض پرداخت‌کننده، امکان پیگیری و کنسل کردن تراکنش وجود دارد. اما تراکنش در ارزهای دیجیتال این طور نیست و در صورت انجام دیگر بازگشت‌پذیر نخواهد بود.

حفظ هویت کاربر تفاوت بعدی است. در تراکنش‌های معمول آنلاین، هویت کاربر احراز می‌شود، اما در ارزهای دیجیتال هویت کاربر محفوظ می‌ماند. البته هر از گاهی اخباری در زمینه احتمال شناسایی هویت کاربران در این فضا نیز منتشر می‌شود. همچنین کارمزد تراکنش‌های ارز دیجیتال پایین‌تر از شیوه معمول بوده و یا حتی گاهی صفر است. حفظ هویت کاربر، عدم نیاز به واسطه، کارمزد پایین و سرعت بالای انجام تراکنش از مهم‌ترین مزایای ارزهای دیجیتال به شمار میرود.

دفترکل توزیع شده Distributed Ledger

دفتر کل محلی است برای ذخیره و نگهداری داده ها، اما پیدایش آن با پیدایش پول همزمان بود. در زمان های قدیم اطلاعات مربوط به حساب ها در ابتدا بر روی لوح های گلی و چوب نوشته می‌شد و با گذر زمان و پیشرفت تکنولوژی این اطلاعات بر روی کاغذ و بعد از پیدایش کامپیوترها به صورت دیجیتالی بر روی کامپیوترها ذخیره می‌شد.

دفتر کل توزیع شده پایگاه داده ای است که بر اساس سازوکار تفاهم و معماری داده مورد قبول مشارکت کنندگان شبکه نگهداری و به‌روزرسانی می‌شود یک شبکه همتا به همتا به همراه الگوریتم اجماع مورد نیاز است تا از تکرار در سراسر گره‌ها اطمینان حاصل شود.

دفتر کل توزیع شده همانطور که از نامش مشخص است مرکزیت خاصی ندارد و توسط نهاد یا ارگانی مدیریت و کنترل نمی‌شود. تمامی اطلاعات موجود اعم از داده های مالی، غیر مالی و سایر داده ها، دیگر داخل یک سرور نگهداری نمی‌شود، بلکه بین بی شمار سیستم توزیع می‌شود. افراد در این تکنولوژی یک شبکه را تشکیل می‌دهند و اگر قرار است تراکنش یا اطلاعاتی ثبت شود، این اطلاعات داخل سیستم تمامی اعضا شبکه ثبت می‌شود. تمامی اعضای شبکه یک نسخه از دفتر کل را در سیستم های خود دارند. به هر یک از این سیستم ها یک گره یا NODE گفته می شود. اگر تراکنش یا اطلاعاتی بخواهد ثبت شود می‌بایست با توافق تمامی اعضای شبکه این اتفاق بیفتد و پس از تایید بیش از نیمی از اعضای شبکه (بستگی به سیاستهای اجماع آن شبکه دارد)، آن تراکنش یا اطلاعات ثبت می‌شود و دفتر کل تمامی اعضای شبکه به روز رسانی می‌شود. بنابراین هر تغییری در شبکه از چشم اعضای آن دور نخواهد ماند و می‌بایست آن تغییر با موافقت و تایید اعضا شبکه صورت گیرد.

مزایای دفتر کل توزیع شده

امنیت : از آنجا که سرور مرکزی وجود ندارد و تمامی اطلاعات در سیستم های اعضا توزیع شده است، بنابراین امکان هک و یا حمله به آن بسیار دشوار است. زیرا اگر فردی بخواهد اطلاعاتی را تغییر دهد یا هک کند می‌بایست این کار را در سیستم تمامی اعضای شبکه انجام دهد که واضح است تقریبا نشدنی است.

صرفه جویی در هزینه : از آنجا که شخص واسط حذف می‌شود، دیگر نیازی نیست برای انجام تراکنش ها و یا سایر فعالیت های خود به شخص واسط هزینه ای را بپردازید. همان بانک را در نظر بگیرید. برای انجام تراکنش های شما و انتقال پولتان کارمزد دریافت می‌کند که این واسطه در تکنولوژی دفتر کل توزیع شده از میان رفته است (بیشتر ارزهای دیجیتال برای حفظ شبکه و ترغیب دیگران به مشارکت در اجماع جهت تایید تراکنش ها مبلغی را به عنوان Transaction fee دریافت می کنند).

سرعت : در این تکنولوژی افراد به صورت همتا به همتا (peer to peer) به یکدیگر متصلند و برای انجام تراکنش ها و یا فعالیت های دیگر نیاز به شخص واسط نیست و تمامی فعالیت های توسط اعضای شبکه صورت می‌گیرد که این امر باعث افزایش سرعت تا حد قابل قبولی می‌شود.

شفافیت : از آنجا که هیچ تمرکزی از سمت هیچ نهادی روی آن نیست بنابراین همه چیز شفاف اتفاق میفتد و هر اتفاق و تغییری توسط اعضای شبکه مورد بررسی قرار می‌گیرد. بنابراین کسی نمی‌تواند اطلاعات را به دلخواه خودش تغییر دهد و یا اطلاعات اشتباه وارد کند.

کاربردهای دفتر کل توزیع شده

از دفتر کل توزیع شده می‌توان در تمامی زمینه ها و صنایعی که با داده و ذخیره و استفاده از آنها سروکار دارند، استفاده کرد، به عنوان مثال در زمینه‌ی بهداشت میتوان از طریق دفتر کل توزیع شده، سوابق بیماران و اطلاعات پزشکی مربوط به آنها را ثبت کرد. همچنین در اسناد و املاک می‌توان اطلاعات مربوط به خرید و فروش ها را ثبت کرد و یا اینکه ثبت احوال می‌تواند برای ثبت اسامی و شماره ملی ها از این تکنولوژی بهره ببرد. بانک ها، اداره پست، اداره برق و خیلی از صنایع و شرکت های دیگر نیز می‌توانند از دفتر کل توزیع شده برای ثبت و ذخیره اطلاعات و انجام تراکنش های خود استفاده کنند.

انواع دفتر کل:

یک شکل از دفترکل توزیع شده زنجیره بلوکی یا Blockchain است که می‌تواند عمومی یا خصوصی باشد. اما همه دفاتر کل توزیع شده نباید لزوماً از زنجیره ای از بلوک‌ها استفاده کنند تا با موفقیت اجماع توزیع شده معتبر و ایمن عرضه کنند: یک زنجیره بلوکی تنها یک نوع از ساختار داده‌هایی است که دفترکل توزیع شده به‌شمار می‌رود.

شکل دیگری از طراحی دفتر کل توزیع شده، شبکه‌های گوریده(Tangle Network)است که از یک گراف جهت دار غیر مدور شبکه‌ای به جای ساختار زنجیره‌بلوکی استفاده می‌کنند. گوریدگی ایجاد شده توسط ایوتا (IOTA)ضرورت معدن‌کاوی را از بین می‌برد و شبکه ای پیشنهاد می‌دهد از هزینه معاملات صفر و مقیاس پذیری نامحدود پشتیبانی می‌کند. شکل دیگر دفاتر کل توزیع شده هش گرف (HASH Graph) می باشد.

زنجیره بلوکی (Blockchain)

زنجیره بلوکی یا Blockchain پایگاه داده توزیع شده و مبتنی بر اجماع است که به صورت مستمر فهرستی از رکوردها (رده‌ها) را که هرکدام به گزینه‌های قبلی فهرست ارجاع می‌دهند را حفظ می‌کند و بدین وسیله در مقابله با تضعیف یا بازنگری غیرمجاز تقویت می‌شود. زنجیره بلوکی خود زیربخشی از فناوری‌های دفترکل توزیع شده (Distributed Ledger) است. زنجیره بلوکی گونه ای از معماری‌های داده مورد استفاده در فناوری دفاترکل توزیع شده است که در آن سوابق تراکنش‌ها در زنجیره‌های متصل به یکدیگر ذخیره می‌شوند.

در این فناوری با وجود کاربران متعددی که به‌طور هم‌زمان داده‌هایی را ثبت و اصلاح می‌کنند و ممکن است که آن داده‌ها با هم تداخل داشته باشند، شبکه قادر به حفظ یکپارچگی محتوای پایگاه داده است. با توجه به ساختار داده‌ای رمزنگاری شده که بلاک چین دارا می‌باشد یکپارچگی بدون هیچ کنترل‌کننده مرکزی حفظ می‌شود. در دفاتر کل توزیع شده مربوط به بیتکوین برای مرتب کردن تراکنش‌ها و ممانعت از تناقض یک مسئله ریاضی مطرح می‌شود که حل کردنش سخت است اما پس از حل مسئله تأیید درست بودن راه حل آسان است به این سازوکار، اثبات کارکرد یا Proof of work می‌گویند. در روش زنجیره بلوکی بیت کوین کسی می‌تواند تراکنش‌های هر مرحله را مرتب کند که جواب این سؤال سخت را پیدا کرده باشد و هم‌زمان تغییراتی که قصد اعمال آن را دارد (بلوک جدید) با مراحل قبلی زنجیره تناقض نداشته باشد. شیوه کشف عدم تناقض به این صورت است که تراکنش‌های هر بلوک وارد تابع هش می‌شوند و پاسخ آن تابع هش را همه دارند اگر کسی که تراکنش‌ها را مرتب و اضافه می کند حتی یک تغییر جزئی در تراکنش های قبلی تایید شده ایجاد کند جواب هش تراکنش‌ها تغیر می‌کند و بدون اینکه افراد نیاز باشد بدانند کدام بخش تغییر کرده می‌توانند با تغییر غیر مجاز مخالفت کنند.

زنجیره بلوکی معاملات آنلاین امن را تسهیل می‌کند. زنجیره بلوکی یک کتابخانه دیجیتالی غیر متمرکز و توزیع شده‌است که برای ضبط معاملات در میان رایانه‌های بسیاری استفاده می‌شود تا بتوان بدون تغییر تمام بلوک‌های بعدی و بدون همکاری شبکه مقادیر ثبت شده را با استفاده از پس‌انداز تغییر داد .این امر به شرکت کنندگان اجازه می‌دهد تا به بررسی و حسابرسی معاملات ارزان بپردازند. اصالت‌سنجی آن‌ها توسط همکاری جمعی توسط اشتراک منافع جمعی خود تأیید می‌شوند. نتیجه، یک گردش کار قوی است که عدم قطعیت شرکت کنندگان در مورد امنیت داده‌ها یک امر حاشیه‌ای است. استفاده از یک زنجیره بلوکی ویژگی مشخصه تکثیر بی‌نهایت از یک دارایی دیجیتال را حذف می‌کند. این تأیید می‌کند که هر واحد ارزش تنها یک بار منتقل می‌شود، و مشکل دیرینه Double spending را حل کرده‌است. زنجیره بلوکی به عنوان یک پروتکل رمزنگاری ارزش‌گذاری تعریف شده‌است. این مبادله بر مبنای زنجیره بلوکی می‌تواند سریع تر، با خیال راحت و ارزان‌تر از سیستم‌های سنتی تکمیل شود. زنجیره بلوکی می‌تواند حقوق عنوان را اختصاص دهد، زیرا رکوردی را فراهم می‌کند که باعث ارائه و پذیرش می‌شود.

تمرکز زدایی

با ذخیره داده‌ها در سراسر شبکه، زنجیره بلوکی خطراتی را که با ذخیره داده‌ها به‌طور مرکزی نگه داشته می‌شوند حذف می‌کند. زنجیره بلوکی غیر متمرکز ممکن است از ارسال پیام AD Hoc و شبکه توزیع شده‌استفاده کند.

شبکه آن دارای نقاط متمرکز آسیب‌پذیری است که Crackerها می‌توانند از آن استفاده کنند؛ به همین ترتیب، هیچ نقطه مرکزی از شکست وجود ندارد. روش‌های امنیتی زنجیره بلوکی شامل استفاده از رمزنگاری کلید عمومی است

مدیریت زنجیره تامین

برای مدیریت زنجیره تأمین، فناوری بلاک چین مزیت‌های مانند قابلیت ردیابی و به صرفه بودن را به همراه دارد. بلاک چین می‌تواند برای دنبال کردن حرکت کالاها، مبدأ آن‌ها، تعداد و ... به کار رود. در نتیجه سطح جدیدی از شفافیت را برای اکوسیستم B2B به ارمغان می‌آورد. همچنین ساده کردن فرایندهایی مانند انتقال مالکیت، بیمه، فرایند تولید و پرداخت از دیگر مزایای استفاده از زنجیره بلوکی است.

بیت کوین، طلای دیجیتال نامگذاری شده است و دلایل خوبی نیز برای این امر وجود دارد. بلاک چین می‌تواند انواع دیگری از ارزش دیجیتال را ایجاد کند. مانند اینترنت یا خودرو، شما برای استفاده از بلاک چین لازم نیست بدانید چگونه کار می‌کند. با این حال، داشتن دانش اولیه در مورد این فناوری جدید به شما نشان خواهد داد که چرا انقلابی محسوب می‌شود.

بلاک چین یک دفترکل دیجیتالی غیرقابل تخریب از معاملات اقتصادی است که می‌تواند نه تنها برای ضبط معاملات مالی بلکه تقریبا برای ثبت هر دارایی ارزش‌مندی استفاده شود.

توضیح فنی فناوری بلاک چین :

از آنجایی که مفهوم بلاک چین و بیت کوین اساساً به هم متصل‌اند، می‌توان مفهوم بلاک چین را با توضیح چگونگی کارکرد بیت کوین توضیح داد. هرچند که فناوری بلاک چین برای همه نوع تبادلات و تراکنشی های مربوط به ارزهای دیجیتال برخط قابل استفاده است.

تجارت اینترنتی به طور انحصاری با مؤسسات مالی که به عنوان طرف سوم با ارائه خدمات مطمئن، واسطه تراکنش‌های الکترونیکی‌اند، عجین است. نقشی طرف سوم مورد اعتماد، شناسایی، محافظت و نگهداری از تراکنش‌هاست. درصد معینی از تقلب در معاملات برخط یا آنلاین اجتناب ناپذیر است و همین امر باعث می‌شود تا نیازمند حضور طرف سوم برای واسطه گری در تراکنش‌های مالی باشیم و این موجب بالا رفتن هزینه تراکنش‌ها می‌شود. بیت کوین به جای استفاده از طرف سوم مورد اعتماد در اجرای تراکنش برخط بین دو طرف، از نشانه‌های رمزگذاری استفاده می‌کند. هر تراکنش از طریق یک امضای دیجیتالی حفاظت می‌شود. هر تراکنش که با کلید خصوصی فرستنده امضای دیجیتالی شده باشد به کلید عمومی گیرنده ارسال می‌شود. به منظور خرج کردن پولی، صاحب پولی رمزگذاری شده، باید ثابت کند که مالکیت کلید خصوصی را داراست. نهادی که ارز دیجیتالی را دریافت می‌کند، امضای دیجیتالی (مالکیت کلید خصوصی) آن را با استفاده از کلید عمومی فرستنده شناسایی می‌کند.

هر تراکنش به تمامی گره‌های شبکه بیت کوین انتشار می‌یابد و بعد از شناسایی در دفتر کل عمومی ثبت می‌شود. هر تراکنش مجزا پیش از آنکه در دفتر کل عمومی ثبت شود، باید شناسایی شده و معتبر شناخته شود.

گره‌های شناسایی کننده باید پیش از ثبت هر تراکنشی از دو موضوع اطمینان یابند:

1. پرداخت کننده، امضای دیجیتالی معتبر رمزگذاری شده ای، برای انجام تراکنشی را داراست
2. پرداخت کننده، پول رمزگذاری شده کافی در حساب خود دارد: تمامی تراکنش‌های حساب (کلیدعمومی) پرداخت کننده در دفتر کلی باید کنترل شود تا از کفایت موجودی حساب خود مطمئن شود.

در اینجا مسئله حفظ ترتیب تراکنش‌های منتشر شده به سایر گره‌ها در شبکه همتا به همتای بیت کوین، مطرح می‌شود. تراکنش‌ها به ترتیبی که ایجاد شده‌اند انجام نمی‌شوند و به همین علت به سامانه‌ای نیاز داریم که به ما اطمینان دهد که پول رمزگذاری شده، دو بار پرداخت نشود. برای در نظر گرفتن این موضوع، تراکنشی‌ها باید گره به گره در طول شبکه بیت کوین منتقل شوند و هیچ ضمانتی وجود ندارد که ترتیب دریافت تراکنش‌ها در گره‌ها با ترتیب ایجاد آنها مطابقت داشته باشد.

این بدان معناست که مکانیسمی مورد نیاز است تا کلی شبکه بیت کوین بتواند در مورد ترتیب تراکنش‌ها به توافق برسد و این مشکلی اساسی در سیستم‌های توزیع یافته است.

بیت کوین این مشکل را با مکانیسم فناوری بلاک چین حل کرده است. سیستم بیت کوین با قرار دادن تراکنش‌ها در گروهی از زنجیره‌های بلوکی و سپس اتصال این زنجیره‌های بلوکی به هم، آنها را مرتب می‌کند. تراکنش‌های هر بلوک باید به طور همزمان روی دهند. این زنجیره‌های بلوکی مانند زنجیرهای در یک خط با توالی زمانی به هم متصل هستند و هر بلوک خروجی تابع درهم سازی (هش)" از بلوک پیشین خود را ذخیره می کند.

هنوز یک مشکل باقی است. هر گره روی شبکه می تواند درخواست تراکنش های تأیید نشده را گرفته و از آن یک بلوک بسازد و روی شبکه به عنوان پیشنهادی برای تولید بلوک بعدی بلاک چین منتشر کند. شبکه چطور باید تصمیم بگیرد که کدام بلوک باید بلوک بعدی بلاک چین باشد؟

ممکن است زنجیره‌های بلوکی مختلفی توسط گره‌های مختلف به طور همزمان ایجاد شده باشند. تا زمانی که زنجیره‌های بلوکی بتوانند با ترتیب‌های مختلف در نقاط مختلف شبکه دریافت شوند، نمی‌توان به هیچ ترتیبی اعتماد کرد. بیت کوین این مسئله را با تعریف یک معمای ریاضی حل کرده است. هر بلوکی که بخواهد به بلاک چین اضافه شود، باید در محتوای خود پاسخی برای یک مسئله ریاضی بسیار خاصی داشته باشد که به آن (اثبات کارکرد) میگویند. گرهای که یک بلوک را تولید می‌کند، باید ثابت کند که منابع محاسباتی کافی برای حل معمای ریاضی را دارد. برای مثال، یک گره باید بتواند یک (مقدار موقت) را بیابد که با استفاده از آن خروجی تابع درهم‌ساز بلوک پیشین یا هشی را که با تعدادی مشخصی از صفرها شروع می‌شود، ایجاد کند. متوسط تلاش‌های لازم، بر اساس تعداد بیت‌های صفر مورد نیاز تعریف می‌شود. اما فرآیند بازشناسی آن بسیار ساده است و با اجرای یک تابع درهم‌ساز انجام پذیر است.

حل این معمای ریاضی ساده نیست و میزان پیچیدگی آن قابل تنظیم است. برای مثال می‌توان درجه دشواری مسئله را طوری تنظیم کرد که میانگین زمان حل آن برای یک گره در شبکه بیت کوین برای تولید بلوک ده دقیقه باشد و امکان اینکه بیش از یک بلوک در سیستم در زمان داده شده ساخته شود، بسیار ناچیز است. اولین گرهای که مسئله را حل کند بلوک خود را به سایر گره‌های بلاک چین انتشار می‌دهد. اگر در حالت خاصی بیش از یک بلوک به صورت همزمان ساخته شود، به چند انشعاب مختلف منجر خواهد شد. هرچند مسئله‌ای که باید حل شود به قدری پیچیده است که بلاک چین به سرعت تثبیت می‌شود و تمامی گره‌ها در مورد ترتیب زنجیره‌های بلوکی اخیر زنجیره توافق دارند. گره‌ها، منابع محاسباتی خود برای حل مسئله به اشتراک می‌گذارند و بلوکی به عنوان (کمینه) را می‌سازند و در نهایت برای تلاش‌هایشان پاداش می‌گیرند.

شبکه فقط بلندترین بلاک چین را به عنوان بلاک چین معتبر شناسایی می‌کند. از این رو برای یک مهاجم تقریباً غیرممکن است که بتواند تراکنش تقلبی خود را تعریف کند، زیرا نه تنها باید بلوکی تولید کند که مسئله ریاضی را حل کرده باشد، بلکه باید به طور همزمان زنجیره‌های بلوکی پیشین را نیز بازسازی کند، به طوری که سایر گره‌های شبکه، آنها را مجاز بدانند. انجام این کار به علت اینکه زنجیره‌های بلوکی به صورت رمزگذاری شده به هم متصل شده‌اند، دشوارتر نیز می‌شود.

انواع بلاک چین:

بلاک چین یک ساختمان داده است که امکان ایجاد یک دفتر کل عمومی از داده‌ها و به اشتراک گذاشتن آنها میان شبکه ای از طرف های مستقل را فراهم می‌کند بلاکچین انواع بسیاری دارد:

- بلاک چین های عمومی: بلاک چین های عمومی نظیر بیت کوین شبکه های بزرگ توزیع شده هستند که از طریق یک توکن بومی اجرا می‌شوند. اینها برای هر کسی که در هر سطحی مشارکت می‌کند، باز بوده و دارای کد منبع باز برای جامعه ای است که آنها را نگه میدارد.
- بلاک چین های دارای مجوز: بلاک چین های دارای مجوز نظیر ریپل، نقش هایی را که افراد می‌توانند داخل شبکه ایفا کنند، کنترل می نماید. این ها همچنان سیستم های بزرگ و توزیع شده ای هستند که از یک توکن بومی استفاده می‌نمایند. کد اصلی آنها ممکن است منبع باز باشد یا نباشد.
- بلاک چین های خصوصی: بلاک چین های خصوصی کوچک تر بوده و از توکن استفاده نمی کنند عضویت در اینگونه بلاک چین ها بسیار کنترل شده است. این نوع بلاکچین ها مورد علاقه کنسرسیوم هایی هست که دارای اعضای مورد اعتماد بوده و اطلاعات محرمانه مبادله می کنند.

سامانه زنجیره بلوک معمولاً از دو جزء اصلی تشکیل می شود. این دو جزء عبارتند از:

۱. شبکه فرد به فرد یا همتا به همتا
۲. پایگاه داده

در رابطه با شبکه زنجیره گروهی متشکل از رایانه های متصل به یک الگوی ارتباطی با نام شبکه فرد به فرد یا همتا به همتا است. این ساز و کاری است که رایانه‌ها با استفاده از آن تغییرات جدید به پایگاه داده را منتقل می کنند. دومین جزء اصلی سامانه زنجیره بلوک خود پایگاه داده است. پایگاه‌داده شامل انباشت تاریخچه تراکنش ها است این سیستم تراکنش ها را به همان ترتیب که انجام می‌شوند، ثبت می‌کند.

بلاک چین به زبان ساده

بیت کوین اولین کاربرد از این فناوری بود و از بلاک چین برای ذخیره اطلاعات دارایی کاربران بهره برد. اگر بلاک چین یک سیستم عامل باشد، بیت کوین نرم افزاری روی این سیستم عامل است. در هر بلاک هر اطلاعاتی می‌تواند ثبت شود; از جرم و جنایت‌های یک فرد تا نمایش اطلاعات حساب برای دارایی‌ها مانند بیت کوین. در بلاک چین، اطلاعات در بلاک‌ها قرار می‌گیرند و با هم به صورت زنجیره‌ای مرتبط می‌شوند. هر کدام از این بلاک‌ها چیزی به نام هش دارند. یک هش رشته‌ای از کارکترهاست که با توابع خاصی ساخته می‌شود .در بلاک چین، هش بلاک‌های بعدی حاوی هش بلاک قبلی هم هستند .هش در هر بلاک چین با یک تابع ریاضی خاص به‌دست می‌آید که توسعه دهندگان آن را مشخص میکنند. کوچک‌ترین تغییر در اطلاعات یک بلاک، هش آن را به طور کلی تغییر می‌دهد. اگر کسی محتوای یک بلاک را تغییر دهد و هش بلاک‌های بعدی را به روز رسانی کند، چه می‌شود؟ این امکان وجود دارد اما شما توزیع را در نظر نگرفته‌اید. داده‌های بلاک چین در یک کامپیوتر یا سرور خاص ذخیره نمی‌شوند. هر کامپیوتر یا سیستمی که به شبکه وصل شود یک نسخه از بلاک چین را دریافت می‌کند.

محدودیت ها

- فرض اصلی در بلاک چین این است که نودهای درستکار بیشتر از گروه هکرها، قدرت پردازش را در دست خواهند داشت. اگر گروه هکرها بتوانند بیشتر از نودهای درستکار قدرت پردازنده را در دست بگیرند می‌توانند از مردم کلاهبرداری کنند.
- هر نود تا زمانی که بلاک شکل بگیرد، تراکنش ها را جمع آوری می‌کند و سپس برای بلاک، براساس الگوریتم اثبات کار، nonce می‌یابد. در آخر، این بلاک برای دریافت تاییدیه به نودهای دیگر فرستاده می شود. این موضوع بین ایجاد تراکنش و تایید آن، تاخیر ایجاد می‌کند و میزان این تاخیر متاثر از تعداد تراکنش های باز و قدرت اجرایی نودها می‌باشد.

تمام نودهایی که در ایجاد و تایید بلاک ها دخیل اند، تشویق می‌شوند. کاربری که درخواست انتقال (تراکنش) را ایجاد می‌کند موظف است کارمزد انتقال را پرداخت کند تا زمان و انرژی مورد استفاده نودها برای انتقال‌هایی با مقادیر کم را هم که بسیار گران است، جبران شود.

زنجیره جانبی (Sidechain)

زنجیره‌های جانبی (Sidechains) امکان جابجایی توکن‌ها و دیگر دارایی‌های دیجیتالی را از بلاک چین اصلی به بلاک چین‌های دیگر و درصورت نیاز بازگشت این دارایی‌ها به بلاک چین اصلی را می‌دهد. زنجیره‌های جانبی پتانسیل عظیمی جهت ارتقای قابلیت بلاک چین‌های فعلی دارند.

زنجیره‌های جانبی چگونه کار می‌کنند؟

زنجیره جانبی (Sidechain)، بلاک چین جداگانه‌ای است که با بلاک چین اصلی بصورت دوطرفه پیوند دارد. پیوند دوطرفه تعویض‌پذیری بین دارایی‌ها را با نرخ ارزی از پیش تعیین شده‌ای برای زنجیره جانبی و بلاک چین مادر ممکن می‌سازد. بلاک چین مادر در این مکانیزم با نام (زنجیره اصلی) (Main Chain) و بلاک چین‌های دیگر با نام (زنجیره جانبی) شناخته می‌شوند. (در بلاک چین Ardor، زنجیره‌های جانبی تحت عنوان زنجیره‌های فرزند (Childchains) شناخته می‌شوند)

یک کاربر در صورتی که قصد انجام تراکنش بین زنجیره اصلی و زنجیره جانبی را داشته باشد، ابتدا باید کوین‌های خود را به آدرس دوم بفرستد. سپس کوین‌ها در بلاک چین اصلی قفل می‌شوند و امکان استفاده از آن‌ها دیگر وجود ندارد و باید منتظر بود تا تراکنش بین زنجیره‌ها تایید شود. پس از صدور پیغام تایید مدت زمانی اضافه جهت اطمینان از امنیت بیشتر تراکنش صرف می‌شود. پس از سپری شدن این مدت زمان امنیتی، مقدار معادل کوین‌ها در زنجیره جانبی فعال می‌شوند و امکان خرج کردن و انتقال آن‌ها بوجود می‌آید. برعکس این عمل یعنی انتقال از زنجیره فرعی به اصلی نیز با همین مکانیزم صورت می‌گیرد.

فدراسیون ها

فدراسیون گروهی است که به عنوان واسطه بین زنجیره اصلی و جانبی عمل می‌کند. این گروه درباره قفل بودن و آزاد کردن کوین‌هایی که کاربر از زنجیره اصلی انتقال داده، تصمیم می‌گیرند. سازندگان زنجیره جانبی می‌توانند اعضای فدراسیون را تعیین کنند. مشکلی که ساختار فدراسیون دارد، اضافه کردن لایه‌ای دیگر بین زنجیره اصلی و زنجیره جانبی است.

امنیت

زنجیره‌های جانبی مسئول امنیت خودشان هستند. اگر قدرت استخراج کافی در شبکه جانبی وجود نداشته باشد، امکان هک شدن و حمله ۵۱ درصدی در آن وجود خواهد داشت. از آنجایی که هر زنجیره جانبی مستقل است، با هک شدن آن، زنجیره اصلی در معرض خطر قرار نمی‌گیرد. این امر بصورت برعکس نیز صادق است؛ یعنی در صورت هک شدن بلاک چین مادر، زنجیره جانبی بدون مشکل به فعالیت خود ادامه می‌دهد اما نرخ تبدیل بین زنجیره‌ها و پیوند دوطرفه قبلی، بیشتر ارزش خود را از دست خواهد داد.

زنجیره جانبی استخراج‌کنندگان خود را دارد. جهت انگیزه دادن به ماینرها برای فعالیت در زنجیره جانبی، می‌توان از (استخراج ترکیبی) (Merged Mining) استفاده کرد. در این روش دو ارز دیجیتال جدا که الگوریتم یکسانی دارند، به صورت همزمان توسط ماینرها استخراج می‌شود.

پلتفرم های زنجیره جانبی موجود

۱- پلتفرم RSK فضای متن باز شبکه آزمایشی خود را که جینجر (Ginger) نام دارد، برای ساخت زنجیره‌های جانبی در اختیار توسعه‌دهندگان قرار داده است. این زنجیره‌های جانبی پیوند دوطرفه‌ای با بلاک چین بیت کوین دارند و مزیت استخراج ترکیبی را برای استخراج‌کنندگان بیت کوین دارند. هدف RSK به نوعی استفاده از قابلیت قراردادهای هوشمند بر بلاک چین بیت کوین است تا پرداخت‌ها سریع‌تر از قبل انجام شوند.

۲- بلاک چین آردور به عنوان یک پلتفرم خدماتی برای کسب‌وکارهای تجاری است. آردور از مکانیزم اثبات سهام استفاده می‌کند. زنجیره‌های جانبی همانطور که قبلا هم گفته شد تحت عنوان زنجیره‌های فرزند در این پلتفرم شناخته می‌شوند، بطوری که با زنجیره اصلی یکپارچگی محکمی دارند. امنیت در این پلتفرم بهبود یافته است بطوری که تمامی تراکنش‌ها توسط ماینرهای زنجیره اصلی پردازش و تایید می‌شود. البته بیشتر تراکنش‌ها به سطح زنجیره‌های فرزند انتقال می‌یابد بطوریکه زنجیره مادر قدرت استفاده از قابلیت‌های خود را به حداقل می‌رساند. همچنین تمامی دارایی‌ها و ارزهای دیجیتال در این پلتفرم، قابلیت دسترسی از زنجیره‌های جانبی مختلف را دارند.

آینده زنجیره های جانبی

زنجیره‌های جانبی این اجازه را به ارزهای دیجیتال می‌دهند که با یکدیگر ارتباط داشته باشند. انعطاف پذیری در این زنجیره‌ها افزایش می‌یابد و دست توسعه‌دهندگان جهت آزمایش نسخه‌های بتا و یا آپدیت‌ها قبل از اجرا آن در بلاک چین اصلی را باز می‌گذارد. برخی فعالیت‌های بانکی نظیر صدور و رهگیری مالکیت سهام نیز قابلیت آزمایش بر روی زنجیره‌های جانبی را قبل از انتقال آن‌ها به زنجیره اصلی دارد. در صورتی که بر روی مکانیزم‌های امنیتی زنجیره‌های جانبی بیشتر کار شود، این فناوری آینده بسیار درخشانی خواهد داشت که مقیاس پذیری بلاک چین را به شدت افزایش خواهد داد.

حمله Dusting

حمله‌ی داستینگ فعالیتِ مخربی است که در آن، هکران و مهاجمانِ سایبری قصد دارند با ارسال مقدار کمی کوین‌های دیجیتالی به کاربران بیت کوین و ارزهای دیجیتال (کیف پول‌های دیجیتالی شخصی آن‌ها)، هویت آن‌ها را شناسایی کرده و به حریم خصوصی آن‌ها تجاوز کنند. معاملاتِ مربوط به کیف پول‌های دیجیتالی به وسیله‌ی هکران ردیابی و رصد می شوند.

داست (dust) چیست؟

در دنیای ارزهای دیجیتال، اصطلاح داست (dust) به معنای مقدار بسیار ناچیزی از کوین‌ها یا توکن‌های دیجیتالی است که در ته حساب کاربری کاربران ارزهای دیجیتال وجود دارد، این مقدار آن قدر کم و ناچیز است که کاربران ارزهای دیجیتال به آن توجه نمی کنند.

به عنوان مثال، به رمزارز بیت کوین توجه کنید. کمترین مقدار رمزارز بیت کوین، یک ساتوشی یا ۰.۰۰۰۰۰۰۰۱ BTC بوده بنابراین، می توانیم از اصطلاح داست (dust) برای یک یا چند صد ساتوشی استفاده کنیم. علاوه بر این، باید به این نکته توجه کرد که این خرده کوین‌ها را نمی توان خرید و فروش کرد، تنها کاربران صرافی رمزارز Binance این امکان را دارند که خرده کوین‌ها را به BNB چنج کنند. همچنین در دنیای رمزارز بیت کوین، هیچ گونه تعریف رسمی‌ای درمورد اصطلاح داست وجود ندارد زیرا هر نرم افزار یا مشتری‌ای، آستانه و میزانِ متفاوتی را برای این خرده کوین‌ها یا داست در نظر می گیرند.

از لحاظ فنی، میزان داست براساس اندازه میزان ورودی‌ها و خروجی‌ها سنجیده و محاسبه می شود که به طور معمول برای معاملات بیت کوین (بدون سگویت) ۵۴۶ ساتوشی و برای معاملات سگویت نیتیو حدود ۲۹۴ ساتوشی است.

حملات داستینگ

اخیرا، هکران و مهاجمان سایبری به این نکته پی برده‌اند که اکثر کاربران ارزهای دیجیتال توجه زیادی به مقادیرِ بسیار کم دارایی‌های دیجیتال موجود خود که در ته حساب کیف پول‌های دیجیتالی‌شان است، نمی دهند بنابراین هکران این خرده کوین‌ها را به کیف پول دیجیتالی قربانیان ارسال می کنند. با ارسال این داست‌ها و با توجه به مقدیر بسیار کم آن‌ها، کاربران ارزهای دیجیتال توجه زیادی به این خرده کوین‌ها نمی کنند موقعیت مناسبی برای هکرها به منظور انجام حملات داستینگ فراهم می شود.

زمانی که کاربران، خرده کوین‌های دیجیتالی را به حساب دیگری منتقل می کنند، هکران به راحتی می توانند آن‌ها را شناسایی کنند. سپس، شروع به تجزیه و تحلیلِ آدرس‌های شناسایی شده می کنند و کیف پول دیجیتالی کاربران را تحت بررسی قرار داده و تراکنش‌های آن‌ها را پیگیری می کنند. هکران با استفاده از اطلاعات جامعی (هویت کاربر و اطلاعات مربوط کیف پول دیجیتالی) که از کاربران ارزهای دیجیتال به دست می آورند شروع به انجام حملات فیشینگ یا اخاذی سایبری می کنند.

در ابتدا حملات داستینگ پیرامون رمزارزهای بیت کوین صورت می گرفت اما در حال حاضر، هکران پا را فراتر گذشته و به رمزارزهای دیگر نیز روی آورده‌اند. در ماه اکتبر سال ۲۰۱۸ میلادی، توسعه دهندگان کیف پول دیجیتالی "Bitcoin's Samourai" اعلام کردند که کاربران این کیف پول دیجیتالی، تحت حمله‌ی داستینگ قرار گرفته‌اند. در پی این حمله‌ی سایبری، شرکت مورد نظر با انتشار توییتی به کاربران خود در این رابطه هشدار داده و علاوه بر این، توضیح داد که چگونه می توانند در برابر این حملات از دارایی‌های دیجیتال خود محافظت کنند. از آنجایی که انجام حملات داستینگ براساسِ تجزیه و تحلیل چندین آدرس مختلف است، اگر یکی از صندوق‌های مورد نظر شناسایی نشوند، حملات داستینگ را نمی توان انجام داد.

حمله SYBIL

حمله سیبل (Sybil) اقدامی برای کنترل شبکه همتا با ایجاد کردن چندین هویت جعلی می‌باشد. برای ناظران بیرون از این حمله، این هویت های جعلی مانند کاربران واقعی به نظر می‌رسند. هرچند پشت این هویت های جعلی، یک هویت حقیقتی وجود دارد که چندین هویت جعلی را کنترل می‌کند. در نتیجه، آن هویت می‌تواند از طریق قدرت رای دهی مضاعف که در شبکه دموکراتیک و مردمی، یا توانایی پیام رسانی پژواکی در شبکه اجتماعی دارد، بر شبکه تاثیرگذار باشد.

مشکل اخیر ایالات متحده با تاثیر روسیه بر انتخابات این کشور از طریق حساب های کاربری جعلی در شبکه اجتماعی، مثال خوبی از حمله شبه سیبل می‌باشد. اگرچه حساب های کاربری جعلی و ربات ها نتوانستند فیسبوک و توییتر را هک کنند، با این وجود از چندین هویت

استفاده کردند تا بر کل شبکه تاثیر بگذارند. از آنجایی که حمله سیبل بسیار خرابکارانه می‌باشد و به راحتی پنهان می‌شود، بیان این که چه زمانی یک هویت در حال کنترل چند حساب کاربری می‌باشد دشوار است. قطعا فیسبوک حتی از میزان حساب های کاربری جعلی در پلتفرم خود مطلع نبود تا اینکه چند ماه پس از اعمال آسیب و خسارت ها به بررسی داخلی پلتفرم خود پرداخت.

اسم حمله سیبل از یک کتاب به اسم سیبل برداشته شده است. این کتاب درباره زنی مبتلا به اختلال چند شخصیتی می‌باشد. محققان مایکروسافت ابتدا در اوایل قرن اخیر در خصوص تاثیرات حمله های سیبل بر شبکه های همتا به بررسی پرداختند. در این مقاله به طور خلاصه به تاثیرات حمله های سیبل و و نحوه جلوگیری شبکه ها از بروز چنین حملاتی پرداخته می شود. اگر در نظر دارید که از یک پلتفرم بلاک چیناستفاده کنید، دانستن رویکرد آن بلاک چین به تهدیدات حملات سیبل و بی اثر کردن اثرات آن از طریق ایجاد هویت در شبکه بسیار مهم است.

کنترل بی تناسب

حمله سیبل نفوذ نامحدودی به یک هویت واحد می‌دهد، فقط به این دلیل که آن هویت، چندین اسم مستعار و جعلی را کنترل می‌کند. ما همیشه درباره حساب های کاربری جعلی سایت رددیت (Reddit) شنیده ایم که باعث بالا آمدن و افزایش رتبه پست ها می‌شوند. فروشندگان سایت آمازون می‌توانند نقد و بررسی های جعلی از سراسر جهان خریداری کنند. شناسایی و حذف این اسامی جعلی دشوار می‌باشد.

درحالی که این مداخله های انتخاباتی در فیسبوک و نقد و بررسی های جعلی در آمازون به اندازه کافی بد می‌باشند، یک حمله سیبل موفقیت آمیز علیه بلاک چین یا شبکه انتقال فایل به عاملان امکان کنترل بی تناسب و غیرمستقیم شبکه را می‌دهد. اگر شبکه این هویت های جعلی را تایید کند، می‌توانند از جانب پروپوزال های مختلف رای دهند یا جریان انتقال اطلاعات را در سراسر شبکه مختل کنند.

هم چنین ممکن است گره های سیبل سایر گره های شبکه را محاصره کنند و بر دسترسی آن ها به اطلاعات تاثیر بگذارند و در آخر از طریق سانسور کردن بر لجر یا دیتابیس تاثیرگذار باشند.

جلوگیری از حمله سیبل

بلاک چین ها و شبکه های همتا گزینه های مختلفی در خصوص جلوگیری از حمله سیبل دارند. هر گزینه مزایا و معایب خود را دارد. رویکردهای ترکیبی برای جلوگیری از حمله سیبل شامل سه عامل کلیدی می‌باشد. این عوامل عبارتند از:

هزینه ایجاد هویت

اولین روش کاهش حمله سیبل، افزایش هزینه ایجاد هویت جدید می‌باشد. از آنجایی که هویت ها می‌توانند بیش از یک حساب کاربری ایجاد کنند، به روشی نیاز داریم تا ایجاد هویت های جدید هزینه بر باشد. چالشی که در این بین وجود دارد این است که دلایل قانونی بسیار زیادی برای کنترل و عملکرد چندین هویت وجود دارد. هویت فراوان، به اشتراک گذاری منابع، اعتبار و ناشناس بودن دلایل خوبی برای ایجاد چندین هویت در شبکه همتا می‌باشد .هزینه ایجاد هویت نباید افراد را در خصوص پیوستن به شبکه یا حتی ایجاد هویت های مفید محدود کند. در عوض این هزینه باید مقداری باشد که ایجاد چندین هویت در یک دوره زمانی کوتاه را امکان پذیر نکند.

بلاک چین ها از هزینه ایجاد هویت برای ویژگی محافظت از حملات سیبل طی استخراج استفاده می‌کنند. در الگوریتم های اثبات کار، به منظور ایجاد هویت جدید در شبکه استخراج، به یک رایانه دیگر با توان پردازشی مناسب نیاز خواهید داشت. این امر، هزینه قابل توجهی را به صدها یا هزاران گره جعلی تحمیل می‌کند که می‌توانند بر پذیرش فورک یا سایر رای گیری های بلاک چین تاثیر بگذارند.

این موضوع برای الگوریتم اثبات سهام نیز صادق است که در آن خرید توان رایانشی جایگزین ارائه و به خطر انداختن ارز شده است. برای پیوستن به شبکه و داشتن حق رای باید هزینه پرداخت شود. این پیش نیاز به منابع، تعداد حساب های کاربری جعلی افراد سودجو را محدود می‌کند.

زنجیره اعتماد

روش دوم برای جلوگیری از حملات سیبل اینگونه است که قبل از آنکه به یک هویت اجازه پیوستن به شبکه داده شود، نوعی اعتماد ایجاد شود. این امر معمولا منجر به شکل گیری سیستم اعتبار می‌شود که در آن فقط کاربران شناخته شده و بلند مدت می‌توانند کاربران جدید را

دعوت کنند یا به ورود آن ها به شبکه رای دهند. انواع دیگر این روش به سیستم آزمایشی بستگی دارد که در آن حساب های کاربری جدید امکان پذیر می‌باشند اما قبل از اینکه حق رای به دست آورند باید برای مدتی فعال و منحصر به فرد باقی بمانند.

زنجیره اعتماد هم چنین تا تایید هویت نیز گسترش می‌یابد. بعضی از شبکه های همتا از شما می‌خواهند تا قبل از پیوستن، هویت خود را تایید کنید. سایر شبکه ها در صورتی به شما اجازه پیوستن به شبکه را می‌دهند که بتوانید کد امنیتی دو تاییدی را پاسخ دهید. در عین حال بعضی از شبکه ها نیز ایجاد حساب های کاربری جدید را بر اساس آدرس IP محدود می‌کنند. تمام این شبکه ها قبل از آنکه به هویتی حق رای بدهند به سطحی از تایید هویت یا اعتمادسازی نیاز دارند و به این ترتیب ایجاد اسامی مستعار بیشتر را چالش برانگیز می‌کنند.

اعتبار نابرابر

روش آخر برای کاهش خطر حملات سیبل، قدرت دادن به کاربران بر اساس اعتبار آن ها می‌باشد. کاربرانی که مدت بیشتری در شبکه حضور داشته اند و خود را اثبات کرده اند، قدرت رای دهی بیشتری در تصمیمات رایج خواهند داشت. این امر، به جای ایجاد یک محیط کاملا دموکراسی، سیستم را به شایسته سالاری تبدیل می‌کند و قدرت کاربران جدید را کاهش می‌دهد. در نتیجه، بسیاری از حساب های کاربری جدید یا غیرفعال نسبت به کاربران قدیمی و با اعتبار بیشتر، هیچ منفعتی برای حمله کننده سیبل نخواهند داشت.

جلوگیری از حملات سیبل دشوار است

حمله سیبل شامل هویت های جعلی و انگیزه های پنهان می‌باشد. بدین ترتیب، شناسایی و جلوگیری از این حملات قبل از اجرای آن ها، امری بسیار دشوار است. در عین حال شبکه هایی که ترکیبی از این اقدامات پیشگیرانه را پیاده سازی و اجرا می‌کنند، محافظت بیشتری در مقابل حملات سیبل مشاهده خواهند کرد و در صورت بروز حملات، از شدت آن می‌کاهند.

انتقال توکن (token swap) چیست و چگونه کار می کند؟

جابجایی توکن (token swap) یا انتقال توکن (token migration) به فرایندی گفته می شود که در آن توکن شما به یک بلاک چین جدید فرستاده می‌شود. انتقال توکن هیچ ارتباطی با کلاهبرداری ندارد و در بین پروژه های بلاک چین بسیار محبوب شده است. قابل ذکر است که دو ارز دیجیتال از بین ۲۵ ارز دیجیتال برتر یعنی ترون و EOSدر حال چنین انتقالی می‌باشند و انتظار می‌رود حداقل بیش از ۲ توکن از بین ۳۰ توکن برتر نیز این مسیر را ادامه دهند.

با وجود ارزش میلیونی و حتی میلیارد دلاری توکن های موجود، خطرات بسیار زیادی در از دست دادن سرمایه وجود دارد. اما با وجود این موضوع، صنعت بلاک چین در خصوص انتقال توکن و تاثیرات آن کاملا یکسان و بدون تغییر باقی مانده است .بسیاری از اطلاعات در زمینه انتقال توکن را می‌توان از پیشروهای این حرکت دریافت کرد. پروژه هایی که دستخوش این انتقالات بوده اند، قدم های دشوار اما در عین حال ضروری در تحقق چشم انداز پروژه خود برداشته اند.

شاون ویلکینسون موسس استارت آپ استورج (Storj) که انتقال توکن را از سال ۲۰۱۷ شروع کرده است در این خصوص بیان کرد: ایده این کار این است که باند زخم خود را باز کنید و مسیری را دنبال کنید که به پرتگاه منتهی نمی‌شود.

چرا یک پروژه به انجام انتقال توکن نیاز دارد؟

اغلب اوقات، این انتقال ها توسط پروژه هایی صورت می‌گیرد که برای افزایش سرمایه و توزیع توکن های خود از بلاکچین اتریوم استفاده می‌کنند. در این فاز، توکن های توزیع شده پروژه معمولا به عنوان جایگزین برای توکن هایی عمل می‌کنند که هنگام فعالسازی پروژه استفاده خواهند شد .یکی از مزایای این استراتژی این است که معامله کنندگان دیگر مجبور به راکد کردن سرمایه خود نیستند. در عوض هنگامی که فناوری خود را توسعه می‌دهند، قادر به تبادل این توکن های جایگزین در صرافی ها می‌باشند.

بنابراین انتقال توکن، فرایند را اینگونه شرح می دهد که کدام موجودی توکن از کیف پول اتریوم به کیف پول جدید پروژه مورد نظر انتقال یابد. پس از جابه‌جایی، توکن ها از یک بلاک چین به بلاک چین دیگر انتقال یافته اند .قابل توجه است که انتقال توکن ها منحصرا به عرضه

بلاک چین فعال مرتبط نیست و هنگامی که پروژه ها از یک پروتکل به پروتکل دیگر جابه‌جا می‌شوند نیز رخ می‌دهد. برای مثال انتقال توکن استورج با تصمیم مبنی بر انتقال از یک پروتکل مبتنی بر بیت کوین به اتریوم انجام شد. دلیل این انتقال نیز مشکلات مقیاس پذیری بود.

ویلکینسون در این خصوص گفت: ما دریافتیم که انجام ندادن این انتقال توکن، عواقب بزرگی خواهد داشت.

نحوه کار آن ها چگونه است؟

برای کاربران و سرمایه گذاران، میزان حضور آن ها در فرآیند انتقال توکن متفاوت است و معمولا بر اساس این نکته است که توکن های خود را کجا ذخیره و نگهداری می‌کنند سخت یا بسیار آسان خواهد بود .برای کسانی که توکن های خود را در صرافی ها ذخیره می‌کنند معمولا بعید است که نیاز باشد اقدامی در این راستا انجام دهند. برای مثال صرافی بزرگ بایننس می‌گوید تمام شرایط فنی مورد نیاز فرآیند انتقالEOS ، ترون، ICONو آنتولوژی (Ontology) را فراهم می‌کند. صرافی کراکن نیز در صدد کاهش سختی این فرآیند است.

جسی پاول موسس و مدیرعامل کراکن خاطر نشان کرد: ما قبل از انتقال و تبادل تمام کوین های قدیمی به کوین های جدید، جذب سرمایه را متوقف می‌کنیم و پس از اتمام انتقال کوین ها، تمام موجودی پیشین برای کوین جدید می باشد. نحوه کار به همین سادگی است .اما کاربرانی که توکن های خود را در کیف پول ذخیره می‌کنند ممکن است مجبور شوند این فرآیند را خودشان آغاز کنند. به طور دقیق تر آنها باید ثبت توکن یا همان مپینگ را بگذرانند تا توکن ها را از بلاک چین قبلی به شبکه جدید ارسال کنند .در عمل، این فرآیند معمولا مستلزم تولید آدرس جدید برای مثال EOS و ارسال توکن ها از آدرس قدیمی که توکن ها پس از خریداری در آن ذخیره شدند به این می‌باشد.

پروژه ها معمولا هنگام سواپ، جذب سرمایه خود را قطع می‌کنند که در این دوره، کاربران باید تبادل توکن های خود را انجام دهند. در پروژه های نظیرEOS ، این دوره ها مهلت های دشواری است که پس از آن توکن ها در بلاک چین قدیمی مسدود و از دسترس کاربر خارج خواهد شد. سایر پروژه ها می‌توانند انتقال توکن را بدون مهلت خاصی انجام دهند.

خطرات انتقال توکن چیست؟

اما علی‌رغم اقدامات صرافی ها در خصوص تسهیل انتقال توکن ها، خطرات این فرآیند کاملا از بین نرفته است. ویلکینسون در این خصوص گفت: به نظرم روش بی نقصی برای انتقال توکن وجود ندارد. همواره مشکلات وجود دارند و احتمال بسیار زیادی وجود دارد که اوضاع به هم بریزد .صحبت با اعضای جامعه یکی از روش هایی است که پروژه ها می‌توانند یک مشکل رایج عدم آگاهی دارندگان توکن را کاهش دهند.

طبق سخنان ویلکینسون، علی رغم گذشت یک سال پس از شروع انتقال توکن استورج از سال ۲۰۱۷، کاربران هم چنان در حال انتقال توکن های خود می‌باشند. استورج هم چنان انتقال توکن ها را پشتیبانی می‌کند اما برای پروژه هایی با مهلت مسدود شدن توکن ها، دارندگان توکن اگر از فرآیند انتقال آگاهی نداشته باشند سرمایه خود را از دست می‌دهند .شاید مهم ترین خطر موجود در انتقال توکن این است که چنین فرایندهایی غیر قابل اعتماد هستند. کاربران باید به مسئولان پروژه در خصوص انتقال توکن اعتماد کنند. از آنجایی که انتقال توکن موضوعی نسبتا جدید است، اغلب اوقات الگویی برای اجرای آن وجود ندارد. به این دلیل ویلکینسون گفت: خیلی مسائل پیرامون انتقال استورج را از صفر ساختیم. اگرچه این خطرات موضوع کم اهمیتی نمی‌باشند، با این وجود برای فناوری های پیشرفته و جدید غیرمنتظره نیست.

Hyper Ledger چیست؟

در دنیای بلاک چین و ارزهای دیجیتال، پروژه‌های زیادی وجود دارد .معروف ترین آن‌ها، پروژه‌های بیت کوین و اتریوم است که محبوبیت زیادی را به دست آورده‌اند .بسیاری از بلاک چین‌ها از همان ابتدا، برای برطرف کردن نیازهای موجود ایجاد شده‌اند .پروژه هایپر لجر که به وسیله بنیاد لینوکس راه اندازی شده است نیز برای استاندارد سازی و دموکراتیزه کردن بلاک چین در دنیای کسب و کارها ایجاد شده است. شرکت‌ها، دیگر نیازی ندارند که خودشان به تنهایی مسائل به وجود آمده را حل و برطرف کنند، هایپر لجر با ترکیب دانش و صنعت، این امکان را به شرکت‌ها می دهد که با ایجاد Customized Blockchain مسائل خود را حل کنند.

لینوکس در سال ۲۰۱۵ اعلام کرد که با رهبران صنعتی، به منظور توسعه و پیشرفت تکنولوژی بلاک چین در سطح سازمانی همکاری خواهد کرد .هدف اصلی از توسعه و پیشبرد تکنولوژی بلاک چین، ایجاد یک فریم ورک منحصر به فرد اوپن سورس، برای ساخت برنامه‌های کاربردی قوی و صنعتی، پلتفرم و سخت افزار برای پشتیبانی از معاملات تجاری است؛ به همین ترتیب پروژه هایپر لجر ایجاد شده است.

اولین نفراتی که به این پروژه ملحق شدند، بانک‌ها، شرکت خدمات مالی و شرکت‌های فناوری اطلاعات بودند .اما با گذشت زمان شرکت‌ها و افراد بیشتری به این پروژه اضافه شدند در صورتی که در ۲۶ سپتامبر، لیست شرکت‌ها و افراد اضافه شده به پروژه هایپر لجر به ۲۷۰ رسید . بزرگ ترین شرکت‌هایی که به این پروژه اضافه شده‌اند، شرکت‌های IBM و Intel بودند.

در ماه جولای ۲۰۱۸ هایپر لجر میزبان ۱۰ پروژه با ۳.۶ میلیون خط کد و نزدیک به ۲۸.۰۰۰ شرکت کننده از سراسر جهان بود. بلاک چین تکنولوژی جدیدی است که اخیرا راه اندازی شده است و یک مفهوم سخت برای پروفایل‌های غیرتکنیکی می باشد، به همین خاطر نیاز به یک همکاری متقابل صنعتی، در دنیای کسب و کارها ایجاد شده است .به دلیل این که سودمند بودن بیت کوین و اتریوم میان توسعه دهندگان و کاربران آن ثابت شده است، درک آن‌ها به وسیله عموم مردم راحت تر شده است اما هایپر لجر پروژه جدیدی است که درک آن یک چالش بسیار بزرگی خواهد بود.

اهداف هایپر لجر:

- ایجاد مقیاس سازمانی
- ایجاد فریم ورک توزیعی اوپن سورس
- ترویج مشارکت اعضای اکوسیستم

لینوکس قصد دارد از طریق پروژه هایپر لجر، محیطی ایجاد کند که در آن توسعه دهندگان نرم افزاری و شرکت‌ها برای ایجاد فریم ورک بلاک چین، با یکدیگر همکاری کنند .بنابراین پروژه هایپر لجر زیرساختی است که در آن می توان پروژه‌های مرتبط با بلاک چین را پیدا کرد.

پروژه‌های هایپر لجر

- Hyperledger sawtooth

بلاک چینی است که به وسیله شرکت اینتل راه اندازی و توسعه یافته است .هدف از راه اندازی آن، تست عملکرد مکانیسمی به نام PoeT است و به شرکت‌ها این امکان را می دهد که بدون داشتن یک مقام مرکزی، مجلات توزیع شده را مدیریت کنند. PoeT الگوریتمی است که هدف آن توزیع حقوق ماینینگ شبکه از طریق سیستم تصادفی است Hyperledger sawtooth .در Python نوشته شده است و هدف آن ارائه بلاک چینی است که بتواند به اینترنت و سیستم‌های مختلف مالی اعمال شود.

- Hyperledger Fabric

این پروژه به وسیله شرکت IBM راه اندازی شده است. در حال حاضر این بلاک چین توسط بعضی از شرکت‌ها مورد استفاده قرار گرفته است. این بلاک چین از پلتفرم اتریوم برای ساخت اپلیکیشن‌های کاربردی شرکت‌ها استفاده می کند زیرا اتریوم دارای پروتکل مخصوص به خود است و به همین دلیل کمتر انعطاف پذیر است. آنچه که این پروژه ارائه می دهد، پایه‌ای برای ساخت بلاک چین مخصوص برای صنعت است. همچنین این بلاک چین خدماتی مانند شفافیت، غیرمتمرکزسازی و امنیت نیز ارائه می دهد.

- Hyperledger Burrow

دستگاه قرارداد هوشمند قابل توجهی است که به منظور مشخص کردن دستگاه مجازی اتریوم EVM توسعه یافته است.

- Hyperledger Indy

سربرگ توزیع شده برای هویت‌های غیرمتمرکز است. ابزاری را برای استفاده از هویت‌های دیجیتال مستقل فراهم می کند.

- Hyperledger iroha

فریم ورک بلاک چینی است که برای آسان کردن پروژه‌های زیربنایی که به تکنولوژی لجستیک توزیع شده نیاز دارند، طراحی شده است. اگر چه پروژه‌های هایپر لجر در حال توسعه هستنند اما همانگونه که گفته شده برخی از شرکت‌ها از پروژه‌های Hyperledger sawtooth و Hyperledger Fabric استفاده می کنند. برای مثال Everledger شرکتی است که کالاهای باارزش خود را بر روی بلاک چین، ردیابی می کند. همچنین هایپر اعلام کرده است که قصد همکاری و مشارکت با رقیب اصلی خود (EEA) را دارد. EEA سازمان استاندارد جهانی است که برای پاسخ به نیازهای تجاری از پلتفرم اتریوم استفاده می کند.

انواع بلاک در بلاک چین؟

بلاک اورفان(Orphan blocks)

این بلاک ها معمولا در رابطه با بیت کوین می‌باشد. آنها بلاک هایی معتبر هستند که تمامی ملزومات را برای اضافه شدن به بلاک چین دارند اما رد می‌شوند. بلاک های اورفان هنگامی که دو استخراج کننده در یک زمان مشابه یک بلاک را تولید می‌کنند، ایجاد می‌شود. این اتفاق به دلیل پذیرش یک بلاک توسط گره ها (node) در یک بلاک چین بر روی یک شبکه و بلافاصله اتفاق می‌افتد. بلاک های ساخته شده برای تائید اعتبارشان باید به گره ها در سراسر شبکه متصل شوند که در این نقطه ممکن است تاخیری اتفاق بی‌افتد. در نتیجه یک استخراج کننده‌ی دیگر می‌تواند در همان زمان بلاک خود را ساخته و توسعه داده باشد. این اتفاق باعث یک شکاف موقتی در شبکه می‌شود تا گره ها تصمیم بگیرند که کدام بلاک را برای ادامه‌ی کار بلاک چین انتخاب کنند. یک بلاک با اجماع بهتر و بیشتر گزینه‌ی انتخابی شبکه برای ادامه‌ی روند و کار بلاک چین است.

اجماع بر سر یک بلاک از طریق میزان قدرت پردازشی شبکه در ساخت آن شناسایی می‌شود. هرچه میزان این قدرت پردازشی بیشتر باشد اجماع بر سر تایید آن بلاک راحت تر اتفاق می‌افتد. پس بلاکی با توان پردازشی کمتر انتخاب نمی‌شود و این همان بلاک اورفان است. در صورت دیگر، اگر یک هکر سعی کند تراکنش را برعکس کند و یا با خلل مواجه کند این نوع از بلاک نیز می‌تواند تولید شود.

همانطور که در تصویر فوق قابل مشاهده است، دو بلاک در یک روز واحد و تقریبا در یک زمان ۱۳:۴۴:۱۹ pmو ۱۳:۴۴:۳۱ pmتوسط گروهی ازاستخرهای استخراج مانند AntPool و SlushPool برای شبکه بیت کوین ساخته شده اند. اما از آنجایی که AntPool میزان بیشتری انرژی گواه اثبات کار در روند ساختش صرف شده است نسبت به بلاک SlushPool برای انتخاب در اولویت قرار می‌گیرد. علاوه بر این، این نکته حائز اهمیت است که گاهی بلاک های اورفان نیز به دلیل قوانین مورد توافق عمومی در پروتکل بیت کوین دارای اعتبار می‌شوند اما استخراج کنندگانش پاداشی دریافت نمی‌کنند. لازم به ذکر است که بر اساس تصویر بالا می‌توان فهمید که میزان تراکنشهایی که یک بلاک در بر می‌گیرد معیاری برای انتخاب آنها نمی‌باشد.

بلاک های استِیل(Stale blocks)

بلاک هایی هستند که استخراج کنندگان هنگامی که یک بلاک دیگر با موفقیت از سوی شبکه مورد تایید قرار گرفت، رها شود و یا به تعبیری دیگر دور انداخته شود. از آنجایی که امر استخراج با حل کردن یک مساله ریاضی آغاز می‌شود بنابراین یک استخراج کننده از این طریق بلاک بعدی را به بلاک چین اضافه می‌کند. اما این مساله هم ممکن است که استخراج کننده‌ی دیگری زودتر این مساله ریاضی را حل کند. بنابراین در این صورت یک استخراج کننده باید فعالیت خود را بر روی یک بلاک استِیل متوقف کرده و استخراج بلاک دیگری را از سر بگیرد.

بلاک های آنکل(Uncle blocks)

معمولا با پروتکل اتریوم همکاری می‌کنند و همچنین برابر با بلاک های اورفان هستند البته با تفاوتی اندک. بلاک های آنکل همچنان بلاک های معتبری هستند که توسط شبکه ساخته شده و رد گشته اند. اما برخلاف پاداش نگرفتن استخراج کننده بلاکهای اورفان، استخراج کنندگان این بلاک پاداش می‌گیرند. برای استخراج یک بلاک معتبر در شبکه اتریوم، یک استخراج کننده به ازای هر بلاک ۳ اتر دریافت می‌کند. این پاداش دادن به دو دلیل انجام می‌شود:

- در راستای ترویج تمرکز زدایی بهتر استخراج، به استخراج کنندگان برای تولید بلاک آنکل پاداش داده می‌شود. این امر تسهیلاتی برای استخراج کنندگان مستقلی است که پتانسیل دریافت پاداش را دارند. حتی اگر بلاک استخراج شده شامل زنجیره اصلی نباشد باز هم فرد استخراج کننده پاداش دریافت می‌کند.
- به طور کلی زمانیکه قدرت پردازش برای تولید بلاک معمولی و بلاک آنکل صرف می‌شود، باعث بالا رفتن امنیت شبکه خواهد شد. در نتیجه توان محاسباتی برای تولید بلاک آنکل هدر نرفته است، چرا که قدرت پردازش شما برای تولید این دو بلاک تقسیم شده است.

بلاک جنسیس(Genesis blocks)

اولین بلاک هر پروتکل بلاک چینی محسوب می‌شود. این بلاک را می‌توان در روند ساخت یک بلاک چین به مثابه فندانسیون قلمداد کرد. بلاک جنسیس (بلاک مادر) بیت کوین شامل یک پیغام از طرف پدید آورنده آن است. پیغام این است :تاریخ ۳ ژانویه ۲۰۰۹ ، آغاز تلاشی برای نجات دوباره بانک ها .تفسیر این پیام بسیار متنوع می‌تواند باشد اما به عنوان یک پیام به درستی در بلاک تشکیل دهنده بلاک چین بیت کوین عمل می‌کند.

ساختار بلاک در بلاک چین بیت کوین

بلاک چین زنجیره‌ای از ساختارهای اطلاعاتی به نام بلاک است. هر بلاک را می‌توان صفحه‌ای از یک دفتر کل در نظر گرفت. هربلاک از اجزای مختلفی تشکیل شده است که به‌طور دقیق‌تر این اجزا را می‌توان در دو بخش بلاک هدر (Block Header) و بدنه‌ی بلاک (Block Body) قرار داد.

بلاک هدر به شش جز تقسیم می‌شود:

- شماره‌ی نسخه‌ی برنامه (Bitcoin Version Number)
- هشِ بلاک قبلی (Previous Block Hash)
- ریشه‌ی هشِ درخت درهم سازی یا درخت مرکل (Merkle Tree)
- زمان‌سنج از تاریخ ۱ ژانویه‌ی ۱۹۷۰ (Timestamp Unix)
- هدف سختی فعلی (Difficulty Target)
- عدد تصادفی نانس (Nonce)

شماره‌ی نسخه‌ی برنامه : در بسیاری از موارد اهمیتی ندارد. به‌هرحال یک ماینر با یک شماره‌ی نسخه، می‌تواند مشخص کند که از تصمیمات کدام پروتکل پشتیبانی می‌کند.

هشِ بلاک قبلی : در اصطلاح زنجیره‌ی بلاک چین نامیده می‌شود. از آن‌جایی که بلاک قبلی، هش بلاک جدید را دربردارد، بلاک‌های بلاک چین براساس یک‌دیگر بنا می‌شوند. بدون این مولفه، هیچ ارتباط و گاه‌شماری بین بلاک‌ها شکل نمی‌گیرد.

ریشه‌ی درخت درهم‌سازی : همه‌ی تراکنش‌های موجود در بلاک می‌تواند در یک هش خلاصه شود. این هش، ریشه‌ی هشِ درخت درهم‌سازی است.

ثانیه‌شمار از تاریخ اول ژانویه‌ی ۱۹۷۰ : یک تایم استمپ در خودِ بلاک. مقدار این ثانیه‌شمار از ابتدای روز اول ژانویه ۱۹۷۰ است.

هدف سختی فعلی : هدفِ سختی نشان می‌دهد که هشِ فعلی، چه‌اندازه باید کوچک باشد تا اعتبار آن توسط ماینرها تائید شود. به‌عبارت دیگر یک هش، سایزی را به بیت دارد که باید مساوی یا کوچک‌تر از هشِ هدف باشد. یک هش با تعداد زیادی صفر در ابتدا، کوچک‌تر از هشِ بدون صفر در ابتدا می‌باشد.

نانس : متغیر افزوده شده توسط الگوریتم اثبات کار است. بدین طریق ماینر هشِ معتبری را که کمتر از هدف سختی می‌باشد، حدس می‌زند.

شش جزء ذکر شده بلاک هدر را تشکیل می‌دهند. بلاک هدر نقش بنیادی را برای بیت کوین دارد؛ بدلیل این‌که تمام بلاک‌ها را به‌یکدیگر مرتبط می‌سازد. شما می‌توانید آن را مانند اتاق فرمان تصور کنید؛ در این اتاق اسنادی موجود است که از طریق کنترل شبکه مشخص می‌کند کدام کامیون به کدام سمت برود.

بدنه‌ی بلاک (Block Body)

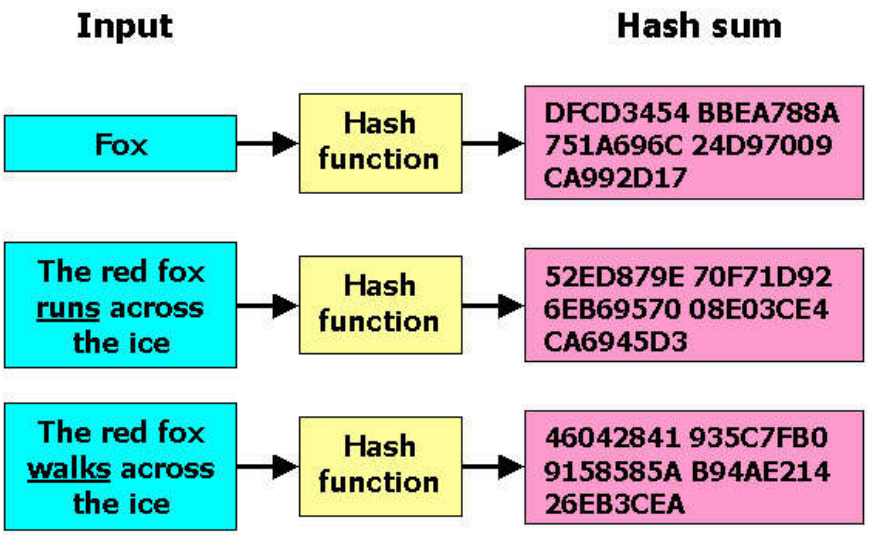
بدنه‌ی بلاک، همانند فضای بارگیری کامیون است که شامل تمام تراکنش‌های تایید شده می‌شوند. وقتی که ماینر یک بلاک را می‌سازد، در واقع تراکنش‌ها را تایید می‌کند. به این ترتیب، یک ماینر بررسی می‌کند که فرستنده بیت کوین به‌اندازه‌ی کافی بیت کوین برای خرج کردن دارد. ماینر، این اطلاعات را از طریق بلاک چین بررسی می‌کند. ماینر با بررسی اطلاعات گذشته آگاه می‌شود که آیا فرستنده‌ی ۱۰ بیت کوین قبلاً ۱۰ بیت کوین دریافت کرده است؟ تراکنش‌های بلاک فقط در یک لیست موجود نمی‌باشد بلکه به‌اصطلاح در درخت درهم‌سازی هم موجود است.

درخت مرکل

درخت مرکل یکی از مفاهیم اساسی در فناوری زنجیره‌بلوک است که ذخیره‌سازی ایمن و کارآمد ساختارهای داده‌ای را فراهم می‌کند . پیاده‌سازی درخت مرکل در شبکه‌های زنجیره‌بلوکی مزایای بشماری دارد که ازجمله آن‌ها می‌توان به افزایش مقیاس‌پذیری، حفظ یکپارچگی داده‌ها از طریق معماری مبتنی بر رشته‌های درهم (Hash) و ارائه روشی ساده برای تأیید صحت داده‌ها اشاره کرد.

توابع درهم‌ساز رمزگذاری شده

به بیان ساده یک تابع درهم‌ساز (Hash Function) نوعی از تابع است که می‌تواند یک واحد داده با حجم تصادفی را به یک حجم داده با مقدار ثابت تبدیل کند. در حال حاضر الگوریتم‌های متفاوتی برای درهم‌سازی وجود دارد و شما می‌توانید بر اساس نیاز هرکدام از آن‌ها را انتخاب کنید. پس از اجرای الگوریتم، خروجی حاصل نه‌فقط اندازه ثابت دارد بلکه برای هر ورودی، منحصربه‌فرد هم هست. مثلاً در تصویر زیر رشته درهمی که برای واژه FOX تولیدشده با رشته درهمی که برای جمله The red fox runs across the ice تولیدشده کاملاً متفاوت هستند. این ویژگی باعث می‌شود تا هرکدام از رشته‌های درهم بتوانند به‌عنوان یک سند معتبر ایفای نقش کنند و در یک دید کلی‌تر شاکله تغییرناپذیری زنجیره‌بلوک‌ها را شکل دهند.

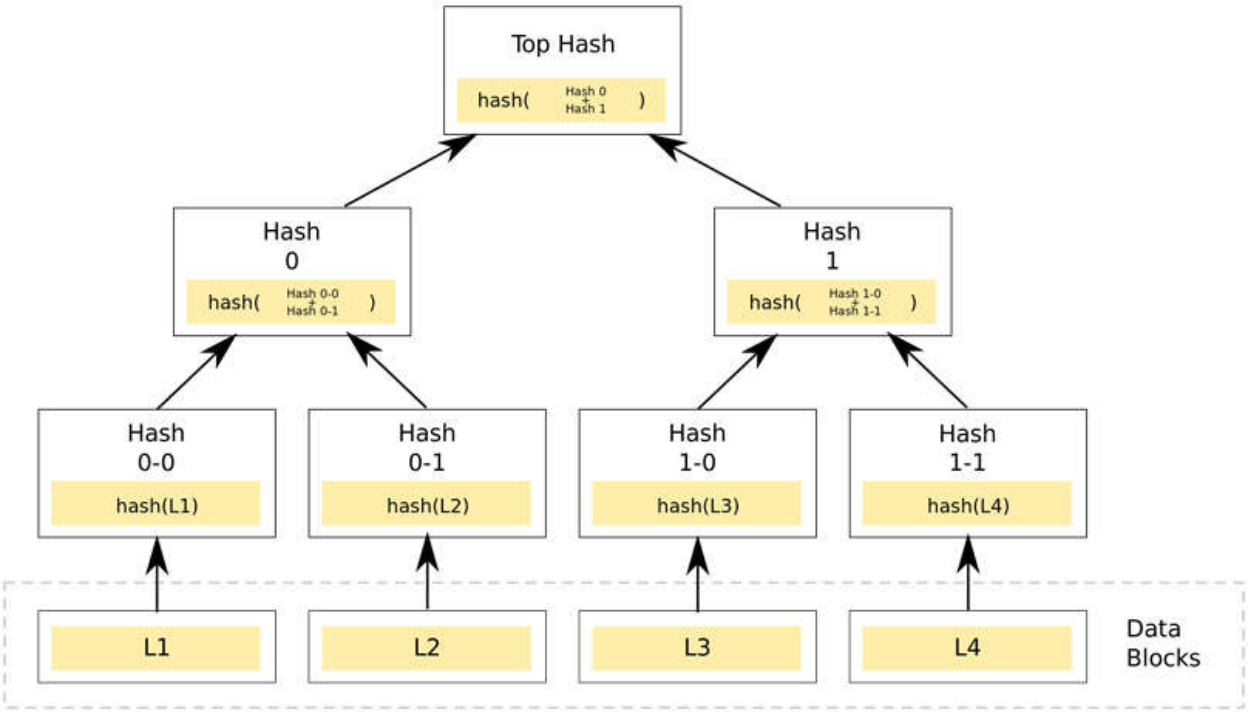


یکی دیگر از مزایای الگوریتم‌های درهم‌ساز برای سیستم‌های زنجیره‌بلوکی فشرده‌سازی مقادیر عظیم داده‌ای است. به‌علاوه شناسایی این مقادیر صرفاً با داشتن رشته درهم آن‌ها امکان‌پذیر است که باعث سهولت کار کردن با شبکه‌های زنجیره‌بلوکی می‌شود. در بلاک‌چین بیت‌کوین هر بلوک یک سرعنوان (heading) دارد که در آن رشته درهم مربوط به بلوک قبلی همراه با داده‌های دیگری ثبت‌شده است. با این شیوه تمام بلوک‌ها در یک ترتیب منطقی به همدیگر متصل می‌شوند و رشته درهم بلوک در واقع وضعیت کل بلوک‌های موجود در شبکه تا یک‌لحظه خاص را به نمایش می‌گذارد. در نتیجه امکان دست‌کاری داده‌ها در بلاک‌چین بیت‌کوین و البته آلت‌کوین‌ها تقریباً غیرممکن می‌شود.

اما داستان از جایی دردناک می‌شود که ذخیره این حجم از رشته‌های درهم‌ساز باعث کاهش کارایی و مقیاس‌پذیری شبکه‌های زنجیره‌بلوکی می‌شود. برای درمان این درد متخصصان از تکنیکی با نام درخت مرکل استفاده می‌کنند که می‌تواند سایه خودش را بر سر زنجیره‌بلوک بگستراند.

درختان مرکل و اثبات‌های مرکل

ایده اصلی رالف مرکل که در سال ۱۹۷۹ برای آن پروانه ثبت اختراع گرفت درواقع ساختارهای داده‌ای درختی هستند که در آن هر گره بدون برگ، یک‌رشته درهم‌ساز از گره‌های فرزند خودش هستند و گره‌های با برگ (برگ‌ها)، پایین‌ترین گروه گره‌ها در درخت را تشکیل می‌دهند. شاید درک این جمله‌ها اندکی پیچیده باشد اما تصویر زیر تا حد زیادی این پیچیدگی را کاهش می‌دهد.

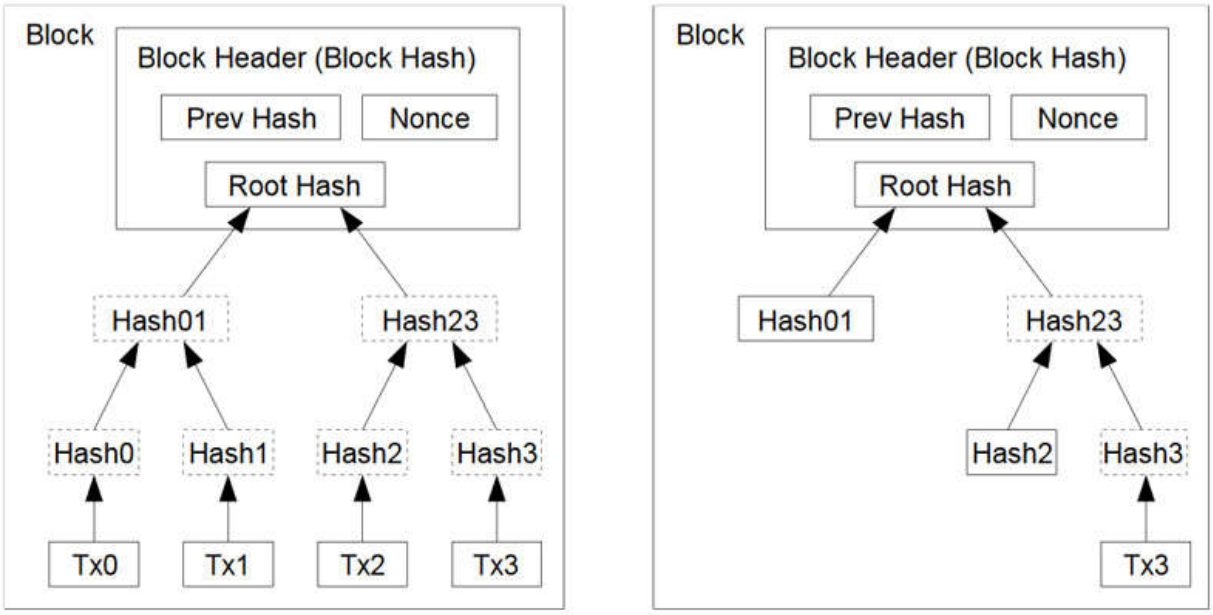


در این تصویر گره‌های بدون برگ یا شاخه‌ها (رشته درهم ۰-۰ و رشته درهم ۰-۱) در سمت چپ تصویر، از رشته‌های درهم فرزندانشان که ۱L و ۲L هستند تشکیل‌شده‌اند و در سطح بالاتر رشته درهم ۰ خودش درهم شده رشته‌های درهم ۰-۰ و ۰-۱ است. تصویری که از آن استفاده‌شده یک مدل ساده و رایج از درخت مرکل است که به نام درخت مرکل دودویی شناخته می‌شود. در این تصویر یک‌رشته درهم در بالای همه رشته‌ها قرارگرفته که درواقع هش تمام درخت است و به آن رشته درهم ریشه هم می‌گویند. درواقع این تصویر نشان می‌دهد که درخت مرکل یک ساختار داده‌ای است که می‌تواند هر تعداد از رشته‌های درهم را به‌عنوان ورودی دریافت کند و یک‌رشته درهم واحد تولید کند. ساختار درخت امکان مکان‌یابی مقادیر وسیعی از داده‌ها را فراهم می‌کند و شناسایی آسان تغییرات درداده‌ها را امکان‌پذیر می‌سازد. این مفهوم شواهدی تحت عنوان اثبات مرکل را به وجود می‌آورد که با استفاده از آن می‌توان بدون نیاز به بررسی تمام رشته‌های درهم تأیید کرد که فرایند درهم‌سازی داده‌ها در سراسر ساختار درخت پایدار بوده و در جایگاه درست قرار دارد.

البته نقش رشته درهم ریشه در این فرایند حیاتی‌تر است چون با داشتن آن می‌توان تمام شبکه زنجیره‌بلوک را به‌سرعت بررسی کرد. درنهایت یکی از مزایای اصلی درخت مرکل برای سیستم‌های توزیع‌شده تجزیه داده‌های کلان به بخش‌های کوچک‌تر قابل مدیریت است که در این صورت موانع تأیید صحت داده‌ها به طرز چشمگیری کاهش پیدا می‌کنند.

درخت مرکل در بیت‌کوین

تابع درهم‌سازی رمزگذاری شده در بیت‌کوین SHA-۲۵۶ نام دارد. خروجی این تابع یک مقدار ۲۵۶ بیتی ثابت است و عملکرد اصلی درخت مرکل در شبکه بلاک‌چین بیت‌کوین ذخیره‌سازی و درنهایت حذف رشته‌های درهم زائد در هر بلوک است. تصویر زیر که از مقاله سفید بیت‌کوین گرفته‌شده به‌خوبی نحوه عملکرد درخت مرکل در بلاک‌چین این رمزارز را نشان می‌دهد.



Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

تراکنش‌ها توسط ماینرها در بلوک‌ها ذخیره می‌شوند و به عنوان بخشی از درخت مرکل درهم‌سازی می‌شوند که درنهایت یک ریشه مرکل درست می‌شود که در سر عنوان (header) بلوک ذخیره می‌گردد. مهم‌ترین امتیاز درخت مرکل در بیت‌کوین امکان شکل‌گیری گره‌های تأییدکننده پرداخت ساده (SPV = Simple Payment Verification) است که بیشتر آن‌ها را با نام کلاینت‌های سبک (Lightweight clients) می‌شناسیم. عملکرد این گره‌ها وابسته به دانلود تمام شبکه بلاک‌چین بیت‌کوین نیست و فقط با داشتن سر عنوان بلوک‌های طولانی‌ترین زنجیره هم کار می‌کند. یک گره SPV می‌تواند با استفاده از اثبات مرکل یک تراکنش را به یک درخت مرکل خاص با داشتن رشته درهم ریشه آن درخت در یک بلوک ارتباط دهد.

مفهوم درخت مرکل نه‌فقط در زنجیره‌بلوک بیت‌کوین بلکه در سایر رمزارزها مثل اتریوم هم پیاده‌سازی شده است. هرکدام از پروژه‌های رمزارزی بنا بر قابلیت‌ها و ویژگی‌هایی که دارند از طرح‌های مختلفی برای درختان مرکل استفاده می‌کنند که ساده‌تر یا پیچیده‌تر هستند. به‌علاوه درختان مرکل یکی از اجزای جدایی‌ناپذیر سیستم‌های کنترل توزیع‌شده مثل Git و IPFS هستند. در واقع توانایی آن‌ها در تضمین و تأیید یکپارچگی داده‌های مشترک بین رایانه‌ها در یک قالب بدون واسطه در این سیستم‌ها است. به هر حال آشنایی با مفهوم درخت مرکل و نقش آن در الگوریتم‌های درهم‌سازی و تأثیر آن بر روی مقیاس‌پذیری و امنیت شبکه‌های

بلاک‌چین یکی از مسائل مهمی است که همه افرادی که قصد دارند استارتآپ‌هایی در این حوزه تأسیس کنند یا کوین‌های اختصاصی را تولید کنند باید از آن اطلاع داشته باشند.

فرآیند انجام یک تراکنش در شبکه

اگر فردی در شبکه درخواستی را ارسال کند صحت آن درخواست توسط سرویس دهنده های شبکه و یا اصطلاحا نود ها تایید می‌شود سپس آن درخواست به شکل یک تراکنش داخل یک بلوک قرار می‌گیرد چگونگی این اقدامات سعی شده است طی فرآیندهایی شرح داده شود.

ساخت آدرس

شما برای ارتباط با شبکه بلاک چین می بایست یک آدرس برای خود داشته باشید، ساخت آدرس کار سخت و زمان بری نیست اما برای برقراری ارتباط با شبکه لازم است. آدرس شما از دو قسمت تشکیل شده، آدرس عمومی و آدرس خصوصی، که در این بین آدرس خصوصی آدرسی است که حتما می بایست در اختیار خودتان باشد و به نوعی امضای شماست، اگر هر کسی به آدرس خصوصی شما دسترسی داشته باشد به راحتی میتواند هرکاری با حساب شما بکند، از جمله به سرقت بردن دارایی های دیجیتالتان.

بهتر است این مفهوم را با مثال ملموسی بیان کنیم، تصور کنید شما از بانک خود برای حسابتان یک کارت اعتباری دریافت می‌کنید، آن شماره ۱۶ رقمی روی کارت حکم آدرس عمومی شما را دارد و میتوانید آن را در دسترس دیگران قرار دهید تا به حسابتان مبلغی را بفرستد، اما کلید خصوصی حکم رمز کارت و رمز اینترنتی شما را دارد که اگر کسی این اطلاعات را داشته باشد میتواند به راحتی از طریق حساب شما پولی جا به جا و یا خرج کند.

رمزنگاری

درخواست شما با امضای شما (که از طریق کلید خصوصی انجام می‌شود) در شبکه ارسال می‌شود و صحت این درخواست از طریق کلید عمومیتان تایید می‌شود، حال می‌خواهد این درخواست انتقال ارز دیجیتال باشد و یا تنها فرستادن یک متن.

هر کاری بخواهید بکنید رمزنگاری میشود !اگر شما بخواهید مثلا "سلام سپهر" را به فردی ارسال کنید این کلمه از طریق تابع هش رمزنگاری می‌شود و به صورت یک سری حروف و عدد بی معنی در می آید. مثلا "سلام سپهر" به bce ۹c۷۲f۴dbde۳baa۱d۳cac۳d۴۳۲d۷ تبدیل می‌شود.

تایید درخواست و رمزگشایی و پاداش

از "سلام سپهر" به این رشته اعداد و حروف رسیدن کار راحتی است، یعنی به راحتی می‌توان هر چیزی را هش کرد اما از این رشته اعداد و حروف به "سلام سپهر" رسیدن کار آسانی نیست و نیاز به پردازش بسیار زیاد و محاسبات بسیار فراوانی دارد. در شبکه بلاک چین این کار را ماینر ها انجام میدهند و به پاس زحمتی که برای این محاسبات و رمزگشایی می‌کشند از شبکه پاداش دریافت می‌کنند. البته این نحوه ی پاداش دهی بسته به نوع کارکرد آن بلاک چین دارد، این مثالی که مطرح شد برای بلاک چین هایی است که بر مبنای گواه اثبات کار (pow)عمل می‌کنند.

حال اگر کسی بخواهد "سلام سپهر" را عوض کند حتی اگر به "سلم سپهر" تبدیل کند، عبارت هش آن به طور کامل تغییر می‌کند و وابستگی بین بلوک ها به هم می‌ریزد. سوال پیش می‌آید که چگونه؟ که در فرآیند ۵ توضیح داده می‌شود.

جلوگیری از ایجاد هش تکراری

ممکن است این سوال پیش بیاید که اگر داده های یکسان موجود باشد چه می‌شود؟ در اینصورت که هش های یکسان ایجاد می‌شود!

مثلا در نظر بگیرید یک تراکنش با داده های یکسان از یک آدرس به آدرس دیگری ارسال شود، در اینصورت هش های تکراری تولید می‌شود، چون همه چیز یکسان است. شبکه برای این مشکل هم چاره اندیشیده؛ نانس(Nonce)

نانس برای همین منظور ساخته شده است، نانس یک مقدار تصادفی است که به داده ها اضافه می‌شود و پس از اضافه شدن یک هش جدید ساخته می‌شود، در این حالت داده های یکسان هش های یکسان نخواهند داشت.

تشکیل زنجیره بلوک

در بلاک چین هر بلوک به بلوک قبلی خود وابسته است، به این صورت که وقتی یک سری تراکنش ها در یک بلوک قرار می‌گیرند و به طور کلی آن بلاک هش می‌شود، این هش (که شامل اطلاعاتی از همه تراکنش های قبلی است) در بلاک بعدی قرار داده می‌شود، الی آخر...

- اولا به این دلیل است که می‌گویند زنجیره بلاک ها، زیرا در هر بلوک هش بلوک قبلی موجود است و زنجیره وار بهم متصلند.
- ثانیا به همین دلیل است که تغییر در اطلاعات هر بلوک باعث به هم خوردن پیوستگی بین بلوک ها می‌شود، زیرا اگر حتی هش یک داده تغییر کند، هش تمامی بلوک ها تغییر می‌کند.

که این از چشم اعضای شبکه پنهان نمی‌ماند، بنابراین اگر کسی بخواهد تغییری ایجاد کند این تغییر را سرویس دهنده های شبکه متوجه می‌شوند و آن را تایید نمی‌کنند، مگر اینکه ۵۱ درصد سرویس دهنده ها این تغییر را بپذیرند و آن را قبول داشته باشند.

Mempool؟ اتاق انتظاری برای تراکنش‌های تایید نشده!

Mempoolیا Transaction Pool در واقع یک جور اتاق انتظار برای تراکنش‌های (Unconfirmed Transactions) تایید نشده است و فضایی است که گره‌های کامل (Full Node) شبکه به ذخیره تراکنش‌های تایید نشده اختصاص می‌دهند. هر تراکنش بعد از آنکه ایجاد شد و در شبکه منتشر شد، هر گره‌ی کاملی، بعد از آنکه آن را تایید کرد در Mempool خود ذخیره می‌کند و سایر گره‌های مجاور آن هم از وجود این تراکنش که هنوز در بلاکچین ثبت نشده، مطلع می‌شوند و آن‌ها هم آن را در MemPool خود ذخیره می‌کنند.

روند تایید تراکنش های تایید نشده

در کل هر گره ای در شبکه بیت کوین بعد از دریافت یک تراکنش جدید، جزئیات آن را بر اساس قواعد تعریف شده در پروتوکل بیت کوین ابتدا بررسی می‌کند و بعد از آنکه تراکنش توسط گره (نود) تایید شد، در Mempool ذخیره می شود و در شبکه منتشر می‌شود تا سایر گره‌ها هم از وجود آن مطلع شوند. اما در نظر داشته باشید که با وجود تایید شدن تراکنش توسط گره ها با توجه به آنکه تراکنش هنوز توسط ماینرها در بلاک‌چین ثبت نشده است کماکان تراکنش تایید نشده تلقی می شود. تراکنش‌هایی هم که به هر نوعی با پروتوکل بیت کوین در تضاد باشند، توسط گره‌ها رد می‌شوند و اصلا در شبکه منتشر نمی‌شوند.

اما همانطور که گفته شد یک تراکنش تایید نشده توسط گره های کامل شبکه در فضای Mempool گره به انتظار می نشیند تا یک ماینر، آن تراکنش را در بلاکی که قصد دارد آن را استخراج کند قرار دهد و موفق به پیدا کردن هش مربوط به آن بلاک شود و با اضافه شدن آن بلاک در بلاکچین، آن تراکنش هم تایید شده تلقی شود. توجه داشته باشید که یک گره کامل شبکه می‌تواند خود ماینر هم باشد، اما تمام گره‌های کامل (Full Node) لزوما اقدام به صرف انرژی برای پیدا کردن هش بلاک جدید (ماینینگ) نمی‌کنند و تنها وظیفه ذخیره کل اطلاعات بلاکچین و تایید تراکنش ها و بلاک‌های جدید را به عهده دارند.

فضایMemPool

بعد از آنکه تراکنش بالاخره در بلاکچین ثبت شد، بقیه‌ی گره های شبکه آن را ازMempool های خود حذف می‌کنند. به این ترتیب بعد از استخراج هر بلاک جدید حجم MemPool گره‌ها افت پیدا می‌کند و دوباه با انتشار تراکنشهای جدید در شبکه این حجم به تدریج افزایش پیدا می‌کند. در شبکه بیت کوین با توجه به آنکه حجم هر بلاک به ۱ مگابایت محدود شده است و هر ده دقیقه به صورت میانگین یک بلاک جدید به بلاکچین اضافه می شود، در زمان های شلوغی شبکه، تعداد تراکنشهای تایید نشده که در فضای MemPool به انتظار تایید هستند، افزایش می‌یابد. در واقع در این مواقع که حجم MemPool از حجم یک بلاک که یک مگابایت است، بیشتر می‌شود، برای ثبت شدن یک تراکنش در بلاکچین ممکن است زمان بیشتری نیاز باشد.

ماینرها برای انتخاب تراکنش‌ها از بین تراکنش‌های تایید نشده موجود در فضای Mempool کاملا مختار هستند. از آنجاکه هدف ماینرها کسب سود بیشتر از توان محاسباتی خرج شده است، اولویت آن‌ها با تراکنش‌هایی است که کارمزد (Fee) بیشتری را به ماینرها پیشنهاد می‌دهند نه زمانی که تراکنش در انتظار تایید بوده است. به همین دلیل است که با افزایش میزان کارمزد پرداختی، سرعت تایید تراکنش و ثبت آن در بلاکچین افزایش می‌یابد و تراکنش‌های با کارمزد خیلی کم شاید مجبور باشند مدت زمان زیادی در صف انتظار Mempool باقی بمانند.

به تعداد گره‌های شبکه Mempool وجود دارد

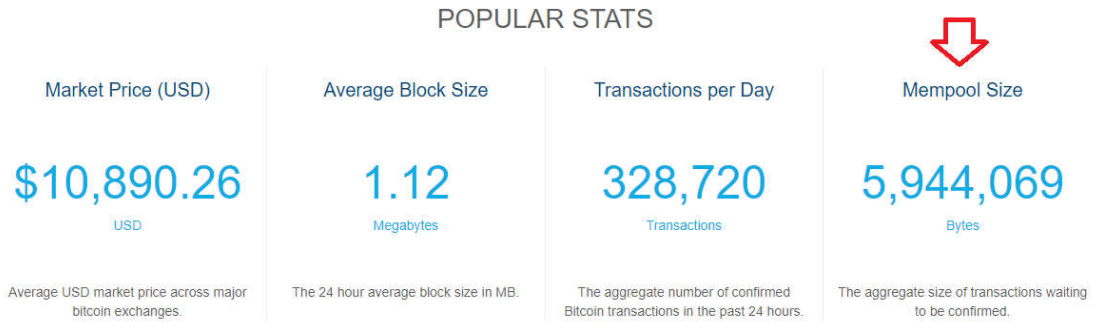
هر گره کامل شبکه، در واقع یک کامپیوتر است که بر اساس پروتوکل شبکه بیت کوین عمل می‌نماید و یک فضایی مخصوص به ذخیره تراکنش های تایید نشده یا Mempool دارد که بر روی حافظه RAM ذخیره می‌شود. از آنجا که شبکه بیت کوین یک شبکه توزیع یافته است، تراکنشهایی که هر گره دریافت می‌کند لزوما با سایر تراکنش های دریافتی سایر گره‌ها یکی نیست. به علاوه آنکه هر شخصی برای راه‌اندازی یک گره کامل، سخت افزار انتخابی خود، با ظرفیت RAM مد نظر خود را می‌تواند داشته باشد. در نتیجه هر گره ای از شبکه می‌تواند تراکنش‌های در صف انتظار مخصوص به خودش را داشته باشد و لزوما تمام تراکنش‌های موجود در تمام Mempool های گره‌های شبکه با هم یکسان نیستند.

در صورت پر شدن فضای MemPool یک گره چه اتفاقی رخ می‌دهد؟

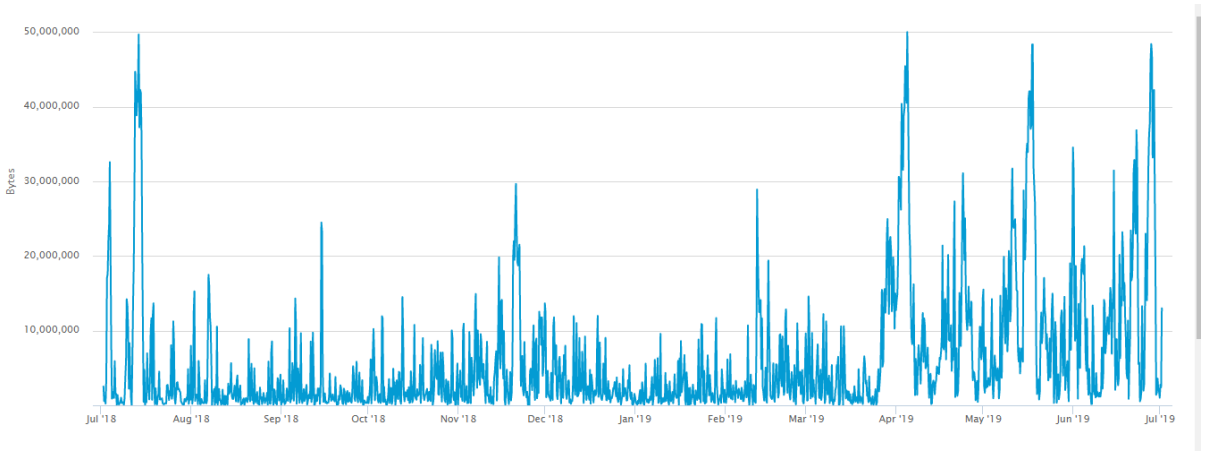
در نسخه‌های قدیمی‌تر نرم‌افزارBitcoind ، با پر شدن فضای RAM اختصاصی یک گره برای تراکنش‌های تایید نشده یاMemPool ، گره کرش می‌کرد و با MemPool خالی ری‌استارت می‌شد. اما در نسخه‌های جدید تر نرم افزارBitcoind ، می‌توان در نرم‌افزار یک آستانه کارمزد (Fee) تعریف کرد که با رسیدن به حداکثر ظرفیت Mempool تراکنش‌های با کارمزد کمتر از آستانه، به طور خودکار از فضای Mempoolحذف شوند.

مشاهده حجم کلی تراکنش‌های در صف انتظارMemPool

در اکثر مرورگرهای بلاکچین بیت کوین مانند Blockhchain.infoقسمتی برای مشاهده حجم کلی تراکنش‌های در صف انتظار تایید و تغییرات آن در طول زمان وجود دارد. در زمان نگارش این مطلب همانطور که در تصویر زیر می توان دید حجم کل تراکنشهای موجود در MemPoolهای بیت کوین، حدود ۶ مگابایت است.



در این تصویر هم تغییرات مربوط به حجم MemPool بیت کوین در طول یک سال گذشته را می توان دید.



آدرس های مخفی در بلاک چین چیست ؟

به طور خلاصه میتوان گفت آدرس های مخفی (Stealth Addresses) روشی است برای ایجاد امنیت بیشتر هنگام ارسال تراکنش در یک شبکه بلاکچین. در این حالت فرستنده لازم است که یک آدرس تصادفی و یک بار مصرف را برای تراکنش مورد نظر ایجاد کند. وقتی تراکنش های متعددی وجوه را به یک آدرس مخفی می فرستند، به جای اینکه این تراکنش ها به عنوان پرداختی های متعدد بر روی بلاک چین ظاهر شوند، آنچه که ثبت خواهد شد در واقع پرداخت های خروجی متعدد به آدرس های متفاوت است. ممکن است در ابتدا این جملات کمی گیج کننده باشد اما این کار؛ مرتبط کردن تراکنش ها را به آدرس عمومی فرد گیرنده و یا آدرس یک بار مصرف او غیر ممکن می سازد. مالک آدرس مخفی می تواند کلید رویت خصوصی تراکنش ها را مورد استفاده قرار دهد تا همه تراکنش های ورودی را ببیند.

برای مثال اگر وبسایتی بخواهد کمکهای مالی که به صورت ارز دیجیتال دریافت میکند را در معرض عام قرار ندهد، می تواند به جای یک آدرس عمومی یک آدرس مخفی را منتشر کند. با انجام دادن این کار، هر کمک جدید نیازمند ایجاد یک آدرس یک بار مصرف است و این امر ردیابی تراکنش ها را غیر ممکن می کند.

معایب آدرس های مخفی

علی الرغم ناشناسی بیشتری که توسط آدرس های مخفی به وجود می آید، این آدرس ها معایبی هم دارند که از جمله آنها می توان استفاده نادرست از آدرس های مخفی و اکتشاف موجودی را نام برد.

استفاده نادرست از آدرس های مخفی

آدرس های مخفی شمشیری دو لبه هستند. از یک طرف، روشی قدرتمند برای اضافه کردن امنیت برای کاربران واقعی است اما از طرف دیگر، یک روش قدرتمند برای افزایش امنیت برای کاربران بدکار فراهم می آورد. اگر آدرس عمومی کاربری که درگیر فعالیت بدکارانه شده مشخص باشد، فورا می توان برای پیگیری تراکنش ها بر روی بلاک چین اقدام کرد. اما اگر این کاربر به جای آدرس عمومی از آدرس مخفی استفاده کند، ردیابی آن بسیار دشوار خواهد بود. در اساس می توان گفت که کار کاربرانی که درگیر فعالیت های خرابکارانه هستند توسط آدرس های مخفی آسان تر خواهد شد.

اکتشاف موجودی

این موضوع به این اشاره دارد که چگونه یک پروتکل بلاک چین محور که آدرس های مخفی را اعمال کرده، تشخیص می دهد که تراکنش انجام گرفته یا نه و متعلق به کدام کاربر است. به مثال قبل بر می گردیم، اگر همان وبسایت هزاران کمک را با آدرس ایجاد شده خود دریافت کند، کشف این تراکنش ها و نسبت دادن آنها به کاربری خاص می تواند از لحاظ فنی چالش برانگیز باشد.

نتیجه گیری

در حال حاضر این راهکار در شبکه هایی مانند مونرو پیاده می شود و ردیابی تراکنش ها روی مونرو؛ تقریبا کاری غیرممکن به نظر می رسد. آدرس های مخفی ابزار بسیار قدرتمندی هستند زیرا لایه ای اضافی از ناشناسی را فراهم می آورند. این آدرس ها از کاربران محافظت می کنند تا موجودی حسابشان بر روی بلاک چین در معرض عام قرار نگیرد و این کار با ایجاد آدرس های یک بار مصرف انجام می گیرد. با استفاده از کلید رویت شخصی، مالکین آدرس های مخفی می توانند همه تراکنش های ورودی را مشاهده کنند. این لایه امنیتی اضافی می تواند هم به نفع کاربران خوش نیت و هم به نفع کاربران بداندیش باشد. علاوه بر این، چالش های فنی در اعمال این آدرس ها وجود دارد مانند همان چالش اکتشاف موجودی که مورد بحث قرار گرفت.

HASH GRAPH

دفتر کل عمومی غیرمتمرکز هش‌گراف، توسط شورای هش‌گراف هدرا (Hedera Hashgraph Council) اداره می‌شود. هش‌گراف در صدد برطرف کردن موانع عملکرد، امنیت، نظارت، ثبات و معرفی رویه قانون گذاری است تا جایگزین بهتری برای بلاک چین باشد. هش‌گراف تقریبا راندمان کامل پهنای باند را ارائه داده و از تحمل خطای بیزانس (aBFT) برای رسیدن به اجماع و حفظ استانداردهای برتر امنیتی استفاده می‌کند. هسته هش‌گراف بر اساس جاوا می‌باشد. در نتیجه، اجرای قراردادهای هوشمند و برنامه غیرمتمرکز با استفاده از جاوا کدگذاری می‌شود .هش‌گراف هدرا(Hashgraph Hedera) ، ارزهای دیجیتال را برای انجام پرداخت ها و کارمزدهای پرداخت را برای استفاده از پلتفرم تعیین کرده است.

معماری

بلاک چین ساختار درختی دارد. زنجیره اصلی ریشه درخت و نودها شاخه های آن می‌باشند. در بلاک چین برای جلوگیری از رشد بیش از حد شاخه ها، آنها را هرس می‌کنند. در مقابل، هش‌گراف شاخه‌های جدید را شکل می‌دهد و نود را به زنجیره اصلی برمی‌گرداند .سیستم فایل هش‌گراف به کابران اجازه می‌دهد تا با به اجماع رسیدن، دقیقا تعیین کنند چه اطلاعاتی ذخیره شود و کدام یک ذخیره نشود. یک فایل باید توسط هش خود در دسترس باشد و یک شماره شناسه ID داشته باشد. فایل ها در هش‌گراف در درخت مرکل ذخیره می‌شوند اما برای اینکه توسعه دهندگان بتوانند آن ها را تغییر دهند، کلاس‌هایی در جاوا ارائه شده است.

نودها تراکنش هایی که از کاربران گرفته اند را با استفاده از پروتکل شایعه پراکنی (gossip protocol) در سراسر شبکه به اشتراک می‌گذارند. پس از اینکه تراکنش میان تمام نودها پخش شد، نودها الگوریتم اجماع هش‌گراف را اجرا می‌کنند تا به توافقی بر سر زمان بندی برسند و به ترتیب زمانی هر تراکنش را مرتب کنند. سپس هر نود نسخه وضعیت هش گراف خود را به روز رسانی می‌کند.

در ساختار پروتکل گاسیپ هر گره خودش یک گراف می باشد که ترتیبی از ارسال کنندگان و شاهدان برای انجام یک تراکنش است. همه گره ها دید یکسانی در مورد همه تراکنش ها و شاهدان دارند. علاوه بر این، با اجرای یک نظرسنجی مجازی درباره یک تراکنش، هر گره می تواند تشخیص دهد که آیا بر این اساس که تراکنش مورد نظر بیش از دو سوم گره ها را در شبکه به عنوان شاهد دارد یا خیر، معتبر است یا خیر. توجه داشته باشید که هش گرف در شرایط بیزانس کار می کند که در آن فرض بر این است که کمتر از یک سوم گره ها بیزانس هستند. (گره هایی که می توانند در قبال حذف، پاسخ یا جعل پیام های دریافتی یا ارسالی رفتار بدی داشته باشند)

اجماع

هش‌گراف از مکانیزم اجماع (aBFT) استفاده می‌کند. این مورد بدان معناست که هیچ عضوی به تنهایی نمی‌تواند باعث جلوگیری رسیدن جامعه به اجماع شود و هم چنین نمی‌تواند پس از رسیدن به اجماع، آن را تغییر دهند. در هش‌گراف، حتی اگر هکرها بتوانند پیام های مورد نظر خود را کنترل یا حذف کنند، باز هم اجماع به دست خواهد آمد. فرض این است که بیش از دو سوم نودها درستکار باشند و اگر یک پیام مکررا از یک نود به نود دیگر در سراسر اینترنت فرستاده شود، هر نود می تواند توسط دیگری و الی آخر از پیام آگاه شود.

مقایسه با بلاک چین

- با کنار گذاشتن الگوریتم اجماع اثبات کار، راندمان هش‌گراف با توجه به عدم نیاز به پهنای باند و انجام هزینه برای سخت افزار، افزایش یافته است. کاربران می‌توانند از سخت افزار مقرون به صرفه و در دسترس استفاده کنند و پهنای باند مورد نیاز تنها برای اطلاع دادن به تمام نودهای در رابطه با تراکنش است. هم چنین تاخیر و زمان بین تراکنش و تایید را کاهش می‌دهد.
- مکانیزم شایعه پراکنی سریعتر و ارزانتر از PoW است اما هر دو یک فرض را دنبال می‌کنند و آن این است که هکرها نمی‌توانند همزمان به بیش از یک‌سوم نودها حمله کنند. اگر هکرها با قدرت کافی پردازنده، بیش از یک سوم نودهای شبکه را مسدود کنند، ممکن است شبکه با اختلال مواجه شود.

ویژگی ها و معایب فناوری هش گرف(Hashgraph)

سریع : هش گرف سریع است چون که از پروتکل شایعه پراکنی برای پخش پیام ها در شبکه استفاده می کند و همچنین یک سری بهینه سازی ها برای پیام های پراکنده شده برای کاهش بار ترافیکی ارتباطی انجام می دهد.

در یک محیط بدون نیاز به اجازه دسترسی (در بلاک چین) مانند بیت کوین و اتریوم، گره هایی که در پروتکل جمعی شرکت می کنند به عنوان گره نامعتبر شناخته نمی شوند چرا که تا زمانی که هر گرهی امکان پیوستن یا ترک شبکه را در آینده دارد. علاوه بر این ساز و کار جمعی برای انجام چنین کاری باید به عنوان کار تخریبی به حساب بیاید. احتمالا حمله Sybil که یک کاربر تنها، چند موجودیت می سازد که باعث بروز حملات می شود. حل این مشکل در یک محیط بدون نیاز به اجازه دسترسی روی خروجی کل تاثیر می گذارد.

در سویی دیگر، در یک دفتر کل توریع شده دارای اجازه دسترسی شناسایی همه گره ها پیش از هر چیز شناخته می شود و شبکه برای هر شرکت کننده ای باز نیست. دانش قبلی درباره هویت شرکت درباره هویت گره های شرکت کننده نوعی محافظت طبیعی در برابر حملات Sybil ارائه و رسیدن به یک توافق را ساده تر می کند. این بدان معناست که نیاز به هیچ ساز و کاری برای مقابله با Sybil نیست و در این صورت خروجی به صورت چشمگیری افزایش می یابد. (وقتی که با بلاک چین عمومی مقایسه می کنیم)

با توجه به این که هش گرف در حال حاضر یک دفتر کل توزیع شده خصوصی است، خروجی آن باید با چیز هایی مشابه با بلاک چین خصوصی مقایسه شود .برای مثال IBM HyperLedger Fabric (با قابلیت انجام ۷۰۰ تراکنش در ثانیه). خروجی آن نباید با بلاک چین عمومی مانند بیت کوین یا اتریوم مقایسه شود که می توانند ۱۰ تراکنش را در ثانیه انجام دهند چرا که مانند مقایسه سیب با پرتقال است! در حال حاضر هش گراف هنوز جزئیات فنی درباره این که آیا به عنوان یک دفتر کل عمومی مورد استفاده قرار می گیرد یا خیر، منتشر نکرده است.

عادلانه : هش گرف با استفاده از زمان سنجی توافقی (consensus time stamping) عدالت را بر قرار می کند. این بدان معناست که اگر یک تراکنش به دو سوم دیگر تراکنشها در ابتدای شبکه برسد، آن تراکنش اولین به حساب می آید. این سیستم نسبتا عادلانه است چرا که دو سوم شبکه شاهد هستند و برای اکثر آن ها سخت است که تصمیمات ناعادلانه بگیرند. به هر حال هش گرف بر اساس پروتکل شاعه پراکنی است و این بدان معناست که زمانی که یک گره جانشینان خود را به طور یکنواخت و تصادفی انتخاب می کند، احتمالی وجود دارد (مثلا یک سوم، اگر همسایگان گره به طور جهانی، یکنواخت و تصادفی انتخاب شوند) که تمام گره های انتخاب شده احتمالا یا بیزانس یا مخرب هستند.

این جانشینان مخرب می توانند انتقال تراکنش به گروه بعدی از گره ها را متوقف کنند که یعنی ممکن است تراکنش به دو سوم شبکه نرسد که نتیجه آن می شود که سازنده آن تراکنش که صادقانه عمل کرده، به مشکل می خورد. به علاوه سعی می شود که هر گره صادق به گره های صادق متصل شود که در این صورت هر پیام به دیگر گره های صادق ارسال می شود بدون این که توسط گره های مخرب و نادرست متوقف شود. اگر چه این موضوع در حال حاضر مربوط به طبیعت خصوصی هش گرف نمی شود و این مشکل زمانی رخ می دهد که یک دفتر کل توزیع شده عمومی عرضه شود.

ایمن : هش گرف یک BFT ناهمگام است ولی قطعی نیست. یکی از مختصصان در این حوزه در سال ۱۹۸۵ نشان داد که در سیستم های ناهمگام، پروتکل های قطعی توافقی حتی در موارد ساده با یک گره مشکل دار نیز امکان پذیر نیستند. یک پروتکل توافقی می تواند در محیط بیزانس بدون قطعیت و همگام سازی شده یا قطعی بدون همگام سازی کامل باشد.

در مورد پروتکل های قطعی، همه گره های صادق تا دوره r برای یک ثابت از پیش شناخته شده به توافق می رسند. در مورد پروتکل های احتمالاتی یا غیر قطعی، احتمال این که یک گره صادق بعد از r دو به موازات r که به بی نهایت می رسد، به صفر می رسد، تصمیمی گرفته نمی شود. در مورد پروتکل های همگام، تضمین می شود که پیام ها بعد از گذشت یک محدوده خاص برسد ولی پروتکل های ناهمگام چنین محدوده ای ندارند.

هش گرف با اضافه کردن تصادفی بودن، یک پروتکل ناهمگام غیر قطعی است. مصالحه این است که پروتکل قطعی ناگهانی از بین می برد ولی در این مورد چه زمانی از بین بردن رخ می دهد، موارد نامشخصی وجود دارد. در طراحی فعلی اش، هش گرف نوعی بازی شیر یا خط را برای گره ها و برای تصمیم گیری در زمانی که هیچ پردازشی در پروتکل قطعی نیست، به کار می گیرد. از این رو احتمال همه گره های صادق که بعد از چندین بار شیر یا خط کردن مقدار یکسان دارند، غیر صفر است. در نهایت همه گره های راستگو تبدیل به یک توافق دست جمعی می شوند. به هر حال اگر همه گره های بیزانس تلاش کنند تا پروتکل را با دستکاری پروتکل شایعه پراکنی همانطور که در بخش دوم گفتیم، دچار اختلال کنند، اثر بخشی و بهره وری هدف شیر یا خط سوال بر انگیز می شود چرا که ممکن است نیاز به تعدا زیادی دور برای رسیدن به قطعیت باشد.

آیا هش گرف فناوری بلاک چین را منسوخ می کند؟

هش گرف یک پروتکل قطعی جالب است که هدف اصلی آن افزایش خروجی در محیط های ایستا و خصوصی است. هش گرف سریع، عادلانه و ایمن است در محیط با اجازه دسترسی کار می کند. ولی اگر در محیط عمومی مورد استفاده قرار بگیرد، هش گرف با همان مشکلی که بلاک چین در محیط عمومی مواجه هست، روبرو می شود و احتمالا نمی تواند ایمنی و عملکرد خود را نگهداری کند. در واقع، مقایس پذیری همچنان مشکل برای بلاک چین های عمومی است. این که راهکار های تازه ای توسط انجمن ها معرفی می شود جالب است. مثلا اتریوم از PoSبرای پروتکلCasper ، نئو ازdBFT ، ای او اس از راهکار dPoS و زیلگا از sharding استفاده می کند. همه این راهکار ها مزایا و معایب خودشان را دارند چرا که هنوز راه حل قطعی برای حل مشکل مقیاس پذیری وجود ندارد

تنگل TANGLE

تنگل، فناوری دفتر کل توزیع شده برای اینترنت اشیا (IoT) است و ویژگی های مورد نیاز برای ایجاد سیستم ریزپرداخت ماشین به ماشین را ارائه می‌دهد IOTA .ارز دیجیتالی دارای فناوری تنگل است.

ریزپرداخت ها به دلیل کارمزد بالا تراکنش و مکانیزم اجماع اثبات کار، معضل جدی در بلاک چین می‌باشند. تنگل این معضل را با حذف تفاوت بین صادرکننده و تاییده کننده برطرف می‌کند.

معماری

تنگل برای ذخیره سازی تراکنش ها از ساختار گراف جهت دار غیرمدور یا (DAG) بهره برده است. هنگامی که تراکنش جدیدی ایجاد می‌شود، DAGدو تراکنش قبلی را تایید می‌کند. اگر تراکنش A تراکنش B را تایید کند، نشان دهنده این است که A به طور مستقیم B را تایید کرده است. در سناریویی که A مستقیما B و B مستقیما C را تایید می‌کند، پس A غیرمستقیم C را تایید می‌کند.

به منظور صدور یک تراکنش، نود بر اساس الگوریتم، دو تراکنش دیگر را برای تایید انتخاب می‌کند. سپس بررسی می‌کنند که دو تراکنش با یکدیگر تناقض نداشته باشند. در صورت وجود تناقض، نود تراکنش متناقض را تایید نمی‌کند. برای تایید تراکنش، نود باید پازل کریپتوگرافیک مشابه با بلاک چین بیت کوین را حل کند Tangle .به نوعی پاسخی از طرف IOTA است به آنچه که افراد شرکت کننده در پروژه فکر می‌کنند مشکلات رایج تکنولوژی بلاک‌چین است. اساسا Tangle یک ساختار اداره‌ی گراف داده‌ها در زیر پوسته‌ی IOTA است.

مقایسه با بلاک چین

- معماری تنگل با بلاک چین متفاوت است. بلاک چین دارای ساختار توزیع شده جهانی می‌باشد که در آن نودها نسخه ای از لجر را حفظ می‌کنند. در تنگل، داده ها در DAG ذخیره می‌شوند.
- در تنگل، تراکنش ها مستقیما توسط تراکنش های جدید تایید می‌شوند و مجبور نیستند منتظر بمانند تا در بلاک قرار گیرند. این مورد تاخیر بین شروع به کار و تراکنش را کاهش می‌دهد.
- نهاد مجزایی برای تایید تراکنش ها وجود ندارد. برای اینکه تراکنش جدیدی رخ دهد، باید دو تراکنش دیگر تایید شوند، بنابراین باعث حذف مفهوم مشوق پولی و کاهش چشمگیر هزینه تراکنش می‌شود و ریز تراکنش ها را در سیستم امکان پذیر می‌کند.

Coin و Token

همه ارزهای دیجیتال در دو دسته کلی coin و token دسته بندی می شوند. گاها از ارز دیجیتال بیت کوین به عنوان coin و از دیگر ارزها مانند لایت کوین، کاردانو، اتریوم و ... به عنوان Altcoin یاد می شود.coin ها همگی دارای دفترکل توزیع شده مختص به خود هستند که می توانند جهت مقاصد خاص و یا با کاربری هایی خاص مانند قرارداد هوشمند، برنامه های توزیع شده، ... و یا امکان میزبانی از ارزهای دیگر ارائه شوند.

Token به ارزهایی گفته می شود که بر روی دفتر کل توزیع شده دیگر ارزها ارائه و نگهداری می شوند و برای ادامه حیات به وجود آنها نیازمند هستند مانند توکن BAT که بر روی بلاک چین اتریوم عرضه شده.

بیشتر ICO ها جهت تامین مالی بهتر و شفافیت بالاتر و از بین بردن واسطه با استفاده از قرارداد هوشمند و بر روی Ledger دیگر ارزها مخصوصا اتریوم به عنوان توکن عرضه می شوند. البته این توکن ها بعدها می توانند ledger اختصاصی خود را داشته باشند. از آن جمله می توان به کاردانو و ترون اشاره کرد که در ابتدا به عنوان توکن بر روی بلاک چین اتریوم عرضه شده سپس بلاک چین خود را تشکیل دادند و حالا از توکن های دیگر میزبانی می کنند. بطور کلی می توان گفت یک ارز دیجیتال مانند بیت کوین، بیت کوین کش، اتر و ... می‌تواند مستقل از پلتفرم خود، عمل کند. ما می‌توانیم از آنها به عنوان ارز مستقلی در خارج از بستری که توسعه‌یافته‌اند استفاده کنیم.

از طرف دیگر، USDT, BNC و غیره مثال‌هایی از توکن‌هایی هستند که مربوط به یک پلتفرم خاص (در این مثال‌ها اتریوم) می‌شوند. درواقع یک توکن، نماد یک دارایی و یا کاربردی است که یک سازمان به سرمایه‌گذاران خود در مرحله‌ی عرضه‌ی اولیه‌ی سکه (ICO) می‌دهد.

یک توکن چگونه ارزش ایجاد می کند؟

همان‌طور که ویلیام موگایار (William Mougayar) در مقاله خود در سایت Medium می‌نویسد، ارزش آفرینی یک توکن بر سه اصل اساسی استوار است:

- نقش (Role)
- ویژگی‌ها (Features)
- هدف (purpose)

این سه اصل، مثلث طلایی ارزش یک توکن را تشکیل می‌دهند. هر نوع توکن (نقش)، ویژگی‌ها و اهداف مربوط به خود را دارد که در جدول زیر آورده شده‌اند:

نقش	اهداف	ویژگیها
حق	ایجاد بستر تعامل	کاربرد محصول، رای دادن، حاکمیت، دسترسی به امکانات محصول، سهام، مالکیت
تبادل ارزش	خلق اقتصاد	پاداش کار،فروش کالا یا خدمت، خریدن، کار مستقیم یا غیر مستقیم، خرج کردن، ایجاد یک محصول جدید
تحقق حقوق خاص	سرمایه گذاری کردن	اجرای قراردادهای هوشمند، سپرده امن، کارمزد استفاده
عملکرد	بهبود تجربه کاربری	پیوستن به یک شبکه، تعامل با کاربران،انگیزه استفاده از پلتفرم
ارز	تراکنشهای بدون تداخل	واحد پرداخت، واحد تراکنش
درآمدزایی	مزایای توزیع شده	به اشتراک گذاری سود، به اشتراک گذاری مزایا، مزیت تورم

- حق

با خریداری و داشتن چنین توکن‌هایی، دارنده، بسته به میزان توکنی که در اختیار دارد، شامل حقوق خاصی در شبکه می‌شود. به‌عنوان‌مثال، با خریداری یک توکن DAO، شما حق رای در داخل DAO پیدا می‌کنید و می‌توانید تعیین کنید که چه پروژه‌هایی تأمین سرمایه شوند یا به کدامیک از آنها سرمایه‌ای تعلق نگیرد.

- تبادل ارزش

این توکن‌ها یک سیستم اقتصادی داخلی در پلتفرم ایجاد می‌کند که به خریداران و فروشندگان کمک می‌کند تا ارزش را در آن اکوسیستم با یکدیگر مبادله کنند. به‌وسیله این توکن‌ها افراد می‌توانند با به اتمام رساندن وظایف مشخص شده، پاداش دریافت کنند. ایجاد و نگه‌داری سیستم‌های داخلی و مستقل اقتصادی، از جمله وظایفی است که این توکن‌ها بر عهده دارند.

- تحقق حقوق خاص

به‌وسیله این توکن‌ها می‌توان حقوق خاصی را برای دارنده آن ایجاد نمود که به‌وسیله آنها بتواند در یک سیستم، عملکردهای مختلفی داشته باشد. گولم(Golem) یکی از این نمونه‌ها است. شما با خریداری توکن‌های گولم که GNT نام دارند می‌توانید به ابررایانه‌های گولم دسترسی یافته و از آنها استفاده نمایید.

- عملکرد

این توکن‌ها، یک تجربه‌ی کاربری غنی برای دارندگانشان ایجاد می‌کنند. برای مثال در اکوسیستم مرورگر Brave دارندگان BAT (توکن‌های این پلتفرم)، می‌توانند از توکن‌های خود برای تبلیغات و سرویس‌های دیگر استفاده کنند.

- ارز

این توکن‌ها برای ذخیره‌ی ارزش و انجام تراکنش‌ها در داخل و خارج از اکوسیستم به کار می‌روند.

- درآمدزایی

سود و دیگر منافع اقتصادی را بین سرمایه‌گذاران در یک پروژه‌ی خاص توزیع می‌کند.

این تعاریف چگونه به ارزش‌گذاری یک توکن کمک می‌کند؟

یک توکن برای ارزش باالاتر بایدبیش از یکی ازاین نقش‌ها را داشته باشد. در واقع هر چه نقش‌هایی که یک توکن می‌تواند ایفا کند، بیشتر باشد، ارزش آن توکن بالاتر خواهد رفت.

انواع TOKEN

توکن های ارزی

نوع اول کریپتوها همانی است که در باورعموم وجود دارد. یک محصول برای ذخیره سرمایه یا ابزاری برای مبادلات، مانند بیت کوین. به این نوع ارز دیجیتال، توکن های تراکنشی نیز گفته می شود. توکن های تراکنشی دارای ارزش می باشند، زیرا طرفین مبادله به این نکته قبول دارند.

فیل گلیزر از شرکت هکرنون (Hackernoon) اظهار داشت همانند ارزهای رایج سنتی نظیر دلار یا یورو، بیت کوین نیز به عنوان یک کالا دارای ارزش ذاتی محدود می باشد و ارزش آن به این دلیل است که افراد، آن را ارزش گذاری می کنند.

بیت کوین در سال ۲۰۰۹ به منظور ایجاد و توسعه یک ارز بهتر معرفی شد تا بتواند پاسخگوی بعضی از محدودیت های ارزهای رایج سنتی باشد. دیوید گودبوی از بورس نزدک (Nasdaq) بیان کرد، قطعا روزی فرا می رسد که بعضی از ارزهای دیجیتال جایگزین ارزهای سنتی خواهند شد.

اما حتی ارزهای دیجیتال نیز محدودیت های خاص خود را دارند. یکی از بزرگترین نقص های بیت کوین اندازه و حجم یک مگابایتی بلاک های داده و ظرفیت بازدهی شبکه آن می باشد. مسئله دیگر بیت کوین، حفظ حریم خصوصی آن می باشد. گلیزر در این خصوص توضیح داد در حالی که آدرس های بیت کوین ناشناس می باشند و در دیتابیس آن، کیف پول به اشخاص متصل نمی باشد، موجودی و تراکنش های کیف های پول به طور عمومی در دفتر کل قابل مشاهده می باشند. در پاسخ به این محدودیت ها، ارزهای دیجیتال دیگری نظیر لایت کوین و دش کوین ایجاد شده اند تا به چالش های موجود بپردازند.

توکن های کاربردی

توکن های کاربردی با اسامی کوین های اپلیکیشنی یا توکن های کاربر نیز شناخته می شوند. این توکن ها دسترسی های آتی به محصولات و خدمات را به کاربران ارائه می دهند. در چشم انداز فعلی بلاک چین، جذب سرمایه از طریق ICO ها و صدور توکن برای استارت آپ ها دارای محبوب می باشد. کاربران می توانند با استفاده از این توکن ها به خدمات آتی استارت آپ های مورد نظر دسترسی داشته باشند. برای ایجاد انگیزه بیشتر، دارندگان این توکن ها برای خرید محصولات نهایی و یا در قیمت نهایی، تخفیف دریافت می کنند.

توکن های کاربردی نظیر ریپل برای اهداف خاصی طراحی شده اند. ریپل برای ایجاد انتقال بدون هزینه از طریق پول رایج طراحی شده اند و توسط بانک ها و موسسات مالی نظیرRBC ، امریکن اکسپرس، BMO، SEBوچندین موسسه دیگر مورد استفاده قرار می گیرند.

توکن های پلتفرمی | اپلیکیشنی

ارزهای دیجیتال پلتفرمی، فناوری های کامل بلاک چین با پروتکل ها و مجموعه قوانین خاص خود می باشند که برای اپلیکیشن ها یا برنامه هایی که بصورت غیر متمرکز طراحی خواهند شد، زیرساختی مهیا می کنند تا بر بستر این بلاک چین ها ایجاد شوند. گودبوی در این خصوص می نویسد: این توکن ها برای حذف واسطه ها، ایجاد بازارهای مختلف و حتی عرضه سایر ارزهای دیجیتال ایجاد شده اند.

اتریوم محبوب ترین نمونه ارز دیجیتال پلتفرمی می باشد. توکن های اتریوم، توکن های دیجیتال بر پایه بلاک چین اتریوم می باشند که یک پلتفرم غیرمتمرکز می باشد و برای اجرای قراردادهای هوشمند و هم چنین ایجاد بلاک ارزهای دیجیتال جدید در سایر طبقه بندی ها و بخش ها مورد استفاده قرار می گیرد.

توکن اپلیکیشنی یک توکن دیجیتال برای برنامه هایی است که بر بستر پلتفرم مورد نظر ایجاد شده اند. برای مثال آگوریس (Auguris) یک برنامه غیرمتمرکز پیش بینی بازارهای مختلف می باشد که بر بستر بلاک چین اتریوم ایجاد شده است. آگور توکن های خود را به اسم REP صادر کرده است. اگر دارای توکن REP می باشید و پیش بینی دقیقی از بازار آگور انجام دهید، سهمی از هزینه های بازار دریافت می کنید.

توکن های اپلیکیشنی ممکن است بیانگر اشتراک یا عضویت دیجیتال باشند که دارندگان آن می توانند برای کسب سود یا سهمی از فروش به صورتREP ، به معامله این توکن ها بپردازند.

انواع استانداردهای توکن بر بستر اتریوم Ethereum Request for Comments

ERC مخفف عبارت Ethereum Request for Comments است، یعنی نسخه اتریوم RFC یا Request For Comment که RFC به مجموعه ای از یادداشت های تکنیکی و سازمان یافته گفته می‌شود. بنابراین ERC ها شامل دستورالعمل های تکنیکی برای ساخت شبکه اتریوم هستند.

این دستورالعمل ها توسط توسعه دهندگان اتریوم برای جامعه اتریوم نوشته می‌شود. بنابراین فرآیند تولید یک ERC به وجود یک توسعه دهنده نیاز دارد. برای ساخت یک استاندارد برای پلتفرم اتریوم، توسعه دهنده یک پروپوزال بهبود اتریوم یا همان EIP ارائه می‌دهد. این پروپوزال شامل ویژگی های پروتکل و استانداردهای قراردادها است. زمانی که EIP توسط کمیته پذیرفته و نهایی شود، تبدیل به یک ERC می‌شود .همان طور که گفته شد، EIPهای نهایی شده مجموعه ای از استانداردهای قابل پیاده سازی را برای توسعه دهندگان اتریوم فراهم می‌کند.قراردادهای هوشمندی که با استفاده یک استاندارد ERC ساخته شوند، یک رابط مشترک دارند و ارتباط گرفتن با همه این قراردادها می‌تواند با یک روش مشخص انجام شود .استفاده از استانداردها در نوشتن قرارداد هوشمند یک توکن اجباری نیست ولی استفاده از آنها این اطمینان را به صاحبین پروژه می‌دهد که توکن آنها به راحتی می‌تواند با انواع کیف پول ها، صرافی ها و قراردادهای هوشمند دیگر بدون مشکل کار کند.

ERC-10

ERC-20

استاندارد ERC-20 لیستی از قوانینی است یک روی یک توکن باید پیاده سازی شود تا بتواند روی اکوسیستم اتریوم فعالیت داشته باشد. توکن‌های ERC-20 به دلیل امکان استفاده در عملیات‌های جذب سرمایه یا ICO بسیار کاربردی هستند. پروژه‌های مبتنی بر بلاک چین می‌توانند تا زمان ساخت بلاک چین اصلی خود، با ساخت و فروش توکن‌های ERC-20 اقدام به جذب سرمایه کنند. توکن‌های ERC-20 روی تمامکیف پول‌های معتبر اتریوم قابلیت ذخیره‌سازی و انتقال دارند.

به زبان ساده، ERC20 مجموعه‌ای از قواعد و مقرراتی است که به شما کمک می‌کند یک قرارداد هوشمند را به همراه توکن‌هایش بر بستر اتریوم بسازید. ERC کوتاه‌شده‌ی عبارت Ethereum Request for Comment است و عدد ۲۰ شماره‌ای بوده که به این درخواست تخصیص می‌شود.

توکن ERC20 چگونه کار می‌کند؟

زمانی که یک قرارداد هوشمند قصد ایجاد یک توکن در پلتفرم اتریوم را داشته باشد، توکن ERC20 وارد بازی می‌شود. در حقیقت ERC20 زبان مشترکی است که تمام قراردادهای هوشمند اتریوم از آن استفاده می‌کنند. این زبان به توکن‌ها، امکان مبادله شدن توسط یکدیگر را می‌دهد. برای چگونگی نحوه‌ی کار این استاندارد مثالی می‌زنیم.

فرض کنید می‌خواهیم یک بازی بسازیم که کاربران با استفاده از توکنی که برای این بازی طراحی شده است قابلیت‌هایی را در مراحل مختلف بازی به دست آورده و با یکدیگر به رقابت می‌پردازند. کاربران برای اینکه بتوانند وارد این بازی شوند باید توکن ما را با استفاده از یکی از ارزهای مجازی مثل بیت‌کوین یا غیره بخرند.

فیلدهای اختیاری استاندارد ERC20 :

- اسم توکن (Token name): نامی است که به توکن پلتفرم خود اختصاص می‌دهید.
- نماد یا علامت اختصاری (Symbol): نماد اختصاری مربوط به توکن است.
- تعداد اعشار (Decimal): در حقیقت شما در این فیلد، میزان تقسیم‌پذیری توکن خود را تعیین می‌نمایید. مثلا اگر مقدار این فیلد را ۱ قرار دهیم، کمترین مقدار توکن در پلتفرم ما ۱/۰ می‌شود.

برای مثال بازی فیلدهای اختیاری را به شکل زیر قرار می‌دهیم:

- اسم توکن: ArzdigitalGame
- نماد اختصاری توکن: AGM

- اعشار کمترین مقدار: ۲ رقم اعشار

فیلدهای اجباری استاندارد ERC20 :

- مقدارکلی (Total Supply): تعداد کل توکن‌هایی است که برای پلتفرم خود در نظر می‌گیریم.
- موجودی (balance of): این متغیر تعداد توکن‌های مربوط به هر آدرس کاربری را نشان می‌دهد.
- انتقال (Transfer): فرآیند تخصیص توکن‌های اولیه به کاربران است.
- انتقال از (Transfer From): تابع transferFrom به یک بازیکن امکان می‌دهد به بازیکنی دیگر توکن بفرستد.
- تایید (approve): این تابع، تراکنش‌ها را بر مبنای تعداد کلی توکن‌ها می‌سنجد.
- مجوز (allowance): این تابع، موجودی حساب هر بازیکن را چک کرده و در صورتی که تعداد توکن‌ها کافی نباشد تراکنش را کنسل می‌کند.

```
contract ERC۲۰Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint
remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

حالا با استفاده از این فیلدها می‌توانیم مشخص کنیم که:

- تعداد کل توکن‌ها چقدر باشد.
- موجودی هر کاربری که در ابتدا توکن برای او ارسال می‌شود چه مقدار باشد.
- به چه کسانی توکن‌ها ارسال شوند.
- و...

تفاوت توکن‌های ERC-20 و کوین های با بلاک چین مستقل

توکن ها در بستر بلاک چین اتریوم، دارایی‌هایی هستند که ارزش دارند. آنها همانند بیت کوین، لایت کوین و اتریوم ارسال و دریافت می‌شوند. تفاوت این توکن ها با ارزهای دیجیتالی که مانند بیت کوین بلاک چین جداگانه دارند، این است که این توکن ها از آدرس های اتریوم استفاده می‌کنند و تراکنش های خود را روی بلاک چین اتریوم می‌فرستند؛ درحالی که کوینی مثل بیت کوین، بلاک چین مخصوص خودش را دارد و تراکنش های آن روی بلاک چین بیت کوین ثبت می‌شوند.

مزایای توکن های ERC20

پیش از اینکه این استاندارد به وجود بیاید، برنامه نویس‌ها از اسامی متفاوتی برای نوشتن کد خود استفاده می‌کردند. برای مثال یکی از اسم تابع totalAmount برای ارائه تعداد کل توکن‌های عرضه شده استفاده می‌کرد و دیگری از .totalNumber به دنبال آن کیف پول‌ها و صرافی‌ها برای ارتباط گرفتن با هر توکن مجبور بودند کد هر توکن را بخوانند و برای ارتباط با آن توکن، تغییرات لازم را در پلتفرم خود اعمال کنند. بنابراین استفاده از یک استاندارد مشخص مزایای زیر را دارد:

۱. یکریختی توکن‌ها
۲. سادگی لیست شدن در اکسچنج ها برای ترید
۳. سادگی برای ارتباط با سایر قراردادهای هوشمند
۴. سادگی برای تعامل با کیف پول های مختلف

معایب ERC20

مسائلی وجود دارد که استاندارد ERC20 به آنها نپرداخته است. در این استاندارد گیرنده از دریافت توکن مطلع نمی‌شود و این امر می‌تواند منجر به از دست رفتن سرمایه کاربر شود. برای مثال اگر شما توکن‌های خود را به آدرس قرارداد هوشمند یک توکن ERC20 دیگر ارسال کنید، توکن های شما در آن آدرس گیر می‌افتد؛ درحالی که چنین تراکنش هایی باید برگشت بخورند. تا آخر سال ۲۰۱۷ حدودا ۳ میلیون دلار به این دلیل از دست رفته است .برای حل این مشکل جامعه اتریوم اکنون استاندارد جدیدی به نام ERC-223 معرفی کرده است. این استاندارد اجازه نمی‌دهد که توکن به آدرسی که از دریافت آن توکن پشتیبانی نمی‌کند، ارسال شوند.

مشکل نرم افزاری batchOverflow مشکل دیگری است که این استاندارد محدودیتی برای آن در نظر نگرفته است. وجود این مشکل در یک توکن می‌تواند منجر به خرج کردن مبلغی بیش از موجودی، از یک آدرس شود. در ماه آوریل سال ۲۰۱۸ به دلیل این مشکل نرم افزاری، تعدادی از صرافی‌ها امکان برداشت و واریز تعدادی از توکن‌هایERC ۲۰ را موقتا بستند. این مشکل، همان مشکل کلاسیک سرریزی نوع داده‌ای integer است که هکرها از طریق آن می‌توانند مقداری زیادی توکن بدست آورند.

ERC-223

توکن های ERC-20 با دو روش می توانند تراکنش انجام دهند:

۱. تابعtransfer
۲. مکانیزمapprove + transferFrom

موجودی توکن یک متغیر در قرارداد هوشمند یک توکن است. تراکنش های یک توکن متغیرهای داخلی یک قرارداد را تغییر می‌دهند. در زمان اجرای یک تراکنش موجودی فرستنده کم شده و موجودی گیرنده افزایش می‌یابد.

در استاندارد-ERC ۲۰ امکان اطلاع از اجرای یک تراکنش برای گیرنده وجود ندارد. اگر شما بخواهید یک مقدار توکن را برای یک قرارداد ارسال کنید، باید ابتدا با استفاده از تابع approve به قرارداد مربوطه اجازه برداشت از آدرس خودتان را بدهید و بعدا با صدا زدن آن قرارداد که transferFrom را صدا می‌زند، توکن ها را برداشت کنید .حال اگر از تابع transfer استفاده کنید و توکن ها را به آدرس یک قرارداد ارسال کنید، قرارداد گیرنده، تراکنش را تشخیص نمی‌دهد. امکان شناسایی و رسیدگی به تراکنش های ورودی-ERC ۲۰ برای هیچ کدام از قراردادها وجود ندارد و در صورت ارسال توکن به آنها، توکن ها داخل قرارداد گیر می‌افتد و پول شما از دست می‌رود. در اصل چنین تراکنش هایی باید پیش از اجرا رد شوند.

همان طور که گفته شد، تابع transfer پس از اتمام تراکنش به گیرنده اطلاع نمی‌دهد. یعنی گیرنده نمی‌تواند تراکنش ورودی را تشخیص دهد. بنابراین اگر گیرنده یک قرارداد باشد کاربر باید از مکانیزم approve + transferFrom استفاده کند و اگر گیرنده یک آدرس دیگر باشد، کاربر باید از تابع transfer استفاده کند.

استاندارد-ERC ۲۲۳ مشابه استاندارد-ERC ۲۰ است و این مشکل را حل کرده است. در زمان ارسال توکن به یک قرارداد هوشمند دیگر تابع tokenFallbackاز آن قرارداد فراخوانی می‌شود. این تابع به قرارداد گیرنده اجازه می‌دهد تا توکن های دریافتی را نپذیرد و یا اقدامات دیگری انجام دهد. این تابع می‌تواند به عنوان جایگزینی برای تابع approve به کار برود.

ERC-621

این استاندارد توسعه ای روی استاندارد-ERC ۲۰ است. دو تابع increaseSupply و decreaseSupply به این استاندارد اضافه شده است . با استفاده از این توابع می‌توان میزان کل توکن های در حال گردش را کاهش یا افزایش داد. در استاندارد-ERC ۲۰ تنها یکبار امکان مشخص کردن کل عرضه توکن، در زمان تولید توکن ها وجود دارد.

ERC-721

ERC-721زمانی که CryptoKitties در سال ۲۰۱۷ میلادی به محبوبیت رسید (بر پایه‌ی پلتفرم اتریوم)، در دنیای ارزهای دیجیتال به شهرت رسید .اما ارزش ERC-721 بسیار بالاتر از یک بازی است.

استاندارد جهانی ERC-721 که بر روی قراردادهای هوشمند کار می کند، به یک رویداد واقعی و نقطه‌ی عطفی در دنیای ارزهای دیجیتال تبدیل شده است .در حال حاضر، توکن‌های ERC-20 از ۹۵ ICOs %استفاده می کنند زیرا ICOs باعث سازگاری ارزهای دیجیتال با یکدیگر و خدمات شخص ثالث مانند صرافی‌ها می شوند .با این شرایط، همانطور که گفته شد انواع مختلفی از توکن‌ها وجود دارند .یکی از ویژگی‌های اصلی و متفاوت توکن ERC-721 با توکن معمولی ERC-20 این است که توکن‌های ERC-721 فانگیبل یا قابل جایگزینی با یکدیگر (fungible)نیستند .در نهایت این ویژگی، طیف وسیعی از پیاده سازی‌های پنهانی را تعیین می کند .بدیهی است که توکن‌های منحصر به فرد برای دیجیتالی کردن دارایی‌های منحصر به فرد، مناسب بوده و در نتیجه جایگزین مناسبی هستند .همچنین باید به این نکته اشاره کرد که بخش بزرگی از توابع توکن ERC-721 بسیار شبیه به توابع توکن ERC020 است .به علت این که بتوان از این توکن‌ها روزانه استفاده کرد، آن‌ها را در کیف پول‌های معمولی ذخیره و در صرافی‌ها ترید کرد؛ این پیوستگی و اتصال بین این دو توکن لازم و ضروری است .اما ویژگی‌های منحصر به فرد نیاز به معرفی توابع جدید، برای قراردادهای هوشمند دارند .از آنجایی که هر توکن منحصر به فرد است، بنابراین لازم است که مالکیت یک توکن خاص را در یک بلاک کنترل و ضبط کرد و حرکات آن را ردیابی کرد .به همین علت است که توابع takeOwnership ظاهر شده‌اند.

زمانی که یک کاربر یا شخصی توکن ERC-20 خریداری می کند، حقوق مالکیت آن فرد، در قراردادهای هوشمند نوشته می شود (این قرارداد حاوی اطلاعاتی است که چند توکن برای هر آدرس وجود دارد) .این توکن می تواند با توکن‌های دیگری نیز که ویژگی‌های یکسانی دارند، جابه جا شوند .اما ارزش توکن ERC-721 مانند توکن‌های دیگر نیست و نمی توان آن را با توکن‌های دیگر جایگزین کرد، به این دلیل که توکن‌های ERC-721منحصر به فرد بوده و فانگیبل نیستند .بنابراین تنها اضافه کردن یک آدرس به قراردادهای هوشمند در توکن‌های ERC-721 کافی نیست .هر توکن منحصر به فرد بوده و باید اطلاعاتی در مورد هر توکنی که ترید می شود، داشت .همچنین، مالکیت استاندارد ERC-721 به وسیله‌ی لیستی از توکن‌ها تعیین می شود.

یکی از بهترین پروژه‌های اکوسیستم اتریوم، پروتکل ۰ xاست که اساس آن، اضافه کردن پشتیبانی‌های لازم برای توکن‌های ERC-721 و استانداردهای توکن‌های جدید است .بنابراین، ERC-721توکن و استاندارد رایج اتریوم است که از آن در پلتفرم غیرمتمرکز اتریوم استفاده می شود و با دیگر توکن‌ها و استانداردهای پلتفرم غیرمتمرکز اتریوم تفاوت دارد.

ERC-115

یکی از بنیان گذاران شرکت enjin coin ملقب به CTO که توکن ERC-1155 را توسعه داده است اعلام کرده است که این توکن برای بهبود بازی های ویدیویی بر پایه بلاک چین اتریوم ایجاد گردیده است . یک سال پیش زمانی که توکن ERC-721 ب طور گسترده ای برای استاندارد بازی های مبتنی بر بلاک چین مطرح گردید چندین دی آپ به استفاده از این توکن روی آورده اند اما این توکن با محدودیت هایی روبرو شد . یکی از این ایرادات غیر قابل تعویض بودن توکن ها می باشد و جوابگوی گستردگی صنعت بازی سازی نمی باشد.

اما توکن ERC-1155 به هیچ وجه به صنعت بازی سازی محدود نمی گردد و می تواند مالکیت انواع اقلام فیزیکی و ارزهای دیجیتالی را پشتیبانی کند . در گذشته توکن های شخصی با قراردادهای تکی تعریف می شدند . علاوه بر این مبادله چند آیتم بین بازیکنان به چهار مرحاه جداگانه نیاز داشت زیرا بلاک چین اتریوم هر مبادله را به صورت جداگانه پردازش می کند ERC-1155 . با دسته بندی کردن آیتم ها می تواند زمان مبادله را کاهش دهد و چهار مرحله را به دو مرحله تبدیل کند و کارمزد تراکنش ها را در بلاک چین اتریوم نیز کاهش دهد.

قبل از توکن ERC-721 از توکن ERC20 در بازی ها استفاده می شود و هیچ گاه تصور نمی شد که این توکن ها روزی به عنوان یک ارز مورد استفاده قرار بگیرند . یکسان بودن توکن ها و نداشتن اطلاعات هویت و تاریخ و ... مشکلاتی را رقم می زد ERC-721 . این امکان را فراهم آورد که هر کس توکن منحصر به فرد خود را ایجاد کند.

ERC-1155با گرد هم آوری قابلیت های ERC20 و ERC-1155 امکانی را فراهم آورد که بازی سازها بتوانند توکن های منحصر به فردی ایجاد کنند که قابلیت تکرار را نخواهند داشت.

شرکت enjin که در سال ۲۰۰۹ تاسیس شده است دارای دو محصول enjin coin و enjin network می باشد که برای بازی های مبتنی بر بلاکچین و ارز دیجیتالارائه کرده است . شرکت enjin در حالی ک دومین شرکت در این زمینه می باشد توانسته است ۲۰ میلیون کاربر را در اختیار بگیرد.

مفاهیم کاربردی

رمزنگاری Cryptography

کریپتوگرافی روش محافظت از اطلاعات و ارتباطات از طریق استفاده از کدهای مربوطه است. بنابراین، این اطلاعات تنها برای کسانی قابل خواندن و پردازش است که از قبل، تعیین شده باشد. پیشوند "کریپتو" به معنای مخفی و پسوند "گرافی" به معنای نوشتن است. در علم کامپیوتر، کریپتوگرافی به تکنیک‌های اطلاعات امن و ارتباطی حاصل از مفاهیم ریاضی و مجموعه‌ای از محاسبات مبنی بر قاعده به نام الگوریتم اشاره دارد و تبدیل پیام‌های آن به گونه‌ای است که رمزگشایی آن‌ها بسیار سخت است. از الگوریتم‌ها برای تولید کلید کریپتوگرافیک، امضای دیجیتال، محافظت از حریم خصوصی داده‌ها، مرور وب در اینترنت و ارتباطات محرمانه مانند معاملات کارت اعتباری و ایمیل استفاده می شود.

تکنیک های کریپتوگرافی

کریپتوگرافی با کریپتولوژی و کریپت آنالیز مرتبط است. همچنین شامل تکنیک‌هایی مانندmicrodots ، ادغام کلمات با تصاویر و راه‌های دیگر برای مخفی کردن اطلاعات به منظور ذخیره سازی و عبور است. با این حال، در دنیای امروزی، کریپتوگرافی اغلب با مفاهیم plaintext (clear text, ordinary text)، ciphertext(رمزگذاری) و رمزگشایی همراه بوده و به جلو می رود. افرادی که چنین اقداماتی انجام می دهند به عنوان "کریپتوگرافرز" شناخته می شوند.

کریپتوگرافی‌های جدید چهار معیار را دنبال می کنند: محرمانه بودن، تمامیت (درستی)، عدم تخلف و احراز هویت. روش‌ها و پروتکل‌هایی که با تمام یا برخی از معیارهای بالا مرتبط باشند، به عنوان "کریپتوسیستم" شناخته می شوند. اغلب به نظر می رسد که کریپتوسیستم‌ها تنها به روش‌های ریاضی و برنامه‌های کامپیوتری مرتبط می شوند اما با این حال آن‌ها شامل تنظیم رفتار انسان مانند انتخاب کلمات سخت عبور، ورود به سیستم‌های استفاده نشده و ... نیز می شوند.

الگوریتم های کریپتوگرافی

کریپتوسیستم از مجموعه‌ای از روش‌های شناخته شده‌ای به عنوان الگوریتم‌های کریپتوگرافیک یا رمز استفاده می کند، تا پیام‌ها را برای ایمن سازی ارتباطات بین سیستم‌های کامپیوتری، دستگاه‌های هوشمند و برنامه‌های کاربردی، رمزگشایی کند. گروهی از رمزها، از یک الگوریتم خاص برای رمزگذاری، از گروه دیگر برای احراز هویت و از گروهی دیگری هم به عنوان کلید مبادلات، استفاده می کنند. این فرآیند که در پروتکل‌ها قرارداده می شوند و در نرم افزارها نوشته شده و بر روی سیستم عامل‌ها و سیستم‌های کامپیوتری اجرا می شوند؛ شامل تولید کلیدهای عمومی و خصوصی برای رمزگذاری/رمزگشایی داده‌ها، امضای دیجیتالی و تایید برای احراز هویت پیام‌ها است.

انواع کریپتوگرافی

الگوریتم‌های رمزگذاری Symmetric-Key یاSingle-Key ، طول ثابتی از بیت‌ها را به عنوان رمز بلاک با کلید مخفی‌ای ایجاد می کنند که سازنده یا فرستنده برای رمزگذاری اطلاعات و گیرنده برای رمزگشایی اطلاعات، از آن‌ها استفاده می کنند.

Advanced Encryption StandardsیاAES یک نوع الگوریتم رمزگذاری Symmetric-Key است. AESدر ماه نوامبر سال ۲۰۰۱ به منظور حفاظت از اطلاعات حساس و مهم، توسط موسسه ملی استاندارد و فناوری به عنوان استاندارد پردازش اطلاعات فدرال، تاسیس شد. این استانداردها توسط دولت ایالات متحده آمریکا تعیین شده و به طور گسترده‌ای در بخش خصوصی مورد استفاده قرار می گیرند. در ژوئن سال ۲۰۰۳، AESتوسط دولت ایالات متحده برای اطلاعات طبقه بندی شده، تایید شده است. همچنین AES جانشین Data Encryption Standard) (DESو DES3 است. AESاز کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیتی برای جلوگیری از حملات سایبری استفاده می کند.

الگوریتم رمزگذاری دیگری به نام Asymmetric-Key یا Public-Kry هم وجود دارد. این الگوریتم از دو کلید استفاده می کند .یک کلید عمومی مرتبط با سازنده یا فرستنده برای رمزگذاری پیام‌ها و یک کلید خصوصی برای رمزگشایی اطلاعات.

انواع:Asymmetric-Key

- RSA : به طور گسترده‌ای بر روی اینترنت استفاده می شود.
- ECDSA : توسط بیت کوین استفاده می شود.

- DSA : به عنوان استانداردِ پردازشِ اطلاعتِ فدرال برای امضاهای دیجیتالی توسط NIST استفاده می شود.

توابع هش HASH function

یک تابع هش یک تابع ریاضی است که یک مقدار ورودی را به مقدار فشرده شده‌ی دیگر تبدیل می‌کند. ورودی تابع هش یک مقدار با طول نامعلوم است اما خروجی همیشه طول ثابتی دارد. توابع هش به شدت کاربردی هستند و تقریبا در همه کاربردهای امنیت اطلاعات حضور دارند .مقدار برگشت داده شده توسط یک تابع هش، یک (پیام خلاصه) یا به طور ساده (مقدار هش) نام دارد. شکل زیر یک تابع هش را نشان می‌دهد.

ویژگی‌های توابع هش

- طول ثابت خروجی (مقدار هش)
  - تابع هش، داده با طول متغیر را به طول ثابت تبدیل می‌کند.
  - معمولا اندازه هش بسیار کوچک‌تر از ورودی است، بنابراین توابع هش را گاهی با نام توابع فشرده‌ساز می‌شناسند.
  - تابع هش با خروجی n بیتی، را تابع هش-n بیتی می‌نامند.
- اثربخشی فرآیند
  - به طور کلی برای هر تابع هش h با ورودیx ، محاسبه(h(x ، یک عملیات سریع است.
  - انجام محاسبات در توابع هش بسیار سریعتر از رمزنگاری متقارن هستند.

شرایط توابع هش

- شرط اول
  - این شرط بیان می‌کند که تابع هش باید یک تابع یکطرفه باشد.
  - به بیان دیگر اگر یک تابع هش h یک مقدار هش z را تولید کرد، پیدا کردن یک مقدار x که هش آن با z یکی شود، بایستی فرآیند دشواری باشد.
  - این خاصیت باعث محافظت از پیدا کردن مقدار ورودی هش توسط حمله کننده‌ای می‌شود که مقدار هش را در اختیار دارد.
- شرط دوم
  - اگر یک ورودی و هش آن را در اختیار داشته باشیم، پیدا کردن یک ورودی متفاوت که همان مقدار هش را بدهد، بایستی دشوار باشد.
  - به بیان دیگر اگر یک تابع هش h برای یک ورودیx ، یک مقدار هش h(x) را بدهد، پیدا کردن مقدار ورودی دیگری که h(y) = h(x)شود، بایستی دشوار باشد.
  - این ویژگی باعث می‌شود در برابر حمله کننده‌ای که یک مقدار هش ورودی و هش آن را دارد و می‌خواهد یک مقدار متفاوت را به عنوان مقدار ورودی اصلی جایگزین آن کند، محافظت شود.
- شرط سوم

- پیدا کردن دو ورودی متفاوت با هر طولی که منجر به یک هش مشابه شود، بایستی دشوار باشد. این ویژگی با عنوان (تابع هش بدون تصادم) نیز شناخته می‌شود.
- به بیان دیگر برای یک تابع هش h ، پیدا کردن دو ورودی متفاوت x و y به طوری که h(x) = h(y) شود، باید دشوار باشد.
- چون تابع هش یک تابع فشرده ساز با خروجی ثابت است، نداشتن تصادم برای آن غیر ممکن است. این ویژگی تنها بیان می‌کند که پیدا کردن این تصادم‌ها باید بسیار سخت باشد.

کاربرد توابع هش

- ذخیره رمز عبور
  - توابع هش در زمان ذخیره‌سازی کلمات عبور، از آنها محافظت می‌کنند.
  - بجای ذخیره رمز عبور به صورت شفاف، تمام فرآیندهای لاگین کردن، تنها هش رمز عبور را در یک فایل ذخیره می‌کنند.
  - فایل پسورد شامل جفت‌هایی به شکل (id کاربر ، h(p)) است.
  - یک نفوذ کننده تنها می‌تواند هش پسوردها را ببیند. بنابراین نه می‌تواند توسط این هش‌ها وارد شود نه از طریق آن‌ها کلمه‌های عبور را بدست آورد. دلیل آن یکطرفه بودن تابع هش است.
- بررسی صحت داده

بررسی صحت داده یکی از کاربردهای بسیار رایج توابع هش می‌باشد که از آن برای تولید (چک‌سام‌ها) روی داده‌ی فایل‌ها استفاده می‌شود. این کاربرد به کاربر اطمینان می‌دهد که صحت داده تضمین شده است .این فرآیند بررس صحت، به کاربر کمک می‌کند تا هر تغییر انجام شده روی فایل اصلی را متوجه شود. هر چند تضمینی در مورد اصالت فایل نمی‌دهد. حمله کننده بجای تغییر داده، می‌تواند کل فایل را تغییر دهد و هش جدید را محاسبه کرده و به دریافت کننده بفرستد. این کاربرد بررسی صحت داده، تنها زمانی مفید است که کاربرد در مورد اصالت فایل مطمئن باشد.

طراحی الگوریتم های هشینگ

در مرکز هشینگ، تابع ریاضیاتی وجود دارد که بر روی دو بلاک داده با اندازه ثابت اعمال می شود تا یک کد هش شده را ایجاد کند. این تابع هش، بخشی از الگوریتم هشینگ را تشکیل می‌دهد. اندازه و حجم هر بلاک داده بر اساس الگوریتم، متغیر می‌باشد. معمولا اندازه هر بلاک از ۱۲۸ الی ۵۱۲ بیت است. شکل زیر تابع هش را نشان می‌دهد. الگوریتم هشینگ شامل چندین مرحله است که از توابع هش در آن استفاده می شود. در هر مرحله، ورودی با اندازه ثابت می‌گیرد و آن را با Message Block و خروجی مرحله قبل ترکیب می کند. این فرآیند تا جایی که نیاز باشد تکرار می‌شود تا کل پیام را هش کند. نمای کلی الگوریتم هشینگ در شکل زیر نشان داده شده است. در واقع مقدار هش اولین Message Blockتبدیل به ورودی دومین عملیات هش می‌شود، خروجی به دست آمده نیز برای سومین عملیات مورد استفاده قرار می‌گیرد و این روند ادامه پیدا می کند. به این فرآیند، اثر avalanche هشینگ می‌گویند.

نتیجه اثرavalanche ، مقادیر هش کاملا متفاوت برای دو پیام می باشد، حتی اگر فقط در یک بیت پیام ها تفاوت داشته باشند. الگوریتم و تابع هش با هم تفاوت دارند. تابع هش با اجرا بر روی دو بلاک داده باینری که طول ثابت دارند، یک کد هش تولید می‌کند. الگوریتم هشینگ فرآیندی برای استفاده از تابع هش می باشد. به طور مشخص چگونگی تجزیه پیام و نحوه ترکیب شدن با نتایج Message Block های قبلی را الگوریتم هشینگ می گویند.

توابع هش پرکاربرد

- خلاصه پیام(Message Digest)

الگوریتمMD ۵ تا چندین سال محبوب ترین و پر استفاده ترین تابع هش بود .خانواده MD شامل توابع هشMD ۲، MD۴ ، MD۵ وMD ۶ می باشد که به تصویب استاندارد اینترنت RFC ۱۳۲۱ رسیدند. این توابع هش از سری توابع با طول ۱۲۸ بیت می باشند .تابعMD ۵ به طور گسترده در نرم افزارها استفاده می شد تا یکپارچگی فایل منتقل شده را تضمین کند. برای مثال، سرورها معمولا یک عدد با نام checksum قبل از ارسال فایل محاسبه می کنند. کاربر فایل را از سرور دریافت کرده و checksum ها را مقایسه می کند، اگر مطابقت داشتند، صحت فایل تضمین شده است .در سال ۲۰۰۴، درMD ۵ نواقصی پیدا شد. این گزارش در مورد آنالیز یک حمله بود که توانست در مدت زمان یک ساعت از این نواقص استفاده کند. همین امر باعث شد که استفاده از این تابع هش توصیه نشود.

- تابع هش ایمن(SHA)

خانواده SHA شامل چهار الگوریتم می باشد که عبارتند از-SHA : ۰-SHA, ۱-SHA, ۲-SHA, ۳ .اگرچه این چهار الگوریتم از یک‌خانواده می باشند ، اما از نظر ساختاری متفاوت می باشند.

- نسخه اصلی، -SHA۰ می باشد که یک تابع هش ۱۶۰ بیت است و توسط موسسه ملی استانداردها و تکنولوژی (NIST) در سال ۱۹۹۳ منتشر شد. این الگوریتم ضعف هایی داشت و نتوانست محبوبیت زیادی کسب کند. در سال ۱۹۹۵، -SHA۱برای اصلاح ضعف های-SHA ۰ طراحی شد.
- الگوریتم-SHA ۱ پرکاربردترین تابع هش SHA می باشد. از این الگوریتم در برنامه ها و پروتکل های بسیار زیادی نظیر SSL مورد استفاده قرار گرفت .در سال ۲۰۰۵ ، روشی برای نشان دادن نواقص-SHA ۱ در دوره های زمان یافت شد و باعث شد استفاده بلند مدت از-SHA ۱ با شک و ابهام رو به رو شود.
- خانواده-SHA ۲ بر اساس تعداد بیت در مقدار هش آن ها به چهار عضو تقسیم می شود که عبارتند از-SHA : ۲۲۴ -SHA, ۲۵۶ , -SHA۳۸۴SHA, ۵۱۲ .تاکنون حمله موفقیت آمیزی به تابع هش-SHA ۲ گزارش نشده است. اگرچه-SHA ۲ یک تابع هش قوی است و تفاوت چشمگیری با-SHA ۱ دارد، با این حال طرح اصلی آن هم چنان مشابه-SHA ۱ می باشد. بنابراین NIST در صدد طراحی تابع هش رقابتی جدیدی برآمد.
- در اکتبر ۲۰۱۲، NISTالگوریتم Keccak را به عنوان استاندارد-SHA ۳ انتخاب کرد Keccak .دارای مزایای بسیاری نظیر عملکرد موثر و مقاوم خوب در برابر حمله ها می باشد.

- ریپمد(RIPEMD)

ریپمد مخفف RACE Integrity Primitives Evaluation Message Digest می باشد. این مجموعه توابع هش توسط جامعه تحقیقاتی آزاد طراحی شده است و عموما به اسم خانواده توابع هش اروپایی شناخته می شود.

این مجموعه شاملRIPEMD ، -RIPEMD۱۲۸ و-RIPMED ۱۶۰ می باشد. هم چنین نسخه های ۲۵۶ و ۳۲۰ بیت این الگوریتم نیز موجود می باشد.

ریپمد اصلی که ۱۲۸ بیت است بر اساس اصولMD ۴ می باشد و برای ارائه امنیت موارد مشکوک ایجاد شده است. ریپمد ۱۲۸ بیت به عنوان یک جایگزین برای از بین بردن آسیب پذیری های ریپمد اصلی منتشر شده است.

ریپمد-۱۶۰ نسخه بهبود یافته و پر استفاده این خانواده می باشد. در نسخه های ۲۵۶ و ۳۲۰ بیت ، احتمال وجود اختلال کاهش یافته است اما در مقایسه با ریپمد- ۱۶۰ و ۱۲۸ بیت از سطح امنیت بالاتری برخوردار نمی باشد.

- ویرل‌پول(Whirlpool)

ویرل‌پول یه تابع هش ۵۱۲ بیت می باشد. این تابع از تغییر در نسخه استاندارد رمزنگاری پیشرفته (AES) ایجاد شده است. یکی از طراحان این تابع وینسنت ریمن است که از موسسان AES می باشد.

سه نسخه از ویرل‌پول منتشر شده است که عبارتند از-WHIRLPOOL : WHIRLPOOL۰, WHIRLPOOL-T ,

امضای دیجیتال

نوعی رمزنگاری نامتقارن است. هنگامی که پیغامی از کانالی ناامن ارسال می‌شود، یک امضای دیجیتال که به شکل صحیح به انجام رسیده باشد می‌تواند برای شخص گیرنده پیام دلیلی باشد تا ادعای شخص فرستنده را باور کند یا به عبارت بهتر شخص گیرنده از طریق امضای دیجیتال می‌تواند این اطمینان را حاصل کند که همان شخص فرستنده نامه را امضا کرده‌است و نامه جعلی نیست. امضاهای دیجیتال در بسیاری از جنبه‌ها مشابه امضاهای سنتی دستی هستند؛ انجام امضاهای دیجیتال به شکل صحیح بسیار مشکلتر از یک امضای دستی است. طرح‌ها فایل امضای دیجیتال بر مبنای رمزنگاری نامتقارن هستند و می‌بایست به شکل صحیح صورت گیرد تا مؤثر واقع شود. همچنین امضاهای دیجیتال می‌توانند امضاهایی غیرقابل انکار را ایجاد کنند به این معنی که شخص امضاکننده نمی‌تواند تا زمانی که کلید شخصی فرد به صورت مخفی باقی‌مانده‌است، ادعا کند که من این نامه که امضای من را به همراه دارد، امضا نکرده‌ام؛ ولی در زمانی که کلید شخصی فرد در شبکه از حالت مخفی خارج شود یا زمان اعتبار امضای او به اتمام برسد شخص می‌تواند امضای دیجیتال خود را انکار کند هرچند که در این حالت نیز با وجود ساختار قوی امضای دیجیتال، این امضا اعتبار خود را حفظ می‌کند. پیغام‌های امضا شده با امضای دیجیتال امکان ارائه به صورت یک رشته بیتی را دارند. مانند :پست الکترونیک، قراردادها یا پیام‌هایی که از طریق قواعد رمزنگاری‌های دیگر ارسال شده باشند.

امضاهای دیجیتال اغلب برای به انجام رساندن امضاهای الکترونیکی به کار می‌روند. در تعدادی از کشورها، مانند آمریکا و کشورهای اتحادیه اروپا، امضاهای الکترونیکی قوانین مخصوص به خود را دارند. هرچند، قوانین دربارهٔ امضاهای الکترونیکی همواره روشن نمی‌سازند که آیا امضاهای دیجیتال به درستی به کار گرفته شده‌اند یا اهمیت آن‌ها به چه میزان است. در حالت کلی قوانین به شکل واضح در اختیار کاربران قرار نمی‌گیرد و گاهی آنان را به گمراهی می‌کشاند.

مشخصات امضا دیجیتال

طرح امضای دیجیتال معمولاً سه الگوریتم را شامل می‌شود: ۱- الگوریتم تولید کلید را که کلید خصوصی را بطور یکسان و تصادفی از مجموعه کلیدهای ممکن انتخاب می‌کند. خروجی‌های این الگوریتم کلید خصوصی و کلید عمومی مطابق با آن است. ۲- الگوریتم امضا که توسط آن با استفاده از کلید خصوصی و پیام، امضا شکل می‌گیرد. ۳-الگوریتمی که با استفاده از پیام دریافتی و کلید عمومی صحت امضا را بررسی می‌کند و با مطابقتی که انجام می‌دهد یا امضا را می‌پذیرد یا آن را رد می‌کند.

دو ویژگی اصلی که در امضای دیجیتال مورد نیاز است: اول، امضای تولید شده از پیام مشخص و ثابت هنگامی که توسط کلید عمومی مورد بررسی قرار می‌گیرد فقط در مورد همان پیام ارسالی می‌تواند عمل تطبیق را صورت دهد و در مورد هر پیام متفاوت و خاص می‌باشد. ثانیاً، امضای دیجیتال می‌بایست قابلیت اجرا توسط الگوریتم را داشته باشد و بتواند فایل امضای معتبر برای مهمانی که کلید خصوصی را دارا نمی‌باشد ایجاد نماید.

تاریخچه بر اساس اسناد معتبر (دیدگاه‌های جدید در رمزنگاری) در سال ۱۹۷۶ توسط ویتفید دیفای و مارتین هیلمن برای تشریح ایده‌های اولیه طرح فایل امضای دیجیتال ارائه شد. البته به نظر می‌رسد طرح‌های اولیه دیگری نیز در آن زمان وجود داشته‌است. مدت کوتاهی پس از آن جمع دیگری از محققین به نام‌های ریوست، شمیر و آدلمن، الگوریتم آر اس اِی را ابداع کردند که می‌توانست برای تولید امضای دیجیتال اولیه به کار رود. اول بسته نرم‌افزاری امضای دیجیتال با عنوان لوتوس نت در سال ۱۹۸۹ بر مبنای همین الگوریتم به بازار عرضه شد.

در سال ۱۹۸۴ میشلی، گلدواسر و ریوست با تمام دقت موارد مورد نیاز را برای برقراری امنیت در طرح امضای دیجیتال بررسی کردند. آن‌ها با بررسی مدل‌های مختلف حمله برای امضای دیجیتال توانستند طرح فایل امضای دیجیتال جی ام آر را ارائه کنند که می‌تواند در مقابل حمله به پیام و جعلی بودن آن مقاومت کند.

طرح‌های ابتدایی امضای دیجیتال مشابه همدیگر بودند: آن‌ها از جایگشت (تبدیل) دریچه‌ای استفاده می‌کردند، مانند تابع آر اس اِی یا در برخی موارد از طرح امضای رابین بهره می‌گرفتند. جایگشت دریچه‌ای نوعی از مجموعه جایگشت هاست که به وسیله پارامترها مشخص می‌شود که در محاسبه‌های رو به جلو سریع عمل می‌کند ولی در محاسبه‌های بازگشتی با مشکل مواجه می‌شود. با این وجود برای هر پارامتر یک دریچه وجود دارد که حتی محاسبه‌های بازگشتی را آسان می‌کند. جایگشت‌های دریچه‌ای می‌توانند مانند سیستم‌های رمزگذاری با کلید عمومی باشند. در جایی که پارامتر به عنوان کلید عمومی و جایگشت دریچه‌ای به عنوان کلید پنهان است رمزگذاری مانند محاسبه جایگشت

در جهت رو به جلوست و رمز گشایی مانند محاسبه در جهت معکوس است. همچنین جایگشت‌های دریچه‌ای می‌توانند مانند طرح فایل امضا دیجیتال باشند، به این صورت که محاسبه در جهت معکوس با کلید پنهان مانند امضا کردن است و محاسبه در جهت پیش رو مانند بررسی صحت امضاست. به دلیل این همخوانی امضاهای دیجیتال اغلب بر پایه سامانه رمزنگاری با کلید عمومی تشریح می‌شوند اما این تنها روش پیاده‌سازی امضای دیجیتال نیست.

ولی این نوع طرح امضای دیجیتال در برابر حملات آسیب‌پذیر است و شخص مهاجم می‌تواند با دست کاری در روش بررسی صحت امضا، یک امضای دیجیتال جعلی برای خود ساخته و شبکه را با مشکل مواجه سازد. هرچند این نوع امضا به شکل مستقیم به کار گرفته نمی‌شود ولی ترجیحاً ابتدا پیام را با استفاده از روش‌های درهم سازی خلاصه می‌کنند و سپس خلاصه پیام را امضا می‌کنند و در نتیجه با استفاده از همین ترفند، شخص مهاجم فقط می‌تواند یک امضای دیجیتال جعلی برای خود درست کند که این امضا با محتویات مربوط به خروجی تابع درهم سازی از پیام خلاصه شده تطابق ندارد و شخص مهاجم نمی‌تواند به محتویات پیام خدشه‌ای وارد کند.

همچنین دلایل متنوعی وجود دارد تا افرادی که می‌خواهند از امضای دیجیتال استفاده کنند از خلاصه پیام و خروجی تابع درهم‌سازی برای امضا استفاده کنند. اولین دلیل ایجاد بازدهی مناسب برای طرح امضای دیجیتال است زیرا فایل امضا خیلی کوتاهتر خواهد بود و در نتیجه زمان کمتری صرف می‌شود. دومین دلیل برای سازگاری بیشتر است زیرا با استفاده از تابع درهم‌سازی شما می‌توانید خروجی مطابق با نوع الگوریتمی که به کار گرفته‌اید داشته باشید. سومین دلیل برای درستی اجرای امضای دیجیتال است: بدون استفاده از تابع درهم‌سازی ممکن است پیام شما در هنگام امضا به دلیل مشکل فضا به بخش‌های مختلف تقسیم شود و شخص دریافت‌کننده نتواند به درستی منظور فرستنده را دریافت کند بنابراین از این تابع استفاده می‌کند تا خود پیام را به شکل خلاصه و بدون ایجاد مشکل ارسال کند.

نظریه‌های امنیتی در تحقیقات میشلی، گلدواسر و ریوست مراتب متفاوت حمله به امضاهای دیجیتال را برای ایجاد دیوار دفاعی مناسب بررسی کردند و نتایج زیر به دست آمد:

۱. در حمله کلید یگانه، مهاجم فقط روند بررسی و تأیید کلید عمومی را بدست می‌آورد و از این طریق سامانه را مورد تهاجم قرار می‌دهد.

۲. در حمله با پیام آشکار، مهاجم یک کلید کارآمد برای مجموعه‌ای از پیام‌های آشکار و مشخص در اختیار دارد و فقط با استفاده از پیام مشخص می‌تواند حمله کند و توانایی انتخاب پیام برای مورد حمله قرار دادن نخواهد داشت.

۳. در انطباق پیام انتخاب شده، مهاجم ابتدا امضا را بر روی یک پیام دلخواه که مورد انتخاب مهاجم است یادمی‌گیرد و از آن امضا استفاده می‌کند.

در ادامه مراحل نتایج حمله به سامانه امضای دیجیتال از طریق روش‌های مذکور مطرح می‌شود:

۱. در مرحله اول امکان ترمیم و استفاده مجدد از امضای دیجیتال را از بین خواهد برد.

۲. توانایی جعل امضا در یک سطح گسترده از دیگر نتایج حمله به امضای دیجیتال است. در این مرحله شخص مهاجم توانایی جعل امضا برای هر پیامی را به دست خواهدآورد.

۳. جعل در مورد پیام‌های انتخابی؛ در این مورد مهاجم می‌تواند جعل امضا را در مورد پیام انتخابی خود انجام دهد.

۴. در این مورد از نتایج حمله به امضای دیجیتال شخص مهاجم فقط می‌تواند از طریق امضای در دسترس خود و برخی پیام‌ها به محتویات آن‌ها دست پیدا کند و دیگر شخص مهاجم توانایی انتخاب ندارد و انتخاب‌های او محدود می‌شود.

معایب امضای دیجیتال

با وجود تمام مزایایی که امضای دیجیتال دارد و در ادامه همین مقاله به بررسی آن می‌پردازیم ولی این طرح همچنان در حل برخی مشکلات که در ادامه آن‌ها را مطرح می‌کنیم ناتوان است. الگوریتم و قوانین مربوط به آن نمی‌توانند تاریخ و زمان امضای یک سند را در ذیل آن درج کنند از همین جهت شخص دریافت‌کننده نمی‌تواند این اطمینان را حاصل کند که نامه واقعاً در چه تاریخ و زمانی به امضا رسیده‌است. ممکن

است در محتویات سند تاریخی درج شده باشد و با تاریخی که شخص نامه را امضا کرده باشد مطابقت نداشته باشد. البته برای حل این مشکل می‌توان از یک راه حل با عنوان زمان اعتماد به مهرو امضا استفاده کرد. همان‌طور که در ابتدای تعریف امضای دیجیتال اشاره شد این طرح غیرقابل انکار است و ساختار امضای دیجیتال بر همین اساس شکل گرفته‌است. همان‌طور که می‌دانید تکذیب در لغت به معنی انکار هرگونه مسئولیت نسبت به یک فعالیت است. هنگامی که پیامی ارسال می‌شود و فرستده آن را همراه امضا دریافت می‌کند در واقع این اطمینان در شخص دریافت‌کننده ایجاد می‌شود که نامه را چه کسی امضا کرده‌است و انکار امضا کاری مشکل به نظر می‌رسد. البته تا زمانی که کلید خصوصی به صورت مخفی باقی بماند شخص فرستنده نمی‌تواند چنین ادعایی داشته باشد ولی هنگامی که فایل امضای شخصی مورد حمله قرار بگیرد نه تنها خود فایل امضا اعتبار لازم را از دست می‌دهد بلکه استفاده از زمان اعتبار مهر و امضا نیز دیگر کاربردی نخواهد داشت. البته یادآوری این نکته لازم است هنگامی که شما در سامانه خود از کلید عمومی بهره می‌گیرد دیگر نمی‌توانید امضای خود را انکار کنید و در صورتی این موضوع امکان‌پذیر است که کل شبکه مورد حمله واقع شود و سامانه از اعتبار لازم ساقط شود. بنا براین توجه به انتخاب یک راه حل درست برای پیاده‌سازی طرح امضای دیجیتال از اهمیت ویژه‌ای برخوردار است و همان‌طور که عنوان شد ممکن است با یک مشکل کل اعتبار مجموعه زیر سؤال برود. مطابق اصول فنی امضای دیجیتال که در توضیح‌های ابتدایی آورده شده‌است، فایل امضای دیجیتال رشته‌ای از بیت‌ها را در اجرای این طرح به کار می‌برد. در واقع افراد در این طرح مجموعه‌ای از بیت‌ها را که ترجمه پیام است امضا می‌کنندآن آن‌ها ترجمه معنایی آن‌ها ذره‌ها امضا می‌کنند. مشکل دیگر امضای دیجیتال این است که چون پیام توسط یک تابع مشخص به مجموعه‌ای از بیت‌ها ترجمه و پردازش می‌شود ممکن است در طی مرحله انتقال و دریافت پیام ترجمه پیام دچار خدشه شود و مفهوم دیگری به خود گیرد. برای حل این مشکل از روشی با عنوان دبلیو وای اس آی دبلیو وای اس استفاده می‌شود به این معنا که همان چیزی که مشاهده می‌شود امضا می‌شود. در این روش همان اطلاعات ترجمه شده خود را بدون آن که اطلاعات مخفی دیگری در آن قرار گیرد امضا می‌کند و پس از امضا و تأیید اطلاعات از سوی شخص فرستنده درون سامانه به کار گرفته می‌شود. در واقع این روش ضمانت نامه محکمی برای امضای دیجیتال به‌شمار می‌رود و در سیستم‌های رایانه‌ای مدرن قابلیت پیاده‌سازی و اجرا را خواهد داشت.

مزایای امضای دیجیتال

حال در این بخش مزایای استفاده از امضای دیجیتال را مورد بررسی قرار خواهیم داد. یکی از دلایل به‌کارگیری امضاهای دیجیتالی که یک دلیل عادی به‌شمار می‌رود ایجاد اعتبار برای امضاها در یک سامانه تبادل داده و اطلاعات است. در واقع استفاده از امضای دیجیتال سندیت و اعتبار ویژه‌ای به یک سند می‌بخشند. وقتی که هر فرد دارای یک کلید خصوصی در این سامانه است با استفاده از آن می‌تواند سند را امضا کرده و به آن ارزش و اعتبار داده و سپس آن را ارسال کند. اهمیت ایجاد اطمینان قطعی و محکم برای شخص دریافت‌کننده پیام دربارهٔ صحت ادعای فرستنده در برخی از انواع انتقال اطلاعات مانند داده‌های مالی به خوبی خود را نشان می‌دهد و اهمیت وجود امضای دیجیتال درست را بیش از پیش به نمایش می‌گذارد. به عنوان مثال تصورکنید شعبه‌ای از یک بانک قصد دارد دستوری را به دفتر مرکزی بانک به منظور درخواست ایجاد تعادل در حساب‌های خود را ارسال کند. اگر شخص دریافت‌کننده در دفتر مرکزی متقاعد نشود که این پیام، یک پیام صادقانه است و از سوی یک منبع مجاز ارسال شده‌است طبق درخواست عمل نکرده و در نتیجه مشکلاتی را به وجود می‌آورد. در موارد بسیار زیادی، فرستنده و گیرنده پیام نیاز دارند این اطمینان را به دست بیاورند که پیام در مدت ارسال بدون تغییر باقی‌مانده‌است. هرچند رمزنگاری محتوای پیام را مخفی می‌کند ولی ممکن است امضا در یک سامانه از اعتبار ساقط شود و محتویات یک پیام دست‌خوش تغییرات گردد؛ ولی استفاده از امضای دیجیتال به عنوان روشی از رمز نگاری می‌تواند ضامن درستی و بی نقصی یک پیام در طی عملیات انتقال اطلاعات باشد زیرا همان‌طور که در ساختار اجرایی شدن الگوریتم مشاهده کردید از تابع درهم‌سازی بهره گرفته شده‌است و همین نکته ضمانت بهتری را برای درستی و صحت یک پیام ایجاد می‌نماید.

کلید عمومی رمزنگاری

رمزنگاری با استفاده از کلید عمومی روشی است برای ایجاد یک ارتباط پنهان میان دو شخص بدون اینکه نیازی به تعویض کلیدهای خصوصی باشد. همچنین با استفاده از این روش می‌توان امضاهای دیجیتال را ایجاد کرد .رمزنگاری کلید عمومی اساس و بنیاد تبادل اطلاعات در تکنولوژی‌های امروز در جهان گسترده اینترنت است. همچنین این روش به عنوان رمزنگاری نامتقارن نیز مطرح است زیرا کلیدی که برای رمزنگاری به کار می‌رود با کلیدی که برای رمز گشایی به کار می‌رود متفاوت است. در رمزنگاری با کلید عمومی، هر کاربر یک جفت کلید برای رمزنگاری شامل یک کلید عمومی و یک کلید خصوصی است. کلید خصوصی به عنوان یک راز از سوی کاربر باید نگهداری شود و همه کاربران

امکان استفاده از کلید عمومی را دارند و در اختیار همه قرار می‌گیرد .از رمز نگاری نامتقارن هم برای رمزنگاری استفاده می‌شود هم برای رمز گشایی استفاده می‌شود. پیام‌هایی که با کلید عمومی رمزنگاری می‌شوند فقط با کلید خصوصی مطابق قابلیت رمزگشایی را دارند. هرچند که کلیدهای عمومی و خصوصی مطابق با یکدیگر هستند ولی با استفاده از کلید عمومی نمی‌توان کلید خصوصی را به دست آورد. در طرح رمزنگاری متقارن فرستنده و گیرنده باید با یک کلید مشترک اضافه باشند تا بتوانند عملیات رمزگشایی و رمز نگاری را انجام دهند و به همین دلیل این طرح قابلیت اجرایی شدن کمتری نسبت به روش نامتقارن دارند زیرا روش متقارن یک پهنای باند ویژه جهت تبادل کلید اضافی نیاز دارد به همین دلیل از کارایی مناسبی برخوردار نیستند .دو شاخه اصلی رمزنگاری با کلید عمومی عبارتند از: رمزگذاری کلیدی عمومی: پیامی که با کلید عمومی رمزگذاری شده باشد فقط به وسیله صاحب کلید خصوصی مطابق با آن رمزگشایی می‌شود و این موضوع به همکاری فرستنده و گیرنده بستگی دارد و می‌تواند اعتماد را تا اندازه زیادی در این سیستم تأمین کند و همکاری کرد. امضاهای دیجیتال: در مورد امضای دیجیتال پیام با استفاده از کلید خصوصی فرستنده رمزگذاری می‌شود و با استفاده از کلید عمومی فرستنده نیز رمزگشایی می‌شود. رمزنگاری کلید عمومی در مقایسه با صندوق پستی مانند صندوق پستی قفل شده همراه یک دریچه است که این دریچه در دسترس عموم قرار دارد به‌طور مثال اطلاعاتی از قبیل محل خیابان در اختیار عموم قرار می‌گیرد. هرکس با دانستن آدرس خیابان می‌تواند به درب مورد نظر مراجعه کرده و پیام مکتوب را از طریق دریچه می‌تواند ببیند ولی فقط شخصی که کلید باز کردن صندوق پستی را دارا می‌باشد می‌تواند پیام را بخواند. همچنین امضاهای دیجیتال شبیه پلمب یک پاکت نامه است که هرکس می‌تواند پاکت نامه را باز کند ولی پلمی فرستنده بر روی پاکت نامه به عنوان نشانی از فرستنده باقی خواهد ماند. مسئله اصلی برای استفاده از رمزنگاری عمومی ایجاد اطمینان در مسیر ارسال اطلاعات است. با توجه به مثال‌های ذکر شده باید کلید عمومی برای هر شخص به درستی تولید شود تا از سوی شخص سومی مورد تهاجم واقع نشود و سلامت سیستم حفظ شود. یک شیوه مرسوم برای رسیدگی به این مسئله استفاده از یک سازمان کلید عمومی است که بتواند در مورد شخص سومی که وارد سیستم می‌شود یک دسترسی متناسب تعریف کند. تمامی تکنیک‌های قابلیت اجرای سریعتر نسبت به اجرای سیستم کلید خصوصی را دارند و می‌توانند به اندازه کافی برای برنامه‌های متنوع کلید تولید کنند. در عمل اغلب رمز نگاری با کلید عمومی با سیستم کلید خصوصی به کار می‌رود تا بتواند بازدهی بیشتری داشته باشد. چنین ترکیب‌هایی را سیستم رمزنگاری دو رگه می‌نامند. برای رمزنگاری، فرستنده پیام با استفاده از الگوریتم تولید کلید به‌طور تصادفی یک کلید تولید می‌کند و با استفاده از آن کلید تصادفی عملیات رمزنگاری با کلید عمومی را انجام می‌دهد. برای امضاهای دیجیتالی، فرستنده پیام با استفاده از تابع درهم‌سازی پیام را خرد می‌کنند و پس از تأیید محتوای نامه، آن را امضا می‌کند. همچنین گیرنده با استفاده از تابع درهم‌سازی محاسباتی را انجام می‌دهد و کدی را به دست می‌آورد و این کد را با کد حاصل از اعمال تابع درهم‌سازی بر روی امضا، مقایسه می‌کند و بررسی می‌کند که آیا پیام مورد حمله قرار گرفته‌است یا خیر.

تولید کلید

تولید کلید روند تولید کلیدها برای رمز نگاری است. یک کلید رمزنگاری را انجام می‌دهد و یک کلید رمزگشایی می‌کند. سیستم‌های رمزنگاری جدید، سیستم رمزنگاری متقارن مانند الگوریتم‌های DES و AES و سیستم رمزنگاری با کلید عمومی مانند الگوریتم آر اس اِی را شامل می‌شوند. الگوریتم‌های متقارن از یک کلید به اشتراک گذاشته شده استفاده می‌کنند و الگوریتم‌های کلید عمومی از کلید عمومی و کلید خصوصی بهره می‌گیرند که کلید عمومی دسترسی عمومی دارد و وقتی فرستنده داده‌ها را با کلید عمومی رمزگذاری می‌کند، گیرنده تنها با داشتن کلید خصوصی می‌تواند داده‌ها را رمزگشایی کند.

پروتکل رمز نگاری

یک پروتکل امنیت (پروتکل رمزنگاری) یک مفهوم انتزاعی است و در واقع تضمینی برای امنیت سیستم به‌شمار می‌رود و امنیت سیستم رمزنگاری به برقراری این قواعد وابسته است. پروتکل تعیین می‌کند که الگوریتم‌ها چگونه می‌بایست به کار روند تا همراه با کارایی لازم، امنیت خود را نیز حفظ کنند. پروتکل‌ها به اندازه کافی و به صورت مفصل جزئیات را درباره ساختارهای داده‌ها و شکل استفاده از آن‌ها را تعیین می‌کنند. اجرای کامل و درست پروتکل می‌تواند این اطمینان را در کاربر ایجاد کند که امنیت سیستم تا میزان مورد نیاز تأمین می‌شود .پروتکل رمزنگاری معمولاً در ابتدایی‌ترین حالت موارد زیر را شامل می‌شوند: بررسی و تأیید صحت کلید؛ تعیین اعتبار موجود بودن کلید در سیستم؛ در مورد روش متقارن اعتبار لازم را به یک پیام می‌دهد؛ حفظ امنیت داده در سطح برنامه؛ روش‌هایی که اجازه نمی‌دهد کاربر امضای خود را تکذیب کند (ویژگی غیرقابل انکار بودن). به عنوان مثال؛ پروتکل امنیت لایه‌های حمل اطلاعات یک پروتکل رمزنگاری است که برای حفظ امنیت اتصالات در سطح وب را تأمین می‌کند. طرز کار این پروتکل بر مبنای سیستم X.۵۰۹ است که یک مرحله تولید کلید و با

استفاده از کلید عمومی و روش رمزنگاری با کلید عمومی داده‌ها را در سطح برنامه‌ها حمل می‌کند؛ ولی این پروتکل نمی‌تواند ویژگی غیرقابل انکار بودن رمزنگاری را تأمین کند. انواع دیگری از پروتکل‌های رمزنگاری وجود دارند که برخی از آن‌ها خود شامل چندین پروتکل مختلف دیگر می‌شوند امزوه تنوع گسترده‌ای در زمینه پروتکل‌ها به وجود آمده‌است و شرکت‌های مختلف برای رفع معایب امضای دیجیتال و ایجاد امنیت هر چه بیشتر در این ساختار تلاش هی چشمگیری انجام داده‌اند. به‌طور کلی، یک پروتکل رمزنگاری، مجموعه‌ای از قواعد و روابط ریاضی است که چگونگی ترکیب کردن الگوریتم‌های رمزنگاری و استفاده از آن‌ها به منظور ارائه یک سرویس رمزنگاری خاص در یک کاربرد خاص را فراهم می‌سازد. معمولاً یک پروتکل رمزنگاری مشخص می‌کند که اطلاعات موجود در چه قالبی باید قرار گیرند. چه روشی برای تبدیل اطلاعات به عناصر ریاضی باید اجرا شود. کدامیک از الگوریتم‌های رمزنگاری و با کدام پارامترها باید مورد استفاده قرار گیرند. روابط ریاضی چگونه به اطلاعات عددی اعمال شوند. چه اطلاعاتی باید بین طرف ارسال‌کننده و دریافت‌کننده رد و بدل شود. چه مکانیسم ارتباطی برای انتقال اطلاعات مورد نیاز است. — به عنوان مثال می‌توان به پروتکل تبادل کلید دیفی- هلمن برای ایجاد و تبادل کلید رمز مشترک بین دو طرف اشاره نمود.

حمله ۵۱ درصد Double spending

یکی از خطرناک‌ترین حملاتی که بلاکچین و رمز ارزها را تهدید می‌کند، حمله ۵۱ درصد یا حمله خرج دوباره (double spending) است. اگر با دنیای بلاکچین آشنا باشید حتما می‌دانید که با انجام این حمله می‌توانید کنترل شبکه را در دست بگیرید. حمله ۵۱ درصد یا حمله double spending مربوط به ماینر یا گروهی از ماینرهاست که سعی می‌کنند کریپتوهای خود را در بلاکچین دو بار خرج کنند. هدف از این حمله همیشه این نیست که کریپتوها را دوباره خرج نمایند، بلکه اغلب سعی می‌کنند با از بین بردن تمامیت بلاکچین اعتبار آن شبکه را از تحت‌الشعاع قرار دهند. بگذارید مثال ساده‌ای برای شما بزنیم. فرض کنید من ۱۰ بیت کوین برای خرید یک اتومبیل مصرف کرده‌ام. اتومبیل چند روز بعد به من تحویل داده می‌شود و بیت کوین‌ها نیز به شرکت فروشنده منتقل می‌گردد. با انجام حمله ۵۱ درصد در بلاکچین بیت کوین، می‌توانم انتقال این بیت کوین‌ها را معکوس کنم. اگر موفق شوم، هم اتومبیل و هم بیت کوین‌هایم را به دست می‌آورم، و در نتیجه دوباره می‌توانم از دارایی‌ام استفاده کنم. ایده حمله ۵۱ درصد شاید در دورنمای یک بلاکچین دموکراتیک واضح باشد، ولی سوء تفاهمی درباره‌ی نحوه‌ی کارکرد این حمله وجود دارد. این مقاله سعی دارد توضیح روشنی پیرامون چگونگی کارکرد حمله ۵۱ درصد ارائه کند. اگر هنوز نمی‌دانید ماینرها چطور تراکنش‌ها را به بلاکچین اضافه می‌کنند یا سازوکار بلاکچین چگونه است، بهتر است ابتدا اطلاعات خود را در این زمینه‌ها تکمیل کنید. بلاکچین = حاکمیت پیش از این که به خود حمله ۵۱ درصد بپردازیم، باید بدانیم که پروتکل‌های بلاکچین اساساً قالبی از حاکمیت هستند. بلاکچین بر دفتر کلی از اطلاعات، مثلا اطلاعات تراکنش‌ها، حکومت می‌کند. از آن‌جایی که پروتکل بلاکچین قادر است حاکمیت را برای ما انجام دهد، دیگر به نهادهای شخص ثالث، نظیر دولت‌ها یا بانک‌ها، نیازی نداریم. همین عامل است که باعث می‌شود بلاکچین‌ها غیرمتمرکز باشند. پروتکل بلاکچین بیت کوین بر اساس ایده‌ی دموکراسی عمل می‌کند، یعنی اکثریت مشارکت‌کنندگان (ماینرهای) شبکه می‌توانند تصمیم بگیرند که کدام نسخه از بلاکچین نسخه‌ی حقیقی است. حمله ۵۱ درصد چگونه کار می‌کند؟ وقتی یک مالک بیت کوین تراکنشی را امضا می‌کند، تراکنش او در استخری محلی از تراکنش‌های تاییدنشده قرار می‌گیرد. ماینرها تراکنش‌ها را از این استخر انتخاب می‌کنند تا بلاکی از تراکنش‌ها را به وجود بیاورند. آن‌ها برای افزودن این بلاک به بلاکچین باید پاسخ یک مسئله‌ی سخت ریاضی را بیابند. برای پیدا کردن این پاسخ از توان رایانش استفاده می‌شود. به این کار هشینگ می‌گویند. هرچه توان رایانش ماینر بیشتر باشد، شانس او برای یافتن پاسخ مسئله پیش از سایر ماینرها بیشتر می‌شود. وقتی یکی از ماینرها پاسخ را پیدا کرد، آن را (به همراه بلاک) برای همه ارسال می‌کند تا در صورتی که همه تراکنش‌های داخل بلاک بر اساس سوابق موجود در بلاکچین معتبر بود، آن‌ها بلاک را تایید کنند. به یاد داشته باشید که ماینرهای خرابکار هرگز نمی‌توانند برای بقیه تراکنش بسازند چون برای انجام این کار به امضای دیجیتالی (یعنی همان کلید خصوصی) کاربر نیاز است. در نتیجه ارسال بیت کوین از اکانت یک شخص دیگر عملا بدون دسترسی به کلید خصوصی او غیرممکن می‌شود. استخراج مخفیانه – ایجاد شاخه جدیدی از بلاکچین حالا به این بخش دقت کنید. ماینرهای خرابکار می‌توانند سعی کنند تراکنش‌های موجود را برگردانند. وقتی یک ماینر پاسخی برای مسئله موجود پیدا می‌کند، انتظار می‌رود این پاسخ برای سایر ماینرها ارسال شود تا آن‌ها بلاک را تایید و آن را به بلاکچین اضافه کنند. ولی یک ماینر خرابکار می‌تواند با عدم انتشار عمومی راهکار بلاک

خودش شاخه جدیدی از بلاکچین بسازد. بدین ترتیب دو نسخه از بلاکچین به وجود می‌آید .نسخه‌ای که توسط ماینرهای عادی به کار گرفته می‌شود، و نسخه‌ای که توسط ماینر خرابکار مورد استفاده قرار می‌گیرد. ماینر خرابکار به فعالیت روی نسخه‌ی دوم بلاکچین ادامه می‌دهد و پاسخ‌هایش را به سایر اعضای شبکه نمی‌فرستد. مابقی شبکه از وجود این شاخه جدید مطلع نمی‌شوند. در نتیجه این شاخه از بخش دیگر شبکه جدا می‌ماند. حالا ماینر خرابکار می‌تواند همه بیت کوین‌های خود را در نسخه‌ی حقیقی بلاکچین خرج کند. اگر فرض کنیم او با بیت کوین‌هایش یک لامبورگینی خریده باشد، همه‌ی دارایی او در بلاکچین اصلی خرج شده است. ولی او این تراکنش‌ها را در شاخه بلاکچین خودش اعمال نمی‌کند. به همین خاطر او در آن شاخه هنوز همه بیت کوین‌هایش را دارد .در عین حال، او همچنان در بلاکچین خودش به بررسی و تایید بلاک‌ها ادامه می‌دهد. این‌جاست که مشکل اصلی به وجود می‌آید. بلاکچین بر اساس مدل حاکمیت دموکراتیک طراحی شده، یعنی رای اکثریت اهمیت دارد. بلاکچین این کار را با پیروی دائمی از بلندترین زنجیره (در واقع سنگین‌ترین زنجیره، اما بگذارید بحث را خیلی پیچیده نکنیم) انجام می‌دهد، چرا که اکثر ماینرها زودتر از بقیه بلاک‌ها را به نسخه بلاکچین خودشان اضافه می‌کنند (بنابراین بلندترین زنجیره = اکثریت). بدین ترتیب بلاکچین متوجه می‌شود که کدام نسخه از زنجیره‌اش حقیقی است و بر همین اساس تراز مالی کیف پول‌ها را تعیین می‌کند. در این مرحله رقابت آغاز می‌شود. هر کسی که از بیشترین توان هش برخوردار است سریع‌تر بلاک‌ها را به نسخه زنجیره خودش اضافه می‌کند .

پس ماینر خرابکار به جهت توان هش قدرتمندتری که دارد، سریع‌تر بلاک‌ها را به زنجیره خودش اضافه می‌کند. برگرداندن تراکنش‌ها با مخابره همگانی زنجیره جدید ماینر خرابکار حالا سعی می‌کند بلاک‌ها را سریع‌تر از بقیه به بلاکچین خودش اضافه کند و به محض این که موفق شد بلاکچین بلندتر را بسازد، او بلاکچین خودش را برای بقیه شبکه مخابره می‌کند. سایر اعضای شبکه با بررسی این نسخه از بلاکچین متوجه می‌شوند که این زنجیره از زنجیره خودشان بلندتر است، در نتیجه پروتکل شبکه آن‌ها را مجبور می‌کند تا از آن زنجیره استفاده کنند. بلاکچین دستکاری‌شده حالا به عنوان بلاکچین حقیقی در نظر گرفته می‌شود و همه تراکنش‌هایی که در این زنجیره ثبت نشده بود بلافاصله معکوس می‌گردد. مهاجم قبلا با بیت کوین‌هایش لامبورگینی خریده بود، ولی این تراکنش در زنجیره مخفیانه او ثبت نشد؛ حالا همین زنجیره روی کار آمده است. بنابراین بیت کوین‌ها مجددا به حساب ماینر خرابکار برمی‌گردد و او می‌تواند دوباره آن‌ها را خرج کند. به این اتفاق حمله خرج دوباره می‌گویند و نام دیگر آن حمله ۵۱ درصد است، چون ماینر خرابکار برای این که بتواند سریع‌تر بلاک‌ها را به بلاکچین خودش اضافه کند، باید توان هش بیشتری نسبت به مجموع توان هش سایر اعضای شبکه داشته باشد. بیت کوین چطور با این حمله مقابله می‌کند؟ انجام این حملات در واقعیت بی‌اندازه دشوار است. همان طور که گفتیم کسی که می‌خواهد این کار را انجام دهد باید توان هشی بیشتر از مجموع توان هش سایر اعضای شبکه داشته باشد. با توجه به این که در بلاکچین بیت کوین احتمالا بیش از صدها هزار ماینر وجود دارد، مهاجم باید پول هنگفتی را صرف تهیه تجهیزات استخراجی کند تا بتواند با توان هش سایر اعضای شبکه رقابت کند. حتی قوی‌ترین کامپیوترهای دنیا هم نمی‌توانند مستقیماً از پس مجموع توان رایانشی کل شبکه بربیایند. علاوه بر این، ایرادات مختلفی به حمله‌ی ۵۱ درصد وارد است. مثلاً ریسک لو رفتن و محکوم شدن، یا هزینه‌های مربوط به برق، محل نگهداری از تجهیزات، و پولشویی بسیار بالاست. عملیاتی مثل حمله ۵۱ درصد در مقابل چیزی که به مهاجم برمی‌گرداند، حداقل در بلاکچین بیت کوین، زحمت و تلاش خیلی زیادی می‌طلبد.

آیا سایر بلاکچین‌ها آسیب‌پذیرند؟ با وجود همه‌ی سختی‌ها و مشکلاتی که پیش روی حملات ۵۱ درصد وجود دارد، نمونه‌های این حمله را قبلا چند بار تجربه کرده‌ایم. در حقیقت، جدیدترین آن‌ها همین چند ماه پیش (در آوریل ۲۰۱۸) و در بلاکچین Verg اتفاق افتاد. در این حمله، مهاجم باگی را در کد پروتکل بلاکچین Verge پیدا کرده بود که به او اجازه می‌داد بلاک‌های جدید را با سرعت بسیار زیادی تولید کند و بتواند در مدت زمان خیلی کوتاه‌تری نسخه‌ی طولانی‌ترِ بلاکچین Verge را بسازد. این مثال نشان می‌دهد که چه مشکلات و باگ‌هایی می‌تواند به حمله‌ی ۵۱ درصد منجر شود. باگی که در صورت وجود تیمی مجرب از توسعه‌دهندگان به هیچ عنوان به وجود نمی‌آمد یا به موقع جلوی سوء استفاده از آن گرفته می‌شد. اگر الگوریتم (اثبات کار) را بررسی کنیم، این الگوریتم به ما می‌گوید که توان هش فعال یا توان رایانشی قوی‌تر به ایمنی بیشتر در برابر حملات ۵۱ درصد منجر می‌شود. با این حال بلاکچین‌های کوچک‌تری که از این الگوریتم استفاده می‌کنند، می‌توانند با شدت بسیار بیشتری در برابر این حملات آسیب‌پذیر باشند، چون توان کافی برای رقابت با توان مهاجم در شبکه وجود ندارد. به همین دلیل است که حملات ۵۱ درصد معمولا در بلاکچین‌های کوچک) مثلا بیت کوین (Gold اتفاق می‌افتد. لازم به ذکر است که بلاکچین بیت کوین تاکنون هیچ‌گاه قربانی حمله ۵۱ درصد نشده است.

گره NODE چیست؟

به هر کامپیوتر متصل به شبکه بلاک چین node یا گره گفته می شود. گره ها وظیفه تایید و بررسی و محاسبات تراکنش ها را دارند.

Full node چیست؟

به گره ای که یک کپی کامل از دفترکل توزیع شده داشته باشد یک نود کامل می باشد. از این گونه نودها معمولا جهت ایفای یک نقش در شبکه مانند تایید تراکنش ها، دیدن سابقه تراکنش ها، دیدن میزان دارایی آدرس ها و ... استفاده می شود. تعداد این نودها می تواند به امنیت یک ارز کمک کند.

Lightweight node چیست؟

در حالی که فول نودها ستون فقرات شبکه‌ی بیت کوین را فراهم می‌کنند، لایت نودها یا در اصطلاح گره‌های سبک برای سهولت کاربران در استفاده از فول نودها ساخته شده است.

این نودها به منظور اعمال فعالیت‌های اساسی، به شبکه‌ی بلاک چین بیت‌کوین متصل می‌شوند. چنین نودها برای اعمال تایید تراکنش‌ها کل بلاک‌چین را دانلود نمی‌کنند بلکه فقط فیلدی به اسم بلاک هدر (Block Header) را دانلود می‌کنند. این فیلد فقط ۸۰ بایت حجم دارد بنابراین در زمان فعلی نگارش مقاله که ۵۴۶۴۱۲ بلاک در شبکه‌ی بلاک چین بیت کوین ساخته شده است حجم یک لایت نود حدود ۴۰ مگابایت می‌شود.

فول نودها، لایت نودها را پشتیبانی می‌کنند؛ فول نود کل بلاک چین را دانلود می‌کند و آن‌ها را براساس قوانین ثابت شبکه می‌سنجد. اگرچه لایت نودها ممکن است یک تراکنش معیوب را به دلیل دامنه محدود خود تائید کنند ولی فول نودها آن‌ها را تایید نمی‌کنند.

امنیت و حریم خصوصی

وقتی شما برای ایجاد تراکنش یا دیگر خدمات کیف پول بیت کوین از یک لایت نود استفاده می‌کنید شما با یک سرور ثالث در ارتباط هستید که به فول نود متصل می‌شود این سرور ثالث می‌تواند به اطلاعات موجودی شما و تراکنش‌های قبلی شما دست پیدا کند! اما وقتی که خودتان مستقیم از یک فول نود استفاده کنید دیگر با این مشکل‌ها سر و کار ندارید. همچنین استفاده از لایت نودها برای تراکنش ممکن است دچار رخنه‌ی امنیتی و در نتیجه آسیب به کاربران شود؛ بدلیل این که لایت‌نودها کل دیتای بلاک‌چین را ذخیره نمی‌کنند. برای همین باید صحت اطلاعات خود را از سرور ثالثی بگیرند که این سرورها خود را فول نود می‌نامند؛ خالق بیت کوین ساتوشی ناکاماتو برای ساخت تراکنش از این روش اجتناب می‌کرد و توصیه می‌کرد که برای ساخت تراکنش مستقیم از فول نود استفاده شود.

کلید عمومی و کلید خصوصی

هدر بلاک (Block Header) چیست؟

بیت کوین دنیایی می‌باشد که در چند سال گذشته و از زمانی که ارزهای دیجیتال به سطح پذیرش بی سابقه ای رسیده اند، موضوع صحبت همگان شده است. بیت کوین با ارزش ترین و مهم ترین ارز دیجیتال و اختراعی خارق العاده از ذهن انسان است و به همه ما روشی برای کنترل و مدیریت پول خودمان ارائه می‌دهد بدون آنکه شخص ثالث به آن دسترسی داشته باشد.

دلیل آنکه چرا بیت کوین مهم بود و هم چنان مهم است کاملا واضح می‌باشد: بیت کوین ارز دیجیتال غیرمتمرکز است و به همه امکان می‌دهد در چند ثانیه پول خود را از مکانی به مکان دیگر انتقال دهند و هیچ بانک، موسسه یا دولتی نمی‌تواند آن را کنترل کند.

بیت کوین شامل فناوری نیز می‌باشد که به اندازه ارز دیجیتال از اهمیت ویژه ای برخوردار است. با وجود اینکه ممکن است هنوز بلاک چین کاملا شناخته شده نباشد، اما احتمالا مهم ترین اختراع بیست سال اخیر است. بلاک چین بخشی از فناوری کاملا مرتبط با زمان ما می‌باشد که با گذشت هر روز، بیشتر و بیشتر جای خود را در صنایع مختلف باز می‌کند.

همانند تمام فناوری های مدرن، مباحث فنی بسیار زیاد و جنبه ها و نکات کوچک ولی مهمی وجود دارد که ممکن است از دید و توجه عموم مردم پنهان بماند. در این مقاله به موضوعی خواهیم پرداخت که اغلب اوقات از آن چشم پوشی شده است اما ویژگی بسیار مهم بلاک چین بیت کوین می‌باشد :هدر بلاک.

هدر بلاک چیست؟

برای آنکه دقیقا متوجه شوید هدر بلاک چیست باید ابتدا بلاک چین را بشناسید. بلاک چین که در سال ۲۰۰۸ توسط ساتوشی ناکاموتو اختراع شده است، دفترکل عمومی تراکنش ها و فهرست سابقه تراکنش ها می‌باشد که با استفاده از رمزنگاری محافظت می‌شود. بلاک چین، ساختار داده ای است که برای ذخیره تراکنش ها در مجموعه ای از بلاک های متصل به هم طراحی شده است.

بلاک چین شامل مجموعه ای از بلاک های مختلف است که برای ذخیره اطلاعات مرتبط با تراکنش هایی استفاده می‌شود که بر بستر شبکه بلاک چین صورت می‌گیرند. بلاک شامل هدر منحصر به فرد است و هر بلاک با هش هدر بلاک خود مشخص می‌شود.

هدر بلاک برای شناسایی بلاکی خاص در کل بلاک چین استفاده می‌شود و برای ایجاد گواه اثبات کار برای جایزه ماینینگ، مکررا هش می‌شود.

موضوعات بسیار زیادی وجود دارد که می‌توان در رابطه با آنها صحبت کرد زیرا بلاک چین فناوری پیچیده و بسیار جالبی است، اما در این مقاله سعی بر آن خواهد شد تا به ساده ترین شکل توضیح داده شوند. هر بلاک در بلاک چین، فهرستی از تراکنش ها را داخل خود دارد. در واقع ساختار بلاک شامل دو عنصر اصلی است: هدر بلاک و فهرست تراکنش ها.

ساختار هدر بلاک

محتوای هدر بلاک دارای شناسه منحصر به فردی با نام هش هدر بلاک است. هر هدر بلاک شامل ۳ بخش اصلی است: هش بلاک قبلی، ثبت زمان، سختی و نانس، ریشه درخت مرکل.

شماره نسخه برای پیگیری بروزرسانی ها و تغییر در پروتکل بیت کوین استفاده می‌شود. هش هدر قبلی محتوایی است که به بلاک قبلی متصل شده و باعث ایمن شدن زنجیره می‌شود.

هش بلاک مسئول شناسایی بلاک در بلاک چین است. به طور خلاصه، هر بلاک در بلاک چین توسط هش هدر بلاک خود مشخص می‌شود. هر بلاک به طور منحصر به فرد توسط شماره هش مشخص می‌شود که این شماره هش با هشینگ دوباره هدر بلاک با استفاده از الگوریتم SHA256به دست می‌آید. یکی از نکات مهم این است که هش هدر در ساختار بلاک ذخیره نمی‌شود. در عوض، توسط هر نود محاسبه می‌شود زیرا بلاک از طریق شبکه دریافت می‌شود.

سختی مورد نظر بلاک، تعداد صفرهایی است که باید هنگام هشینگ هدر بلاک پیدا شود تا به سطح تعیین شده گواه اثبات کار برسد. نانس مقداری است که توسط ماینرها تغییر می‌کند تا به منظور دستیابی به سطح سختی مورد نظر بتوانند جایگشت های مختلف را امتحان کنند.

درخت مرکل احتمالا پیچیده ترین بخش هدر بلاک است. درخت مرکل یک درخت باینری است که شامل هش های رمزنگاری شده در برگ های خود است. در مورد بیت کوین، درخت مرکل از جفت هشینگ مکرر نودها ایجاد می‌شود تا زمانی که یک هش با نام ریشه مرکل تعیین شود.

اطلاعات بیشتر درباره هدر بلاک

می‌توان اینطور در نظر گرفت که هدر بلاک نوعی متادیتا یا فراداده بر بستر بلاک تراکنش ها می‌باشد. هدر در واقع زنجیره ای به طول ۸۰ بایت است که شامل شماره نسخه بیت کوین به طول ۴ بایت، هش بلاک قبلی به طول ۳۲ بایت، ریشه مرکل به طول ۳۲ بایت، ثبت زمان بلاک به طول ۴ بایت، سختی مورد نظر به طول ۴ بایت و نانس مورد استفاده ماینر به طول ۴ بایت است.

به طور مثال، هدر بلاک برای بلاک ۱۲۳,۴۵۶ بیت کوین به شرح زیر است:

“010000009500c43a25c624520b5100adf82cb9f9da72fd2447a496bc600b0000000000006cd8623703
95dedf1da2841ccda0fc489e3039de5f1ccddef0e834991a65600ea6c8cb4db3936a1ae3143991”

نتیجه گیری

هدر بلاک محتوای بسیار مهم هر بلاک در بلاک چین است. اگرچه هدر بلاک اهمیت ویژه ای برای اکوسیستم بیت کوین دارد اما اغلب به آن کم توجهی شده است. با این حال، اگر واقعا در صدد دانستن نحوه کار بلاک چین هستید باید یادگیری هرچه بیشتر در خصوص هدر بلاک در صدر اولویت های شما باشد.

آدرس های ارزهای دیجیتال

در روزهای نخست بیتکوین، امکان ارسال پرداخت‌ها به یک آدرس IP مثل ۱۰۴.۲۵.۲۴۸.۳۲ وجود داشت. این کار برای ایجاد راحتی در استفاده از بیتکوین بدون استفاده از آدرس‌های کلید عمومی و خصوصی انجام شد. اما بعد از آن توسعه دهندگان متوجه شدند که این وضعیت ممکن است باعث بروز حمله Man in the middle شود.

آدرس ها در بلاکچین یک چیز سفت و سخت نیستند. بلکه یک شناسه برای پذیرش و ارسال تراکنش‌های بلاکچین هستند. درست مانند آدرس‌های سوییفت. خود آدرس و فرمت آن مساله اصلی نیست. مساله مهم خدمتی است که آدرس ، برای تبدیل پرداخت‌ها به یک موجودیت اطلاعاتی، ارائه می‌کند. معمولا یک کلید خصوصی برای دسترسی به موجودی وجود دارد و آدرس چیزی به جز یک شناسه امن نیست. بعد از کنار گذاشتن آدرس IP در بیتکوین، PKH ۲P به عنوان استاندارد جدید آدرس‌های بیتکوین شناخته شد. این آدرس چیزی شبیه به آدرس زیر است:۱zEXb۲MxFFTHPi۵g۹KZXjcochXpRhjH۳۱K یک آدرس استانداردPKH۲ P، سی و چهار حرف دارد و با ۱ شروع می‌شود . PKH ۲Pمخفف ”Pay to Public Key Hash“ است. یعنی شما توسط هش یک کلید عمومی، پرداخت انجام می‌دهید. برای مبتدیان، این ممکن است بسیار گیج کننده باشد. بنابراین ابتدا باید فرآیند ساخت همچین آدرسی را یاد بگیریم تا بدانیم چگونه عمل می‌کند.

هر نرم‌افزار کیف پول که استفاده می‌کنید یک آدرسPKH ۲ Pتولید می‌کند. این کار ترکیبی از چند عملیات نه چندان پیچیده‌ی رمزنگاری است. ابتدا، کیف پول شما یک کلید خصوصی ECDSA تولید می‌کند ECDSA .یک الگوریتم رمزنگاری در هسته آدرس‌های بیتکوین است که یک الگوریتم امضای غیرمتقارن می‌باشد. یعنی شما می‌توانید یک پیام را با کلید خصوصی امضا کرده و آن را با کلید عمومی تایید کنید. با استفاده از ECDSA و امضا کردن پیام، می‌توانید به بقیه ثابت کنید که شما تنها تولید کننده پیام هستید و اصالت آن را تایید کنید. این مورد بسیار شبیه به امضای یک نامه به طور فیزیکی است. بنابراین بعد از ایجاد کلید خصوصی، کیف پول، کلید عمومی را از روی آن بدست می‌آورد. این کار با استفاده از برخی محاسبات و الگوریتم‌های تصادفی انجام می‌شود. البته جزییات آن مهم نیست. چیزی که اهمیت دارد این است که کلید عمومی تنها چیزی است که شما برای دریافت و جمع‌آوری ارز دیجیتالی به آن نیاز دارید.

ایجاد آدرس بلاکچین در بیتکوین

برای ایجاد آدرس، کیف پول شما کلید عمومی را از طریق یک سری از الگوریتم‌های رمزنگاری بدست می‌آورد. به طور شفاف این چیزی است که اتفاق می‌افتد:

نرم‌افزار هش، کلید عمومی را با SHA ۲۵۶ و سپس-RIPEMD ۱۶۰ بدست می‌آورد. سپس آن را با ۰۰ بایت به عنوان پیشوند در ابتدای نتیجه قبل جمع می‌کند. به همین دلیل است که آدرس‌هایP ۲ PKHبا ۱ شروع شده و با چهار بایت checksum در انتها ختم می‌شود. چهار بایت از checksum توسط دوبار هش گرفتن از نتیجه با SHA ۲۵۶ و جدا کردن ۴ بایت اول آن بدست می‌آید. سپس کیف پول شما نتیجه را به یک رشتهbase ۵۸ تبدیل می‌کند. حالا یک آدرس بیتکوین بدست آمده است.

شما نیاز به دانستن جزییات رمزنگاری ندارید. مهم این است که آدرس، یک کلید عمومی با خوانایی بیشتر ارائه کرده و یک checksum را برای جلوگیری از خطای تایپی به آن اضافه می‌کند. هر وقت شما یک آدرس را در کیف پول خود وارد می‌کنید، پیشوند را چک کرده و checksumرا حساب می‌کند. اگر checksum محاسبه شده با مقدار موجود در آدرس متفاوت باشد، امکان ارسال را در صورت وجود خطای تایپی نخواهید داشت.

اگر شما کلید خصوصی یک آدرس را داشته باشید، فقط شما می‌توانید یک تراکنش را برای توکنی که به این آدرس اختصاص دارد امضا کنید. در حالی که هر کسی که آدرس شما را بداند می‌تواند اعتبار امضای شما را تایید کند. این فرآیند ساده، امضای تراکنش و تایید امضا، تنها چیزی است که رمزنگاری روی تراکنش انجام می‌دهد.

اما بیتکوین آدرس‌های پیشرفته‌تری دارد: یعنی آدرس‌هایP ۲ .SHکه خلاصه "Pay To Script Hash" می‌باشد. یعنی شما به هش یک آدرس پرداخت نمی‌کنید؛ بلکه به هش یک اسکریپت پرداخت می‌کنید. برای امضای یک تراکنش شما به یک امضا که با یک کلید عمومی خاصی تطابق داشته باشد، نیاز ندارید. بلکه به یک اسکریپت که با یک هش مشخص تطابق داشته باشد نیاز دارید. هر چند برای فهم قدرت SH ۲Pبه دانش بیشتری نیاز است، فعلا بیتکوین را کنار گذاشته در ادامه روی آدرس‌ها تمرکز می‌کنیم.

آدرس ها در کوین های دیگر

بسیاری از کوین‌ها از آدرس‌دهی مشابه بیتکوین استفاده می‌کنند. برای مثال لایت کوین ، دش و دوج کوین از روندهای مشابهی برای رمزگذاری استفاده می‌کنند ECDSA, SHA ۲۵۶: RIPEMD ۱۶۰, تنها تفاوت وجود پیشوند هشِ-RIPEMD ۱۶۰ است. در حالی که پیشوند ۰۰ در آدرس بیتکوین باعث شروع آن با «۱» می‌شود، کوین‌های دیگر مانند دش، لایت کوین و دوج کوین از پیشوندهای دیگری استفاده می‌کنند که باعث می‌شود با حروفی مثل «X» و «L» و «D» شروع شوند. مادامی که این کوین‌ها از الگوریتم‌های رمزنگاری متفاوتی استفاده می‌کنند، شما می‌توانید از همان کلید عمومی و خصوصی مشابه برای ذخیره کوین در تمام ارزهای دیجیتال استفاده کنید.

ارزهای دیگر از روش‌های دیگری برای تولید آدرس استفاده می‌کنند. برای مثال مونرو بر اساس الگوریتم Cryptonote می‌باشد. این الگوریتم نوع دیگری از الگوریتم امضای رمزشده را برای تولید کلید عمومی استفاده می‌کند. ارزهای مبتنی بر کریپتونوت (Cryptonote) یک امضای حلقه گونه دارند که حریم خصوصی بیشتری را فراهم می‌کند چرا که شما نمی توانید تعیین کنید یک تراکنش با کدام کلید امضا شده است. به همین دلیل، آدرس‌های کریپتونوت باید شامل دو کلید عمومی باشند: یک کلید مشاهده و دیگری کلید پرداخت.

همانند آدرس‌های بیتکوین، کریپتونوت یک پیشوند اضافه می‌کند و نتیجه را هش می‌کند. این الگوریتم از-Keccak ۲۵۶ بجای-SHA ۲۵۶ دوتایی برای تولید checksum چهاربیتی استفاده می‌کند که به آخر یک رشته اضافه می‌شود. بعد از تبدیل نتیجه بهbase ۵۸ شما آدرس نهایی را بدست می‌آورید که از بیتکوین طولانی تر می‌باشد. و شبیه زیر است:

۷NWiKJRUMnuAJ۳uhEfYoPVAuGHxJcomMHEPp۸۵ZqpGTBP۳AvyMu۴NUoxG۶cajEtc۷X۴۲ZZViHQKd۴۳
a۲dfBrPTcfjYMPJzz

این تنوع در آدرس‌ها، نشان می‌دهد که آدرس‌ها فقط وسیله‌ای برای پرداخت هستند که به یک کلید عمومی مشخص الحاق می‌شود. برای همین، مهم نیست که شما چه کاری با کلید عمومی انجام می‌دهید، از چه الگوریتمی برای تبدیل آن به یک آدرس استفاده می‌کنید و...

روال ساخت یک آدرس، مفاهیمی از امنیت، حریم خصوصی و قابلیت استفاده را در بر دارد. بدون استفاده ازchecksum ، آدرس‌های بیتکوین ممکن است دچار اشتباه تایپی شوند و بدون تعبیه کلید مشاهده در آدرس، مونرو نمی‌تواند آنگونه که هست خصوصی بماند.

آدرس های اتریوم

مانند خیلی از چیزهای دیگر در دنیای رمزارزها، مبحث آدرس‌ها با رسیدن به اتریوم جذاب‌تر می‌شود. بسیاری از افرادی که با بیتکوین شروع کرده‌اند و سپس به سراغ اتریوم می‌روند، با دیدن قالب آدرس آن سردرگم می‌شوند که یک آدرس طولانی، و یک رشته در مبنای ۱۶ است که با ۰ xشروع می‌شود. به عنوان مثال: ۷۳۵f۹f۵e۰c۲a۷۳۴ec۱۳۸۹f۶۰ec۸۱۸۹۲۵۴۰۷۴۷eb۰x۰ از لحاظ فنی، تولید آدرس اتریوم مشابه بیت‌کوین است، اما نه در همه موارد. برای تولید یک کلید عمومی ۶۴ بایتی، باید از یک کلید خصوصی شروع کرده و از ECDSA استفاده کنید. یعنی همان طور که بیت‌کوین عمل می‌کند. سپس آن را توسط-Keccak ۲۵۶ هش می‌کنید. نتیجه که یک رشته ۳۲ بایتی خواهد بود. ۱۲ بیت اول از این بایت‌ها دور انداخته می‌شود و ۲۰ بایت باقی مانده که یک آدرس ۴۰ کاراکتری است با یک پیشوند ۰ xآدرس اتریوم را تشکیل می‌دهند. برخلاف بیت‌کوین یا کریپتونت، اتریوم آدرس را بهbase ۵۸ تبدیل نمی‌کند، بنابراین یک آدرس هگزادسیمال یا مبنای ۱۶ خواهد بود.

تفاوت دیگر اتریوم با رمزارزهای دیگر، این است که آدرس‌های اتریوم checksum ندارند. هر رشته‌ی ۴۰ کاراکتری مبنای ۱۶ می‌تواند یک آدرس اتریوم باشد. یعنی خطای تایپی در وارد کردن آدرس قابل شناسایی نخواهد بود. در مقایسه با سایر رمزارزها، آدرس‌ها برای کاربر اتریوم، خام، خشن و خطرناک خواهد بود. این مساله برای ارزی که دومین بازار بزرگ را در اختیار دارد و به عنوان خلاقانه ترین رمزارز شناخته می‌شود، بسیار پیش پا افتاده است.

دلیل اول برای این مشکل، این است که در زمان ارائه نسخه اول اتریوم، Frontier، کسی واقعا به این موضوع اهمیت نمی‌داد. هدف توسعه دهندگان اتریوم ساخت یک قرارداد هوشمند بود، که پرداخت‌ها به راحتی به اسامی و دامنه‌ها فرستاده شود. البته همانطور که جف کولمن اشاره کرد، استفاده نکردن اتریوم از روش مشابه بیت‌کوین دلیل مهمتری دارد. در حقیقت توسعه دهندگان گمان کردند که این کار می‌تواند بهتر انجام شود. به یاد بیاورید که یک آدرس فقط یک روش رمزنگاری برای ارائه اطلاعات است که موجودی را به یک کلید خصوصی تخصیص می‌دهد. این کار می‌تواند توسط قراردادهایی انجام شود که اطلاعات را به اسامی اختصاص می‌دهد.

ICAPیک شماره بانکی بین‌المللی کاملا معتبر است که نرم‌افزارهای بانکی می‌توانند آن را بفهمند و با آن تعامل کنند IBAN .نیز نمونه متمرکز این پروتکل بوده و شناسه بین‌المللی مشتریان در صنعت بانکداری است. این شناسه از ۲۳ کاراکتر حساس به حروف کوچک و بزرگ تشکیل شده است و شامل یک کد کشور، یک checksum و شماره بانک در کنار شماره حساب می‌باشد.

در حال فرمت ICAP حاضر اینگونه می‌باشد: ZPPZS۵PX۸R۰WZ۲F۰KYGTWWZN۰۷۳O۷۳۳۸E مانند بیتکوین، این آدرس از کاراکترهایbase ۵۸ استفاده می‌کند و شامل checksum می‌شود.

استیم، نام کاربری شما آدرس شماست!

ارز رمزنگاری‌شده استیم (Steem) سیستم مشابه اتریوم را استفاده کرده است. در استیم نام کاربری شما کیف پول شما است. استیم رمزارزی مبتنی بر ایده Bitshares است. این ارز با بستر شبکه اجتماعی Steemit لینک شده است. یعنی شما می‌توانید استیم کوین را با بدست آوردن لایک و کامنت روی پست‌های خود ماین کنید! استیم مانند بیت‌کوین و اتریوم غیرمتمرکز نیست و قسمت‌های مهم آن در پلتفرم خصوصی Steemit میزبانی می‌شود و قسمت اصلی استیم می‌باشد.

هرچند، استیم به روش متمرکزتری ایده‌ی قرارداد هوشمند اتریوم را پیاده‌سازی کرده است اما کاربران در این سیستم نیز یک کلید خصوصی دریافت کرده و همانند ارزهای دیگر می‌توانند تراکنش‌ها را امضا کنند. در استیم نام‌های کاربری، آدرس‌هایی نیستند که از کلید خصوصی مشتق شده باشند. بلکه فقط نام‌هایی هستند که روی پایگاه داده استیم به کلیدهای عمومی وصل شده‌اند. در اینجا مهمترین بخش تایید اتصال بین کلید عمومی و آدرس، براساس محاسبات ریاضی نیست؛ بلکه نیاز به اعتماد به بستر استیم داریم. شیوه آدرس دهی براساس نام کاربری در استیم جالب است چرا که قابلیت استفاده ایده‌آل را فراهم می‌کند. اما هنوز متمرکز بوده و عدم اعتماد کافی را برای بسیاری از کاربران بلاکچین به همراه دارد. یعنی سیستم هنوز از شفافیت کافی برخوردار نمی‌باشد. یک سیستم قرارداد هوشمند مانند اتریوم، می‌تواند هر دو بخش ایده‌آل را داشته باشد؛ غیرمتمرکز بودن، اعتماد طبیعی بلاکچین و راحتی استفاده از آدرس‌های مبتنی بر نام استیم!

هر آنچه باید در مورد انواع فرمت آدرس های بیت کوین بدانید!

آدرس کیف پول شامل رشته ۲۶ الی ۳۵ کارکتری از اعداد و حروف است که تنها وظیفه آن ارسال و دریافت بیت کوین می‌باشد. می‌توان از هر آدرس بیت کوین برای انتقال ارز دیجیتال به هر آدرس دیگر موجود در شبکه که نرم افزار کیف پول ارسال کننده پشتیبانی می‌کند، استفاده کرد. با وجود چندین فرمت آدرس و ارائه دهندگان کیف پول و صرافی هایی که فقط انواع خاصی از آدرس ها را پشتیبانی می‌کنند، بهتر است که تفاوت این آدرس ها را بدانید.

همانطور که چندین نسخه از پروتکل اینترنت نظیر IPv4 و IPv6 وجود دارد، فرمت های آدرس بیت کوین نیز به چندین نوع تقسیم می‌شوند. اکثر اوقات، این آدرس ها با یکدیگر تناقضی ندارند و تراکنش ها بدون مشکل در شبکه و بین کیف پول های دارای تصدی و غیر تصدی انجام می‌شود. سه فرمت آدرس بیت کوین کور وجود دارد که عبارتند از P2PKH و P2SH و bech32 که فقط چند ارائه دهنده خدمات کیف پول از تمام این فرمت ها پشتیبانی می‌کنند. احتمال اینکه کیف پول یا صرافی مورد نظر شما حداقل از یکی از این فرمت ها و معمولا فرمت bech32پشتیبانی نکند وجود دارد.

یادگیری مزایا، معایب و ویژگی های هر کدام از این فرمت ها به شما امکان خواهد داد تا کیف پول، صرافی یا پلتفرم مناسبی انتخاب کنید. یادگیری این فرمت ها هم چنین دانش بیشتری از عملیات داخل بیت کوین به شما ارائه می‌دهد و نقطه قوت و ضعف هر کدام از این فرمت ها را از لحاظ امنیت، انعطاف پذیری و عملکرد مشخص می‌کند.

اگر آدرس بیت کوین شما با عدد ۱ شروع می‌شود، پس از آدرس لگسی (Legacy) یا P2PKH استفاده می‌کنید. برای مثال آدرس ۱ .BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2این فرمت اصلی آدرس بیت کوین بوده است و تاکنون نیز پابرجاست. عنوان P2PKHمخفف عبارت پرداخت برای هش کلید عمومی (Pay to Public Key Hash) است، یعنی آنکه برای هش کلید عمومی دریافت کننده، پرداخت انجام می‌دهید. آدرس های لگسی مطابق با سگویت (Segwit) نمی‌باشند اما هم چنان می‌توانید بدون مشکل از آدرس P2PKHبه آدرس سگویت، بیت کوین ارسال کنید. میانگین کارمزد ارسال از آدرس P2PKH بیشتر از ارسال از آدرس سگویت می‌باشد، زیرا سایز تراکنش های آدرس لگسی بزرگتر می‌باشند.

فرمت آدرس P2SH

ساختار آدرس های P2SH مشابه با آدرس های P2PKH می‌باشد با این تفاوت که به جای عدد ۱ با عدد ۳ شروع می‌شوند. برای مثال آدرس ۳ .J98t1WpEZ73CNmQviecrnyiWrnqRhWNLyعنوان P2SH مخفف عبارت پرداخت برای هش اسکریپت (Pay to Script Hash)است و عملکرد بیشتری نسبت به آدرس های لگسی ارائه می‌دهند. تابع اسکریپت P2SH اغلب برای آدرس های چندامضایی (Multi Signature)استفاده می‌شوند که می‌توانند مشخص کنند به چندین امضای دیجیتال برای تایید تراکنش نیاز است. این فرمت آدرس هم چنین برای امکان پذیر ساختن تراکنش های سگویت غیراصلی که از فرآیند P2WPKH به P2SH استفاده می‌کنند به کار گرفته می‌شود. فرد عادی که فقط به ارسال و دریافت کوین ها می‌پردازد نیازی ندارد خود را درگیر عملکردهای پیچیده تر P2SH کند. چیزی که مهم می‌باشد آن است که این نوع آدرس به طور گسترده پشتبانی می‌شود و می‌توان برای ارسال سرمایه به آدرس های P2PKH و bech32 از آن استفاده کرد.

فرمت آدرس bech32

آدرس های bech32 کاملا با آدرس های P2 فرق دارند. آدرس های bech32 با bc1 شروع می‌شود و به دلیل این پیشوند، بزرگتر از آدرس های لگسی یا P2SH می‌باشند. فرمت bech32 فرمت اصلی آدرس های سگویت می‌باشند و توسط اکثر نرم افزارها و کیف پول های سخت

افزاری پشتیبانی می‌شود، اما صرافی های کمی از آن پشتیبانی می‌کنند. کیف پول های لجر و کیپ‌کی (keepkey) در حال حاضر از bech32پشتیبانی نمی‌کنند و اگرچه اکثر صرافی ها می‌توانند به آدرس های bech32 کوین ارسال کنند اما کاربران این صرافی ها نمی‌توانند از آدرس های این فرمت کوین دریافت کنند. در حال حاضر کمتر از یک درصد بیت کوین ها در آدرس های bech32 ذخیره شده است، هرچند این عدد به تدریج در حال افزایش است.

تراکنش های بیت کوین و ورودی – خروجی ها (Inpute and Output)

وقتی شما از کیف پولتان مقداری بیت کوین منتقل می‌کنید، در واقع کیف پولتان یک تراکنش ایجاد می‌کند و آن را در شبکه بیت کوین منتشر می‌کند تا یک ماینر آن را درون بلاکچین ثبت کند. در واقع بلاکچین یک نوع دیتابیس از تمام تراکنش‌هایی است که تا کنون انجام شده‌اند. اما تراکنش های بیت کوین دقیقا شامل چه اطلاعاتی هستند و چه شکلی هستند؟ آیا این اطلاعات حساس هستند و نباید به دست کسی بیفتد؟ چگونه یک گره کامل (Full Node) شبکه میتواند درستی یک تراکنش را تایید کند؟

تراکنش‌های بیت کوین مانند آنچه در تصویر زیر می‌بینید در اصل یک پیام متنی کوتاه هستند (البته بسته به نوع تراکنش می‌توانند بسیار طولانی‌تر هم باشند)

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

یک تراکنش شامل تمام اطلاعاتی است که یک فول نود شبکه یا یک ماینر برای تایید صحت مالکیت مقدار بیت کوینی که شخص، قصد انتقال آن را دارد، به آن نیازمند است. هرکس این تکه پیام را بعد از تایید بر روی بلاکچین ثبت کند (این کار را ماینرها انجام میدهند)، دقیقا درخواست شخص انتقال دهنده انجام می‌شود، یعنی آن مقدار بیت کوینی که شخص قصد انتقال آن را داشته به همان آدرسی که او مشخص کرده منتقل می‌شود. اما نکته جالبی که در مورد تراکنش‌های بیت کوین وجود دارد این است که اولا با استفاده از رمزنگاری های صورت گرفته، هیچ گونه اطلاعات حساسی مانند کلید خصوصی (Private Key) انتقال دهنده در این پیام وجود ندارد بنابراین یک تراکنش می‌تواند بدون هیچ خطری در یک شبکه عمومی منتشر شود. اما از سوی دیگر هر کسی می تواند با دیدن این تراکنش به سرعت تایید کند که آیا این تراکنش توسط شخصی که به کلید خصوصی بیت کوین خرج شده دسترسی داشته انجام شده یا خیر. نکته جالب دوم این است که هیچ کس جز دارنده کلید خصوصی نمی‌تواند اطلاعات موجود در این پیام (تراکنش) را (مثلا آدرس گیرنده یا مقدار بیت کوین انتقالی) را تغییر دهد، چون در این صورت دیگر این پیام به عنوان یک تراکنش صحیح، تایید نمی‌شود، و این معجزه رمزنگاریست. برای آنکه متوجه شوید چه طور چنین چیزی امکان پذیر می‌شود با ما همراه باشید.

در شبکه بانکی وقتی یک نفر یک تراکنش مثلا ۳۰۰۰ تومنی انجام می‌دهد، ۳۰۰۰ تومان از حساب انتقال دهنده کم می‌شود و به حساب گیرنده همان مقدار اضافه می‌شود. حالا فرض کنید این تراکنش قرار است به صورت فیزیکی و با پول نقد انجام شود، به این صورت که در نظر بگیرید شما در کیف پولتان یک اسکناس ۵۰۰۰ تومانی دارید که قبلا آن را از شخص دیگری گرفته اید و می‌خواهید ۳۰۰۰ تومن آن را به یک نفر بدهید، برای انجام این کار شما اسکناس ۵۰۰۰ تومانی را می‌دهید و یک اسکناس ۲۰۰۰ تومانی را به عنوان مابقی پولتان پس می‌گیرید.

در مورد بیت کوین هم، تراکنش ها از این جهت بیشتر از اینکه شبیه تراکنش های بانکی باشند، شبیه تراکنش هایی است که با پول نقد صورت میگیرد، هرچند آنچیزی که در ظاهر در کیف پول بیت کوینتان می بینید این است که هر مقدار که بیت کوین انتقال می‌دهید از کیف پولتان کم می شود و به کیف پول گیرنده اضافه می‌شود، اما در اصل دقیقا همان بیت کوینی که انتقال داده اید به گیرنده می‌رسد و مانند تراکنشهای بانکی فقط مقدار موجودی‌ها کم و زیاد نمی‌شوند. از این جهت تراکنش‌های بیت کوین بیشتر شبیه تراکنش‌های فیزیکی است تا تراکنش‌های دیجیتالی!

هر تراکنش از دو بخش اصلی تشکیل شده است. ورودی (Input) و خروجی .(Output) اگر بخواهیم مثال پول نقدی که زدیم را به تراکنش های بیت کوین تشبیه کنیم، آن اسکناس ۵۰۰۰ تومانی که شما در کیف پولتان داشتید وقبلا آن را از شخص دیگری گرفته بودید Input تراکنش شماست و آن ۳۰۰۰ تومانی که به گیرنده دادید و ۲۰۰۰ تومانی که به عنوان مابقی پولتان گرفتید، Outputتراکنش شماست. مثلا فرض کنید شما در کیف پولتان ۵ بیت کوین دارید که قبلا طی یک تراکنش آن را از شخص دیگری گرفته اید و می‌خواهید ۳ بیت کوین آن را به دیگری انتقال دهید. در طی این تراکنش ۵ بیت کوین شما به عنوان ورودی تراکنش می‌شود و خروجی تراکنش شامل دو قسمت می‌شود، یک قسمت ۳ بیت کوینی که قصد انتقال آن را دارید و یک قسمت هم ۲ بیت کوینی است که به یک آدرس دیگر کیف پول شما (Change Address)بازگردانده می شود.

ورودی های تراکنش(Input)

در بخش Input قسمتی به نام ScriptSig وجود دارد که در اصل مدرکی است بر مالکیت Input که شما به عنوان انجام دهنده تراکنش قصد خرج کردن آن را دارید ScriptSig .که یک رشته از اعداد و حروف به نظر می‌رسد در اصل همان کلید عمومی (Public Key) و امضای دیجیتال (Digital Signature)شما هستند که به دنبال هم آورده شده‌اند. بخش دیگر Input هم که Previous Tx نام دارد شناسه تراکنشی (Transaction ID) است که طی آن قبلا ۵ بیت کوین به شما انتقال یافته. اگر ساده تر بخواهیم بگوییم شما در قسمت Inputابتدا نشانی تراکنشی که طی آن قبلا ۵ بیت کوین را دریافت کرده آید را میدهید و بعد ثابت می‌کنید که اکنون شما مالک آن هستید.

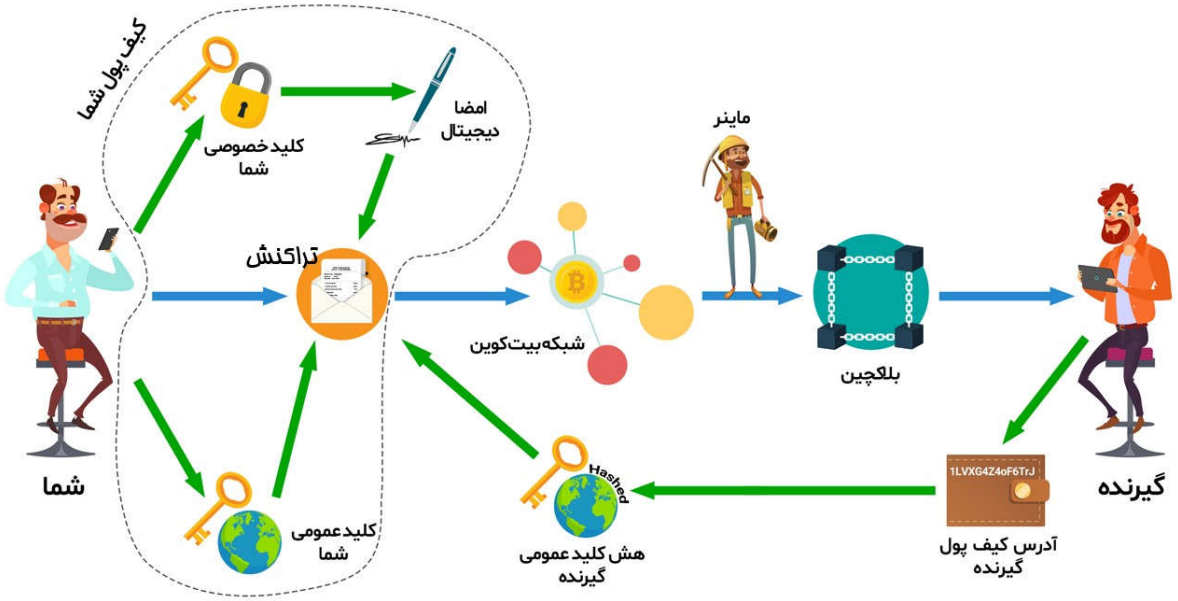
در این بین آن چیزی که هم ثابت می‌کند شما کلید خصوصی این Input را در دست دارید و مالک آن به شمار می‌روید و هم مانع تغییر جزئیات تراکنش توسط شخص سوم می‌شود، امضای دیجیتال است. امضای دیجیتال بر اساس کلید خصوصی و کلیه اطلاعات موجود در تراکنش بوسیله کیف پول شما بوجود می‌آید. بنابراین اگر هر کدام از اطلاعات موجود در تراکنش تغییر کنند، دیگر با امضای دیجیتال شما همخوانی نخواهند داشت. بنابراین تراکنش های بیت کوین همانند یک چک رمزدار است که مبلغ آن به شماره حسابی که شما خواسته‌اید رمز شده است و کسی نمی تواند آن را تغییر دهد.

خروجی های تراکنش(Output)

قسمت Output هم شامل Value یا مقدار خروجی (به ساتوشی) و ScriptPubKey است ScriptPubKey .از یک سری کدهای دستوری Scriptبیت کوین) کدهایی که با OP شروع می‌شوند (و هرکدام یک عملی را انجام می‌دهند و همچنین یک رشته از اعداد و حروف تشکیل شده است، این اعداد و حروف در واقع همان هش کلید عمومی (public Key) گیرنده است که از آدرس گیرنده‌ای که شما وارد کرده اید بدست آمده. بازهم اگر به زبان ساده تر بخواهیم بگوییم ،شما در این قسمت مشخص می کنید گیرنده تراکنش چه کسی است. بعد از آنکه این تراکنش انجام شود، گیرنده می‌تواند این مقدار ۳ بیت کوینی که شما به او منتقل کرده اید را در یک Input به کار ببرد و با امضای دیجیتال و کلید عمومی خودش ثابت کند مالک آن است، این در حالی است که شما دیگر بر این ۳ بیت کوین کنترلی ندارید چون مالکیت آن را طی یک تراکنش انتقال داده اید .

تراکنش های بیت کوین در ساده ترین حالت ممکن، حداقل یک Input و یک Output باید داشته باشند (همانند تراکنش تصویر اول). اما تراکنشی که برایتان مثال زدیم یک Input و دو Output داشت (تصویر بالا). نکته مهم این است که در یک تراکنش بدون توجه به تعداد ورودی‌ها و خروجی ها، مجموع مقدار خروجی ها باید از مجموع مقدار ورودی‌ها کمتر باشد. جالب است بدانید که کارمزد تراکنش‌ها که به ماینرها می‌رسد، همان اختلاف بین Input ها و Output های یک تراکنش است. در واقع هر چه شما قصد پرداخت کامزد (fee) بیشتری داشته باشید مقدار کمتری به عنوان ما بقی پولتان به شما بازگردانده خواهد شد.

سفر تراکنش از کیف پول تا بلاکچین



تمام پروسه ای که در این مقاله توضیح داده شد در اصل توسط کیف پول بیت کوین شما انجام می گردد. شما در کیف پولتان فقط مشخص می‌کنید چه مقداری را می‌خواهید به چه آدرسی منتقل کنید (در بعضی از کیف پول‌ها شما مقدار کارمزد تراکنش را هم خودتان می‌توانید تعیین کنید)، بعد کیف پولتان یک تراکنش همانند آن چیزی که دیدید درست می‌کند و با استفاده از کلید خصوصیتان که توسط کیف پول نگهداری می‌شود آن را امضا می‌کند، بعد کیف پولتان که خود یک گره بر روی شبکه بیت کوین دارد این تراکنش را در شبکه بیت کوین منتشر می‌کند. هر گره‌ای از شبکه که تراکنش شما به آن می‌رسد، ابتدا تراکنش شما را با استفاده از امضای دیجیتال، کلیدعمومی شما و هش کلید عمومی گیرنده تایید می‌کند و مجدد آن را در شبکه پخش می‌کند. این تراکنش در محلی به نام MemPool به انتظار ماین شدن توسط ماینرها می‌مانند تا اینکه یک ماینر تراکنش شما را در بلوک خود قرار دهد و بتواند آن بلوک را ماین کند و به بلاکچین اضافه کند، زمانی که بلوک حاوی تراکنش شما به بلاکچین اضافه شد آن تراکنش، انجام شده تلقی می‌شود) یا اصطلاحا Confirm می‌شود(، هرچه تعداد بلوک بیشتری بعد از این بلوک، ماین شود و به بلاکچین اضافه شود تعداد Confirm های تراکنش شما بیشتر می‌شود و تراکنش امن تر می‌شود. در اینفوگرافی فوق کل فرایندی که تراکنش های بیت کوین از ابتدا تا انتها طی می کنند، نشان داده شده است.

جمع بندی

تراکنش های بیت کوین؛ بعد از انجام شدن و گرفتن تاییدیه نهایی روی مرورگر بلاکچین آن قابل رویت هستند. شاید با دیدن آنها آنچه که حقیقتا پشت پرده اتفاق افتاده قابل درک نباشد. اما با خواندن این مقاله متوجه شدید؛ دنیای جذابی ورای آنچه دیده می شود در پروسه یک تراکنش بیت کوین وجود دارد. برای اطلاعات بیشتر راجع به بیت کوین میتوانید به مقالات زیر مراجعه کنید.

Whitepaper

{توضیحاتی و تعریفی از وایت پیپر ارائه شود}

وایت پیپر بیت کوین (چکیده)

بیت کوین یک نسخه کاملا همتا به همتا از پول نقد الکترونیک است که سبب انجام پرداختهای آنلاین می شود طوریکه مستقیما از یک طرف به طرف دیگر فرستاده می شود و نیازی به گذر از یک موسسه مالی (نهاد مرکزی واسطه) نیست. بخشی از این راه حل را امضا های دیجیتال فراهم می کنند اما اگر هنوز هم نیاز به یک شخص ثالث مطمئن باشد تا از خرج شدن دوباره ممانعت به عمل آید، در واقع مزایای اصلی این سیستم از دست می رود. این شبکه تراکنش ها را با تبدیل آنها به یک زنجیره مستمر بر پایه الگوریتم گواه اثبات کار (proof of work)هش محور برچسب زمانی می زند و سابقه ای را ایجاد می کند که بدون انجام دوباره گواه اثبات کار قابل تغییر نیست. طولانی ترین زنجیره نه تنها به عنوان گواه توالی رویداد های مشاهده شده عمل می کند بلکه ثابت می کند که از بزرگترین استخر قدرت پردازشی CPU تشکیل شده است. تا زمانی که اکثریت قدرت سی پی یو توسط نود هایی کنترل شود که در حمله به شبکه همکاری نمی کنند، بلدترین زنجیره ایجاد خواهد شد و مهاجمان را عقب می گذارند. این شبکه خودش نیازمند کمترین ساختار می باشد. پیام ها بر مبنای بهترین تلاش انتشار می یابند، نود ها می توانند شبکه را ترک کنند یا دوباره به خواست خود به آن ملحق شوند و طولانی ترین زنجیره اثبات کار را به عنوان مدرک آنچه اتفاق افتاده بپذیرند.

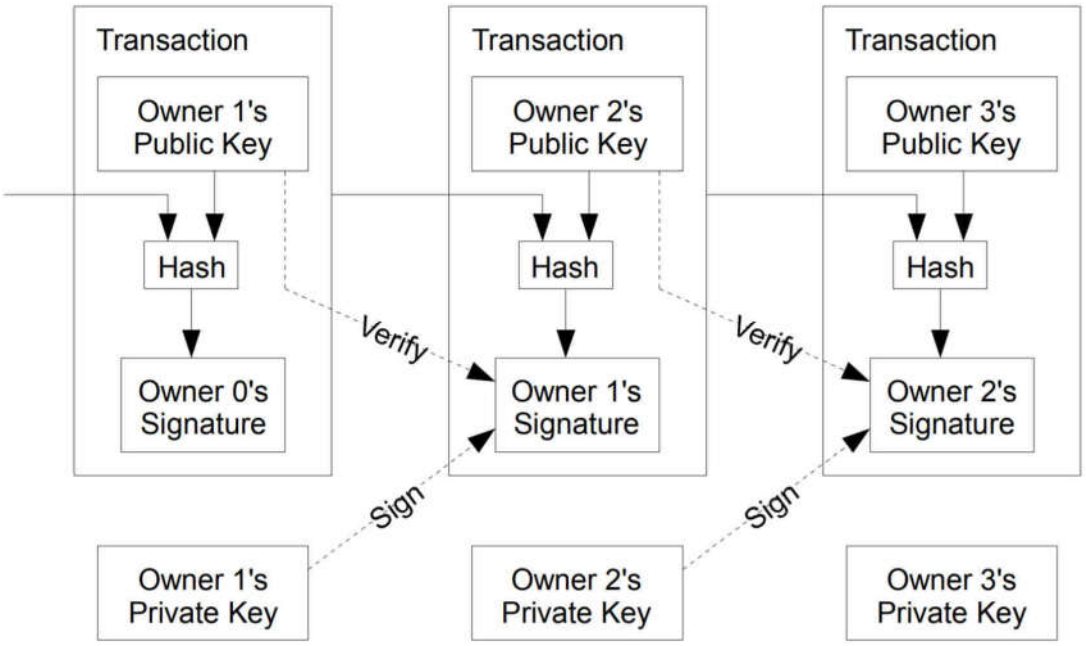
مقدمه

تجارت بر روی اینترنت تقریبا به طور انحصاری متکی بر موسسات مالی شده است که این موسسات به عنوان شخص ثالث مورد اعتماد برای پردازش پرداخت های الکترونیک عمل می کنند. در حالی که این سیستم برای اکثریت تراکنش ها به خوبی عمل می کند اما این سیستم یک ضعف ذاتی دارد و آن **وابستگی به اعتماد** است .تراکنش های کاملا غیر قابل برگشت در این مدل امکان پذیر نیست زیرا موسسات مالی این قدرت را دارند تا تراکنشی را به اختیار خود برگشت بزنند. هزینه این میانجی گری به افزایش هزینه تراکنش ها ختم می شود و امکان تراکنش های غیر رسمی کوچک را از میان بر می دارد و همچنین هزینه بیشتری برای فقدان توانایی پرداخت های غیر قابل برگشت موجود خواهد بود .با مطرح کردن امکان برگشت، نیاز به اعتماد بیشتر احساس می شود. در این حالت بازرگانان محتاط می شوند و درصد معینی از کلاه برداری غیر قابل اجتناب خواهد شد. این هزینه ها و شک و تردید ها در مورد پرداخت را می توان حضوری و با استفاده از پول فیزیکی حل کرد اما هیچ مکانیسمی برای انجام پرداختی بر روی یک کانال ارتباطی بدون نیاز به شخص ثالث موجود نیست.

آنچه امروزه مورد نیاز است یک سیستم پرداخت الکترونیک بر اساس تکنولوژی رمزنگاری است که جایگزین اعتماد شود و به هر دو طرف مشتاق اجازه دهد که مستقیما با همدیگر تراکنش داشته باشند و در این میان نیاز به شخص ثالث مورد اعتماد نباشد. تراکنش هایی که برگشت آنها از لحاظ محاسباتی غیر عملی است از فروشندگان در برابر تقلب محافظت می کنند. در این رساله، راه حلی برای مشکل **دوبار خرج کردن** با استفاده از سرور برچسب زمانی همتا به همتا پیشنهاد می شود و با استفاده از این راه حل، مدرک محاسباتی ترتیب زمانی تراکنش ها تولید می شود. این سیستم تا زمانی که نود های صادق مجموعا کنترل بیشتر قدرت CPU را به نسبت نود های مهاجم در دست داشته باشند، ایمن خواهد بود.

تراکنش ها

ما یک کوین دیجیتالی را به عنوان زنجیره ای از امضا های دیجیتال تعریف می کنیم. هر مالکی با استفاده از امضای دیجیتال هش بلاک قبلی، کوین و کلید عمومی فرد بعدی را انتقال می دهد و این موارد را به انتهای تراکنش جدید اضافه می کند. گیرنده وجه می تواند امضا ها را تایید کند و زنجیره مالکیت تایید شود.

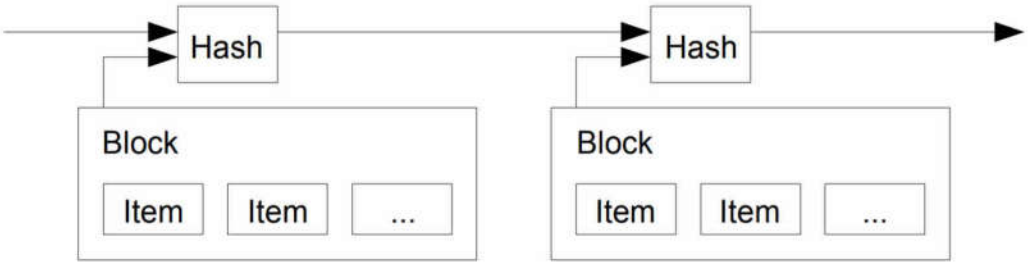


مشکل البته این است که دریافت کننده وجه نمی تواند تایید کند که یکی از مالکان این کوین را دو بار خرج کرده است یا نه. یک راه حل رایج، معرفی یک مقام متمرکز مورد اعتماد است که هر تراکنش را مورد بررسی قرار می دهد. بعد از تایید هر تراکنش، کوین باید به محل ضرابخانه (جایی که کوین جدید تولید می شود) برگردانده شود تا کوین جدیدی صادر شود و تنها کوین هایی که مستقیما از ضرابخانه صادر شده اند مورد اعتماد هستند .مشکل این راه حل این است که سرنوشت کل سیستم پول بستگی به شرکتی دارد که کوین را ضرب می کند و هر تراکنشی باید از طریق آنها انجام شود، درست مانند یک بانک.

اما ما به روشی نیاز داریم که دریافت کننده وجه بداند که مالکین قبلی پیش تر هیچ تراکنشی را امضا نکرده اند. در اینجا منظور از اولین تراکنش، آن تراکنشی است که شمرده می شود و بنابراین به تلاش های بعدی برای خرج کردن دوباره اهمیت داده نمی شود .تنها راه برای تایید غیاب یک تراکنش، اگاهی از همه تراکنش ها می باشد .در مدل ضرابخانه، آن شرکت ضرب کننده از تمامی تراکنش ها آگاه بود و تصمیم می گرفت که کدام یک از آنها اول صورت گرفته است. برای انجام این کار بدون نیاز به یک شخص مورد اعتماد، تراکنش ها باید به شیوه عمومی اعلام شوند و در اینجا نیاز به سیستمی است تا مشارکان بر روی یک تاریخچه مجزا در مورد سفارش دریافتی توافق کنند. گیرنده وجه نیاز به مدرکی دارد که ثابت کند در زمان هر تراکنش، اکثریت نود ها بر آن تراکنش توافق داشته و آن را اولین تراکنش محسوب کرده اند.

سرور برچسب زمانی(Timestamp Server)

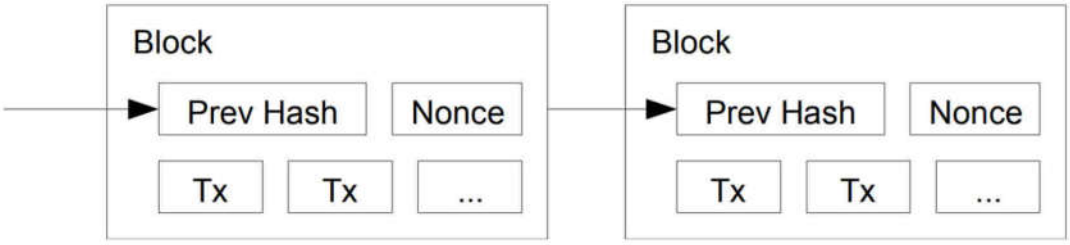
راه حل پیشنهاد شده در بالا با یک سرور برچسب زمانی شروع می شود و این سرور با برداشتن هش یک بلاک برای برچسب زمانی زدن و انتشار گسترده هش کار می کند و این شبیه کار یک روزنامه است .برچسب زمانی ثابت می کند که داده ها در آن زمان به منظور کنترل هش وجود داشته اند. هر برچسب زمانی شامل برچسب زمانی قبلی در هش خود می باشد که یک زنجیره را شکل می دهد و هر برچسب زمانی اضافه شده برچسب های پیشین را تقویت می کند.



گواه اثبات کار(Proof of Work)

برای پیاده سازی یک سرور برچسب زمانی توزیع شده در یک مبنای همتا به همتا، لازم است که از یک سیستم گواه اثبات کار مشابه Hashcashکه توسط Adam Back اختراع شده، استفاده کرد. گواه اثبات کار شامل جستجوی ارزش در زمانی است که هش صورت می گیرد مانند **SHA-256**که در آن هش با عدد صفر بیت شروع می شود. متوسط کار مورد نیاز در تعداد صفر بیتی های مورد نیاز نمایان گر است و می تواند با اجرای یک هش مجزا تایید شود.

برای شبکه برچسب زمانی، گواه اثبات کار با افزایش یک عدد اختیاری در بلاک پیاده سازی می شود و این ادامه می یابد تا زمانی که ارزشی پیدا شود که به هش بلاک، صفر بیت مورد نیاز را بدهد. زمانی که تلاش سی پی یو برای راضی کردن گواه اثبات کار گسترش یافت، بلاک بدون انجام دوباره کار، قابل تغییر نخواهد بود .از آنجا که بلاک های بعدی در زنجیره دنبال آن قرار می گیرند، کار تغییر بلاک شامل تغییر دوباره همه بلاک های بعد از آن است.



گواه اثبات کار همچنین مشکل تعیین نماینده را در اکثریت تصمیم گیری ها حل می کند. اگر اکثریت بر اساس مدل یک رای برای هر آی پی آدرس باشد، این می تواند توسط هر فردی که قادر به تخصیص آی پی های زیاد باشد دستخوش تغییر شود. گواه اثبات کار اساسا دارای مدل یک رای برای هر سی پی یو می باشد. تصمیم اکثریت توسط طولانی ترین زنجیره ارائه داده می شود که عظیم ترین تلاش گواه اثبات کار در آن زنجیره سرمایه گذاری شده است. اگر اکثریت قدرت سی پی یو توسط نود های صادق کنترل شود، این زنجیره صادق سریعتر از همه رشد می کند و زنجیره های رقیب و خرابکار را کنار می زند. یک مهاجم برای تغییر بلاک قبلی مجبور است که گواه اثبات کار آن و همه بلاک های بعد از آن را دوباره انجام دهد و بعد از این کارهاست که می تواند از کار نود های صادق سبقت گیرد و پیش بیافتد. در ادامه خواهید دید که احتمال موفقیت یک مهاجم با افزایش بلاک ها به طور فزاینده ای کاهش می یابد.

برای جبران سرعت سخت افزاری در حال افزایش و تغییر علاقه به مدیریت کردن نود ها به مرور زمان، سختی گواه اثبات کار توسط یک میانگین متحرک که عدد متوسطی از بلاک ها را در ساعت هدف می گیرد، تعیین می شود. اگر بلاک ها خیلی سریع تولید شده باشند، سختی نیز افزایش پیدا می کند.

شبکه

مراحل راه اندازی شبکه به شرح زیر می باشد:

۱ .تراکنش های جدید به همه نود ها فرستاده میشود.

۲ .هر نود تراکنش جدید را در یک بلاک قرار می دهد.

۳ .هر نود برای پیدا کردن صحت تراکنش با الگوریتم گواه اثبات کار شروع به فعالیت میکند.

۴ .وقتی که نودی به پاسخ درست رسید؛ بلاک را برای همه نود ها انتشار می دهد.

۵ .نود های دیگر تنها زمانی بلاک را می پذیرند که صحت تراکنش های آن را بپذیرند و قبلا خرج نشده باشد.

۶ .نود ها پذیرش بلاک را با کار کردن روی ایجاد بلاک بعدی در زنجیره ابراز می کنند؛ در این حالت از هش بلاک پذیرفته شده به عنوان هش قبلی استفاده می شود.

نود ها همیشه طولانی ترین زنجیره را به عنوان زنجیره درست تلقی می کنند و به کار کردن برای گسترش آن ادامه می دهند. اگر دو نود نسخه های متفاوتی از بلاک بعدی را به طور همزمان انتشار دهند، بعضی از نود ها یکی از این نسخه ها را زودتر دریافت می کنند. در این حالت این نود ها بر روی اولین نسخه ای که دریافت می کنند، کار خواهند کرد اما در صورتی که نسخه دیگر طویل تر شود، آن را ذخیره خواهند کرد. زمانی که گواه اثبات کار بعدی پیدا شود چنین رابطه ای بر هم زده می شود و یکی از این شاخه ها طویل تر خواهد شد. در این حالت، نود هایی که بر روی شاخه دیگر کار کرده اند به شاخه طولانی تر انتقال خواهند یافت.

انتشار تراکنش جدید لازم نیست که به تمامی نود ها برسد. زمانی که این تراکنش ها به نود های کافی برسند، طولی نخواهد کشید که تبدیل به یک بلاک خواهند شد. اگر یک نود بلاکی را دریافت نکند، در زمان دریافت بلاک بعدی آن را تقاضا می کند و غیاب یک بلاک را تشخیص می دهد.

انگیزه

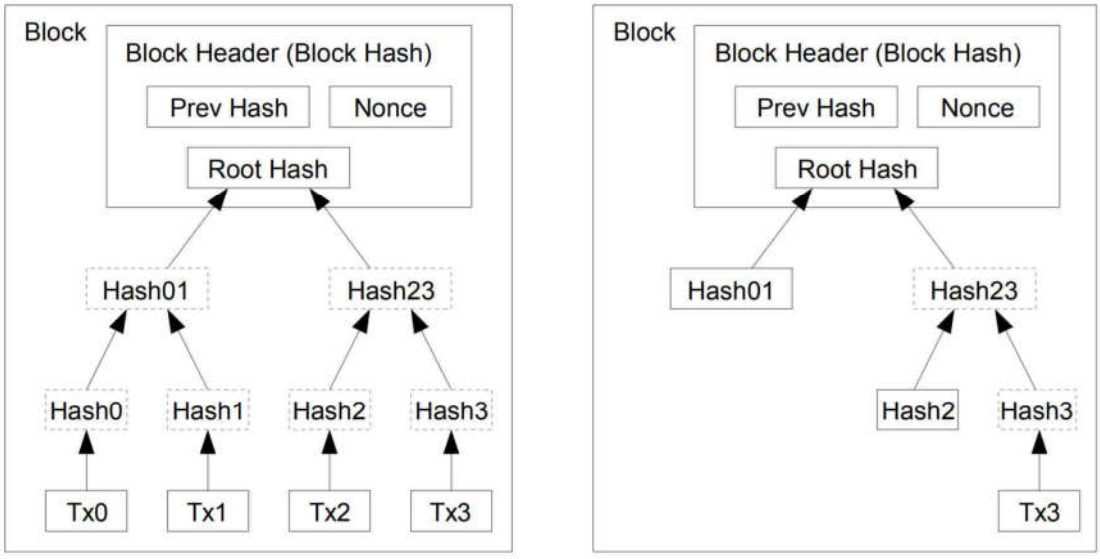
معمولا اولین تراکنش در یک بلاک تراکنش خاصی است که کوین جدیدی را شروع می کند و خالق بلاک، مالک آن خواهد شد. این انگیزه ای را برای نود ها ایجاد می کند تا از شبکه پشتیبانی کنند و شیوه ای را فراهم می کند که در ابتدا به توزیع کوین ها به داخل حلقه پرداخته شود زیرا مقامی مرکزی برای صادر کردن آنها وجود ندارد. اضافه شدن یکنواخت مقدار ثابتی از کوین های جدید قابل مقایسه با استخراج گران طلا است که منابع را برای افزودن طلا به چرخه مصرف می کنند. در مثال ما زمان، سی پی یو و الکتریسیته مصرف می شود.

این انگیزه را همچنین می توان از طریق کارمزد های تراکنش تامین وجه کرد. اگر ارزش خروجی یک تراکنش کمتر از ارزش ورودی آن باشد، این تفاوت به صورت کارمزد یک تراکنش خواهد بود که به ارزش انگیزه بلاک محتوی تراکنش اضافه می شود. وقتی که مقدار از قبل تعیین شده ای از کوین ها به چرخه داخل شدند، انگیزه را می توان تماما از کارمزد های تراکنش تامین کرد و کاملا از تورم آزاد شد.

این انگیزه ممکن است به نود ها کمک کند که صادق باقی بمانند. اگر یک مهاجم طماع قادر باشد که قدرت سی پی یو بیشتری از نود های صادق جمع کند، او باید بین استفاده از آن برای فریب مردم با پس گرفتن و دزدیدن پرداختی های خود و یا استفاده از آن برای تولید کوین های جدید یکی را انتخاب کند .برای چنین شخصی پیروی از قوانین سود بیشتری خواهد داشت زیرا تخلف از قوانین و ایجاد کوین های جدید برای آن فرد، سیستم را تضعیف خواهد کرد و اعتبار ثروت آن فرد را نیز از میان می برد.

احیای فضای دیسک

زمانی که آخرین تراکنش در یک کوین زیر بلاک های کافی پنهان شد، تراکنش های خرج شده قبلی را می توان رها کرد تا در فضای دیسک ذخیره شود. برای تسهیل این کار بدون شکستن هش بلاک، تراکنش ها به صورت درخت Merkle در خواهند آمد که تنها ریشه آن در هش بلاک داخل شده است. بلاک های قدیمی را می توان با بریدن شاخه های درخت فشرده کرد. هش های داخلی لازم نیست که ذخیره شوند.

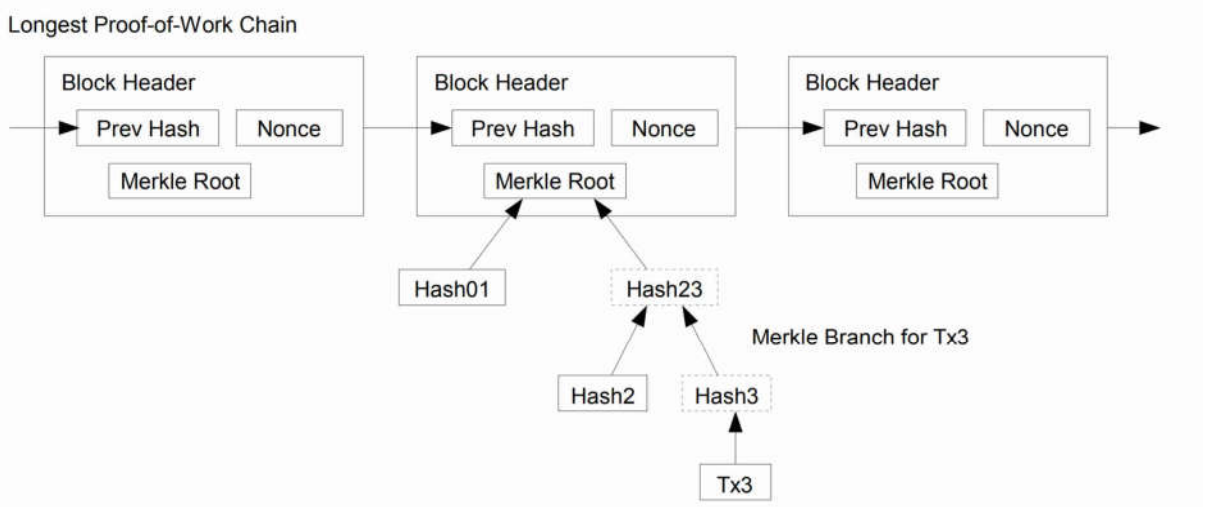


Transactions Hashed in a Merkle Tree — After Pruning Tx0-2 from the Block

یک هدر بلاک بدون تراکنش حدود ۸۰ بایت است. اگر فرض کنیم که بلاک ها هر ده دقیقه ایجاد شوند، این مقدار در سال ۴.۲ MB خواهد شد. معمولا سیستم های کامپیوتری که در سال ۲۰۰۸ فروخته میشدند ۲ گیگ رم دارند و بنا بر قانون مور (Moore) می توان پیش بینی کرد که رشد حال حاضر ۱.۲ GB در سال می باشد؛ حتی اگر هدر بلاک ها هم در حافظه نگه داری شوند مشکل ذخیره پیش نخواهد آمد.

تایید پرداخت تسهیل شده

تایید پرداختی ها بدون راه اندازی یک نود کامل نیز ممکن است. یک کاربر تنها نیاز است که یک کپی از هدر بلاک های درازترین زنجیره گواه اثبات کار را نگه دارد که این کاربر می تواند با بررسی نود های شبکه به این کپی دست یابد و قانع شود که او طولانی ترین زنجیره را دارد. این کاربر باید شاخه Merkle که تراکنش را به بلاکی که در آن برچسب زمانی شده مرتبط می کند، حفظ کند. او نمی تواند تراکنش را به تنهایی بررسی کند بلکه با مرتبط کردن آن به مکانی در زنجیره می تواند آن را انجام دهد؛ او می تواند ببیند که یک نود شبکه آن تراکنش را پذیرفته است و بلاک های اضافه شده بعد از آن بیشتر مورد پذیرش شبکه می باشد.

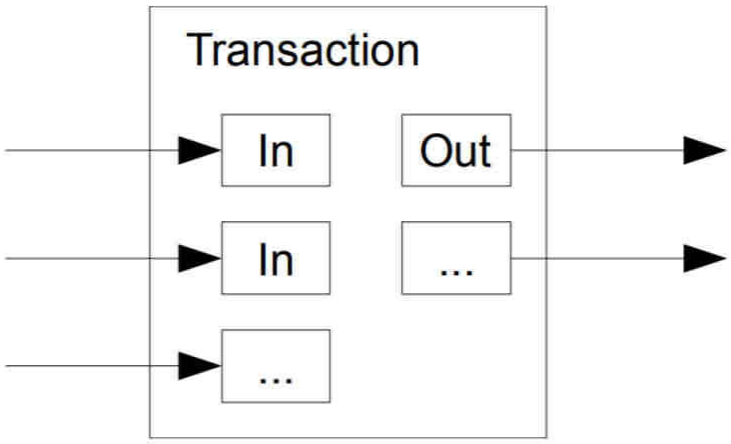


چنین تاییدی تا زمانی که نود های صادق شبکه را کنترل می کنند، قابل اعتماد است. اما زمانی که مهاجم در شبکه بیشتر قدرت بگیرد، این تایید آسیب پذیر خواهد بود. در حالی که نود های شبکه می توانند تراکنش ها را به تنهایی تایید کنند؛ این روش تسهیل شده می تواند توسط

یک مهاجم مورد سوء استفاده قرار بگیرد و تا زمانی که بر شبکه سیطره دارد، قادر به ایجاد تراکنش های جعلی خواهد بود. یک استراتژی برای محافظت در برابر این تهدید، پذیرفتن هشدار از جانب نود های شبکه می باشد که این هشدار ها در زمانی داده می شود که نود ها بلاک نامعتبری را شناسایی می کنند. این بلاک های نامعتبر نرم افزار کاربر را به فعالیت وا می دارند تا کل بلاک و تراکنش های هشدار داده شده را دانلود کند و این ناسازگاری را تایید کند. کسب و کار هایی که پیوسته پرداختی دریافت می کنند احتمالا هنوز بخواهند که نود های خودشان را برای امنیت مستقل تر و تایید سریعتر راه اندازی کنند.

ترکیب و تقسیم ارزش

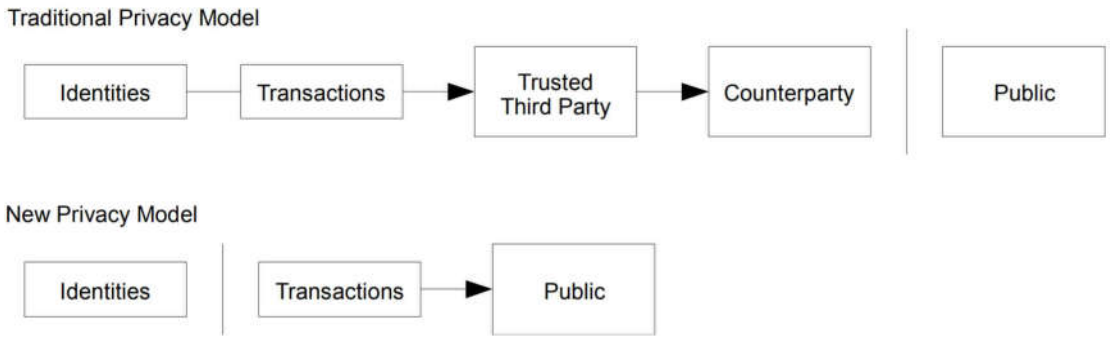
اگرچه مدیریت کوین ها به صورت فردی ممکن است اما انجام تراکنش جداگانه برای هر یک سنت (دلار) انتقالی دشوار می باشد. با اجازه دادن به تقسیم و ترکیب ارزش، تراکنش ها شامل ورودی ها و خروجی های متعددی می شوند. معمولا یا یک ورودی مجزا از تراکنش بزرگتر قبلی موجود خواهد بود یا ورودی های متعددی مقادیر کوچک تر را ترکیب می کنند و حداکثر نیز دو خروجی موجود خواهد بود: یکی برای پرداختی و دیگری برای بازگرداندن تغییر به فرستنده در صورتی که چنین تغییری موجود باشد.



البته این گنجایش خروجی باید مورد توجه قرار بگیرد که در آن یک تراکنش به چندین تراکنش وابسته است و آن تراکنش ها نیز بر بسیاری دیگر وابسته می باشند که البته این موضوع در اینجا مشکل نیست. هرگز نیاز به استخراج یک کپی کاملا مستقل از تاریخچه تراکنش نیست.

حریم خصوصی

مدل بانکداری سنتی با محدودیت دسترسی اطلاعات برای طرفین و تبدیل خود به یک شخص ثالث مورد اعتماد، تا حدودی حریم خصوصی ایجاد می کند. نیاز به اعلام همه تراکنش ها به صورت عمومی این مدل را در اینجا غیر ممکن می سازد اما هنوز هم می توان حریم خصوصی را با تجزیه جریان اطلاعات در مکان دیگر حفظ کرد و کلید های عمومی را ناشناس نگه داشت. عموم می توانند ببینند که فردی در حال فرستادن مقداری به فرد دیگر است اما اطلاعاتی که تراکنش را به فرد خاصی مرتبط کند، موجود نیست. این مشابه همان سطح اطلاعاتی است که توسط صرافی های سهام بیرون داده می شود که زمان و اندازه ترید های فردی که به آن tape گفته می شود، در معرض عموم قرار می گیرد اما مشخص نمی شود که طرفین تراکنش چه کسانی هستند.



یک جفت کلید جدید نیز به عنوان یک محافظ اضافی برای هر تراکنش به کار می رود و این باعث می شود که تراکنش ها به یک مالک مشترک مرتبط نشوند. در مورد تراکنش های با ورودی متعدد چنین ارتباطی هنوز غیر قابل اجتناب است و مالکیت ورودی ها توسط یک فرد خاص را برملا می کند. خطر در اینجاست که اگر مالک یک کلید آشکار شود، ارتباط می تواند تراکنش های دیگری را متعلق به همان مالک هستند، برملا سازد.

محاسبات

ما این سناریو را مورد بررسی قرار می دهیم که یک مهاجم سعی کند زنجیره دیگری را سریعتر از زنجیره اصلی (درست) ایجاد کند. حتی اگر چنین کاری انجام شود، سیستم را در معرض تغییراتی مانند ایجاد ارزش به صورت غیر منتظره یا برداشت پولی که هرگز متعلق به مهاجم نبوده، قرار نخواهد داد. نود ها یک تراکنش نامعتبر را به عنوان پرداختی نمی پذیرند و نود های صادق هرگز بلاکی را که محتوی آن است، قبول نخواهند کرد. یک مهاجم تنها می تواند سعی کند که یکی از تراکنش های خود را تغییر دهد تا پولی را که اخیرا خرج کرده، دوباره خرج کند.

رقابت بین زنجیره صادق و زنجیره مهاجم را می توان به عنوان Binomial Random Walk توصیف کرد. اگر زنجیره اصلی یک بلاک پیدا کند و رهبری خود را به اندازه +۱ افزایش دهد و اگر زنجیره مهاجم به اندازه یک بلاک گسترش یابد و خلا را به اندازه -۱ تغییر دهد، شکست حاصل خواهد شد و هک صورت می گیرد.

احتمال اینکه یک مهاجم بتواند کمبود ایجاد شده را جبران کند مشابه مسئله Gambler`s Ruin (نابودی قمارباز) می باشد. فرض کنید یک قمارباز که اعتبار نامحدودی دارد از یک کسری شروع می کند و احتمالا به دفعات نامحدود بازی می کند تا سر به سر شود. ما می توانیم احتمال سر به سر شدن او را محاسبه کنیم یا اگر به بحث خودمان برگردیم می توانیم احتمال اینکه یک مهاجم به زنجیره اصلی برسد را به صورت زیر محاسبه کنیم.

خب فرض کنیم P احتمال اینکه نود اصلی بلاک بعدی را پیدا کند، qاحتمال اینکه مهاجم بلاک بعدی را پیدا کند و q_z احتمال اینکه مهاجم بتواند z بلاک عقب افتاده را جبران کند.

اگر p بزرگتر از q باشد، احتمال به صورت نمایی و در حد زیاد کاهش می یابد زیرا تعداد بلاک هایی که مهاجم قصد جبران آن را دارد، افزایش پیدا می کند. در این حالت احتمالات بر ضد مهاجم است و اگر او در اوایل کار یک خیزش خوش شانسانه به سمت جلو نداشته باشد، شانسش بسیار کاهش می یابد و خیلی عقب می افتد.

حال به بررسی مدت زمانی می پردازیم که گیرنده یک تراکنش جدید باید منتظر باشد قبل از اینکه به اندازه کافی مطمئن شود که فرستنده نمی تواند تراکنش را تغییر دهد. فرض می کنیم فرستنده مهاجمی است که می خواهد گیرنده را قانع کند که برایش پرداختی ارسال کرده است، سپس این مهاجم بعد از مدتی پرداختی را برای خود بر می گرداند. وقتی که چنین چیزی روی می دهد، گیرنده هشدار دریافت می کند اما فرستنده امیدوار است که برای این کار دیر شده باشد.

گیرنده یک جفت کلید جدید را ایجاد می کند و کلید عمومی را به زودی و قبل از امضا به فرستنده می فرستد. این مانع از آماده کردن یک زنجیره بلاک پیش از موعد توسط فرستنده می شود. فرستنده این را با کار کردن پیوسته روی زنجیره انجام می دهد تا زمانی که به اندازه کافی خوش شانس باشد و پیش بیافتد و سپس تراکنش را در آن لحظه انجام خواهد داد. زمانی که تراکنش فرستاده شد، فرستنده ناصادق شروع به کار کردن سری بر روی زنجیره موازی می کند که شامل نسخه دیگری از تراکنش او است.

گیرنده تا زمانی که تراکنش به یک بلاک اضافه می شود، صبر می کند و z بلاک بعد از آن متصل می شود. گیرنده مقدار پیشرفت دقیق مهاجم را نمی داند اما فرض می کند که بلاک های صادق زمان مورد انتظار متوسط برای هر بلاک به طول بیانجامند. پیشرفت احتمالی مهاجم توزیع Poisson با ارزش مورد انتظار خواهد بود:

برای محاسبه احتمال اینکه مهاجم هنوز بتواند به جبران برسد، تراکم Poisson برای هر مقدار پیشرفتی که مهاجم می توانسته انجام دهد در احتمال جبران از آن نقطه ضرب می کنیم:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

برای اجتناب از جمع کردن دنباله نامحدود توزیع به تنظیم دوباره می پردازیم...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

حال به فرمول های بالا را در زبان C تبدیل به کد میکنیم....

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

تعدادی از نتایج را اجرا می کنیم و می بینیم که احتمال با z به طور ن مایی کاهش می یابد.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

حل برای p کمتر از ۰.۱ درصد...

```
P < 0.001
q=0.10    z=5
q=0.15    z=8
q=0.20    z=11
q=0.25    z=15
q=0.30    z=24
q=0.35    z=41
q=0.40    z=89
q=0.45    z=340
```

نتیجه گیری

در این طرح سیستمی برای تراکنش های الکترونیک بدون نیاز به اعتماد پیشنهاد شد. این نوشتار از قالب معمول کوین های ساخته شده از امضا های دیجیتال شروع شد که این مدل کنترل قاطع مالکیت را فراهم می کند اما بدون روشی برای اجتناب از حمله دوبار خرج کردن، این مدل ناقص خواهد بود. برای حل این مشکل یک شبکه همتا به همتا پیشنهاد شد که از گواه اثبات کار برای ثبت تاریخچه عمومی تراکنش ها استفاده می کرد. تغییر این تراکنش ها سریعا از لحاظ محاسباتی برای مهاجم غیر عملی می شود به شرطی که نود های صادق اکثریت قدرت

سی پی یو را کنترل کنند. این شبکه به دلیل ساختار غیر متمرکز آن قوی می باشد. نود ها همه با هم با هماهنگی کار می کنند. آنها نیازی به شناخته شدن ندارند زیرا پیام ها به مکان خاصی فرستاده نمی شوند و تنها نیاز است که بر مبنای بهترین تلاش تحویل داده شوند. نود ها می توانند شبکه را ترک کنند و به میل خود دوباره به آن بپیوندند و زنجیره گواه اثبات کار را به عنوان مدرک آنچه که در غیاب آنها انجام گرفته بپذیرند. آنها با قدرت پردازشی خود رای می دهند و پذیرش بلاک های معتبر را با کار بر روی توسعه آنها نشان می دهند. همچنین رد بلاک های نامعتبر با امتناع از کار بر روی آنها انجام می شود. هر گونه قانون و انگیزه مورد نیاز را می توان با استفاده از الگوریتم اجماع اعمال کرد.

کارمزد ارزهای دیجیتال

HASH rate چیست؟

خروجی یک تابع Hash که توسط یک سیستم اجرا می شود یک Hash می باشد که با توجه به توان محاسباتی آن دستگاه (کامپیوتر، ریگ، ASIC و ...) و همچنین الگوریتم Hash مورد استفاده (برای بیت کویت از الگوریتم SHA-256) زمان خاصی جهت تولید این Hash نیاز می باشد. به تعداد Hashهای تولید شده در ثانیه توسط آن دستگاه Hash rate دستگاه و به مجموع Hash rate همه ماینرهای متصل به هر بلاک چین Hash rate آن شبکه گفته می شود

به زبان ساده هش ریت سرعت عملکرد دستگاه ماینینگ می‌باشد. استخراج ارز دیجیتال (ماینینگ کریپتو) شامل یافتن بلاک ها از طریق محاسبات پیچیده می‌باشد. بلاک ها مشابه پازل های ریاضیاتی اند. دستگاه های ماینینگ باید هزاران یا حتی میلیون ها حدس در ثانیه بزنند تا جواب صحیح برای حل بلاک بیابند.

به عبارت دیگر برای استخراج موثر یک بلاک، ماینر باید طوری هِدرِ بلاک را هش کند که کمتر یا برابر با هدف (تارگت) شود. با تغییر سختی، هدف نیز تغییر می‌کند. برای رسیدن به هش (یا هدف) مورد نظر، ماینر باید بعضی از هدرهای بلاک که نانس (nonce) نام دارند را تغییر دهد. هر نانس با "۰" شروع شده و برای رسیدن به هش (یا هدف) ضروری افزایش می‌یابد. از آن جا که تغییر نانس کاملا تصادفی می‌باشد، احتمال رسیدن به هش (یا هدف) مورد نظر بسیار کم است. بنابراین ماینر با تغییر نانس باید تلاش زیادی کند. تعداد دفعاتی که ماینر در ثانیه برای رسیدن به هش تلاش می‌کند را هش ریت یا قدرت هش می‌گویند.

اندازه گیری هش ریت و واحدهای آن

واحد اندازه گیری هش ریت، هش در ثانیه h/s می‌باشد. بعضی از اصطلاحات رایج مورد استفاده شامل مگا، گیگا و ترا است که براساس تعداد هش ها گفته می‌شوند. برای مثال دستگاهی با سرعت ۶۰ هش در ثانیه ، هنگام تلاش برای حل کردن بلاک، ۶۰ حدس در ثانیه می‌زند. برای ۱۰۰۰ هش از کیلوهش KH/s ، برای ۱۰۰۰ کیلوهش از مگاهش MH/s ، برای ۱۰۰۰ مگاهش از تراهش TH/s و برای ۱۰۰۰ تراهش از پتاهش PH/s استفاده می‌شود.

دستگاه های مختلفی که برای استخراج ارزهای دیجیتال متفاوت به کار گرفته می‌شوند دارای هش های برابر نیستند. برای مثال، یک دستگاه ماینینگ بیت کوین هش ریت متفاوتی با دستگاه ماینینگ اتریوم دارد. این موضوع را با الگوریتم های متفاوتی که ارزهای دیجیتال به کار می‌گیرند می‌توان توضیح داد، زیرا برای استخراج آن ها از میزان حافظه و محاسبات یکسان استفاده نمی‌شود.

رابطه بین هش ریت، سودآوری ماینر و سختی استخراج

هش ریت، سودآوری ماینر و سختی استخراج از چند طریق به هم وابسته اند. برای مثال بیت کوین را در نظر می‌گیریم. هربار که سختی شبکه بیت کوین افزایش می‌یابد، هش ریت نیز زیاد می‌شود و به دنبال آن، ماینر ۱۲.۵ بیت کوین BTC و کارمزد تراکنش را به دست می‌آورد. تعداد ماینرها در شبکه بیت کوین، سختی را افزایش می‌دهد زیرا ماینر باید حدس های بیشتری در ثانیه محاسبه کند.

تاثیر برق مصرفی بر سودآوری

برای سودآوری، بیت کوین را در نظر می‌گیریم. در حال حاضر یک دستگاه ماینینگ بیت کوین نظیر ASIC تقریبا قدرت ماینینگ ۱۲ تراهش در ثانیه دارد. با در نظر گرفتن سختی حال حاضر شبکه، این دستگاه می‌تواند ۰.۳۱۸ بیت کوین BTC در سال تولید کند.

هرچند هنگام محاسبه سودآوری، باید هزینه برق مصرفی تجهیزات ماینینگ را در نظر بگیرید. به این مورد، بازده (راندمان) ماینر می‌گویند. افزایش سختی ماینینگ ارز دیجیتال، هزینه های برق مصرفی را نیز بیشتر می‌کند. برای مثال، یک دستگاه ماینینگ با ۱۰ درصد هش ریت بیشتر نسبت به دستگاهی دیگر، ۵۰ درصد بیشتر برق مصرف می‌کند. بنابراین، هرچند هش ریت عاملی مهم در ماینینگ می‌باشد، اما همواره راندمان را نیز در نظر بگیرید.

Testnet

سختی شبکه

سختی شبکه مقدار زمانی‌ست که یک ماینر بتواند یک بلاک را استخراج کند و بلاک بعدی را برای فرآیند استخراج استارت بزند، برای این کار یک سختی در نظر گرفته میشه که ساخت این بلاک از یک زمانی بیشتر یا کمتر نشود، این سختی برای اینکه در همان بازه زمانی تعریف شده همیشه ثابت بماند هر ۲هفته یک‌بار تنظیم می‌شود، به‌طوری که ساخت یک بلاک را در بازه ثابت ۱۰ دقیقه سعی دارد که تنظیم نماید. بنابراین تا الان متوجه شدیم که یک مدت زمان بین ساخت ۲بلاک(در بیت‌کوین) داریم و آن مدت زمان ۱۰دقیقه هست که با سختی شبکه تنظیم می‌شود.

سختی شبکه برای این مهم است که تضمین می‌کند در هر زمان که شبکه استخراج کنندگان چه زیاد شوند چه کم شوند توجیح زمانی که بین ساخت هر ۲بلاک باشد به میزان ۱۰ دقیقه انجام بگیرد، یعنی هرچقدر تعداد ماینرها زیاد و کم شوند سختی شبکه به تناسب آن طوری خودش را تنظیم کند که نهایتا به‌طور میانگین تولید هر بلاک ۱۰دقیقه زمان ببرد. فرض کنید اگر این سختی ثابت باشد، با اضافه شدن ماینرها میزان اضافه شدن هر بلاک کمتر می‌شود.

سختی شبکه هر ۲۰۱۶ بلاک تغییر می‌کند، که همان ۲ هفته یکبار است، در واقع ۲۰۱۶ بلاک ۲۰۱۶ تا ۱۰ دقیقه زمان باید صرف بشود که بعد از آن تغییر سختی شبکه انجام بگیرد، اما یک نکته هم وجود دارد، اینکه اینجا ۱۰ دقیقه زمانِ ثابتی نیست، یعنی به طور میانگین ۱۰ دقیقه می‌باشد به هر حال برای محاسبه نیاز است که ۲۰۱۶ رو ضرب در ۱۰(دقیقه) کنیم، حالا اگر ماینرها به نحوی استخراج کنند که میانگین ۹ دقیقه بشود، مدت زمان تغییر سختی شبکه تغییر می‌کند و ۲۰۱۶ ضرب در ۹ (دقیقه) می‌شود. وقتی سختی شبکه کمتر از ۱۰ دقیقه باشد زمان ماینِ هر بلاک در ۱۰ دقیقه و در وسعت ۲۰۱۶ بلاک، بیشتر از ۱ میشه، به این معنی که در هر ۱۰ دقیقه یک رابطه ۱.۱ به وجود می‌آید که به زبان ساده می‌گوید در هر ۱۰ دقیقه ما ۱بلاک و ۱دهمِ بلاک داریم، که از این طریق بدست می‌آید:

Expected / actual

20160 / actual

۲۰،۱۶۰ حاصل ضربِ ۱۰ دقیقه در ۲۰۱۶ بلاک است که در حالت ایده آل نیاز می‌باشد.

20160 / 18144 = 1.11

۱۸،۱۴۴ هم حاصل ضرب ۹ در ۲۰۱۶ است، و نسبت دوم هم که نسبت حالت ۱۰ دقیقه به حالت ۹ دقیقه است. به همین جهت این نسبت سختی جدید برای شبکه تعیین می‌شود که به صورت رابطه زیر نمایش داده شده:

Difficulty * 1.11 = new difficulty

حال ۲شرط داریم:

- اگر عددِ نسبت بزرگتر از ۱ باشد(به این معنی که بلاک ها سریعتر از حالت ایده آل(۱۰ دقیقه) استخراج شده اند)، پس بنابراین باید سختی شبکه زیاد شود که به سمت ۱۰ دقیقه ایده آل برسد.
- اگر عددِ نسبت کمتر از ۱ باشه(به این معنی که بلاک ها کمتر از حالت ایده آل(۱۰ دقیقه) استخراج شده اند)، بنابر این باید سختی شبکه کمتر شود تا شبکه به سمت ۱۰ دقیقه مورد نظر برسد.

و به این صورت سختی برای ۲۰۱۶ بلاک آینده که دوباره تا آن زمان با تعداد ماینرهای آن سنجیده خواهد شد تنظیم می‌شود. باید در نظر داشت سختی زمانی که تنظیم می‌شود به گونه‌ای هست که از یک محدوده خاص بیشتر یا کمتر نمی‌تواند برود(حداقل یک‌چهارم برابر و حداکثر ۴برابر)، و بیشتر از حداکثر و کمتر از حداقل ممکن نیست.

فرض کنیم فردی به شما تعدادی از اعداد بین ۱ تا ۱۰۰ داده می‌شود. شما می توانید در هر دقیقه یک عدد بین ۱ تا ۱۰۰ به صورت تصادفی انتخاب کنید، اینقدر این انتخاب را می‌توانید انجام دهید تا به عدد که آن فرد مد نظرش هست برسید .فرض می‌کنیم فرد عدد ۵۰ را در نظر گرفته است. براساس اینکه شما در هر۱ دقیقه تنها قادر به یک شماره بین ۱ تا ۱۰۰ هستید بنابراین این مورد ۲ دقیقه زمان می‌برد. اما این خیلی آسان است، بنابراین هدف را به ۲۰ تغییر می دهیم، حالا شما می‌توانید هر ۱/۵ امتحان کنید، به معنی اینکه هر ۵ دقیقه یک بار بدست بیاورید. هرچه هدف کم‌تر باشد، رسیدن به عدد صحیح دشوارتر می‌شود. شاید شما بار اول که عددی را انتخاب می‌کنید خوش شانس باشید و مستقیما ۲۰ را انتخاب کنید، ولی در بلند مدت به همان ۵ دقیقه خواهید رسید و یعنی به صورت هر ۵ دقیقه به عدد می رسید. بنابراین بر اساس میزان انتخابی که شما می توانید در هر دقیقه انجام دهید، می توانید از مقدار هدف استفاده کنید برای اینکه چه میزان زمان طول بکشد تا عدد صحیح مورد نظر بدست بیاید.

معرفی سختی شبکه

در اینجا سر و کار با کامپیوتر است و کامپیوتر می تواند بجای اینکه به طور مستقیم به هدف اشاره کند آن را به تقسیماتی از محدوده ای از اعداد تبدیل کند که از درون آن اعداد جدیدی بدست بیاورد که نهایتا به جواب یا هدف مسئله برسد. این شماره جدید همان سختی شبکه هست، که خیلی ساده می‌شود از آن استفاده کرد برای تغییر مقدار عدد مورد نظر و به تناسب آن طول زمان مورد نظر، تمام این فرآیند در رابطه زیر نشان داده شده است:

Target = targetmax / difficulty

نمونه های مختلفی رو برای مثال در زیر می‌بینیم که با تغییر سختی شبکه چطور طولِ پیدا کردن هدف را سخت‌تر می‌شود کرد:

هر چه سختی بالاتر باشد، هدف پایین تر است

شبکه بیت کوین

شبکه بیت‌کوین همانند مثال ساده که در بالا گفته شد کار می کند، به این منظور فرآیند هشینگ کاندید بلاک انجام می‌گیرد تا ماینرها بتوانند بهترین شانس‌های خودشان را امتحان کنند تا به عدد مورد نظر برسند، در اینجا ماینرها امیدوارند که محدوده بازه ای کمتری را بتوانند انجام بدهند که سریعتر به عدد مورد نظر برسند.

و همان طور که می‌بینید ماینر ها قادر به تولید هزاران مقادیر درهم سازی (hash values)در دقیقه هستند، بیت کوین به طرز مضحکی از اعداد بزرگ استفاده می‌کند

از آنجایی که هزاران ماینر در حال تلاش برای بدست آوردن شانس خود هستند، بنابراین طوری این مقدار تغییر می‌کند که اطمینان حاصل شود میزان کم و زیاد شدن ماینرها به اندازه ۱۰ دقیقه(نه چند ثانیه) زمان خواهد برد، بنابراین عدد های هدف به تناسب ماینرها متغییر هستند.

با توجه به اینکه اعداد سختی شبکه بزرگ به نظر می‌رسد رسیدن به هدف هم مثل یک لاتاری بسیار دشوار است.

می‌توان با وارد کردن دستور getdifficulty در کنسول رفرنس کلاینت بیت‌کوین(فول‌نود) خود به این موضوع رسید. همینطور می‌توان سختی شبکه را توسط فرمان getmininginfo مشاهده کرد.

پارامتر nonce

Nonceیک بخش مرکزی از الگوریتم ماینینگ proof of work برای تکنولوژی بلاک چین‌ها و ارزهای دیجیتالی مانند بیت کوین است. ماینرهای ارزهای دیجیتال بر سر پیدا کردنnonce ی که به وسیله‌ی آن بتوانند هشی با قدرت پردازش کمتر یا برابری از سختی‌های موجود در شبکه تولید کنند، با یکدیگر رقابت دارند. اگر ماینری بتواند یک nonce پیدا کند، nonceمورد نظر "golden nonce" نامیده می شود و پس از آن، ماینرها می توانند یک بلاک به بلاک چین اضافه کرده و پاداش دریافت کنند. Nonce یک عدد تصادفی است.

ماینرها در هر ثانیه، میلیون‌ها nonces را آزمایش کرده و آن‌ها را از بین می برند. بیشتر ماینرها به این امید هستند که هشی تولید کنند که از طریق آن بتوانند به هدف خود رسیده و پاداش دریافت کنند. بنابراین، این چیزی است که در طول مراحل ماینینگ PoWدر سطح بنیادی رخ می دهد.

ایجاد بلاک‌ها به وسیله‌ی Nonces!

Nonceیک عدد (شماره) ۳۲ بیتی است. این پارامتر همراه با داده‌های کلیدی‌ای مانند برچسب زمانی در بلاک هدر (block header) باقی می مانند. هنگامی که ماینرها شروع به ساخت بلاک‌ها می کنند، به صورت رندوم یک nonce انتخاب کرده و آن را در بلاک هدر قرار می دهند سپس یک هش جدید در بلاک هدر ایجاد می شود.

هش یک عدد ۲۵۶ بیتی است که با صفرهای زیادی شروع می شود، یعنی به طور باور نکردنی‌ای، ارزش کوچکی دارد. اگر تعداد صفرها کافی نباشند، ماینر، هش ایجاد شده را از بین می برد و تلاش می کند که یک nonce جدیدی پیدا کند! این فرآیند تا زمانی تکرار می شود که ماینر بتواند یک nonce ی پیدا کند که از طریق آن، یک هشی که ارزشی برابر یا کمتر از سختی‌هایی که در شبکه وجود دارد، تولید کند.

اندازه ۳۲ بیتی nonce به این معنی است که احتمال چهار میلیارد ترکیبِ ممکن وجود دارد. Nonceتنها پارامتری است که یک ماینر آن را تغییر می دهد و بقیه‌ی پارامترها ثابت هستند. بنابراین، اگر ماینری بتواند یک golden nonce پیدا کند، می تواند یک بلاک به بلاک چین اضافه کرده و پاداش دریافت کند. در حال حاضر، هیچ راهی برای سرعت بخشیدن به منظور پیدا کردن nonce مورد نظر وجود ندارد. این بدین معنی است که ماینرها، بارها آزمون و خطا انجام می دهند تا بتوانند یک golden nonce پیدا کنند.

سختی‌های موجود در فرآیند ماینینگ!

همانگونه که در بالا گفتیم، ماینر، در تلاش برای پیدا کردنnonce ی است که بتواند به وسیله‌ی آن، هشی تولید که ارزش آن کمتر از سختی‌های موجود در شبکه باشد. پروتکل بیت کوین، سختی‌های فرآیند ماینینگ را تعیین می کنند. بنابراین، اگر سختی‌های موجود افزایش پیدا کنند، مقدار هدف برای هش نیز کاهش پیدا می کند. این به این معنی است که در ابتدای عدد هش، تعداد زیادی صفر وجود خواهد داشت. با تمام این شرایط، احتمال پیدا کردن هشی با ارزش کمتر، کاهش پیدا می کند و ماینرها بایدnonce های زیادی را آزمایش کنند. هنگامی که یک ماینر، بلاکی را هش می کند، مقدار هش باید برابر یا کمتر از تعداد اهداف باشد تا بتواند موفق شود.

هنگام ماینینگ رمزارز بیت کوین، سختی‌های موجود در شبکه در هر ۲۰۱۶ بلاک ، مطابقت داده می شوند. این در حالی است که PoW blockchainهای دیگر، تنظیمات سریع تری را انجام می دهند. به عنوان مثال، رمزارز لیت کوین به دلیل زمان بلاک کوتاه تر آن، در هر سه و روز نیم، سختی‌های موجود در شبکه‌اش تنظیم شده و مطابقت پیدا می کنند. این در حالی است که، Digibyteسختی‌های موجود در شبکه‌ی خود را در هر بلاک تنظیم می کند. همچنین، اگر سختی‌های موجود در شبکه برطرف نشوند، یک رابطه‌ی خطی بین قدرت هش و پاداش بلاک به وجود خواهد آمد.

قرارداد هوشمند Smart contract چیست ؟

قرارداد هوشمند یک پروتکل برای تنظیم قراردادها است. یک قرارداد هوشمند، یک پروتکل ویژه است که برای مشارکت، تأیید یا اجرای مفاد یک قرارداد خاص، فعال می شود. قراردادهای هوشمند معاملات و فرایند ها را به صورت کاملا تضمینی و بدون اشخاص ثالث انجام می دهند. فعالیت و ثبت های قرارداد هوشمند قابل پیگیری و غیر قابل برگشت هستند. قراردادهای هوشمند شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای تمام اقدامات هدف گذاری شده به طور خودکار می شوند.

قراردادهای هوشمند چگونه ظاهر شدند؟

این ایده ابتدا توسط دانشمند کامپیوتر و رمز نگاری، نیک سابو در سال ۱۹۹۴ مطرح شد. او اصول اصلی کار را تعریف کرد، اما در آن زمان فضای مناسب برای تحقق ایده ها وجود نداشت. با ظهور فناوری بلاک چین، ایده ی قرارداد های هوشمند عملیاتی شد. بیت کوین به عنوان اولین ارزدیجیتال غیرمتمرکز جهان پایه گذار نوعی قرارداد در بلاک چین بود اما پروتکل بیت کوین فقط با هدف ایجاد یک ارز خصوصی توسعه یافته بود و نمی توانست تمام نیاز ها و فرایند ها را انجام دهد. اتریوم امکان ایجاد قراردادهای هوشمند را برای تمام پروژه ها عملی کرد و گام نوینی در جهت هوشمند سازی جهان برداشت.

قراردادهای هوشمند چگونه کار می کنند؟

برای درک بهتر می توان اینگونه آن ها را توصیف کرد: آن ها مانند دستگاه های فروش خودکار فعالیت می کنند. وقتی شما قصد خرید یک نوشابه با استفاده از این دستگاه ها را دارید، پول را به دستگاه وارد می کنید و دستگاه به صورت خودکار پول شما را پردازش می کند و نوشابه را تحویل می دهد. جدا از مسائل فنی، قرارداد های هوشمند هم تقریبا مانند دستگاه های فوق کار می کنند. بدون نیاز به افراد یا سازمان های واسطه فرایند پرداخت یا اجرای یک قرارداد را پردازش می کنند و در صورت صحیح بودن مفاد قرارداد مشخص شده، فعالیت را انجام می دهند. آن ها تنها دستورالعمل هایی را که به آن ها داده شده را به طور خودکار اجرا می کنند. در ابتدا، دارایی ها و شرایط قرارداد، کد گذاری می شوند و در بلاک بلاک چین قرار می گیرند. این قرارداد بین نود های پلتفرم توزیع و چندین بار کپی شده است. بعد از پردازش انجام شد، قرارداد مطابق با شرایط مشخص شده اجرا می شود. شاید برایتان سوال باشد که هوشمند سازی فرایند ها خیلی وقت است که انجام می شود اما تفاوت فرایند قرارداد های هوشمند با فرایند های معمولی در اینترنت غیرمتمرکز بودن و عدم بازگشت آن است. مثلا تراکنش های بانکی به صورت هوشمند انجام می گیرند اما مثلا بانک مرکزی میتواند جلوی یک تراکنش را بگیرد. در قرارداد های هوشمند شخص یا نهادی قادر به کنترل یک قرارداد نیست و وقتی مفاد یک قرارداد صحیح باشد، این قرارداد به صورت کاملا خودکار اجرا می شود.

برای ایجاد یک قرارداد هوشمند به موارد زیر نیاز است:

- موضوع قرارداد (Subject of the contract) : این برنامه باید به محصول یا خدمات تحت قرارداد دسترسی داشته باشد تا به طور خودکار آن ها را در عرضه یا خرید کنترل کند.
- امضای دیجیتال : همه شرکت کنندگان با امضای قرارداد با کلید خصوصی خود، توافقنامه را آغاز می کنند.
- شرایط قرارداد : شرایط قرارداد هوشمند به شکل دقیق دنباله ای از عملیات است. همه شرکت کنندگان باید این شرایط را امضا کنند.
- پلتفرم انحصاری : قرارداد هوشمند به بلاک چین یک پلتفرم خاص صادر می شود و در میان نودهای پلتفرم مورد نظر توزیع می شود.

کاربرد قرارداد های هوشمند در زندگی واقعی

- انتخابات : نتایج رأی گیری در بلاک چین قرار خواهد گرفت و در میان نودهای شبکه توزیع می شود. تمام داده ها رمزنگاری شده و ناشناس هستند. این روش از هرگونه دستکاری یا تقلب در انتخابات جلوگیری می کند.
- مدیریت : به عنوان مثال می توان قراردادی برای پرداخت حقوق به کارمندان نسبت به ساعات فعالیت تنظیم کرد.
- بیمه : پرداخت خودکار خسارت با قراردادهای هوشمند و ...
- همچنین از قرارداد های هوشمند می توان در سیستم هایی مثل بانکداری، حمل و نقل، ردیابی و اینترنت اشیا استفاده کرد.

مزایای قراردادهای هوشمند چیست؟

- امنیت : قرارداد هوشمند رمزنگاری شده و بین نود ها توزیع می شود. این موضوع تضمین می کند که فقط با خواست طرفین قرارداد متوقف خواهد شد.
- صرفه جویی در وقت و هزینه : اکثر فرایندها به صورت خودکار صورت می گیرد و اغلب واسطه ها حذف می شوند.
- شخصی سازی : در حال حاضر طیف وسیعی از انواع مختلف قراردادهای هوشمند وجود دارد. شما می توانید یکی را انتخاب کنید و آن را با توجه به نیازهای خود ویرایش و شخصی سازی کنید.

مشکلات قراردادهای هوشمند چیست؟

- عامل انسانی : کد قرارداد ها توسط برنامه نویسان نوشته می شود احتمال اشتباه وجود دارد. اگر قرارداد هوشمند در بلاک چین ثبت شود، دیگر نمی توان تغییر داد. مثال خوبی از خطای انسانی پروژه DAO است. اشتباهات برنامه نویسان در کدنویسی مشکلات زیادی را به وجود آورد – برخی از هکرها از اشتباهات سوء استفاده کردند و ۶۰ میلیون دلار به سرقت بردند
- وضعیت قانونی : در حال حاضر، قراردادهای هوشمند توسط همه دولت ها پذیرفته نیستند. بنابراین اگر نهادهای دولتی تصمیم به ایجاد یک چارچوب قانونی برای قراردادهای هوشمند داشته باشند، مسائل جدیدی به وجود خواهد آمد.
- هزینه های پیاده سازی : قراردادهای هوشمند بدون برنامه نویسی قابل اجرا نیست. باید یک یا چند برنامه نویس ماهر داشته باشید تا قراردادهای هوشمند به خوبی تنظیم شوند.

برنامه غیر متمرکز DApp

یکی از مشکلات ساختار غالب اینترنت این است که اطلاعات کاربران به صورت متمرکز در سرورهایی ذخیره می‌شود. در نتیجه، مدیران شرکت‌های صاحب این سرورها (از جمله شبکه‌های اجتماعی) نیز به این اطلاعات دسترسی دارند. در این میان، نرم افزار غیرمتمرکز می‌تواند راه‌حلی برای این مساله باشد. نرم افزار غیرمتمرکز (Distributed Application) را به صورت اختصاری dApp می‌نامند. این دسته از برنامه‌ها بر بستر بلاک چین اجرا می‌شوند و نیاز به سرور مرکزی ندارند.

به طور کلی می‌توان گفت که نرم افزار غیرمتمرکز دارای چهار ویژگی است. اگر یک نرم افزار همه این ویژگی‌ها را همزمان نداشته باشد، نمی‌تواند در دسته بندی نرم افزار غیرمتمرکز جای گیرد. این چهار ویژگی به شرح زیر است:

۱.متن باز (اپن سورس): کدهای منبع باید برای همه کاربران در دسترس باشد.

۲ .غیرمتمرکز: از فناوری رمزگذاری مشابه بلاک چین استفاده کند.

۳ .دارای جنبه تراکنش مالی: نرم افزار دارای توکن و یا دارایی دیجیتال باشد.

۴ .الگوریتم/پروتکل: توکن‌هایی ایجاد کند و دارای سازوکار درونی برای توافق عمومی کاربران باشد.

عملکرد نرم افزار غیرمتمرکز به چه شکل است؟

یک نرم افزار غیرمتمرکز با چهار معیار ذکر شده در بالا کار می‌کند. به کلامی دیگر، یک نرم افزار غیرمتمرکز یک پلتفرم متن باز است که بر روی بلاک چین غیرمتمرکز عمل می‌کند. همچنین توکن‌هایی خاص را مورد استفاده قرار می‌دهد که توسط یک پروتکل/الگوریتم مشخص تولید شده است. متن باز بودن نرم افزار غیرمتمرکز موجب می‌شود همه بتوانند کدهای آن را مشاهده کرده و در توسعه آن مشارکت کنند. این امر فرآیند مقیاس‌پذیری توسعه محصول را نیز تسریع می‌کند. گام بعدی نیز قرار دادن نرم افزار مورد نظر بر روی بلاک چین است. بلاک چین به عنوان یک دفتر کل دایمی عمل می‌کند و همه اطلاعات و تراکنش‌ها را برای همیشه در خود ثبت می‌کند. برای ثبت داده‌ها یا تراکنش‌ها بر روی بلاک چین باید پاداشی به گره‌های شبکه پرداخت شود. برای این کار از توکن‌ها استفاده می‌شود. توکن‌ها نیز توسط الگوریتم یا پروتکل‌هایی مشخص استخراج می‌شوند. دو پروتکل معروف برای استخراج ارزهای دیجیتال به ترتیب گواه اثبات کار) که توسط بیت

کوین استفاده می‌شود) و نیز گواه اثبات سهام (که توسط دش استفاده می‌شود) هستند. پلتفرم‌های بلاک چین متفاوتی برای توسعه نرم افزار غیرمتمرکز وجود دارد. در مطلبی مجزا با عنوان (فهرست ۸ پلتفرم بلاک چین برتر و مقایسه آنها) به بررسی دقیق‌تر چند پلتفرم اصلی پرداختیم.

اتریوم: بستری برای نرم افزار غیرمتمرکز

اتریوم پروتکلی است که امکان ساخت انواع نرم افزار غیرمتمرکز را به کاربران می‌دهد. اتریوم در واقع یک شبکه بلاک چین را در اختیار کاربارن قرار می‌دهد. هر کاربری می‌تواند بر اساس این بستر، نرم افزار غیرمتمرکز و یا قراردادهای هوشمند خود را بنویسد. تعریف مقررات و شرایط انجام تراکنش و نیز عملیاتی که باید در تراکنش به انجام برسد نیز در اختیار کاربر قرار دارد. در مجموع، سه نوع نرم افزار غیرمتمرکز در اتریوم وجود دارد.

آشنایی با سه شکل اصلی نرم افزارهای غیرمتمرکز

شاید بسیاری از طرفداران الگوی غیرمتمرکز مبتنی بر بلاک چین (به ویژه اتریوم (با خود فکر کنند که می‌توان همه چیز را بر اساس این الگو ایجاد کرد. اما واقعیت این است که چند دسته اصلی از کاربردها را می‌توان برای این فناوری متصور شد. سپیدنامه (وایت پیپر (اتریوم، نرم افزارهای غیرمتمرکز را به سه دسته اصلی تقسیم می‌کند. دسته اول برای مدیریت پول، دسته دوم برای مواردی که به نوعی با پول ارتباط دارد (ولی پول تنها مولفه نیست) و دسته سوم نیز سایر انواع نرم افزار غیرمتمرکز است. کاربردهایی نظیر انتخابات و یا سامانه‌های مدیریتی در دسته سوم قرار می‌گیرد.

- نرم افزار غیرمتمرکز مالی(financial application)

این دسته از نرم‌افزارها، ابزارهایی قدرتمند را برای مدیریت قراردادهای هوشمند و استفاده از ارز دیجیتال در اختیار کاربر قرار می‌دهند. کاربر باید مبلغی را در قالب اتر (ارز دیجیتال اتریوم) به کاربری دیگر انتقال دهد. این تراکنش در راستای اجرای یک قرارداد با کاربری دیگر صورت می‌گیرد. شبکه‌ای از گره‌های مختلف در شبکه اتریوم این تبادل اطلاعات را انجام می‌دهند.

- نرم افزار غیرمتمرکز نیمه مالی(semi-financial application)

در این نرم افزارها، پول وجود دارد ولی جنبه غیر پولی عملکرد نیز قابل توجه است. در واقع، دومین دسته از نرم افزار غیرمتمرکز ترکیبی از پول و داده‌های خارج از بلاک چین را در خود دارد. برای نمونه، نرم افزار بیمه محصولات کشاورزی که نیازمند دریافت اطلاعات آب و هواست. فرض کنید یک کشاورز بیمه نامه‌ای را که یک نرم افزار غیرمتمرکز است خریداری می‌کند. در صورت بروز خشکسالی یا طوفان، بیمه به صورت خودکار خسارت وارده را به حساب کشاورز واریز می‌کند. قراردادهای هوشمند برای اجرایی شدن نیاز به مولفه‌ای دارند که در اصطلاح (اوراکل) (oracle) نامیده می‌شوند. اوراکل در واقع اطلاعات به‌روز دنیای واقعی را به قرارداد هوشمند اعلام می‌کند. گفتنی است برخی توسعه‌دهندگان تردید دارند که بتوان این اطلاعات بیرونی را به شکلی غیرمتمرکز به بلاک چین اعلام کرد.

- نرم افزار غیرمتمرکز مدیریتی(governance application)

نرم افزارهایی نظیر اخذ رای (انتخابات) و نیز سازمان غیرمتمرکز از جمله مثل‌های این دسته هستند. یک شکل از نرم افزار غیرمتمرکز نیز به سازمان‌های غیرمتمرکز مستقل (DAO) مربوط می‌شود. یک سازمان غیرمتمرکز مستقل در واقع سازمانی بدون رهبر است که مقررات آن برای اعضا مشخص شده است. اعضا می‌توانند با رای دادن در تصمیم‌گیری‌ها مشارکت کنند.

نرم افزار غیرمتمرکز : ارتباط مستقیم کاربران با فراهم‌کنندگان خدمت

یکی از کاربردهای نرم افزار غیرمتمرکز را می‌توان برای طراحی یک شبکه اجتماعی نظیر توییتر، اما به شکل غیرمتمرکز دانست. این شبکه می‌تواند در برابر سانسور ایستادگی کند. به محض اینکه پیامی را بر روی چنین شبکه‌ای که بر بستر بلاک چین قرار دارد منتشر کردیم، دیگر کسی نمی‌تواند آن را پاک کند. حتی شرکت عرضه کننده این سامانه میکروبلاگ نیز نمی‌تواند پیام‌های کاربران را حذف کند. سامانه بلاک استک (Blockcstack) یک فهرست جامع از انواع برنامه‌های غیرمتمرکز را در اختیار کاربران قرار می‌دهد.

مبادلات اتمی

همیشه اینگونه بنظر می رسیده که بیت کوین ضد سایر ارزهای بازار است. هنگامیکه مبادلات اتمی (Atomic Swaps)شناسانده شود، این دیدگاه می تواند بسرعت تغییر یابد. هدف مبادله اتمی ایجاد رابطه مشارکت میان بیت کوین و آلت کوین است. انتظار می رود این ویژگی از طریق شبکه لایتنینگ شناسانده شود.

افراد نیاز مبرمی به شیوه ای جهت تبدیل آلتکوین به بیت کوین دارند. در حال حاضر این فرایند تنها از طریق سرویس های متمرکز همچون صرافی ها (exchanges) امکانپذیر می باشد. خوشبختانه بنظر می رسد یک راهکار تکنولوژیک همین گوشه کنار منتظر سر برآوردن است. بدین مفهوم که ما شاهد آن خواهیم بود که شبکه لایتنینگ در شبکه بیت کوین فعال گردد. فعالسازی فورک های نرم افزاری فعال کاربر(Fork Soft Activated User) مسیر را برای این رویداد که در ۱ آگوست(۱۰ مرداد) واقع شد، هموار کرد.

این ویژگی تکنولوژیک به عنوان مبادله اتمی(Atomic Swap) قلمداد می شود. در برخی مقالات از آن بعنوان مبادله متقابل اتمی(atomic cross-chain trading) نیز یاد شده است و این دو یک مفهوم را می رسانند.

مفهوم مبادله اتمی مفهوم چندان جدیدی نیست. پیش از این در سال ۲۰۱۳(۱۳۹۲) به این مفهوم اشاره شده است. زمان زیادی بطول نیانجامید که ارتقا دهندگان(developers) ارزهای رمزگذاری شده جهت تبدیل این مفهوم به واقعیت به شیوه جدیدی دست یافتند. اما بنظر می رسد شبکه لایتنینگ این قدرت را به ما اهداء خواهد کرد.

مبادله اتمی به همان شیوه که کاربران مبالغی را به شبکه دیگر ارسال می کنند، کار می کند اما تفاوتهایی در این خصوص وجود دارد. این شبکه به کاربران این امکان را می دهد که بدون اتکا به بخش های متمرکز، ارزهای رمزگذاری شده مختلف را معامله کنند. بعنوان مثال چنانچه کاربر "الف" بیت کوین در اختیار دارد و کاربر "ب" قصد خرید اتریوم کلاسیک را داشته باشد، می توانند بر سر یک قیمت ثابت به توافق رسیده و این معامله را بسرعت(immediately) به سرانجام برسانند.

مبادله اتمی ممکن است مستلزم حد خاصی از اعتماد و اطمینان باشد. در هر مبادله اتمی از یک قراردارد مبتنی بر زمان استفاده(hashed time-locked contract) می شود که بخشی از زبان اسکریپتی(scripting) می باشد که در خصوص ارزهای رمزگذاری شده موجود بکار می رود. هر دو طرف معامله پیشنهاد خود را طی یک بلاکچین متناسب مطرح می کنند. کاربر "الف" بیت کوین را به بیت کوین بلاکچین(blockchain) ارسال نموده و کاربر "ب" اتریوم را به زنجیره(chain) اتریوم کلاسیک می فرستد. گیرنده تنها در صورت آشکار نمودن شماره های رمز می تواند مدعایی در خصوص این معامله داشته باشد. این بدین مفهوم می باشد که علیرغم اینکه تراکنش ها در دو بلاکچین مختلف روی داده اند اما به یکدیگر لینک می شوند. بنظر می رسد این فرایند قدری پیچیده تر از آن است که در واقعیت رخ می دهد. بطور دقیق تر می توان گفت چنانچه این فرایند طی شبکه لایتنینگ که بطور موفقیت آمیز در شبکه بیت کوین فعال گشته است، روی دهد، قدری ساده تر خواهد بود. هر آلتکوینی که از یک منبع کد(codebase) بیت کوین منشعب می شود دارای قابلیت اجرایی بیشتری می باشد. ممکن است لایتکوین یکی از اولین ارزهایی باشد که چنین عملی در مورد آن صورت می گیرد. سایر ارزهای رمزگذاری شده جهت مبادلات اتمی مستلزم قابلیت های گسترده تر اسکریپتی می باشند.

چنانچه شبکه های لایتنینگ مختلف بتوانند مبادلات اتمی را در خودشان به منصه اجرا بگذارند، کل این فرایند از پیچیدگی کمتری برخوردار خواهد بود. کاربران می توانند کانالهای پرداخت را در هر دو بلاکچین باز گذارده و اقدام به ایجاد یک پردازشگر تراکنش بنمایند. این بدین معناست که کاربران قادر خواهند بود تا زمانیکه کانال پرداخت برای شخص مالک ارز باز است، ارزهای رمزگذاری شده مختلف را که حتی به خودشان اختصاص ندارد، مبادله کنند. این فرایند بطور بالقوه جایگزین مبادلات ارزهای رمزگذاری شده خواهد شد. قدری زمان می برد که این مبادلات اتمی به واقعیت بپیوندد اما مطمئنا در آینده شاهد آن خواهیم بود.

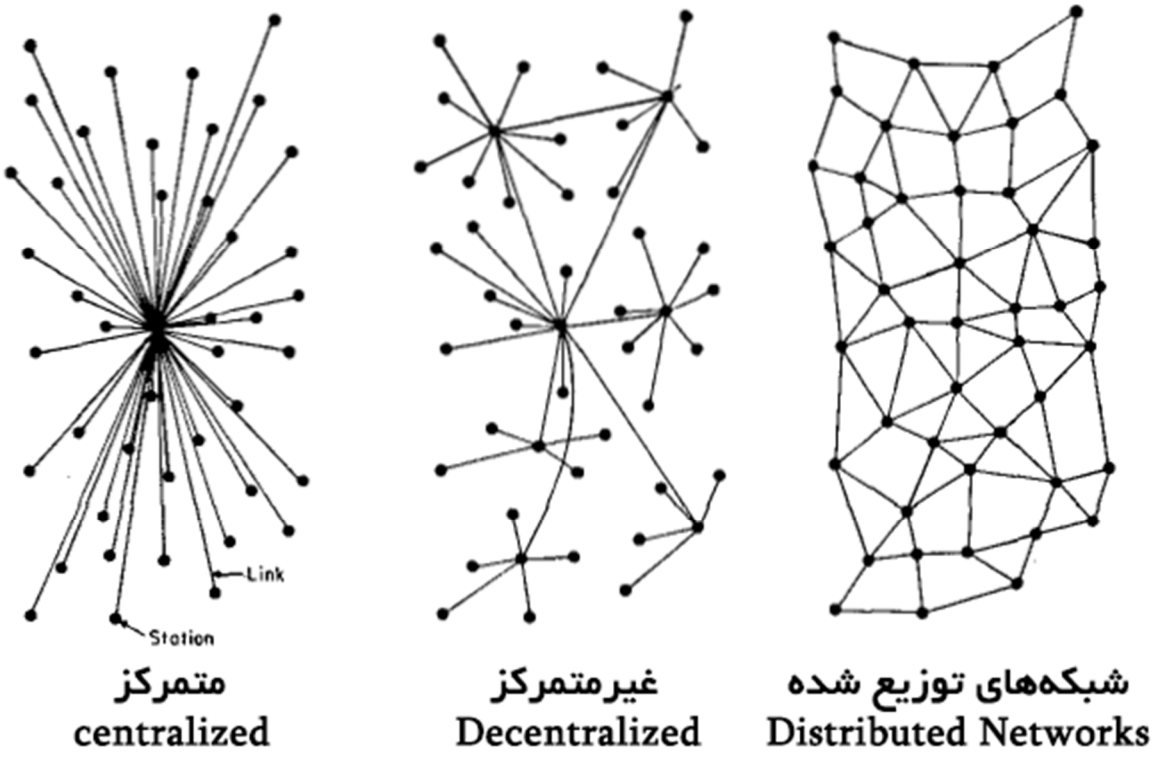
غیر متمرکز Decentrelized

مفهوم جامع تمرکززدایی (غیرمتمرکزسازی) از زبان ویتالیک بوترین

ویتالیک بوترین، خالق اتریوم، در این مقاله درباره مفهوم به اشتباه تعبیر شده تمرکززدایی (Decentralization) صحبت می‌کند و با شکافتن این کلمه جنبه‌های مختلف آن را مورد بحث قرار می‌دهد. در این مقاله مثال‌هایی برای درک جوانب مختلف تمرکززایی (Centralization) و تمرکززدایی ذکر شده تا درک مفاهیم عنوان شده را آسان‌تر سازد. از طرقی روش‌های دستیابی به تمرکززدایی و موانع بر سر راه آن نیز از دیگر موضوعاتی است که ویتالیک به آن پرداخته است.

غیرمتمرکزسازی یکی از واژه‌هایی است که در فضای ارزهای دیجیتال بسیار استفاده می‌شود و از سویی اغلب به عنوان تنها علت به وجود آمدن بلاک چین به آن نگاه می‌کنند. با این حال گویا این لغت یکی از ضعیف‌ترین کلمات تعریف شده به حساب می‌آید. هزاران ساعت مطالعه و میلیاردها دلار در قالب توان هش برای دستیابی به یگانه هدف تمرکززدایی و حفظ و بهبود آن صرف شده است؛ و زمانی که بحث‌ها رقابتی می‌شود، به وفور دیده می‌شود که یکی از پروتکل‌ها ضربه آخر را با متهم کردن طرف مقابل به متمرکز بودن به آن‌ها می‌زند.

اما همواره ابهامات زیادی درباره معنای واقعی این کلمه وجود داشته است. برای مثال شکل زیر که متأسفانه بسیار رایج است و هیچ کمکی نیز به ما نمی‌کند را در نظر بگیرید:



حال این دو جواب را برای سوال «غیرمتمرکز و توزیع شده چه تفاوتی با هم دارند؟» در وبسایت کورا (Quora) با همدیگر بررسی کنیم. اولین جوابی که به این سوال داده شده به صورت طوطی‌وار شکل بالا را تکرار کرده است، در حالی که پاسخ دوم ادعای کاملاً متفاوتی دارد. در این پاسخ آمده که «توزیع شده به این معنی است که پردازش تمام تراکنش‌ها در یک نقطه انجام نمی‌شوند» در حالی که «غیرمتمرکز به معنی نداشتن کنترل یک واحد مستقل بر روی تمامی تراکنش‌ها می‌باشد». ضمناً بهترین جوابی که در استک اتریوم به این سوال داده شده، نمای

بسیار مشابهی دارد؛ اما تفاوت آن با جواب قبلی، جابه‌جا شدن کلمات غیرمتمرکز و توزیع شده است. به همین خاطر نیز باید در این باره شفاف‌سازی انجام شود.

سه نوع تمرکززدایی

هنگامی که مردم درباره تمرکززدایی نرم‌افزارها صحبت می‌کنند، در واقع حول سه محور مجزا از تمرکز زدایی/تمرکز زایی به گفتگو می‌پردازند. با اینکه در برخی موارد تفکر درباره داشتن یکی از این محورها بدون دیگری کار دشواری است، اما در کل این موارد کاملاً مجزا از هم می‌باشند. این محورها به شرح زیر است:

- **تمرکز زدایی/زایی از نظر معماری:** چند کامپیوتر فیزیکی این سیستم را به وجود آورده‌اند؟ سیستم توانایی تحمل از کار افتادن چه تعداد از این کامپیوترها را در یک لحظه دارد؟
- **تمرکز زدایی/زایی از نظر خط مشی:** چندنفر یا سازمان در حال کنترل کامپیوترهای تشکیل دهنده این سیستم هستند؟
- **تمرکز زدایی/زایی از نظر منطقی:** ساختار داده و رابط کاربری که توسط سیستم حفظ و ارائه می‌شود، شبیه به یک شی واحد یکپارچه است یا گروهی بدون نظم؟ به بیانی ساده‌تر، اگر شما سیستم را به دو نیم تقسیم کنید که شامل هر دو گروه سرویس‌دهندگان و کاربران است، آیا هر دو نیم جداشده به عنوان واحدهای مستقلی فعالیت‌های خود را ادامه خواهند داد؟

توجه داشته باشید که این جاگیری‌ها نسبی بوده و می‌تواند مورد بحث و گفتگو واقع شود. اما بیایید هر کدام از این‌ها را بررسی کنیم:

• شرکت‌های مرسوم از نظر خط مشی متمرکز (یک مدیرعامل)، از نظر معماری متمرکز (یک دفترمرکزی) و از نظر منطقی هم متمرکز هستند (قابل بخش به دو نیمه نیستند)

• قانون مدنی (Civil law) به یک بدنه متمرکز قانون‌گذار تکیه دارد، در حالی که حقوق عرفی (Common law) به دست قاضی‌های انفرادی و افراد واحد زیادی در طول زمان شکل گرفته‌اند. قوانین مدنی از برخی جوانب معماری، غیرمتمرکز محسوب می‌شوند چرا که دادگاه‌های بزرگ و با صلاحدید زیادی وجود دارند اما بازیگران بیشتری در حقوق عرفی دخیل هستند. هر دو این‌ها از نظر منطقی متمرکزند (قانون، قانون است)

• زبان‌ها از نظر منطقی غیرمتمرکز هستند؛ زبان انگلیسی که آلیس و باب به آن صحبت می‌کنند لزومی ندارد با زبان انگلیسی که چارلی و دیوید از آن استفاده می‌کنند، یکی باشد. به هیچ زیرساخت متمرکزی نیاز نیست تا زبان وجود داشته باشد، قواعد دستورزبان انگلیسی نیز توسط یک فرد واحد ساخته و کنترل نشده است. (اگرچه برای مثال زبان فراساخته‌ای مانند اسپرانتو وجود دارد که توسط لودویک زامنهوف به وجود آمده، اما اسپرانتو هم‌اکنون مانند زبان زنده‌ای عمل می‌کند و در حال طی کردن روند صعودی تکامل بدون وجود شخص یا نهاد صاحب‌اختیاری است)

• بیت تورنت نیز مشابه زبان انگلیسی از نظر منطقی غیرمتمرکز است. شبکه‌های تحویل‌دهی محتوا نیز مشابه بوده و تنها تفاوتی که وجود دارد کنترل شدن آن توسط یک شرکت واحد است.

• بلاک چین‌ها از نظر خط مشی غیرمتمرکز بوده (هیچ کسی آن‌ها را کنترل نمی‌کند) اما از نظر منطقی متمرکز هستند (یک وضعیت مورد قبول عمومی وجود دارد که همه بر روی آن به توافق رسیده‌اند و سیستم همانند یک کامپیوتر واحد عمل می‌کند)

بسیاری از اوقات که مردم درباره فضیلت‌های بلاک چین صحبت می‌کنند، در واقع در حال توصیف مزایای استفاده از یک پایگاه داده مرکزی هستند؛ این تمرکززایی یک تمرکززایی منطقی است و به نوعی در بسیاری از موارد خوب است. (هرچند خوان بنت از IPFS، هر جا که ممکن باشد خواستار تمرکززدایی از نظر منطقی است؛ چرا که ذاتاً سیستم‌های غیرمتمرکز از تقسیم‌بندی شبکه‌ای زنده بیرون می‌آیند و در مناطق با اتصال ضعیف خوب کار می‌کنند)

تمرکززایی از نظر معماری اغلب به خط مشی‌های متمرکز منجر می‌شود، اما این الزاماً همیشه صحیح نیست. در یک مراسم رسمی دموکراسی، سیاست‌مداران در تالاری افراد رأی‌دهنده به خود را ملاقات کرده و آن‌ها را حفظ می‌کنند. اما برگزارکنندگان این محافل رسمی قدرت قابل توجهی در گرفتن تصمیمات ندارند. در سیستم‌های بر پایه کامپیوتر نیز جنبه معماری و نه خط مشی تمرکززدایی می‌تواند زمانی اتفاق بیافتد

که یک جامعه آنلاین برای سهولت کار از انجمن متمرکز استفاده کنند. اما همچنین قراردادهای اجتماعی مورد توافقی بین اعضا وجود دارد که اگر صاحبان یک انجمن بدجنسانه رفتار کنند، همه به انجمن دیگری بروند. (جوامعی که در مقابل چیزی که در انجمن دیگر سانسور می‌خوانند، شکل گرفته‌اند در عمل این ویژگی را دارند)

تمرکززایی از نظر منطقی رسیدن به تمرکززدایی از نظر معماری را دشوار می‌کند، اما آن را غیرممکن نمی‌سازد. به الگوریتم‌های اجماع غیرمتمرکز در شبکه‌های مختلف نگاه کنید که چگونه با اثبات کار کنار آمده‌اند اما به مراتب دشوارتر از بیت تورنت هستند. از طرفی تمرکززایی منطقی نیز رسیدن به خط مشی غیرمتمرکز را سخت می‌کند. در سیستم‌های متمرکز از لحاظ منطقی، برطرف کردن مشاجرات با توافق بر استدلال ساده «زندگی کن و بگذار زندگی کنند» به نسبت دشوارتر اتفاق می‌افتد.

سه دلیل تمرکززدایی

- **تحمل خطا:** سیستم‌های غیرمتمرکز احتمال شکست تصادفی کمتری دارند چرا که به اجزای مختلفی تکیه دارند که شبیه هم نیستند.
- **مقاومت در برابر حملات:** هزینه زیادی برای حمله، تخریب یا دستکاری سیستم‌های غیرمتمرکز باید صرف شود، چرا که نقاط حساس مرکزی در آن‌ها وجود ندارد که با هزینه‌های کمتری نسبت به حجم اقتصادی سیستم پیرامون به آن‌ها حمله کرد.
- **مقاومت در برابر توطئه:** برای شرکت‌کنندگان در سیستم‌های غیرمتمرکز بسیار دشوارتر است که با یکدیگر توطئه کنند، بطوریکه خود به سود برسند و هزینه‌اش را دیگر شرکت‌کنندگان بپردازند؛ چرا که سردمداران شرکت‌ها و دولت‌ها به طریقی ساخت‌وپاخت می‌کنند که سود آن به خودشان برسد و زیان آن بین شهروندان، مشتریان، کارمندان و عموم مردم هماهنگ‌شده در زمان مشابه پخش شود.

هر سه استدلال طرح شده مهم و معتبر هستند، ولی هر سه آن‌ها زمانی که شما درباره تصمیمات پروتکل با در نظر داشتن این سه چشم‌انداز فکر می‌کنید، به برخی نتایج متفاوت و جالب می‌انجامد. بیایید یک به یک درباره هرکدام از این موارد صحبت کنیم.

با توجه به تحمل خطا، استدلال اصلی ساده است. احتمال وقوع کدام یک کمتر است؟ خرابی یک کامپیوتر، یا خراب شدن همزمان ۵ کامپیوتر از ۱۰ کامپیوتر. این اصل غیرقابل بحث و جدل است و در زندگی واقعی و در شرایط بسیاری از جمله موتورهای جت، ژنراتورهای کمکی در مکان‌هایی مانند بیمارستان، زیرساخت‌های نظامی، تنوع‌سازی‌های سبدسهام مالی و صدالبته شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرد.

هرچند این نوع تمرکززدایی، که از جهتی بسیار مهم و موثر است گاهی اوقات عملکردی بسیار ضعیف‌تر از آن چیزی که در نظر ما به عنوان نوش‌دارو نقش بسته نسبت به یک مدل ساده ریاضی که پیش‌بینی‌هایش درست از آب درمی‌آید، ایفا می‌کند. دلیل آن هم وضعیت خرابی متداول (Common Mode Failure) است. البته که احتمال از کارافتادن چهار موتور جت بسیار کمتر از یکی است، اما اگر هر ۴ تای آن‌ها در یک کارخانه تولید شده باشند چه؟ و یا اینکه این خطا به دست یک کارگر در هر ۴ موتور اتفاق افتاده باشد؟

آیا بلاک چین‌ها در شکل امروزی قادر به مدیریت برای محافظت در برابر وضعیت خرابی متداول هستند؟ نه لزوماً. سناریوهای زیر را در نظر بگیرید:

• تمامی نودها در بلاک چین نرم‌افزار کلاینت مشابهی اجرا کنند و مشخص شود که این نرم‌افزار یک باگ داشته است.

• تمامی نودها در یک بلاک چین نرم‌افزار کلاینت مشابهی اجرا کنند و مشخص شود که تیم توسعه‌دهنده این نرم‌افزار از لحاظ اجتماعی فاسد است.

• مشخص شود تیم توسعه‌دهنده‌ای که به‌روزرسانی‌های پروتکل را پیشنهاد می‌دهد، از نظر اجتماعی فاسد است.

• در سیستم‌های اثبات کار بلاک چین، ۷۰ درصد ماینرها از کشور مشابهی باشند و دولت این کشور تصمیم بگیرد تمام فارم‌های ماینینگ را با مقاصد امنیت ملی تصاحب کند.

• غالب سخت‌افزارهای استخراج توسط یک شرکت تولید شود و با رشوه دادن یا اجبار آن یک در پشتی (Backdoor) در دستگاه‌ها جاسازی شود که به شرکت اجازه دهد هر زمان که می‌خواهد دستگاه‌ها را خاموش کند.

• در یک بلاک چین با الگوریتم اثبات سهام، ۷۰ درصد کوین‌های گروگذاشته در یک صرافی نگه‌داری شود.

یک دیدگاه همه جانبه از تحمل خطای تمرکززدایی تمامی این جوانب را در نظر می‌گیرد و راه‌حل به حداقل رساندن آن‌ها را به دست می‌آورد. برخی نتایج طبیعی برخاسته از این کاملاً واضح است:

• داشتن پیاده‌سازی‌های رقابتی چندگانه یک امر بسیار حیاتی است.

• دانش ملاحظات فنی که در زیرلایه به‌روزرسانی‌های پروتکل قرار دارد، باید دموکراتیک شود. با این حساب مردم بیشتری با شرکت کردن در بحث‌های تحقیقاتی و نقد تغییرات پروتکل‌هایی که به وضوح بد هستند، احساس راحتی می‌کنند.

• توسعه‌دهندگان اصلی و پژوهشگران باید توسط شرکت‌ها یا سازمان‌های مختلف استخدام شوند. (یا در گزینه‌ای جایگزین، بسیاری از آن‌ها داوطلبانه می‌توانند کار کنند)

• الگوریتم‌های استخراج باید به صورتی طراحی شوند که ریسک تمرکززایی را به حداقل برسانند.

• ما در وضعیتی ایده‌آل الگوریتم اثبات سهام را برای رهایی یافتن از خطر متمرکزشدن کلی سخت‌افزارها به کار می‌گیریم. (همچنین باید درباره خطراتی که با استفاده از این الگوریتم ظهور می‌کنند، هوشیار باشیم)

توجه داشته باشید که پیش‌نیازهای تحمل خطا در ساده‌ترین حالت خود بر روی تمرکززدایی از نظر معماری فعالیت دارد، اما همینکه به تحمل خطا در جامعه هدایت‌کننده توسعه جاری پروتکل فکر کنید، تمرکززدایی از لحاظ خط مشی نیز اهمیت خود را نشان می‌دهد.

حال به مقابله در برابر حملات نگاهی بیاندازیم. گاهی اوقات در برخی مدل‌های ناب اقتصادی، شما به نتیجه‌ای مبنی بر اهمیت نداشتن تمرکززدایی می‌رسید. اگر شما پروتکلی بسازید که تاییدکنندگان تراکنش‌ها در صورت وقوع یک حمله ۵۱ درصدی به طور تضمین شده ۵۰ میلیون دلار از دست دهند، دیگر مهم نیست که این تاییدکنندگان توسط یک شرکت یا ۱۰۰ شرکت کنترل می‌شوند. ۵۰ میلیون دلار یک حاشیه امنیت اقتصادی است. در واقع دلایلی محکمی از نظریه بازی‌ها وجود دارد که نشان می‌دهد چرا متمرکزسازی می‌تواند باعث افزایش این حاشیه اقتصادی شود. (از آنجا که گنجایش تراکنش در داخل بلاک‌ها یک دیکتاتوری بسیار چرخشی است، مدل انتخاب تراکنش از بلاک چین‌های فعلی بازتاب این تفکر است)

هرچند اگر مدل اقتصادی غنی‌تری به کار گیرید و مخصوصاً یک نفر به امکان وقوع تهدید و اجبار اقرار کند، (یا به موارد ملایم‌تری مانند مورد هدف قرار دادن نودها در حملات DoS) تمرکززدایی به یک موضوع اساسی تبدیل می‌گردد. اگر شما فردی را به مرگ تهدید کنید، دیگر آن ۵۰ میلیون دلار برایش اهمیتی نخواهد داشت. اما اگر این ۵۰ میلیون دلار بین ۱۰ نفر تقسیم شود، شما هر دفعه باید این تهدید را به تعداد ۱۰ بار باید انجام دهید. در حالت کلی بسیاری از موارد در جهان مدرن بر اساس ناقرینگی مهاجم/ مدافع و به نفع مهاجم تعریف می‌شود. ساختمانی که ۱۰ میلیون دلار هزینه ساخت آن است، تنها ۱۰۰ هزار دلار برای تخریب نیاز دارد. اما موضوع مورد تأکید، اغلب میزان نفوذ مهاجم است. اگر هزینه ساخت ساختمانی ۱۰ میلیون دلار و هزینه تخریب آن ۱۰۰ هزار دلار باشد، ساختمانی که ۱ میلیون دلار هزینه ساخت آن باشد، شاید هزینه مورد نیاز برای تخریب آن ۳۰ هزار دلار باشد. اعداد کوچکتر معمولاً نسبت‌های بهتری می‌دهند.

این نتایج به چه چیزی ختم می‌شود؟ اول از همه به خوبی نمایانگر مزیت استفاده از اثبات سهام در برابر اثبات کار است، چرا که سخت‌افزارهای کامپیوتری به آسانی قابل شناسایی، قانون‌گذاری و مورد هدف قرار گرفتن حملات هستند اما سکه‌ها برای مخفی ماندن، کار به نسبت راحتی در پیش دارند (اثبات سهام به دلایلی دیگر در برابر حملات مقاومت بیشتری دارد). دلیل دوم، این خود نقطه مثبتی برای داشتن تیم‌های توسعه‌دهنده به شدت توزیع شده مانند یک توزیع جغرافیایی است. سومین مورد نیز تأکید دارد که به مدل اقتصادی و تحمل خطا حین طراحی پروتکل‌های اجماع باید نگاه ویژه‌ای شود.

در نهایت به بحث‌برانگیزترین مورد یعنی استدلال سوم، مقاومت در برابر توطئه، می‌رسیم. تعریف توطئه یا تبانی کار سختی است؛ شاید تنها ساختار حقیقی که این کلمه را بتوانیم در آن جا دهیم، «یک هم‌آهنگی (coordination) ناپسند یا به عبارتی ناخواسته از نظر ما» باشد. موقعیت‌های مشابه زیادی در زندگی واقعی وجود دارد که هرچند یافتن یک هم‌آهنگی تمام‌عیار بین همه افراد یک حالت ایده‌آل محسوب می‌شود، اما هم‌آهنگ بودن تنها یک زیرگروه و ناهم‌آهنگ بودن بقیه نیز می‌تواند موضوع خطرناکی باشد.

مثال ساده‌ای از این دست، قانون رقابت (ضد انحصاری) می‌باشد. موانع قانونی که از عمد برای این منظور ساخته شده، کار را برای بازیگران حاضر در یک سمت از بازار که قصد دارند با گرد هم آمدن یک مونوپولی (انحصار) ایجاد کنند و تمام سود بازار را به قیمت زیان رقبای خود و رفاه اجتماعی عمومی به خود اختصاص دهند، بسیار سخت می‌کند. نمونه دیگر قوانینی است که در برابر هم‌آهنگی‌های فعال بین نامزدها و کمیته‌های اقدام سیاسی بزرگ (Super-PACs) در ایالات متحده ایجاد شده است؛ در حالی که اثبات شده اجرای این مقررات در عمل دشوار است. یک مثال دیگر و در ابعادی کوچکتر قانونی است که در برخی تورنومنت‌های شطرنج بین دو بازیکن اجرا می‌شود و آن‌ها را از انجام بازی‌های متعدد در برابر یکدیگر که سبب افزایش امتیاز یکی از آن‌ها شود، باز می‌دارد. مهم نیست به کجا می‌نگرید، تلاش برای جلوگیری از هم‌آهنگی‌های ناخواسته در تمامی موسسات سطح بالا دیده می‌شود.

در رابطه با پروتکل‌های بلاک چین، استدلال‌های اقتصادی و ریاضی که امنیت یک اجماع را تعیین می‌کند، شدیداً به مدل انتخاب ناهم‌آهنگ یا این فرضیه تکیه دارند که این بازی از بازیگران کوچک بسیاری تشکیل شده که به صورت مستقل تصمیم می‌گیرند. اگر یکی از بازیگران بیش از یک سوم توان استخراج سیستم اثبات کار را به دست گیرد، به تسلط بی‌حدوحصری در سود استخراج خودخواهانه‌اش دست می‌یابد. هرچند آیا واقعاً می‌توان اظهار داشت که مدل انتخاب ناهم‌آهنگی وجود دارد، آن هم زمانی که ۹۰ درصد از قدرت شبکه بیت کوین به قدری هم‌آهنگ باشند تا همزمان در کنفرانسی شرکت کنند؟

مدافعان بلاک چین نیز این نکته را مدنظر قرار می‌دهند که بلاک چین‌ها از آنجا که هرکس تنها به اختیار خود و هر زمان که بخواهد، نمی‌تواند قوانین را تغییر دهد گزینه امنی محسوب می‌شوند. اما دفاع از این استدلال زمانی که توسعه‌دهندگان نرم‌افزار و پروتکل همه برای یک شرکت کار کنند و همانند خانواده‌ای در یک اتاق نشسته باشند، امری دشوار خواهد بود. هدف این است که نباید این سیستم‌ها مانند واحدهای انحصارگری که تنها به منافع شخصی خود می‌اندیشند، عمل کنند. بنابراین شما با قطعیت می‌توانید بگویید که بلاک چین‌ها زمانی امن‌تر هستند که ناهم‌آهنگی در آن‌ها بیشتر باشد. هرچند که این سبب ظهور یک تناقض بنیادین می‌شود. بسیاری از جوامع مانند جامعه اتریوم اغلب به خاطر روح جمعی مستحکم و اقدام سریع که مثلاً در پیاده‌سازی،آزادسازی و فعال‌سازی هاردفورکی که برای مقابله با مشکلات DoS در پروتکل طی تنها ۶ روز انجام می‌گیرد، مورد ستایش واقع می‌شوند. اما چگونه می‌توان این هم‌آهنگی خوب را بهبود و پرورش داد اما به صورت همزمان از هم‌آهنگی بد که در آن ماینرها در حال توطئه هستند و قصد اجرای حملات هم‌آهنگ ۵۱ درصدی را دارند، جلوگیری کرد؟

- نباید نگران هم‌آهنگی‌های ناخواسته بود و درعوض پروتکلی ساخت تا در برابر آن مقاومت کند.
- تلاش برای یافتن حالت بینابینی که به پروتکلی که قصد تکامل و حرکت روبه‌جلو را دارد، اجازه هم‌آهنگی بدهد اما این اختیارات به‌اندازه‌ای نباشد که آن‌ها را قادر به انجام حملات کند.
- برای مرزبندی بین هم‌آهنگی سودمند و خطرناک تلاش کرده بطوریکه کار اولی را راحت‌تر و دومی را سخت‌تر کنید.

قسمت اعظم فلسفه طراحی کسپر (اتریوم ۲) بر روی رویکرد اول تمرکز کرده است. هرچند این به تنهایی کافی نیست؛ چرا که صرف تکیه کردن به اقتصاد، در مواجهه با دو دسته دیگر نگرانی‌های تمرکززدایی بازمی‌ماند. طرح ریزی مورد دوم به خصوص در بلندمدت دشوار است، اما این مورد اغلب به طور تصادفی اتفاق می‌افتد. برای مثال، اینکه توسعه‌دهندگان بیت کوین اغلب انگلیسی اما ماینرهای آن بیشتر چینی صحبت می‌کنند، از آنجا که این مدیریت دوگانه ایجاد هم‌آهنگی را دشوار می‌سازد، می‌تواند اتفاق مثبتی تلقی شود. از سوی دیگر اکوسیستم جوامع چینی و انگلیسی به سبب دشواری‌های جغرافیایی و ارتباطی که آن‌ها را به نحوی از هم جداکرده، از مزایای جانبی کاهش ریسک وضعیت خرابی متداول به دلیل کاهش احتمال انجام خطای مشابه از هر دوسو بهره می‌برند.

مورد سوم بیش از بقیه یک چالش اجتماعی است؛ راه‌حل‌های این موضوع شامل موضوعات زیر می‌شود:

- مداخلات اجتماعی که درصدد افزایش وفاداری و صداقت شرکت‌کنندگان نسبت به جامعه بلاک چین به عنوان یک واحد کلی است که جایگزین وفاداری مستقیم بازیکنان به همدیگر در یک سمت از جامعه می‌شود یا از آن جلوگیری می‌کند.

• ترویج ارتباط بین طرف‌های مختلف بازار در بستر یکسان که امکان همدست شدن تاییدکنندگان (Validator)، توسعه‌دهندگان یا ماینرها و از اینکه خود را به عنوان دسته‌ای جدا که برای دفاع از حقوق صنف خود باید در برابر دسته‌های دیگر بایستند را کاهش می‌دهد.

• طراحی پروتکل در مسیری که دخیل شدن به صورت یک به یک را برای تاییدکنندگان/ماینرها با انگیزه «روابط ویژه»، ایجاد شبکه‌های متمرکز و دیگر سازوکارهای مشابه مافوق پروتکلی کاهش دهد.

• هنجارهای صریح درباره اینکه انتظار می‌رود پروتکل چه مشخصات بنیادینی داشته باشد، یا چه چیزهایی نباید داشته باشد یا حداقل تحت شرایط بسیار محدودی اعمال شود.

نوع سوم از تمرکززدایی، تمرکززدایی برای جلوگیری از هم‌آهنگی‌های ناخواسته، احتمالاً دشوارترین آن‌ها برای دستیابی است. بده‌بستان‌ها هم در این میان اجتناب‌ناپذیر است. احتمالاً بهترین راه‌حل اتکا کردن به گروهی است که تمرکززدایی آن تا حد نسبتاً خوبی تضمین شده باشد: یعنی کاربران پروتکل.

مقیاس پذیری Scalability

مشکل مقیاس‌پذیری بلاکچین / راهکارهای موجود برای حل این مشکل پیچیده

من Preethi Kasireddy در حال معماری و پیاده‌سازی یک پروتکل جدید در اتریوم Ethereum بوده‌ام و شخصاً با مشکل مقیاس‌پذیری (scale) بلاکچین برای آینده رودررو شده‌ام و مجذوب حجم عظیم تحقیقات، مباحثات و از همه مهم‌تر، آزمایش‌های انجام‌گرفته پیرامون حل این مشکل هستم. در ادامه مطلب تعدادی راه‌حل پیشنهادشده برای حل مشکل مقیاس‌پذیری بلاکچین و نقاط قوت و ضعف بخصوص هریک را شرح خواهم داد.

بلاک‌چین مقیاس‌پذیر نیست؛ اما امیدهایی هست!

ده سال پیش اولین مقاله بیت‌کوین منتشر شد و از آن روز شور و اشتیاق من درباره‌اش هرروز زیادتر شده است. روزی را به یاد می‌آورم که ارز رمزنگاری‌شده غیرمتمرکز یک هدف دست‌نیافتنی به نظر می‌رسید، ولی اکنون بالاخره در حال رایج شدن است. من مشتاقم که یک روز بالفعل شدن کاربردهای غیرمتمرکز آن را در عرصه مبادلات مالی، پیش‌بینی بازار و مدیریت دارایی مشاهده کنم.

بنیان این مهم بر بی‌نیاز بودن سامانه از اعتمادسازی استوار بوده (trustless systems) که بررسی‌اش از جذابیت بالایی برخوردار است؛ سامانه‌های احراز هویت، دارایی هوشمند (smart property)، مقابله با سانسور، بنیان‌های اجتماعی، ساختار خودکار و مدل‌های کنترل مانند سازمان نامتمرکز خودگردان (DAO) و... که جسورترین کاربردها هنوز به فکر کسی خطور نکرده است.

بااینکه عده‌ای از کارآفرینان و علاقه‌مندان پیشرو مشغول تلاش برای رسیدن به این رؤیا هستند اما ممکن است این فکرها هیچ‌وقت به واقعیت تبدیل نشود و قطعه گم‌شده پازل همان مشکل مقیاس‌پذیری بلاکچین است. بلاکچینی که امروز در اختیار ما است ازنظر مقیاس‌پذیری بسیار محدود است. نمی‌خواهم بگویم که همه‌چیز این‌گونه خواهد ماند، اما واقعیت تلخ امروز ما این است که مانع اصلی در برابرمان همین مشکل مقیاس‌پذیری بلاکچین است که به عرصه فعال تحقیق در میان محققین ارزهای رمزنگاری‌شده تبدیل‌شده است.

چرا مشکل مقیاس‌پذیری بلاکچین وجود دارد؟

تمام پروتکل‌های اجماع در بلاکچین (مانند بیت‌کوین (Bitcoin)، اتریوم، ریپل (Ripple) و تندرمینت (Tendermint)) در حال حاضر یک محدودیت چالش‌برانگیز دارند: هر گرهی که به‌طور کامل در شبکه مشارکت می‌کند باید تمام تراکنش‌ها را پردازش کند و این ناشی از مشخصه ذاتی غیرمتمرکز بودن بلاکچین است.

بااین‌که مکانیسم اجماع غیرمتمرکز دارای مزیت‌های کلیدی مانند تحمل خطا (fault tolerance)، بی‌طرفی سیاسی، امنیت زیاد و صحت بالا است، همه‌ی این‌ها به قیمت از دست رفتن مقیاس‌پذیری تمام می‌شود. تعداد تراکنش‌هایی که بلاکچین می‌تواند پردازش کند، هیچ‌وقت نمی‌تواند از تعداد تراکنش‌هایی که یک گره در شبکه قادر به انجام است فراتر رود. درواقع با افزایش تعداد گره‌های یک شبکه، به علت افزایش تأخیر بین گره‌ها (inter-node latency)، بلاکچین ضعیف‌تر می‌شود.

برای رسیدگی به تعداد بیشتری از تراکنش‌ها در سامانه‌های پایگاه داده سنتی، افزایش تعداد رایانه‌های سرور راه‌حل رایج برای ارتقای مقیاس‌پذیری است. در جهان بلاکچین غیرمتمرکز که هر گره باید تک‌تک تراکنش‌ها را پردازش و تائید کند، برای ارتقای سرعت شبکه باید تعداد رایانه‌ها در هر گره افزایش یابد. نداشتن کنترل روی تمام گره‌های عمومی ما را در بن‌بست قرار می‌دهد. درنتیجه، در بلاکچین غیرمتمرکز یک پروتکل اجماع عمومی مجبور است بین بازده بالای تراکنش‌ها و سطح بالایی از غیرمتمرکز بودن یکی را انتخاب کنند.

به‌بیان‌دیگر با افزایش اندازه بلاکچین، نیاز شبکه به فضای ذخیره‌سازی، پهنای باند و قدرت پردازشی افزایش می‌یابد. زمانی خواهد رسید که بلاکچین چنان حجیم خواهد شد که تنها راه‌حل برای ادامه پردازش‌ها انجام آن در چند گره بخصوص در شبکه است و این یعنی وجود یک مرکزیت و از دست رفتن ویژگی غیرمتمرکز بودن بلاکچین.

چرا حل مشکل مقیاس‌پذیری بلاکچین دشوار است؟

بلاکچین باید به مکانیسمی دست پیدا کند که ضمن کاهش تعداد گره‌های لازم برای تائید تراکنش‌ها، اعتماد شبکه را به صحت تراکنش‌ها هم حفظ نماید. این امر ممکن است در ظاهر ساده به نظر آید اما ازنظر فنی بسیار سخت است.

- با سلب اجازه از تمام گره‌ها برای تأیید صحت هر تراکنش، نیاز خواهیم داشت گره‌ها روش‌هایی آماری و اقتصادی برای حصول اطمینان از امنیت سایر بلاک‌ها در دست داشته باشند.
- روشی برای تضمین در دسترس بودن داده‌ها نیاز خواهیم داشت. به‌بیان‌دیگر، حتی اگر در گرهی که توانایی تأیید مستقیم امنیت داده‌های بلوک را ندارند، امنیت به روشی محرز شده باشد، اگر به هر علتی، اعم از قطع برق یا حمله هکرها در یک گره، این داده‌ها در دسترس نباشند، وضعیتی پیش می‌آید که هیچ تأییدکننده دیگری در شبکه نیز نخواهد توانست تراکنش را تأیید کرده یا بلوک جدیدی ایجاد کنند و درنتیجه شبکه در حالت کنونی گیر خواهد کرد.
- برای حصول مقیاس‌پذیری تراکنش‌ها باید توسط گره‌های مختلف به‌طور موازی پردازش شوند؛ با این وجود، اجزای متعددی در فرایند تغییر حالت در بلاکچین هستند که قابلیت اجرای موازی را ندارند. حفظ تعادل میان کارایی و موازی‌سازی ما را با محدودیت‌هایی در چگونگی تغییر حالت بلاکچین مواجه می‌کنند.

اعداد چه می‌گویند

مشکل مقیاس‌پذیری بلاکچین در چه حد مشکل امروز ما است؟ حداکثر ظرفیت پردازش تراکنش‌ها در یک گره اتریوم به‌صورت نظری بیش از ۱۰۰۰ تراکنش در ثانیه است. متأسفانه بازده واقعی به این اندازه نیست و علت این امر محدودیت حد سوخت (gas limit) اتریوم است که اکنون چیزی حدود ۶٫۷ میلیون سوخت برای هر بلوک است.

در اتریوم سوخت مقیاسی برای اندازه‌گیری تلاش پردازشی است و برای هر عملیاتی میزان مشخصی سوخت اختصاص می‌یابد. برای مثال اطلاع از موجودی حساب ۴۰۰ سوخت، ایجاد یک قرارداد ۳۲۰۰۰ سوخت و ارسال یک تراکنش ۲۱٬۰۰۰ سوخت پردازش نیاز دارد. تراکنش‌ها جایی برای درج حداکثر میزان سوختی که ارسال‌کننده حاضر به خرید آن است هم دارند. بنابراین، حد سوخت برای هر بلوک مشخص می‌کند چه تعداد تراکنش با حد سوخت‌های متفاوت در آنجا می‌شوند. حد سوخت اتریوم را می‌توان معادل محدودیت ۱ مگابایتی بیت‌کوین برای حجم هر بلوک گرفت و تفاوت آن‌ها هم این است که حد سوخت در اتریوم به‌صورت پویا (dynamic) توسط استخراج‌گر (miners) تعین می‌شود درحالی‌که حجم بلوک در بیت‌کوین ثابت بوده و در پروتکل ثبت گردیده است.

حد سوخت یک محدودیت نرم در شبکه برای اختصاص توان پردازشی برای هر بلوک تعیین می‌کند. با احتساب حد سوخت ۶٫۷ میلیونی و فرض به‌طور متوسط ۲۱٬۰۰۰ سوخت مصرف‌شده برای یک تراکنش استاندارد به رقم ۳۰۰ تراکنش برای هر بلوک می‌رسیم. زمان متوسط هر بلوک در حال حاضر ۲۰ ثانیه است که ما را به عدد ۱۵ تراکنش در ثانیه می‌رساند. در تراکنش‌های پیچیده‌تر که تا ۵۰٬۰۰۰ سوخت مصرف شود، این رقم به ۷ تراکنش در ثانیه کاهش می‌یابد. تعداد تراکنش‌ها روی شبکه اتریوم با سرعت قابل‌ملاحظه‌ای در حال افزایش است (رشد تقریبی ٪۵۰۰ در سال). ماه گذشته تعداد تراکنش‌های روزانه به ۴۴۰٬۰۰۰ عدد هم رسید و این یعنی چیزی حدود ۵ تراکنش در ثانیه!

به‌طور مشابه بیت‌کوین روی کاغذ محدودیت ۴۰۰۰ تراکنش در ثانیه و درواقع محدودیت سخت حدود ۷ تراکنش معمولی و ۳ تراکنش پیچیده در ثانیه را دارد. در نظر داشته باشید که این محدودیت‌ها برای بلاکچین‌های خصوصی به این میزان نیستند. یک بلاک‌چین خصوصی می‌تواند به بیش از ۱۰۰۰ تراکنش در ثانیه هم دست پیدا کند. وقتی بلاکچین دست خودتان است می‌توانید اطمینان حاصل کنید تمام گره‌های شبکه رایانه‌های قدرتمند با پهنای باند سریع باشند. در حال حاضر برای حل مشکل مقیاس‌پذیری بلاکچین مجبوریم به هر گره قدرت پردازشی بیشتری اضافه کنیم. در شبکه‌های خصوصی که کنترل تمام گره‌ها مقدور است، این امر امکان‌پذیر است. در یک شبکه خصوصی همچنین می‌توان قسمتی از وظایف معمول را، مانند تشخیص واقعی بودن تمام گره‌ها، از دوش بلاکچین برداشت.

راه حل ها

واقعیت امر این است که هیچ‌یک از راه‌حل‌هایی که در ادامه خواهد آمد به‌تنهایی درمان قطعی مشکل مقیاس‌پذیری بلاکچین را در برندارد و هر یک سعی در بهبود تدریجی مقیاس‌پذیری خواهد داشت؛ اما در ترکیب با یکدیگر خواهند توانست چشم‌انداز امیدبخشی برای آینده مقیاس‌پذیری بلاکچین ترسیم کنند.

لطفاً در نظر داشته باشید هدف این نوشتار مطرح کردن تمام پیچیدگی‌های فنی و قضاوت در مورد شایستگی‌های تمام راه‌حل‌های پیشنهادی نیست. هدف من ارائه نمایی کلی از برخی راه‌حل‌هایی است که از آن‌ها اطلاع داشته‌ام. همچنین فرض بر این بوده که خواننده اطلاعات مقدماتی در مورد کارکرد بلاکچین دارد.

مشکل مقیاس‌پذیری بلاکچین چالشی است شناخته‌شده و تحقیقات در این حوزه چندین سال است به‌صورت فعال انجام می‌پذیرد. اگر ناکامی چندین ساله بیت‌کوین را زیر نظر داشته‌اید احتمالاً راه‌حل سِگویت (SegWit) و افزایش اندازه بلاک به ۲ مگابایت به گوشتان خورده است.

این راه‌حل‌ها برای حل مشکل مقیاس‌پذیری بلاکچین بیت‌کوین متأثر از محدودیت حجم بلاک مطرح شدند که تعداد تراکنش‌های قابل جایگیری در هر بلاک را محدود کرده است. به خاطر همین مشکل است که شاهد تأخیر چندساعته و حتی چندروزه پردازش و تأیید تراکنش‌ها بوده‌ایم. چنانکه شرح آن رفت اتریوم هم با محدودیت‌هایی در مقیاس‌پذیری روبرو است.

تا موفق به حل مشکل مقیاس‌پذیری بلاکچین نشویم، سرعت رشد و گستردگی کاربردهای بلاک‌چین محدود خواهد بود.

راه‌حل اول: سِگویت (مختص بیت‌کوین)

هر تراکنش بیت‌کوینی شامل موارد زیر است:

ورودی:

- جزئیات تراکنش‌های قبلی فرستنده.
- کلید خصوصی (private key) منحصربه‌فرد فرستنده (scriptSig) که کافی بودن موجودی فرستنده را برای انجام تراکنش تأیید می‌کند.

خروجی:

- مبلغ فرستادن
- آدرس عمومی فرستنده (ScriptPubKey)

از میان این عناصر، امضای دیجیتال (کلید خصوصی) ازنظر اندازه از همه بزرگ‌تر است و ٪۶۰ الی ٪۷۰ حجم تراکنش را به خود اختصاص می‌دهد و فقط در مرحله تأیید لازم است.

شاهد مجزا (Segregated Witness) که به‌اختصار سِگویت (Segwit) خوانده می‌شود راه‌حلی است که در آن امضای تراکنش (شاهد) از باقی اطلاعات تراکنش جدا می‌گردد. امضا از درون بخش ورودی جداشده و در پایان تراکنش انتقال می‌یابد.

علاوه بر این در سگویت، شاهد به فیلدی جدید در داده‌های تراکنش انتقال پیدا می‌کند و ما را قادر می‌سازد روش محاسبه اندازه بلوک را تغییر دهیم و به‌جای بایت بلوک‌های تراکنش را با واحدی جدید به نام وزن اندازه‌گیری کنیم. وزن نشان‌دهنده تقاضا و باری است که بلوک بر منابع هر گره تحمیل می‌کند. به‌طور مشخص به هر بایت از شاهد مجزا ۱ واحد وزن داده می‌شود و بایت‌های مربوط به دیگر بخش‌های بلوک ۴ واحد وزن محاسبه می‌گردد. حداکثر وزن مجاز برای یک بلوک چهار میلیون واحد تعیین می‌گردد و به بلوک حاوی شاهد مجزا اجازه می‌دهد میزان بیشتری داده نسبت به قبل در خود جای دهد. در عمل این کار باعث افزایش اندازه بلوک از ۱ مگابایت به چیزی حدود ۴ مگابایت می‌شود و توانایی بلاک‌چین برای انجام تراکنش‌ها را ٪۷۰ افزایش می‌دهد.

سِگویت علاوه بر مشکل مقیاس‌پذیری بلاکچین، مشکل امنیتی (چکش‌خواری تراکنش) (transaction malleability) را هم حل کرده و باعث ارتقای امنیت هم می‌شود.

راه‌حل دوم: بلوک ۲ مگابایتی (مختص بیت‌کوین)

اگرچه کاربران بیت‌کوین حامیان پر و پا قرص سگویت هستند، در طرف دیگر استخراج‌گران یا همان ماینرها طرفدار تغییر کلی پروتکل (hard fork) و افزایش اندازه بلوک از ۱ مگابایت به ۲ مگابایت هستند. ایده اصلی این است که با افزایش اندازه بلوک، تعداد بیشتری تراکنش در هر بلوک می‌تواند جای گیرد و شبکه بتواند تعداد بیشتری تراکنش در هر ثانیه انجام دهد. برنامه افزایش اندازه بلوک مدت‌ها میان جامعه

بیت‌کوین محل مناظرات داغی بوده است و از آغاز سال ۲۰۱۵ با نزدیک شدن اندازه بلوک‌ها به محدودیت سخت ۱ مگابایت کنونی اقبال بیشتری پیداکرده است.

راه‌حل سوم: کانال حالت در خارج زنجیره

کانال‌های حالت (State Channel) اساساً مکانیسمی هستند که به‌وسیله‌ی آن‌ها فعل‌وانفعالاتی که به‌طورمعمول روی خود بلاک‌چین صورت می‌پذیرند، به خارج بلاک‌چین انتقال می‌یابند.

این امر به‌صورت رمزنگاری‌شده و از طریقی امن انجام می‌گیرد و بی آن‌که ریسک دخالت دیگران را زیاد کند، باعث صرفه‌جویی در هزینه و افزایش سرعت می‌گردد. باور من این است که کانال‌های حالت در آینده قسمت مهمی از فناوری خواهد بود که مشکل مقیاس‌پذیری بلاکچین را حل خواهد کرد.

طرز کار یک کانال حالت بدین قرار است:

- قسمتی از حالت بلاکچین از طریق چند امضا یا نوعی قرارداد هوشمند قفل‌شده است و تنها راه به‌روزرسانی‌اش آن است که مجموعه بخصوصی از مشارکت‌کنندگان کاملاً موافق این کار باشند.
- مشارکت‌کنندگان با ایجاد و امضای رمزنگاری‌شده تراکنش‌ها بین خودشان به‌روزرسانی‌هایی انجام می‌دهند اما آن را برای ثبت به بلاکچین عرضه نمی‌کنند. هر به‌روزرسانی جدیدی روی قبلی نوشته می‌شود.
- یک مدت بعد، بالاخره مشارکت‌کنندگان حالت را به بلاکچین ارسال می‌کنند و با این کار کانال حالت بسته‌شده و حالت برای بار دیگر از حالت قفل خارج می‌شود.

مراحل اول و سوم شامل عملیات بلاکچین می‌شوند که در شبکه منتشرشده، کارمزد پرداخته و منتظر تأیید می‌مانند؛ اما در مرحله دوم بلاکچین به‌هیچ‌وجه درگیر نمی‌شود. مرحله دوم می‌تواند شامل بی‌نهایت به‌روزرسانی باشد و بدون محدودیت زمانی بازبماند.

این‌گونه بلاکچین به‌صورت خالص به‌عنوان لایه توافق تسویه نهایی (settlement layer) به کار می‌رود و در آن فقط آخرین تراکنشی که در پی مجموعه‌ای از تعاملات صورت گرفته پردازش می‌شود. با این کار بار زیادی از دوش بلاکچین برداشته می‌شود.

کانال‌های حالت علاوه برافزایش ظرفیت تراکنش، دو ویژگی مثبت دیگر هم به ارمغان می‌آورند: سرعت بیشتر و کارمزد کمتر.

چون اکثر تراکنش‌ها خارج از بلاک‌چین رخ می‌دهند، در به‌روزرسانی بین دو نفر دیگر نیازی به‌صرف زمان برای پردازش و تأیید شبکه نیست و پرداخت‌ها می‌توانند آنی پردازش شوند. علاوه بر این با انتقال اکثر تراکنش‌ها به خارج از بلاک‌چین دیگر نیازی به پرداخت کارمزد برای همه تراکنش‌ها نخواهد بود و ثبت تعداد اندکی از تراکنش‌ها روی بلاکچین برای ثبت توافق تسویه کانال‌های حالت کافی است. این ایده به صورت‌های متعددی پیاده‌سازی شده است. برای مثال شبکه لایتنینگ (lightning) یک شبکه غیرمتمرکز است که با استفاده از قراردادهای هوشمند (smart contracts) از کانال‌های حالت برای حل مشکل مقیاس‌پذیری بلاکچین بهره می‌برد و قادر است پرداخت‌های آنی و مقیاس‌پذیر را روی شبکه برای مشارکت‌کنندگان تأمین نماید.

شبکه لایتنینگ در ابتدا برای بیت‌کوین خلق‌شده بود اما اکنون به نظر می‌رسد اجازه انجام سایر تراکنش‌ها هم ممکن باشد. رِیدن نتورک (raiden network) معادل لایتنینگ نتورک برای اتریوم است و از کانال‌های حالت خارج از بلاکچین برای ارتقای مقیاس‌پذیری و انجام تراکنش‌های آنی با اتریوم بهره می‌برد.

راه‌حل چهارم: بخش‌بندی

بخش‌بندی (sharding) در دنیای بلاکچین مشابه بخش‌بندی پایگاه داده در سامانه‌های نرم‌افزاری معمول است. در پایگاه داده سنتی، یک بخش (shard) درواقع یک پارتیشن افقی از داده‌ها است که روی یک نمونه (instance) مجزا از سرور پایگاه داده (database server) ذخیره می‌شود. این امر باعث تقسیم بار روی سرورهای مختلف می‌گردد.

مشابه همین کار در بخش‌بندی بلاکچین، حالت کلی بلاکچین به چندین بخش (shard) تقسیم‌شده و هر قسمتی از حالت روی گره متفاوتی از شبکه ذخیره خواهد شد. تراکنش‌های روی شبکه بسته به این‌که روی کدام بخش تأثیر می‌گذارند به گره متفاوتی هدایت خواهند شد. هر بخش قسمت کوچکی از حالت کل بلاکچین را به‌صورت موازی پردازش می‌کند. برای برقراری ارتباط بین بخش‌ها نیاز به یک مکانیسم برای انتقال پیام است .(message passing) پیاده‌سازی این مکانیسم هم به روش‌های متعددی انجام‌گرفته است. در اتریوم از پارادایم رسید (receipt)برای این امر استفاده‌شده است. وقتی در یک بخش تراکنشی اجرا می‌شود و حالت بخش محلی خود را تغییر می‌دهد، هم‌زمان با این کار یک رسید هم ایجاد می‌شود. این رسید بر روی یک حافظه اشتراکی فقط خواندنی میان بخش‌ها به اشتراک گذاشته می‌شود.

در حالت کلی، برای بخش‌بندی بلاکچین نیاز به شبکه‌ای داریم که با حفظ امنیت کامل، هر گره شبکه فقط بخش کوچکی از تمام تراکنش‌ها را پردازش کند و این چالش بسیار بزرگی است. همان‌طور که قبلاً اشاره شد، در شبکه بلاکچین فرض بر آن است که هر گرهی در شبکه به هیچ گره دیگری اعتماد ندارد و باوجوداین لازم است تراکنش‌ها بر روی حالت واحدی که در رایانه‌های دیگر پرداز شده اجماع داشته باشند. با توجه به عدم وجود اعتماد بین گره‌ها، یک گره روی بخش الف نمی‌تواند به گره‌های روی بخش ب صرفاً بگوید تراکنشی انجام‌گرفته؛ بلکه باید وقوع این تراکنش را به نحوی اثبات نماید. با توجه به اینکه هدف بخش‌بندی این است که نیاز نباشد هر گرهی در شبکه تمام تراکنش‌ها را تأیید کند؛ باید مکانیسمی طراحی کنیم که تعیین کند کدام گره کدام بخش را تأیید نماید. این کار باید با حفظ امنیت انجام گیرد و فرصت حمله به هکرها ندهد.

دلیل دیگری که پیاده‌سازی بخش‌بندی را دشوار می‌کند این است که یک تراکنش اجراشده روی بلاکچین می‌تواند وابسته به هر قسمتی از حالت قبلی بلاکچین وابسته باشد و این مهم انجام موازی کارها را با مشکل مواجه می‌کند. علاوه بر این، موازی‌سازی باید با روشی محفوظ از خطا چالش وضعیت رقابتی (race condition) را هم کنترل نماید. چگونگی پیاده‌سازی بخش‌بندی روی اترویم برای حل مشکل مقیاس‌پذیری بلاکچین جزئیات فنی مفصلی دارد؛ مانند اینکه چگونه با ایجاد انگیزه کریپتو-اکونومیکی (cryptoeconomic) بازیگران از تقلب کردن و ارسال اطلاعات نادرست به دیگر گره‌ها بازداشته می‌شوند.

راه حل پنجم: پلاسما

پلاسما (Plasma) به‌تازگی معرفی‌شده و در میان راه‌حل‌های مشکل مقیاس‌پذیری بلاکچین جزو امیدوارکننده‌ترین‌ها است. اساساً پلاسما یک سری از قراردادها است که مضاف بر یک بلاکچین ریشه (root blockchain) (مثل بلاکچین اصلی اتریوم) اجرا می‌شوند. بلاکچین ریشه صحت حالت زنجیره‌های پلاسما را کنترل می‌کند. این کار به‌وسیله مکانیسمی به نام گواه تقلب (fraud proofs) انجام می‌پذیرد که در آن گره‌ها با اثبات ریاضی می‌توانند نامعتبر بودن یک بلوک را مشخص کنند.

بلاکچین‌ها در یک سلسله‌مراتب درختی انتظام یافته‌اند و با هر شاخه به‌عنوان یک بلاکچین که خودش تاریخچه خودش را دارد رفتار می‌شود. ضمناً پردازش‌های هر شاخه قابلیت نگاشت کاهش پیچیدگی (map-reducable) را هم دارا هست. این زنجیره‌های فرزند (child) را بلاکچین پلاسما می‌خوانیم که هریک زنجیره‌ای درون بلاکچین هستند. بلاکچین پلاسما محتویات خود را برای زنجیره‌ی ریشه آشکار نمی‌کند و فقط هش‌های هدرهای بلوک (blockheader hashes) به زنجیره‌ی ریشه ارسال می‌شوند که برای تشخیص صحت بلوک کافی است. اگر روی زنجیره‌ی ریشه گواهی برای اثبات تقلب یافت شود، بلوک برمی‌گردد و فرستنده تنبیه می‌شود (به‌بیان‌دیگر حل مشکل بیزانس).

نتیجه‌ای که به دست می‌آید آن است که بلاکچین ریشه فقط میزان اندکی از تعداد بلاکچین فرزند را پردازش می‌کند که باعث کاهش ارسال داده به بلاکچین ریشه شده و انجام محاسبات به‌مراتب بزرگ‌تری را ممکن می‌سازد. علاوه بر این، داده‌ها فقط میان کسانی انتشار می‌یابد که خواهان تأیید صحت حالتی خاص هستند. این امر مقیاس‌پذیری اجرای قراردادها (contracts) را بیشتر می‌کند؛ چون دیگر نیاز نیست تمام گره‌ها ناظر بر تمام زنجیره‌ها باشند. به‌جای این کار، گره‌ها فقط بر مواردی که ازنظر اقتصادی بر آن‌ها تأثیر می‌گذارند نظارت کرده و با تشخیص تقلب و اعمال تنبیه بر گره متقلب صحت اطلاعات را تضمین می‌نمایند. روش گواه تقلب به هر طرفی اجازه می‌دهد بر بلوک‌های نامعتبر نظارت داشته و صحت تمام تغییرات حالت را تأیید کنند. اگر حمله‌ای روی یک زنجیره واقع شود، مشارکت‌کنندگان می‌توانند به‌سرعت و بدون صرف هزینه قابل‌توجه همگی از زنجیره فرزند تخریب‌شده خارج شوند.

پلاسما شاید مشابه پیاده‌سازی کانال‌های حالت به نظر برسد؛ اما در پلاسما نیازی به آنلاین بودن تمام مشارکت‌کنندگان برای به‌روزرسانی حالت نیست. علاوه بر این نیازی به ارسال اطلاعات به بلاکچین ریشه جهت همکاری و تأیید تراکنش‌ها هم نیست. با ترکیب پلاسما و کانال

حالت می‌توان ترتیبی اندیشید که کانال حالت لایه رابط اصلی (interface) برای پرداخت‌های مالی با سرعت‌بالا باشد و پلاسما وظیفه اعمال به‌روزرسانی‌ها در حالت را با تحمیل حداقل بار روی زنجیره ریشه عهده‌دار شود.

راه‌حل ششم: پردازش خارج از زنجیره

تروبیت (TrueBit) مثالی از حل مشکل مقیاس‌پذیری بلاکچین با استفاده از پردازش خارج از زنجیره است که مقیاس‌پذیری تراکنش‌ها میان قراردادهای هوشمند (smart contracts) در اتریوم را امکان‌پذیر کرده است. اساساً تروبیت هم مانند کانال‌های حالت از یک لایه خارج بلاکچین برای کشیدن بار اصلی استفاده می‌کند. به‌بیان‌دیگر سامانه‌ای است که پردازش را به روشی قابل‌تأیید در خارج زنجیره اجرا می‌کند تا هزینه پردازش را به‌مراتب پایین‌تر آورد. طرز کار آن به شرح زیر است:

به‌جای تمام گره‌های شرکت‌کننده، تنها مشارکت‌کنندگان بخصوصی در شبکه که حل‌کننده (Solver) نامیده می‌شوند وظیفه پردازش را بر عهده می‌گیرند. این مهم به‌وسیله قراردادهای هوشمند انجام می‌گیرد که در آن راه‌حل مسئله به‌ضمیمه میزانی اعتبار (deposit) ارسال می‌شود. در صورت درست بودن راه‌حل، به حل‌کننده پاداش داده‌شده و اعتبارش بازگردانده می‌شود. در غیر این صورت زمانی که حل‌کننده تقلب کرده باشد، اعتبار ضبط می‌شود. اختلاف‌نظرها در بلاکچین توسط بازی تأیید (Verification Game) صورت می‌گیرد.

بازی تأیید این‌گونه است که مجموعه‌ای از مشارکت‌کنندگان به نام تأییدکننده (Verifier) در شبکه وجود دارند که صحت کار حل‌کننده‌ها را در خارج بلاکچین چک می‌کنند. اگر هیچ تأییدکننده‌ای خطا ارسال نکند، سامانه راه‌حل را قبول خواهد کرد. اگر یکی از تأیید کنندگان صحت راه‌حل را زیر سؤال ببرد، برای حل اختلاف‌نظر بازی به مجموعه مراحل جدیدی کشیده می‌شود که مشارکت‌کنندگان دیگری به نام داور (Judge) باقدرت پردازشی محدود درباره اختلاف‌نظرها داوری می‌کنند. سامانه طوری طراحی‌شده است که اطمینان حاصل شود که کار انجام‌شده توسط داوران در مقایسه باکار موردنیاز برای انجام همان وظیفه در خارج بلاکچین ناچیز باشد. در پایان این بازی، اگر حل‌کننده واقعاً تقلب کرده باشد، کشف‌شده و مجازات خواهد شد. در غیر این صورت، تأییدکننده‌ای که چالش را آغاز کرده بود قیمت منابع مصروف در فرایند بازی را خواهد پرداخت. در آخر، برای توجیه تأیید کننده‌ها در مورد واقعی بودن امکان وجود خطا و تشویق آن‌ها برای مشارکت، تروبیت کار جالبی انجام می‌دهد. تروبیت خودش گاهی حل‌کنندگان را مجبور به ایجاد خطا می‌کند! به این صورت که مدل پاداش‌دهی سیستم عوض‌شده و از حل‌کننده ارسال پاسخ اشتباه خواسته می‌شود. این امر تضمین می‌کند همیشه پاداشی برای تأیید کننده‌ها تراکنش وجود داشته باشد. به‌طور خلاصه، پروتکل به همه اجازه ایجاد وظیفه پردازشی و دریافت پاداش در قبال انجام پردازش را می‌دهد. ساختار پاداش‌دهی در سیستم صحت پاسخ‌ها را تضمین می‌کند. با این کار فرایند تأیید از دوش بلاکچین اتریوم برداشته‌شده و مطابق با پروتکلی مجزا می‌تواند بدون پایبندی به محدودیت سوخت اتریوم به هر میزان پردازش افزایش باید.

دیگر راه‌حل‌های پیشنهادی:

تعدادی راه‌حل در جامعه فعالین ارزهای رمزنگاری‌شده مطرح‌شده که به نظر من جالب هستند. اگرچه راه‌حل‌ها به‌طور مستقیم برای حل مشکل مقیاس‌پذیری بلاکچین ارائه نشده‌اند، به‌طور غیرمستقیم بر ارتقاء سطح مقیاس‌پذیری اثر می‌گذارند.

اثبات-سهام

مشابه اثبات-کار (Proof-of-work)، اثبات-سهام (Proof of stake) مکانیسمی برای اجماع است که امنیت بلاکچین را در برابر خرج-مضاعف (doublespend) تضمین می‌کند.

در بلاکچین‌های متکی به اثبات-کار سنتی، ماینرها صحت داده‌های بلاکچین را با رقابت برای حل کردن معمای ریاضی و دریافت پاداش در برابر اثبات-کار تأمین می‌کنند. آن‌ها برای تأیید تراکنش از قدرت پردازشی استفاده می‌کنند و با دارا بودن قدرت بالای پردازش، توانایی تأثیر در شبکه هم متناسب با آن افزایش می‌یابد. در اثبات-سهام، سهامداران به‌جای قدرت پردازشی با پول (مثلاً در اتریوم با اتر) رأی می‌دهند.

بلاکچین تعدادی گره تأییدکننده بخصوص را زیر نظر می‌گیرد که به آن‌ها اعتبارسنج (validator) خواهیم گفت. اعتبارسنج‌ها برای شرکت در تأیید بلوک‌ها باید میزانی اعتبار (deposit) امنیتی اختصاص دهند. به این کار تضمین (bonding) می‌گویند. اگر یک گره اعتبارسنج محصولی ایجاد کند که بر اساس روشی مبتنی بر رمزنگاری در پروتکل غیر معتبر باشد، مبلغ تضمین اختصاص‌یافته توسط آن‌ها ضبط‌شده و مجوز مشارکت آن‌ها در فرایند اجماع باطل می‌گردد؛ اما اگر کارشان درست باشد، تضمینشان بازگشته و مبلغی را هم به‌عنوان کارمزد تراکنش

دریافت می‌کنند. به‌صورت مؤثری اعتبارسنج‌ها با شرط بستن خلاف جهت اجماع نهایی پول ازدست‌داده و با شرط‌بندی هم‌جهت با آن پول می‌برند. به‌صورت مشابهی در یک سیستم اثبات-کار، هر ماینر باقدرت پردازش خود (hash power) روی بلوکی که تأیید خواهد شد شرط می‌بندد. اگر شرطشان اشتباه باشد و بخواهند تقلب کنند، هر بلوکی که ایجاد کنند یتیم (orphan) خواهد بود و پول از دست خواهند داد.

اثبات-سهام چگونه به حل مشکل مقیاس‌پذیری بلاکچین کمک می‌کند؟

یک مثال برای این کار بخش‌بندی (sharding) است. اجرای بخش‌بندی همراه با اثبات-کار ازنظر امنیتی دشوار است. به یاد بیاورید که با بخش‌بندی، مسئولیت اعتبار سنجی و تأیید را میان گره‌ها تقسیم می‌کنیم به‌طوری‌که نیاز نباشد هر گرهی تمام پردازش را انجام دهد. در اثبات-کار پیاده‌سازی به‌گونه‌ای است که گمنامی به‌طور کامل برقرار باشد؛ و اینجا است که مشکل بروز می‌کند. اگر امنیت یک بخش (shard) باقدرت پردازش محدود یک ماینر برقرار باشد، یک هکر با هدایت قدرت پردازش بزرگی به آن بخش می‌تواند باعث ایجاد اختلال در شبکه گردد. فرض کنید بخش الف ٪۹۰ قدرت پردازش و بخش ب تنها ٪۱۰ آن را در اختیار داشته باشد. بخش الف می‌تواند با اختصاص تنها ٪۵،۱ از قدرت پردازش خود به بخش ب حمله کند (حمله اکثریت).

در اثبات-سهام اتریوم اما ماجرا متفاوت است چون به‌نوعی طراحی‌شده است که گره‌های اعتبارسنج هویت مشخصی دارند (آدرس اتریوم). با دانستن هویت آن‌ها و انتخاب تصادفی مجموعه‌ای از گره‌های اعتبارسنج برای پردازش مجموعه‌ای از تراکنش‌ها روی یک بخش، توانایی حمله به یک بخش معین از اعتبارسنجان سلب می‌شود.

کمک دیگر اثبات-سهام به مقیاس‌پذیری (در مورد اتریوم) آن است که برخلاف اثبات-کار که توکن (token) جدید برای ماینرهای تأییدکننده بلوک صادر می‌شود، درآمد در اثبات-سهام عموماً منحصر به کارمزد تراکنش است. درنتیجه در صورت توانایی سرور، انگیزه افزایش محدودیت سوخت برای هر بلوک در آن‌ها ایجاد می‌شود تا با جای گرفتن تراکنش بیشتر در هر بلوک کارمزد بیشتری کسب کنند. محدودکننده این افزایش چیزی نیست جز توانایی گره‌های دیگر، زیرا در صورت بر هم خوردن همگامی (synchronization) در گره‌های کندتر، درآمدشان کاهش خواهد یافت.

اجاره بلاکچین (مختص اتریوم)

هدف راه‌حل اجاره بلاکچین (Blockchain rent) این است که میزان داده‌ای را که در شبکه ذخیره می‌شود کاهش دهد تا از این طریق سرعت انجام تراکنش‌ها افزایش یابد. در اتریوم کاربران در قبال مراحل پردازشی، حافظه، سوابق پردازش و حافظه بلندمدت حاضر به دادن پاداش هستند. هدف این است که ذخیره‌سازی (storage) از این میان حرف شود. در سیستم فعلی، معیار پرداخت پاداش برای فضای ذخیره‌سازی بایت است. در اجاره بلاکچین معیار بایت*زمان خواهد بود. از طریق تغییر معیار پاداش در پروتکل، شبکه سبک‌تر شده و زمان تراکنش‌ها کاهش می‌یابد.

ذخیره‌سازی غیرمتمرکز

راه‌حل دیگر برای سبک‌تر کردن شبکه استفاده از یک سرویس ذخیره‌سازی غیرمتمرکز (Decentralized storage) مانند سوارم (Swarm) است. سوارم یک پروتکل اشتراک داده همتابه‌همتا (peer-to-peer) برای اترویم است که به شما اجازه می‌دهد کد برنامه را خارج از بلاکچین اصلی و در گره‌های سوارم مرتبط با بلاکچین ذخیره کنید. فرضیه اصلی آن است که به‌جای ذخیره همه‌چیز روی بلاکچین، فقط داده‌هایی که به‌صورت محلی مکرراً درخواست می‌شوند روی بلاکچین ذخیره‌شده و باقی از طریق سوارم روی ابر (cloud) ذخیره شود.

نتیجه‌گیری

این بحث به‌طور غول‌آسایی پیچیده است. امیدوارم این نوشته توانسته باشد تصویری کلی از دلیل اهمیت مشکل مقیاس‌پذیری بلاکچین و راه‌حل‌های ممکن به شما عرضه داشته باشد.

من بر این عقیده‌ام که احتمالاً یک راه‌حل تنها برای حل قطعی مشکل مقیاس‌پذیری بلاکچین وجود ندارد، اما فکر می‌کنم ترکیبی از آن‌ها بتوانند به‌مرور این مسئله را حل کنند؛ و آن‌وقت خواهیم دید چه جهش بزرگی در کاربردهای بلاکچین کلید خواهد خورد.

اجماع Consensus

الگوریتم های اجماع برای رسیدن به قابلیت اطمینان در یک شبکه شامل گره های غیر قابل اعتماد طراحی شده اند و انواع مختلفی از مکانیسم های اجماع توسعه وجود دارد.

الگوریتم اجماع(consensus algorithm) ، فرآیندی در علوم کامپیوتر است که برای دستیابی به توافق بر روی یک مقدار داده ای واحد در میان سیستم های توزیع شده مورد استفاده قرار می گیرد. الگوریتم های اجماع برای رسیدن به قابلیت اطمینان در یک شبکه شامل گره های غیر قابل اعتماد طراحی شده اند. حل این مسئله که معمولاً با عنوان مشکل اجماع شناخته می شود در رایانه های توزیع شده و سیستم های چند عاملی بسیار حائز اهمیت است .برای تطبیق پذیری با این واقعیت، الگوریتم های اجماع لزوماً فرض می کنند که برخی از فرآیندها و سیستم ها در دسترس نیستند و برخی از ارتباطات از بین خواهند رفت. بنابراین، الگوریتم های اجماع باید به صورت تحمل پذیر خطا طراحی شوند.

کاربردهای الگوریتم های اجماع شامل موارد زیر است:

- تصمیم گیری در مورد ارسال یک تراکنش توزیع شده به یک پایگاه داده
- تعیین گره هایی به عنوان سر گروه برای انجام برخی از وظایف توزیع شده
- همگام سازی نسخه های ماشین حالت و تضمین سازگاری در میان آنها

مکانیسم های اجماع

مکانیسم های اجماع روشی برای تضمین یک توافق دو طرفه بر روی نکات داده ای و وضعیت تمام داده ها به شمار می روند. این مکانیسم ها در شبکه بلاک چین تضمین می کنند که هر کدام از بازیگران شبکه، یک کپی از دفتر کل یکسان را در اختیار دارند. مکانیسم های اجماع مختلف، امنیت و چارچوب اقتصادی پروتکل رمزنگاری را تحت تأثیر قرار می دهند. این مکانیسم ها به شکل های متفاوت برای بلاک چین های مختلف ارائه می شوند. مکانیسم های اجماع در آغاز راه قرار دارند و پیش بینی مکانیسم غالب در آینده دشوار است. ایجاد مکانیسم های اجماع بر اساس طراحی مکانیسم انجام می شود که یک فرآیند دو مرحله ای است:

۱. در نظر گرفتن نتیجه مورد نظر
۲. عملکرد وارونه برای ایجاد یک بازی و تشویق بازیگران برای انجام آن بازی و تولید خروجی مورد نظر

اجماع یا توافق جمعی

لایه اجماع یا توافق جمعی یکی از مهمترین لایه‌ها در هر سیستم مبتنی بر بلاک چین است. این لایه برای حفظ قابلیت اعتماد شبکه با فرض وجود اعضای غیر قابل اعتماد ایجاد شده است. یک فرد یا یک رایانه [به عنوان نماینده فرد] می خواهند خدماتی مانند ارسال ایمیل، ثبت تراکنش های مالی، ذخیره سازی اطلاعات یا هر خدمات دیگری را ارائه دهند. اگر انجام این خدمات هزینه ای نداشته باشد یا هزینه آن به اندازه کافی ناچیز باشد، استفاده از این خدمات برای امور نامربوط و بی ارزش و یا به قصد خرابکاری توجیه پذیر خواهد بود که به آن مشکل Nothing at Stake یا سنگ مفت گفته می شود .برای جلوگیری از استفاده نامربوط باید هزینه‌ای برای خدمات ایجاد کرد و خدمات دهنده باید به روشی این هزینه را اثبات کند. در سامانه‌هایی غیر متمرکز استفاده از تنبیه‌های قانونی و نهاد های متمرکز بازرسی و اعمال قانون امکان پذیر نیست و سامانه باید روشی جایگزین برای ثبات هزینه خدمات ارائه نماید.

انواع الگوریتم اجماع

- گواه اثبات کار Proof of Work
- گواه اثبات سهام Proof of Stake
- گواه اجماع گواه اثبات زمان سپری شده Proof of Elapsed Time
- گواه اثبات قدرت Proof of Authority

- گواه اثبات ظرفیت Proof of Capacity
- گواه اثبات فعالیت Proof of Activity
- گواه اثبات سوزاندن Proof of Burn
- واه اثبات سهام اعطایی Delegated Proof of Stake
- گواه اثبات اهمیت Proof of Importance
- گراف جهت‌دار غیرمدور Direct Acyclic Graphs
- تحمل‌پذیری خطای بیزانس Byzantine Fault Tolerance
- تحمل خطای بیزانسی Byzintine Fault Tolerance
- ...

یک شبکه‌ی توزیع شده از گره‌های کامپیوتری چگونه می‌تواند روی یک تصمیم به توافق برسد در حالی که احتمال کوتاهی و ناراستی برخی گره‌ها وجود دارد؟ این پرسش اساسی مساله‌ای به نام ژنرال‌های بیزانسی است که سرچشمه‌ی به وجود آمدن مفهوم تحمل خطای بیزانسی گردیده است. تحمل خطای بیزانسی یا BFT ویژگی سیستمی است که می‌تواند در برابر همه‌ی خرابی‌هایی که در رده قضیه ژنرال‌های بیزانسی قرار می‌گیرند مقاومت کند. یعنی یک سیستم BFT حتی اگر برخی از گره‌های آن کار نکنند یا بدخواهانه کار کنند، قادر است عملیات خود را ادامه دهد .از سال ۲۰۰۸ که بیت کوین به عنوان یک سیستم پول الکترونیکی همتا به همتا کار خود را شروع کرد، ارزهای رمزنگاری شده فراوانی در کنار آن به وجود آمده است و هر یک از آن‌ها ساز و کار خاصی دارد. در این میان یک ویژگی مشترک در میان تمام ارزهای رمزنگاری شده بلاکچین است که عنصر اصلی معماری آن‌ها را تشکیل می‌دهد. به استثنای چند مورد، همه بلاکچین‌ها با این هدف طراحی شده‌اند که تمرکز زدایی کنند و نقش دفتر کل دیجیتالی را بازی کنند که شبکه توزیع شده‌ای از گره‌های کامپیوتری از آن نگهداری می‌کند. از این رو فناوری بلاکچین زمینه‌ی پیدایش سیستم‌های اقتصادی بی‌واسطه را فراهم ساخته است. سیستم‌هایی که به وسیله‌ی آن‌ها می‌توان تراکنش‌های مالی را با اطمینان بالا، شفافیت کامل و بی‌نیاز از هرگونه واسطه انجام داد. ارزهای رمزنگاری شده هم‌اکنون به عنوان یک جایگزین مناسب برای بانکداری و سیستم‌های پرداخت سنتی (که به شدت وابسته به اعتماد هستند) به کار می‌روند. همانند بیشتر سیستم‌های کامپیوتری توزیع شده، مشترکان یک شبکه‌ی کریپتوکارنسی باید به طور مداوم موافقت خود را با حالت کنونی بلاکچین اعلام کنند. این همان دستاوردی است که اجماع نامیده می‌شود. رسیدن به اجماع در شبکه‌های توزیع شده با وجودی که روشی ایمن و دارای اعتماد است، ولی به هیچ وجه آسان نیست. پس یک شبکه‌ی توزیع شده از گره‌های کامپیوتری چگونه می‌تواند روی یک تصمیم به توافق برسد در حالی که احتمال کوتاهی و ناراستی برخی گره‌ها وجود دارد؟ این پرسش اساسی مساله‌ای به نام ژنرال‌های بیزانسی است که سرچشمه‌ی به وجود آمدن مفهوم تحمل خطای بیزانسی گردیده است. مساله ژنرال‌های بیزانسی مساله‌ی ژنرال‌های بیزانسی (Byzantine generals) در سال ۱۹۸۲ مطرح شد. این قضیه منطقی می‌گوید شماری از ژنرال‌های بیزانسی (روم شرقی) که می‌خواهند بر سر اقدام بعدی تصمیم‌گیری کنند به لحاظ ارتباطی مشکل دارند. هر ژنرال سپاه خود را دارد و هر سپاه در یک سوی شهری که قرار است به آن حمله کنند مستقر شده است. ژنرال‌ها باید روی یک تصمیم اجماع کنند؛ یا حمله کنند یا بازگردند. مهم نیست آن‌ها کدام گزینه را انتخاب می‌کنند، مهم این است که همه‌ی ژنرال‌ها روی این گزینه اتفاق نظر داشته باشند زیرا تنها در صورت اجماع روی یک تصمیم می‌توانند هماهنگ و با همه‌ی توان اقدام نمایند. به این ترتیب شرایط زیر باید محقق گردند: هر ژنرال باید تصمیم بگیرد، حمله یا بازگشت (بله یا خیر)؛ پس از گرفتن تصمیم امکان عوض کردن آن وجود ندارد؛ همه‌ی ژنرال‌ها باید روی یک تصمیم به اتفاق آرا برسند و این تصمیم را به صورت همگام اجرا نمایند. مشکل ارتباطی که به آن اشاره کردیم این است که هر ژنرال تنها می‌توان به وسیله‌ی پیام با ژنرال دیگر ارتباط برقرار کند. پیام‌ها به وسیله‌ی پیک جابه‌جا می‌شوند. با این تفاسیر چالش اصلی در مساله‌ی ژنرال‌های بیزانسی این است که امکان تاخیر، نابودی و گم شدن پیام‌های ژنرال‌ها وجود دارد. افزون بر این، حتی اگر پیامی به خوبی به مقصد برسد ممکن است یک یا چند ژنرال (به هر دلیلی) تصمیم بگیرند اقدام بدخواهانه

انجام دهند و برای گیج کردن ژنرال‌های دیگر پیام نادرست بفرستند. در نتیجه همه‌چیز به هم می‌ریزد. اگر این مساله را در زمینه بلاکچین‌ها پیاده کنیم، هر گره شبکه مانند یک ژنرال است و گره‌ها باید بر سر وضعیت کنونی سیستم به اتفاق نظر برسند. به بیان دیگر، بیشتر شرکت کنندگان شبکه‌ی توزیع شده باید با یک اقدام مشترک موافقت کنند و آن را انجام دهند تا همه‌چیز به هم نریزد. به این ترتیب، تنها راه دستیابی به اجماع در این گونه سیستم‌های توزیع شده داشتن دسته‌کم ۲/۳ گره شبکه‌ی راستین و پایا (قابل اعتماد) است. این بدان معناست که اگر بخش عمده‌ی شبکه شبکه تصمیم بگیرد رفتار بدخواهانه انجام دهد، سیستم مستعد پذیرش انواع خرابی‌ها (failures) و حمله‌ها (attacks)می‌شود (مانند حمله ۵۱٪). تحمل خطای بیزانسی (BFT) به بیان ساده، تحمل خطای بیزانسی یا BFT ویژگی سیستمی است که می‌تواند در برابر همه‌ی خرابی‌هایی که در رده قضیه ژنرال‌های بیزانسی قرار می‌گیرند مقاومت کند. یعنی یک سیستم BFT حتی اگر برخی از گره‌های آن کار نکنند یا بدخواهانه کار کنند، قادر است عملیات خود را ادامه دهد. برای مساله‌ی ژنرال‌های بیزانسی بیش از یک راه‌حل وجود دارد، به همین خاطر برای ساختن یک سیستم BFT نیز راه‌های گوناگونی هست. به همین صورت، دستیابی به تحمل خطای بیزانسی در یک بلاکچین با رویکردهای گوناگونی امکان‌پذیر است و این شرایط ما را به چیزی به نام الگوریتم‌های اجماع می‌رساند. الگوریتم‌های اجماع بلاکچین ما می‌توانیم یک الگوریتم اجماع (consensus algorithm) را به گونه‌ای تعریف کنیم که یک شبکه‌ی بلاکچین با به کارگیری آن به اجماع برسد. رایج‌ترین شیوه‌ها در این زمینه (اثبات کار (PoW) (و (اثبات سهام (PoS) (هستند. بیایید به عنوان نمونه بیت کوین را بررسی کنیم. پروتکل بیت کوین دربردارنده‌ی قوانین اصلی سیستم بیت کوین است، ولی این الگوریتم اجماع PoW (اثبات کار) است که تعیین می‌کند این قوانین چگونه در راستای دستیابی به اجماع رعایت شوند (برای نمونه، در طول تایید و اعتبارسنجی تراکنش‌ها). با اینکه مفهوم اثبات کار (PoW) پیش از ارزهای رمزنگاری شده وجود داشته، ساتوشی ناکاموتو یک نسخه‌ی بهسازی شده از آن را به وجود آورد و این نسخه را در غالب الگوریتمی ارائه داد که زمینه‌ی تشکیل بیت کوین به عنوان یک سیستم BFT را فراهم نمود. خوب است بدانیم که الگوریتم اثبات کار ۱۰۰٪ نسبت به خطاهای بیزانسی تحمل ندارند ولی فرآیند استخراج پرهزینه و تکنیک‌های کریپتوگرافیک زیربنایی ثابت کرده‌اند که PoW (اثبات کار) یکی از امن‌ترین و مطمئن‌ترین شیوه‌های پیاده‌سازی برای شبکه‌های بلاکچین است. از این رهگذر، الگوریتم اجماع اثبات کار طراحی شده به دست ساتوشی ناکاموتو یکی از نبوغ‌آمیزترین راه‌حل‌های خطای بیزانسی محسوب می‌شود. نتیجه مساله‌ی ژنرال‌های بیزانسی یک قضیه‌ی جالب توجه است که در نهایت زمینه‌ساز پیدایش سیستم‌های BFT شد؛ سیستم‌هایی که در زمینه‌های گوناگون کاربردهای بسیار گسترده‌ای دارند. افزون بر صنعت بلاکچین، سیستم‌های BFT در زمینه‌های دیگری همچون هوانوردی، فضا و انرژی اتمی به کار گرفته شده‌اند. در زمینه‌ی کریپتوکارنسی، برخورداری از ارتباطات کارآمد در شبکه در کنار داشتن یک ساز و کار اجماع مناسب برای هر اکوسیستم بلاکچینی حیاتی است. تامین امنیت این سیستم‌ها نیازمند کوشش همیشگی است و الگوریتم‌های اجماع کنونی هنوز همه‌ی موانع و محدودیت‌ها (همچون مقیاس پذیری) را از سر راه برنداشته‌اند. در عین حال، PoWو PoS رویکردای بسیار جالبی هستند و سیستم‌های BFT کاربردهای بالقوه‌ی آن‌ها بی‌شک الهام‌بخش نوآوری‌های گسترده‌ای می‌شوند.

این مباحث چه ربطی به بلاکچین دارد؟ بلاکچین یک دفتر کل غیرمتمرکز است که عملا توسط نهادهای مرکزی کنترل نمی‌شود. با توجه به ارزشی که در این دفاتر کل نگهداری می‌شود، خیلی‌ها سعی می‌کنند این سیستم را با خطا مواجه نمایند. به همین خاطر، تحمل خطای بیزانس و راهکاری که بتواند مشکل ژنرال‌های بیزانس را حل کند برای بلاکچین نیز لازم است. در نبود سیستم تحمل خطای بیزانس، اعضای شبکه می‌توانند تراکنش‌های جعلی ارسال کنند و اعتمادپذیری بلاکچین را از بین ببرند. اوضاع زمانی بدتر می‌شود که به خاطر نبود نهادهای مرکزی، هیچ کسی نمی‌تواند مسئولیت ترمیم شرایط را برعهده بگیرد و خرابی‌ها را اصلاح کند. یکی از دستاوردهای بیت کوین این بود که از پروتکل اثبات کار به عنوان راهکاری مبتنی بر احتمال برای حل مشکل ژنرال‌های بیزانس استفاده می‌کرد.

گواه اثبات کار Proof of Work

پروتکل گواه اثبات کار بیت کوین یک شکل از اجماع است که ناکاموتو برای انتخاب گره‌ها طراحی کرده است و عمدتا برای محافظت در برابر خطاهای بیزانس) به طور عمده در برابر double spending توسط گره‌های مخرب (است. یک گره تلاش می‌کند مسئله رمزنگاری شده را حل کند که در آن احتمال یافتن راه حل متناسب با تلاش محاسباتی است و یافتن راه حل محاسباتی بسیار دشوار بوده و می‌توان آن را فقط با حدس زدن تصادفی به دست آورد. بنابراین به دلیل اینکه:

- هر گره در شبکه می‌تواند برای پیدا کردن راه حل تلاش کند.
- تعداد زیادی از گره‌ها برای مدت زمان معینی (تقریبا ۱۰ دقیقه) برای حل پازل رقابت می‌کنند.
- راه حل فقط می‌تواند به صورت تصادفی پیدا شود.

گره‌ای که به صورت مخرب عمل کند، فرصت کمی برای تحمیل بلوک مخرب (double spend) در شبکه دارد، مگر اینکه حمله کننده بیش از ٪۵۰ از منابع محاسباتی شبکه را تامین کند (حمله ۵۱ درصد). بنابراین، PoWیک روش غیر قابل قبول نفوذ ارائه می‌دهد مگر اینکه یک مهاجم بتواند بیش از ۵۰ درصد منابع را جمع آوری کند.

گاهی اوقات، ممکن است بیش از یک گره راه حل را در یک زمان پیدا کند. وقتی این اتفاق می‌افتد، هر یک از این گره‌ها یک بلوک را پیشنهاد می‌دهند و آن را به شبکه ارسال می‌کنند. این بلوک‌ها توسط بلوک‌های مجاور برداشت می‌شود و یک بلاک‌چین به صورت موقت شکل می‌گیرد و بلوک‌ها به زنجیره آنها اضافه می‌شود. در نهایت پروتکل شاخه‌ای که طولانی‌تر از بقیه می‌شود را به عنوان زنجیره رسمی انتخاب می‌کند و بقیه را از بین می‌برد.

نقاط قوت

در بیت‌کوین گره ای که برای ایجاد یک بلوک جدید انتخاب شده است، بابت ثبت تراکنش‌ها پاداش خود به صورت بیت‌کوین را دریافت می‌کند. به دلیل اینکه انجام محاسبات و استخراج پول کار بسیار پر تلاش و پر هزینه‌ای است، ماینرها تنها بر روی یک شاخه‌ای از بلاک‌چین تمرکز می‌کنند .

نقاط ضعف

چندین ضعف در روش PoW وجود دارد که مهمترین آن هزینه‌های انرژی قابل توجهی است که برای استخراج مصرف می‌شود و البته می‌توان به موارد زیر نیز اشاره کرد.

- استخراج متمرکز: به دلیل اینکه اختلافات زیادی در قدرت CPU کامپیوترها وجود دارد، کاربرانی که پردازنده‌های کم قدرت دارند اغلب میدان را به ماشین‌های قدرتمند می‌بازند. بنابراین، PoWنمی‌تواند الزامات الگوریتم اجماع مبنی بر اینکه گره‌های تصادفی باید در میان وسیعترین جمعیت ممکن از شرکت کنندگان انتخاب شوند را بر آورده سازد. این ضعف خطر استخراج متمرکز (استخرهای بزرگ پول) را افزایش می‌دهد.
- تأخیر زمانی زیاد (در بیت کوین): بلوک‌های جدید تقریبا هر ۱۰ دقیقه تولید می‌شود. در نتیجه انتظار برای تایید یک بلوک تولید شده برای یک تراکنش ممکن است تا ساعت‌ها طول بکشد چرا که یک تراکنش باید حتما توسط گره‌های موجود در زنجیر اصلی تایید شود تا مطمئن شد که بلوک تولید شده به شاخه اصلی بلاک‌چین اصلی متصل شده است.
- نرخ پایین تراکنش: حداکثر اندازه بلوک تایید شده تحت الگوریتم اجماع در شبکه بیت‌کوین، حداکثر ۷ تراکنش در ثانیه است که به نسبت تعداد کمی است.

گواه اثبات سهام Proof of Stake

گواه اثبات سهام (PoS) یکی از دو الگوریتم معروف اجماع در بلاک‌چین است (همراه باPoW) .در گواه اثبات سهام، بلوک‌های جدید به جای استخراج، (ساخته) می‌شوند. تحت شرایط گواه اثبات سهام، گره انتخاب شده برای ایجاد بلوک بعدی، از طریق یک فرآیند شبه تصادفی انتخاب می‌شود که این انتخاب به دارایی ذخیره شده در کیف پول (یا استخر سهام) مربوط به آن گره بستگی دارد. در این حالت، هیچ گره‌ای نمی‌تواند نوبت خود را پیش‌بینی کند. شمار مشخصی از سکه‌ها در استخر سهام نگهداری می‌شود تا شانس ایجاد بلوک را خریداری کنند.

برخلاف گواه اثبات کار (PoW) که در آن به ماینرها برای حل پازل ریاضی با هدف تایید تراکنش‌ها و ایجاد بلوک جدید جایزه داده می‌شد، در گواه اثبات سهام این خالق بلوک جدید است که بسته به میزان سرمایه‌اش یک راه قطعی انتخاب می‌کند. پس جایزه‌ای در کار نیست و ماینرها فقط کارمزد تراکنش‌ها را دریافت می‌کنند. البته قابل ذکر است که در سیستم PoS از کلمه Forgers بجای Miners استفاده می‌شود.

نقاط قوت

گواه اثبات سهام دارای مزایایی نسبت به گواه اثبات کار (PoW) است. گواه اثبات سهام قدرت محاسباتی زیادی مصرف نمی‌کند، با ممانعت از ایجاد استخرهای استخراج متمرکز(centralized mining pools) ، خطر حملات مخرب را کاهش می‌دهد و با توجه به اینکه سازنده بلوک‌ها، مالک بخشی از آن سکه‌ها نیز هستند، کسی که مسئولیت (محافظت) از سکه‌ها بر عهده دارد، مالک بخشی از آن سکه‌ها نیز هست. (اتفاقی که در گواه اثبات کار لزوما نمی‌افتد)

نقاط ضعف

یکی از نقاط ضعف گواه اثبات سهام در خطر نبودن سهام‌داران (nothing at stake) است. یک ماینر می تواند در زمان ایجاد انشعاب (Fork)با هر دو شاخه همراهی کند. این می‌تواند مانع شکل‌گیری اجماع بین گره‌ها شود و خطر دو بار خرج کردن (double spend) را افزایش می‌دهد.

گواه اثبات زمان سپری شده Proof of Elapsed Time

فصل امتحانات پایان ترم است و دانش‌آموزان خود را برای آزمون پایان‌ترم ریاضی آماده کرده‌اند. امتحان شروع می‌شود و پس از گذشت مدت زمانی مشخص، توجه همه به صدای مراقب امتحانات در سالن جلب می‌شود: (۳۰ دقیقه تا پایان وقت زمان باقی است.) درست یک ساعت پس از این جمله، همه بیرون از سالن امتحانات هستند و در مورد سوالات و نمرات احتمالی خود صحبت می‌کنند. اگرچه این تصویر برای همه ما آشنا است، اما کمتر کسی می‌تواند نحوه استفاده از آن در فناوری مدرن و شاید پیچیده‌ای همچون بلاکچین را درک کند.

مکانیسم اجماع گواه اثبات زمان سپری شده یا POET نیز به شکلی مشابه عمل می‌کند. در حقیقت، گواه اثبات زمان سپری شده، بر اساس زمان باقیمانده از یک زمان مشخص مانند زمان امتحان عمل می‌کند و برای شروع نیز از یک بلاکچین مجاز (Permissioned Blockchain) استفاده می‌کند. به این مفهوم که تمامی گره‌های موجود در بلاکچین استفاده کننده از این مکانیسم، قابل شناسایی و تایید شده برای شبکه هستند. درست همانند اعضای یک کلاس که یکدیگر را می‌شناسند و همگی برای شبکه (کلاس یا مدرسه) قابل تایید هستند (شما نمی‌توانید قبل از ثبت‌نام در کلاس و کسب مجوز از سوی آن وارد امتحانات پایان فصل شوید.)

اما مکانیسم اجماع گواه اثبات زمان سپری شده یک تفاوت عمده با مثال زمان امتحان دارد و آن، تصادفی بودن زمان باقیمانده برای هریک از اعضا یا گره‌های بلاکچین است. هریک از اعضای شرکت‌کننده در شبکه زمان تصادفی متفاوتی برای انتظار دریافت می‌کنند و هر گرهی که زمان‌اش قبل از بقیه به اتمام برسد می‌تواند بلوک بعدی بلاکچین را ایجاد کند. چیزی شبیه بازی کشیدن چوب کبریت خودمان، با این تفاوت که این‌بار، هرکس که اول از همه چوب کبریت شکسته را پیدا کند برنده می‌شود!

این مکانیسم اجماع نخستین بار در سال ۲۰۱۶ توسط اینتل (Intel) معرفی شد و می‌تواند در پلتفرم هایپر لجر سوتوث (Hyperledger Sawtooth) مورد استفاده قرار گیرد. پلتفرمی برای ایجاده، پیاده‌سازی و اجرای دفاتر کل توزیع‌شده.

تفاوت آن با گواه اثبات سهام: در نظر گرفتن زمان استراحت برای گره‌ها که منجر به ارتقای بهره‌وری در مصرف انرژی می‌شود.

گواه اثبات قدرت Proof of Authority

بلاکچین فناوری مدرن، کارآمد و روبه‌رشدی است، اما با این حال، محدودیت‌هایی را نیز دارد. به‌عبارت بهتر، فناوری بلاکچین نیز همانند بسیاری از سیستم‌های دیگر، بده‌بستان‌های خاص خودش را دارد. ویتالیک بوترین (Vitalik Buterin) از این موضوع تحت عنوان تریلمای مقیاس‌پذیری یاد می‌کند. تریلما به مفهوم سه گانه غیر ممکن، سه مشخصه مقیاس‌پذیری، غیرمتمرکز بودن و امنیت

را در بر می‌گیرد که به‌عنوان سه ضلع یک مثلث، به سختی در کنار هم قرار می‌گیرند. کافی است این سه مشخصه را همانند استراحت کافی، زندگی اجتماعی و نمرات خوب برای یک دانش‌آموز در نظر بگیرید که عملا دست‌یابی به هرسه آن‌ها در کنار هم غیرممکن است و معمولا، تنها دو مورد از این سه مشخصه را می‌توان به‌صورت هم‌زمان پوشش داد. البته با توجه به رشد فزاینده برنامه‌های کاربردی توزیع‌شده (dApps) در بستر ارزهای رمزنگاری‌شده‌ای نظیر اتریوم و امثال آن، به نظر می‌رسد که راهکارهای کوتاه مدت مبتنی بر مقیاس‌پذیری از اهمیت بالاتری برخوردار باشند.

سرمایه اقتصادی در قبال سرمایه اجتماعی

برخلاف مکانیسم اجماع گواه سهام، که سهم هر گره در آن بر اساس ارزش پولی آن مشخص می‌شود، گواه اثبات قدرت، سهم گره‌ها را بر مبنای هویت واقعی هر یک از آن‌ها تعیین می‌کند. درحقیقت، چرخه‌ای که در گواه اثبات سهام جریان دارد، ارزیابی ریسک‌ها متوجه یک سهم توسط اعضای شبکه است و آن‌چه که در مرکز توجه قرار دارد، سرمایه مالی موجود در سیستم است. در حالی که مکانیسم اجماع گواه اثبات قدرت، ماهیت گره‌ها را مورد توجه قرار داده و میزان انگیزه گره‌ها برای ریسک‌پذیری مالی را ارزیابی می‌کند.

برای درک بهتر این مکانیسم، افردی را متصور شوید که مجموع دارایی‌های خود در سطح شبکه را گرد آورده‌اند و ارزش این دارایی، رقمی مانند یک میلیارد دلار است. بدیهی است که اگر کل این سرمایه در اختیار یکی از گره‌ها قرار گیرد، شانس بیشتری برای موفقیت خواهد داشت. آن یک گره، دقیقا همان عضوی است که از آن با عنوان گره ارزیابی یاد می‌شود و این گره‌های ارزیاب، تنها اعضایی هستند که قادرند اعتبار یک بلوک را تعیین کنند. این مکانیسم را می‌توان به مثابه فرایند تایید اعتبار توسط ادمین در سیستم‌های متمرکز کنونی نیز قلمداد کرد که طبیعتا در مورد بلاکچین‌های خصوصی کاربرد بیشتری دارند تا بلاکچین‌های عمومی. به عبارت بهتر، اساس مکانیسم اجماع گواه اثبات قدرت، اعتماد کل سیستم به تعداد محدود و مشخصی از اعضا است و به همین دلیل نیز وجود فرایندهایی استاندارد و قابل اعتماد برای شناسایی و انتخاب این اعتبارسنج‌ها الزامی است.

اعتبارسنج‌ها (validators)، اعضایی هستند که اصطلاحا دارای اشتهار در شبکه هستند و در ضمن، تنها گره‌هایی هستند که می‌توانند بلوک‌ها را ارزیابی و اعتبارسنجی کنند. باتوجه به این‌که بخش اعظمی از سرمایه در اختیار این گره‌ها قرار دارد، طبیعی است که می‌توانند پست خود در تایید بلوک‌ها را موقتا و بدون اجازه رها کرده و جریمه یا خسارت ناشی از آن را به دلیل حجم بالای دریافتی از سیستم در ازای اعتبارسنجی جبران کنند. از همین رو، تعداد این اعتبارسنج‌ها در هر بلاکچین، معمولا تعداد محدودی است تا انگیزه کافی برای ماندن در این پست و عدم ترک آن را داشته باشند. در حالت کلی، برای کنترل این اعتبارسنج‌ها در بلاکچین، لازم است برخی نکات مورد توجه قرار گیرند:

- اطمینان از فرایندی استاندارد و قوی برای شناسایی اعتبارسنج‌ها

- کمیابی اعتبارسنج‌ها به منظور ترغیب آن‌ها برای اعتبارسنجی
- و وجود پروسه‌ای قابل اطمینان برای سازمان‌دهی قدرت اعتبارسنج‌ها

فرایند گواه اثبات قدرت، به دلیل ماهیت آن در انتخاب چندین گره محدود به‌عنوان اعتبارسنج شبکه، به مدلی متمرکز تبدیل می‌شود که بیشتر برای بلاکچین‌های خصوصی و کنسرسیومی، نظیر گروهی از بانک‌ها یا شرکت‌های بیمه مناسب است. پروژه‌های کووان (Kovan)، رینک‌بای (Rinkeby)، گیوِث (Giveth)، تاموچین (TomoChain)، رابلیکس (Rublix)، سوآرم سیتی (Swarm City)، کلونی (Colony) و گو چین (Go Chain)، از جمله پروژه‌هایی هستند که از این مکانیسم اجماع استفاده کرده‌اند.

گواه اثبات ظرفیت Proof of Capacity

با بررسی تعدادی از مکانیسم‌های اجماع می‌توان به این نتیجه رسید که اغلب این الگوریتم‌ها، به نوعی نمونه توسعه یافته یکی از دو مکانیسم گواه اثبات کار و گواه اثبات سهام هستند.

مکانیسم اجماع گواه اثبات ظرفیت، در حقیقت نوعی هارد فورک (hard forks) یا معادل فارسی آن انشعاب سخت است که در مکانیسم رایج و مشهور گواه اثبات کار صورت گرفته است. در حقیقت، تغییرات یا انشعاباتی که در یک مکانیسم صورت می‌گیرد، سبب تولید ارزهای رمزنگاری‌شده شده جدیدی می‌شود که می‌تواند حتی نسبت به ارز رمزنگاری‌شده پایه از قابلیت‌ها و مزایای بیشتری نیز برخوردار باشد. هاردفورک صورت گرفته روی بیت‌کوین، منجر به تولید ارز رمزنگاری‌شده جدید بیت‌کوین‌کش شده یا اتریوم کلاسیک، در حقیقت هاردفورکی از ارز اتریوم است. به همین دلیل نیز اخیرا، شاهد ظهور آلت‌کوین‌های بسیاری هستیم که می‌توانند در صورت اثبات مزایای خود، بیت‌کوین را به‌عنوان اولین ارز رمزنگاری‌شده مبتنی بر اجماع گواه اثبات کار، علیرغم کاربران و علاقه‌مندان بسیاراش، از میدان به در کنند.

حاکمیت تاریخی ارز رمزنگاری‌شده بیت‌کوین می‌تواند با ایجاد ارزهای رمزنگاری‌شده جدید و ارائه راهکارهای بهتر و کارآمدتر برای حل مشکلات کنونی، پایان بپذیرد و این فرصتی مغتنم برای رقابت در صنعت است که در خلال ماهیت متن‌باز این رمزنگاری‌ها ایجاد شده است.

بیایید سراغ مقایسه با کلاس درس خودمان برویم.

تعدادی دانش‌آموز را متصور شوید که در یک مدرسه در حال تحصیل هستند. زنگ آخرین ساعت درسی نیز به صدا درمی‌آید و دانش‌آموزان، دسته دسته و با آرامش به سمت اتوبوس‌های سرویس مدرسه حرکت می‌کنند تا به خانه بروند. هر اتوبوس، از تعداد معینی صندلی تشکیل شده است و می‌تواند برای مثال، ۵۰ الی ۱۰۰ دانش‌آموز را به خانه ببرد. این فرایند هر روز تکرار می‌شود و دانش‌آموزان، هر روز در این صندلی‌های می‌نشینند و راننده با صرف انرژی زمان آن‌ها را به مقصد می‌رساند.

فرایند ایاب و ذهاب این دانش‌آموزان، دقیقا به مثابه همان چیزی است که از آن با عنوان پلات کردن (plotting) یاد می‌شود. اولین گام از فرایند اجماع مبتنی بر گواه اثبات ظرفیت، که تمامی راهکارهای ممکن برای الگوریتم هش (hashing algorithm) قبل از آغاز فرایند استخراج توسط ماینرها را در بر می‌گیرد. مرحله دوم استخراج کردن یا ماینینگ است، ضمن این‌که انرژی موردنیاز برای اجرای این فرایندها نیز به مثابه انرژی مورداستفاده توسط راننده برای رانندگی است.

طی این الگوریتم، ماینرها بخش‌هایی از داده‌ها را که پلات نامیده می‌شوند ایجاد کرده و در هارددیسک ذخیره‌سازی می‌کنند. اکنون در هر بخش از این هارددیسک، یک پلات قرار دارد و در کنار هر پلات نیز یک هش که با آدرس عمومی (Public Key) افراد در ارتباط است.

هرچه بیشتر بهتر! این خصلت ذاتی الگوریتم اجماع گواه اثبات ظرفیت است. همان‌طور که در سرویس مدرسه، تعداد صندلی‌های بیشتر برای دانش‌آموزان بهتر است، در این مکانیسم نیز ظرفیت بالاتر به منزله کارایی بهتر است.

درست همانند گواه اثبات کار، این الگوریتم نیز مبتنی بر ارزش‌دهی به انجام کار و پایبندی به مقررات از سوی ارائه دهنده خدمات است، با این تفاوت که در گواه اثبات ظرفیت، همان‌طور که از نام آن نیز برمی‌آید، گرهی برنده است که بتواند داشتن ظرفیت بالا برای ذخیره‌سازی و

بازیابی اطلاعات را ثابت کند. علیرغم این‌که این مکانیسم نیز دارای هزینه‌هایی برای خرید و نگهداری دستگاه‌های ذخیره‌سازی داده است، اما به دلیل کاهش استفاده از انرژی و به‌عبارتی سبز بودن، بسیار مورد توجه قرار گرفته است.

مزایای گواه اثبات ظرفیت

- پربازده: مصرف انرژی به مراتب پایین‌تر نسبت به تراکنش‌های مبتنی بر بیت‌کوین
- ارزان: عدم نیاز به نرم‌افزارهای تخصصی استخراج
- توزیع‌شده: دسترسی به فضای ذخیره‌سازی بیشتر

Burst coin اولین ارز رمزنگاری‌شده‌ای است که از مکانیسم اجماع گواه اثبات کار برای اعتبارسنجی شبکه خود استفاده کرده است. ارزی که بلوک آن در سال ۲۰۱۴ ایجاد شد و سازنده‌اش نیز درست مثل ساتوشی ناکاموتو، پس از مدتی غیبش زد.

گواه اثبات فعالیت Proof of Activity

آن‌چه که در همه مکانیسم‌های اجماع یکی است، تلاش آن‌ها برای اثبات چیزی است. به‌عنوان مثال، هدف از مکانیسم اجماع گواه اثبات کار، در حقیقت اثبات کار سخت‌افزارهای استخراج برای حل مسائلی است که در بلاکچین مطرح می‌شوند. ضمن این‌که، در گواه اثبات سهام نیز هدف، اثبات میزان سرمایه‌ای است که گره‌ها برای اعتبارسنجی تراکنش‌ها نیاز دارند.

اما گواه اثبات فعالیت چه چیزی را ثابت می‌کند؟

- پاسخ کوتاه: فعالیت!
- پاسخ کامل: دخالت مستقیم در روند استخراج و امضای بلوک بعدی در بلاکچین.

علیرغم اکثر مکانیسم‌های اجماع دیگر، گواه اثبات کار قصد اختراع دوباره چرخ (reinvent the wheel) را ندارد و مدل توسعه یافته مکانیسم‌های اجماع گواه اثبات کار و گواه اثبات سهام به شمار نمی‌رود. اگر به ماهیت این الگوریتم دقت کنید، خواهید دید که گواه اثبات فعالیت، در حقیقت تلفیقی از دو مکانیسم گواه اثبات کار و گواه اثبات سهام است. به‌عبارت بهتر، گواه اثبات فعالیت فرایند استخراج خود را از گواه اثبات کار آغاز کرده و با رفتن به بلوک بعدی، به گواه اثبات سهام انتقال می‌دهد.

وجه تمایز مکانیسم اجماع گواه اثبات فعالیت

تفاوت عمده‌ای که گواه اثبات فعالیت با گواه اثبات کار دارد، ذخیره‌سازی تنها یک هدر یا سرآیند در بلوک است. این در حالی است که در گواه اثبات کار، موارد دیگری نظیر ریشه تراکنش (transaction root) و نانس (nonce) نیز در بلوک‌ها ذخیره‌سازی می‌شود.

برای ارزیابی و اعتبارسنجی بلوک‌ها نیز از یک گروه تصادفی اعتبارسنجی استفاده می‌شود تا بلوک‌ها را ارزیابی کرده و امضا کنند. استفاده از مکانیسم گواه اثبات سهام، دقیقا در این مرحله به منصه ظهور می‌رسد، چرا که گره‌هایی با کیف پول بیشتر (سهام بیشتر)، شانس بیشتری برای انتخاب شدن به‌عنوان اعتبارسنج دارند. هزینه‌های استخراج نیز میان گره‌های ماینر و گره‌های اعتبارسنج یا امضا کننده تقسیم می‌شود.

ارز دیجیتال خودگردان (Autonomous Digital Currency) دیکرِد (Decred)، پروژه‌ای است که در سال ۲۰۱۶ بر اساس این مکانیسم اجماع راه‌اندازی شده است.

گواه اثبات سوزاندن Proof of Burn

اگرچه در مورد سایر مکانیسم‌های اجماع می‌توان نحوه فرایند استخراج و اثبات را با استفاده از نام آن‌ها حدس زود، اما در مورد گواه اثبات سوزاندن ماجرا کمی پیچیده می‌شود. ارزهای رمزنگاری‌شده یا همان سکه‌ها، کاملا دیجیتال هستند و درک مفهوم سوزاندن در مورد آن‌ها اندکی دشوار است.

سوزاندن در مکانیسم اجماع گواه اثبات سوزاندن، در حقیقت به مفهوم ارسال سکه‌ها به یک آدرس غیرقابل برگشت و غیرقابل استفاده (Eater addresses) است که به دلیل ماهیت رمزنگاری تصادفی آن، امکان شناسایی‌اش برای هیچ گرهی، حتی ماینرها میسر نیست.

این آدرس‌های غیرقابل برگشت، سلول‌هایی برای ذخیره‌سازی سکه‌هایی هستند که گره‌ها برای افزایش شانس خود برای تولید بلوک بعدی قربانی می‌کنند و در نقطه پایانی تراکنش‌های گواه اثبات سوزاندن قرار گرفته‌اند. سکه‌های سوزانده شده، یا به‌عبارت دیگر سرمایه‌های کوتاه مدت کاربران، مجوز ادامه فعالیت کاربران در بلاکچین و استمرار فرایند استخراج را به آن‌ها می‌دهند و به همین دلیل نیز هرکس که دارای سرمایه بیشتر و سکه‌های سوزانده شده بیشتری باشد، شانس موفقیت بیشتری نیز در شبکه دارد. علیرغم این‌که هیچ تضمینی برای انتخاب شدن بر اساس سکه‌های سوزانده شده وجود ندارد، اما احتمال موفقیت و دستیابی به سرمایه‌های کلان با شانس به‌دست آمده از سوزاندن چند سکه، انگیزه لازم برای ادامه فرایند را در کاربران ایجاد می‌کند. سکه‌های بیشتر، شانس بیشتر – درست مثل مکانیسم اجماع گواه اثبات سهام، در این مکانیسم نیز نهنگ‌هایی موفق‌تر هستند که سهام و سکه‌های بیشتری برای سوزاندن دارند. با این حال، فرایند سوزاندن سکه‌ها دارای تاریخ انقضا است و نمی‌توان با یک‌بار سوزاندن، هرچند رقم بالایی باشد، برای مدت زمانی طولانی از شانس تولید بلوک برخوردار بود. در حقیقت، پس از مدت زمان نسبتا کوتاهی مجبور خواهید بود تا برای بقا، سکه‌های جدیدتر و بیشتری را روانه ناکجا آباد کنید.

مکانیسم اجماع گواه اثبات سوزاندن در عمل: پلتفرم اسلیم‌کوین (Slimcoin)، از جمله پروژه‌هایی است که از گواه اثبات سوزاندن به‌عنوان الگوریتم اجماع خود استفاده کرده است. ضمن این‌که کانترپارتی (Counterparty) نیز از این مکانیسم، برای سوزاندن توکن‌های دانه (seed tokens) استفاده می‌کند. کاربران این پلتفرم، بیت‌کوین‌های خود را به‌عنوان توکن‌های دانه می‌سوزانند تا در ازای آن، توکن‌های کانترپارتی با عنوان ایکسسیپی (XCP) را دریافت کنند.

گواه اثبات سهام اعطایی Delegated Proof of Stake

مکانیسم‌های اجماع مدرن، ما را در یک چرخه دموکراتیک قرار می‌دهند. همان‌طور که می‌توان حدس زد، گواه اثبات سهام اعطایی که به اختصار DPoS نیز خوانده می‌شود، مدل تغییریافته و پیچیده‌تری از گواه اثبات سهام است که در آن، اعتبارسنجی تراکنش‌ها به گروهی خاص متکی است تا به نمایندگی از سوی کل گره‌های موجود در شبکه، بلوک‌ها را ارزیابی کنند. تعداد این نمایندگان منتخب معمولا بین ۲۱ الی ۱۰۰ گره است که سازمان‌دهی و کنترل شبکه را تسهیل کرده و توزیع شرایط در خلال شبکه را ممکن می‌سازند. نمونه‌ای کوچک شده از کنگره ایالات متحده آمریکا (United States Congress) با ۵۳۵ نماینده، که در صورت تاخیر در ارائه گزارش توسط هریک از نمایندگان منتخب یا بروز اشتباه از سوی وی، دیگر اعضا می‌توانند در مورد صلاحیت و باقی ماندن وی در شبکه رای‌گیری کنند.

بیایید به سراغ مقایسه خود با کلاس درس برویم. احتمالا حداقل برای یک‌بار هم که شده، در کلاس‌های درس مجبور شده‌اید تا کاری را به‌صورت گروهی انجام دهید. پیداکردن جایگاه در میان اعضای گروه، هرچند کوچک، اندکی دشوار است و برای این‌که بتوانید مسئولیت‌های محول شده به خود را به درستی به انجام برسانید، نیاز به بررسی و صرف انرژی زیادی دارید. اکنون تصور کنید که این گروه‌بندی را حذف کرده و از شما بخواهند تا همان فرایندها و مسئولیت‌ها را در یک گروه بزرگ در مقیاس کلاس انجام دهید. بدیهی است که کار پیچیده‌تر از قبل خواهد شد و این‌بار انرژی بسیاری بیشتری را نیاز خواهید داشت.

این دقیقا همان چیزی است که در مورد نمایندگان مجلس کشورها نیز جریان دارد. عده‌ای به‌عنوان نماینده انتخاب می‌شوند و در مورد صحت و تاثیرگذاری برخی از شرایط و قوانین تصمیم‌گیری می‌کنند. ضمن این‌که کنترل بخش‌های مهمی از شبکه در اختیار آن‌ها است. روندی دموکراتیک که می‌تواند علاوه بر ارتقای بهره‌وری در انرژی، هزینه‌ها و خطاهای سیستم را نیز بکاهد؛ هرچند که این امر، قدرت را به عده‌ای خاص متمرکز می‌کند.

مزایای :

- مقیاس‌پذیری
- بهره‌وری در انرژی
- تراکنش‌های ارزان قیمت

معایب :

- نیمه متمرکز

در حقیقت، به دلیل انتخاب تعداد محدودی گره به‌عنوان نماینده، این مکانیسم ماهیتا به روشی نیمه متمرکز تبدیل می‌شود و حاکی از تریلمای مقیاس‌پذیری ویتالیک بوترین است.

BitShares، EOS و Steemit همگی از گواه اثبات سهام اعطایی استفاده کرده‌اند. نکته قابل توجه این است که تمامی از پروژه‌ها، زاییده ذهن دنیل لاریمر (Daniel Larimer)، برنامه‌نویس و کارآفرین ارزهای رمزنگاری‌شده هستند.

گواه اثبات اهمیت Proof of Importance

همان‌طور که مشاهده کردید، امکان گردآوری الگوریتم‌های اجماع مختلف در یک شبکه غیرمتمرکز به منظور ترغیب کاربران به پیروی از مجموعه‌ای از مقررات وجود دارد. در این‌جا، هیچ‌گونه یکسان‌سازی وجود ندارد و هر یک از مکانیسم‌های اجماع مورد بحث، دارای معایب و مزایای مخصوص خود هستند که با توجه به فعالیت‌های تشویقی شبکه برای کاربران، می‌توانند موفقیت‌آمیز یا غیرموفقیت‌آمیز باشند. آن‌چه که گواه اثبات اهمیت به دنبال آن است، شناسایی و اثبات فاکتورهایی است که می‌توانند سبب ارزشمندی بیشتر برخی از گره‌ها در شبکه شوند.

بیایید مکانیسم گواه اثبات سهام را بار دیگر مرور کنیم. همان‌طور که می‌دانید، این مکانیسم تنها گره‌هایی را در اولویت قرار می‌دهد که دارای سهام بیشتری در شبکه هستند. در حقیقت، تنها چیزی که در این الگوریتم حائز اهمیت است، تعداد سکه‌هایی است که هر گره در اختیار دارد. به همین دلیل نیز در شبکه‌هایی که بر گواه اثبات سهام مبتنی هستند، انگیزه‌ای برای گره‌های ضعیف‌تر باقی نمی‌ماند. از همین رو، گواه اثبات اهمیت سعی دارد تا با تغییر این روند، تعداد بیشتری از گره‌های شبکه را برای بقا و فعالیت ترغیب کند.

فاکتورهای کلیدی گواه اثبات اهمیت

- نقل و انتقالات خالص (Net transfers) یا مجموع هزینه طی ۳۰ روز گذشته
- تخصیص بخشی از ارز به تولید بلوک‌ها

- گره‌هایی که خوشه‌بندی شده و یکپارچه‌سازی شده‌اند وزن بیشتری خواهند داشت.

کم‌ترین احتمال برای احتکار

بر خلاف مکانیسم اجماع گواه اثبات سهام، گواه اثبات اهمیت سعی می‌کند تا شانس ذخیره‌سازی سهام برای نهنگ‌ها و به‌عبارت دیگر احتکار را کاهش دهد. شبکه‌های سنتی تنها چیزی که به آن اهمیت می‌دادند، سهام و موقعیت گره‌ها بود و میزان نقل و انتقالات تهیج ارزش در شبکه نداشتند. اما آن‌چه که اهمیت دارد، اولویت دادن انتقال‌های خالص به موقعیت گره‌ها است که درجه‌بندی بهتری از عاملان ایستگاه‌های در گردش ارائه می‌دهند.

ایجاد بلوک، بدون هزینه

در این مکانیسم هزینه‌های حاشیه‌ای برای ایجاد بلوک‌ها معادل صفر است و به همین دلیل نیز زمانی که که انشعاب جدیدی ایجاد می‌شود، کاربران می‌توانند آن‌ها را با استفاده از الگوریتم گواه اثبات سهام اعتبارسنجی کنند.

پلتفرم New Economy Movement اولین پروژه‌ای است که مکانیسم گواه اثبات اهمیت را معرفی کرده است. در این پلتفرم حداقل توکنی که هر گره برای راه‌اندازی سهام خود نیاز دارد معادل ۱۰،۰۰۰ ایکس‌ای‌ام (XEM) است که ارزش آن بر اساس نرخ کنونی بازار، چیزی در حدود ۴،۰۰۰ دلار آمریکا است.

گراف جهت‌دار غیرمدور Direct Acyclic Graphs

اکثر مکانیسم‌های اجماع دارای ماهیتی مشابه هستند و تنها تفاوتی که می‌توان در آن‌ها یافت، کاربردی است که در دفاتر کل توزیع‌شده مختلف از خود نشان می‌دهند. مکانیسم اجماع گراف جهت‌دار غیرمدور یا DAGs، مکانیسم اجماع محبوبی است که در اغلب پایگاه‌های داده غیربلاکچینی مورد استفاده قرار می‌گیرد.

دفتر کل توزیع‌شده آی‌اوتی‌ای (IOTA)، از نوعی مکانیسم اجماع خاص با عنوان تنگل (Tangle) استفاده می‌کند که نوعی گراف جهت‌دار غیرمدور است. در این مکانیسم، هر گره برای این‌که بتواند تراکنشی را ارسال کند، ناچار است دو تراکنش دیگر را اعتبارسنجی کند. ماهیت تنگل باعث شده تا تعداد تراکنش‌ها به شکل فزاینده‌ای افزایش یافته و به همین دلیل، سیستم بررسی و تعادل شبکه ارتقا پیدا کند.

مزیت این دست شبکه‌ها نسبت به بلاکچین: با توجه به این‌که تراکنش‌ها در چنین شبکه‌های ناشی از تعاملات و مشارکت کاربران فعال در شبکه هستند و تامین امنیت شبکه نیز در نتیجه تایید تراکنش‌های گذشته توسط کاربران صورت می‌گیرد، عملا هیچ هزینه‌ای در شبکه وجود ندارد و کلیه تراکنش‌ها بدون کارمزد صورت می‌پذیرند. علاوه بر این، شبکه‌هایی نظیر آی‌اوتی‌ای ناهمگام (asynchronous) هستند و نیازی نیست تا تمام تراکنش‌ها هم‌زمان انجام شوند.

کاربردهای گراف جهت‌دار غیرمدور

معاملات پولی (Monetary transactions) زیرمجموعه‌ای کوچک از تعاملات رایج بین دستگاه‌های متصل را نشان می‌دهند. تنگل مکانیسمی مقیاس‌پذیر بوده و هزینه راه‌اندازی و پیاده‌سازی بسیار پایینی نیز دارد و قادر است، ساختار پایگاه داده سودمندتری نسبت به بلاکچین برای تعاملات اینترنت اشیا فراهم کند.

تحمل‌پذیری خطای بیزانس Byzantine Fault Tolerance

هزاران سال پیش ...

مجموعه‌ای از ژنرال‌های بیزانس شهری را برای حمله ناگهانی به آن محاصره کرده‌اند. اما زمان دقیق حمله، موضوع مهمی است که لازم است تمامی ژنرال‌ها در مورد آن به اجماع برسند. در صورتی که هماهنگی لازم در مورد زمان و نحوه حمله در میان ژنرال‌ها صورت نپذیرد، محاصره شکست خواهد خورد...

مشکل ژنرال‌های بیزانس (Byzantine Generals problem) معضلی کلاسیک است که نوعی از مکانیسم اجماع را برای سیستم‌های مبتنی بر رمزنگاری ارائه می‌کند. مکانیسمی محبوب تحت عنوان تحمل‌پذیری خطای بیزانس یا BFT، که درست مانند مثال محاصره ژنرال‌های بیزانس، برای اعتبارسنجی و تایید نهایی به عده‌ای خاص وابسته است. افرادی که همان ژنرال‌ها، یا در مورد دفتر کل توزیع‌شده، اعتبارسنج‌ها هستند. اما یک مشکل بزرگ‌تر دیگر هم برای ژنرال‌های بیزانس وجود داشت: هریک از این ژنرال‌ها در بخشی از مرز دشمن ساکن می‌شدند و متاسفانه در عصر بیزانس، گوشی تلفن همراه وجود نداشت! ژنرال‌ها برای نهایی‌سازی و هماهنگی پایانی در مورد استراتژی‌های خود امکان ارتباط با یکدیگر را نداشتند. تنها راهکار ارتباطی موجود، پیام‌رسان‌هایی بودند که با صرف زمان و انرژی بسیاری، داده‌های مورد نظر را در میان ژنرال‌ها منتقل می‌کردند.

اکنون کافی است تصور کنید که یکی از این پیام‌رسان‌ها لو می‌رفت و به دست دشمن می‌افتاد. اگر اطلاعات و نقشه‌های او را دست‌کاری می‌کردند چه؟ بدیهی است که اطمینان از اطلاعاتی که به این روش منتقل می‌شدند کار بسیار دشواری بود و می‌توانست کل نیروها را به کام مرگ بکشاند. علی‌رغم این‌که مقیاس‌پذیری و بهره‌وری ارائه شده توسط مکانیسم تحمل‌پذیری خطای بیزانس قابل ملاحظه است، اما این مکانیسم نیز جزو الگوریتم‌هایی است که برای شبکه‌های متمرکز و نیمه متمرکز طراحی و ساخته شده است.

مکانیسم اجماع تحمل پذیری خطای بیزانس

- تحمل‌پذیری خطای بیزانس کاربردی (Practical Byzantine Fault Tolerance) که در پروژه هایپرلجر فابریک (Hyperledger Fabric) مورد استفاده قرار گرفته است. مکانیسمی که از کمتر از ۲۰ اعتبارسنج برای ارزیابی اجماع شبکه استفاده می‌کند.

- توافق بیزانس یکپارچه (Federated Byzantine Agreement) که در شبکه‌های استلار (Stellar) و ریپل (Ripple) مورد استفاده قرار گرفته و از هر کدام از ژنرال‌ها (گره‌ها) می‌خواهد تا اعتماد لازم برای هر یک از زنجیره‌های مربوطه را تامین کنند.

مزایا:

- هزینه‌های پایین تراکنش
- توان عملیاتی بالا
- مقیاس‌پذیری شبکه
- و بهره‌وری بالا

معایب:

- متمرکز
- نیازمند مجوز

قابلیت جابجایی Fungibility

ماینینگ Mining

FPGA

Field Programmable logic Gate Array ها که بعبارتی (آرایه دریچه ای برنامه پذیر منطقی) و به تعبیری ساده تر (آرایه گیت برنامه پذیر در محل) خوانده می شوند، تراشه هایی هستند با معماری داخلی از پیش تعیین شده توسط شرکت سازنده که قابلیت پیکربندی به منظورهای مختلف را توسط طراحان فراهم می آورند. انواع دیگری از این نوع تراشه نیز موجود است؛ معروف ترین آنها، ASICمیباشد که هنوز هم در برخی پروژه های بزرگ و پیچیده مورد استفاده قرار می گیرد. مهمترین اشکال ASIC ها فرایند طراحی و ساخت زمان بر و پرهزینه میباشد که در نتیجه ی ثابت بودن طرح نهایی در سیلیکون ایجاد میشود. بدین معنی که فقط با تولید نسخه ی جدید میتوان مدار را ویرایش کرد، که همین مطلب طول مدت رسیدن به بازار قطعه را طولانی تر می کند. در FPGA ها این اشکالات برطرف شده است

این قطعات دارای بلاک های منطقی برنامه پذیر و اتصالات بین بلاکی قابل پیکربندی هستند. برخی از آنها تنها یک بار قابلیت برنامه پذیری دارند که به OTP(One-Time-Programmable) مشهورند و برخی دیگر چندین بار قابلیت برنامه پذیری را دارا هستند. برای برنامه نویسی و طراحی FPGA ها از دو روش زبان های توصیف سخت افزار (HDL-AHDL-VHDL) و یا طراحی مدار استفاده می شود. این تراشه ها می توانند چندصد میلیون گیت منطقی(قابل پیکربندی) داشته باشند که همین ویژگی آنها را برای پیاده سازی توابع پیچیده و بسیار بزرگ دلپذیرتر می کند.

تعریفی دیگر که در FPGA به آن اشاره شد، (آرایه گیت برنامه پذیر در محل) بود، بعبارت دیگر میتوان گفت FPGA ها ISP(IN-System Programmable)هستند، یعنی برنامه پذیر درون سیستمی ISP .به قطعاتی گفته می شود که توان برنامه پذیری هنگام استقرار در سیستمی سطح بالاتر را داشته باشند. همین ویژگی، امکان تغییر طرح پیاده سازی شده را بصورت ساده برای ما فراهم می آورد؛ بدون آنکه نیاز به تولید نسخه ی جدید باشد! در نتیجه زمان عرضه به بازار طرح بسیار کوتاه تر می سود.

FPGAها برای پیشرفت شرکت های startup (شرکت های نوپا و تازه تأسیس) بسیار مناسبند، چرا که حتی گروه های کوچک مهندسی در محیط های آزمایشگاهی کوچک مبتنی برFPGA ، موفق به اجرای طرح های خود می شوند. و همچنین هزینه های توسعه بسیار پایین تر از نمونه های مشابه است.

در ابتدای ظهور FPGA ها (اواسط دهه ۱۹۹۰) از آنها برای پیاده سازی منطق اتصالی (glue logic) و ماشین هایی با پیچیدگی متوسط و پردازش داده های نسبتاً کم استفاده میشد. در اوایل دهه ۱۹۹۰ و با پیشرفت FPGA ها، از آنها برای ارتباط و شبکه، یعنی پردازش بلاک های بزرگ داده و فرستادن آنها به اطراف استفاده میشد؛ و در اواخر دهه ۱۹۹۰، بازار شاهد ورود آنها به کاربردهای صنعتی، لوازم خانگی و خودروسازی بود. اما امروزه از FPGA ها تقریبا برای پیاده سازی هرچیزی مانند دستگاه های مخابراتی، رادیوهای نرم افزاری، رادارها، پردازش تصویر و دیگر کاربردهای پردازش سیگنال (DSP)وحتی قطعات Soc (System-On-Chip) حاوی عناصر نرم افزاری و سخت افزاری استفاده می شود.

جهت رسیدن به سودآوری بالاتر، کاهش مصرف برق و ... و همچنین بازار پر رونق استخراج ارزهای دیجیتال شرکتهای زیادی اقدام به تولید FPGAهایی جهت استخراج ارزهای دیجیتال کردند این مدارات عملکرد و راندمان بالاتری نسبت به کارتهای گرافیک و CPU داشتند اما خود با آمدن ASICها از بازار خارج شدند.

ASIC

اسیک (ASIC)یا Application Specific Integrated Circuits مدارهای مجتمع با کاربرد خاص هستند. هر کدام از دستگاه های اسیک قابلیت حل کردن الگوریتم خاصی را دارند، به طور مثال اسیک هایی که برای بیت کوین ساخته شده اند توانایی حل کردن الگوریتم ۲۵۶SHA را دارند.

با وجود دستگاه های اسیک، در حال حاضر استخراج بیت کوین با CPU و کارت گرافیک توجیه اقتصادی ندارد و ماینرها از دستگاه های اسیک برای استخراج استفاده می کنند. بیشتر دستگاه های اسیک توسط شرکت بیت مین ساخته می شود و خیلی ها معتقدند که وجود این دستگاه ها باعث می شود که بازار از حالت غیرمتمرکز خارج شود.

یکی از عوامل دیگری که باعث می شد، سود حاصل از ماینینگ کاهش پیدا بکند، هزینه برق بود که باعث شد ماینینگ توجیه اقتصادی نداشته باشد. برای جلوگیری از این اتفاق، ماینرها به سمت استفاده از کارت های گرافیک و بعد از آن FPGA ها رفتند. داستان به همین جا ختم نشد و ماینرها به دنبال سود بیشتری بودند. بعد از این اتفاق چیپست هایی طراحی شد که به صورت تخصصی با الگوریتمSHA ۲۵۶ بیت کوین کار می کردند و سرعت بیشتری نسبت به CPU و کارت گرافیک (GPU)و همچنین FPGA ها داشتند. به این چیپست ها، اسیک (ASIC)می گویند.

با توجه به قدرت پردازشی بیشتر دستگاه های اسیک، این دستگاه توانست خیلی زود طرفداران خود را پیدا کند ولی در دنیای غیر متمرکز ارزهای دیجیتالی حضور اسیک ها مخالفان زیادی هم دارد. یکی از مخالفان اصلی اسیک، سازندگان ارز دیجیتالی اتر هستند و برای جلوگیری از حضور اسیک ها در فرایند ماینینگ ارز دیجیتالی اتر اقداماتی انجام داده اند. در حال حاضر الگوریتم هایی هم هستند که اسیک ها توانایی کار کردن با آن ها را ندارند.

تفاوت اصلی در اسیک ماینر ها را می توان در چهار گزینه زیر خلاصه نمود:

۱. نوع الگوریتم و کوین های قابل استخراج
۲. میزان توان مصرفی دستگاه
۳. نرخ هش یا قدرت هش تولیدی
٤. میزان سودآوری

ریگ Mining rig

مجموعه ای از کارتهای گرافیکی متصل به یک مادربورد (مادربردهای ماینینگ بسیاری تولید شده است با قابلیت اتصال چند ده کارت گرافیک) جهت استخراج ارزهای دیجیتال ریگ استخراج گفته می شود.

برای انتخاب کارتهای گرافیک مورد استفاده در ریگ به پارامترهای : hash rate، برق مصرفی و قیمت دستگاه بیشتر از بقیه مورد توجه قرار می گیرند. به دلیل توان بالای کارتهای گرافیک در پردازش محاسبات پیچیده ریاضی و همچنین ASIC proof بودن تعدادی از رمز ارزها از ریگ ها بصورت گسترده استفاده می شود

استخر استخراج Mining pool

استفاده از تعداد زیادی از سیستم ها (معمولا ریگ و ASIC) جهت استخراج ارزهای دیجیتال در یک مکان بصورت متمرکز جهت مدیریت بهتر برق، سیستم های تهویه و بصورت کلی هزینه ها برای رسیدن به بهره وری بالاتر، این مکان مزرعه Farm نامیده می شود. یک مزرعه می تواند به وسعت یک اتاق یا یک مجموعه از سوله های مکانیزه استخراج چند هزار متری باشد

ماینینگ ابری Cloud mining

ماینینگ ابری مکانیسمی برای ماینِ ارزهای دیجیتالی مانند بیت کوین ارائه می دهد که دیگر نیازی به نصب سخت افزار یا لوازم جانبی مرتبط نیست. شرکت‌هایی وجود دارند که به مردم اجازه می دهند که یک حساب کاربری داشته باشند و در فرآیند استخراج ابری شرکت کنند. بنابراین، این فرآیند باعث می شود که افراد زیادی از فاصله‌های دور هم به این فرآیند ماینینگ دسترسی داشته باشند.

فرآیند ماینینگ ابری سبب می شود که افراد در استخر ماینینگ شرکت کنند و مقدار مشخصی "قدرت هش" بخرند. هر شرکت کننده، نسبت به قدرت هش اختصاص یافته دارای سهم قانونی از سود به دست آمده است. به دلیل این که ماینینگ ابری از طریق فضای ابری ایجاد شده است، هزینه‌هایی مانند هزینه‌های تعمیر و نگه داری تجهیزات و هزینه‌های سر به فلک کشیده‌ی مصرف انرژی ندارد.

ماینینگ ابری، فرآیند ماینینگ را از طریق فضای ابری تسهیل می کند. محاسبات ابری یکی از سریع ترین روندهای موجود در زمینه‌ی خدمات محاسباتی مانند سرورها، پایگاه داده‌ها، نرم افزارها و وذخیره سازی است که از طریق فضای ابری (یا به زبان ساده تر اینترنت) می توان به آن‌ها دسترسی پیدا کرد. از سوی دیگر، فرآیند ماینینگ ستون فقراتِ رمزارزهایی مانند بیت کوین است. به عبارت دیگر، فرآیندی است که به وسیله‌ی آن، تراکنش‌ها تایید شده و به لدجر عمومی اضافه می شوند؛ که با نام "بلاک چین" شناخته شده است. همچنین از طریق این فرآیند، کوین‌های جدیدی نیز منتشر می شوند. ماینینگ ابری، ترکیبی از دو جهان ماینینگ را برای کاربرانی که در مناطق دوری قرار دارند (با دانش و اطلاعات کم یا زیر ساخت‌های سخت افزاری)، ایجاد می کند!

به طور کلی، سه نوع ماینینگ ابری وجود دارد:

- استخراج میزبانی Hosted mining : در این نوع، دستگاه ماینینگی را اجاره می توان کرد که به وسیله‌ی ارائه دهنده، میزبانی شده است.
- استخراج میزبانی مجازی Virtual hosted mining : در این نوع، یک سرورِ اختصاصی مجازی (با هدف عمومی) می توان ایجاد کرد و سپس نرم افزار ماینینگ را بر روی آن نصب کرد.
- قدرت هش اجاره ای Leased hash power : در این نوع، می توان بدون استفاده از کامپیوترهای شخصی یا مجازی، مقدار مشخصی "قدرت هش" به دست آورد. این نوع روش، تا کنون، محبوب ترین روش ماینینگ ابری بوده است.

این فرآیند بسیار ساده است، کاربر فقط نیاز دارد از طریق وبسایت و شرکت‌های مربوطه، حساب کاربری ایجاد کند و در آن مواردی مانند دوره‌ی قرارداد و قدرت هشینگ را انتخاب کند. اما به این نکته نیز باید توجه کرد که در حال حاضر، شرکت‌های تقلبی فراوانی در این زمینه وجود دارند که باید مراقب آن‌ها بود و به هر شرکت ماینینگ ابری نباید اعتماد کرد. همچنین خدمات وب ارائه شده، با پارامترهای سخت افزاری خود طراحی شده‌اند نه با پارامترهای ماینینگ ابری.

مزایای ماینینگ ابری:

- عدم نیاز به خرید تجهیزات اضافی
- عدم نیاز به پرداخت هزینه‌های مرتبط با نگهداری و تعمیر تجهیزات

- هزینه‌ی برق مصرفی آن، کم است
- نیازی به راه اندازی سیستم‌های تهویه نیست

معایب ماینینگ ابری:

- درآمد حاصل از آن کمتر است
- نبود کنترل و انعطاف پذیری در انجام کار
- نبود شفافیت در فرآیند ماینینگ
- ریسک تقلب و کلاهبرداری در آن بالا است
- احتمال متوقف شدن فرآیند ماینینگ وجود دارد

استخر استخراج Mining pool

استخرهای استخراج (Mining Pools) جامعه‌ای از ماینرها را در بر می‌گیرد که منابع (قدرت پردازشی) خود را برای استخراج ارزهای دیجیتال گرد هم آورده‌اند. با افزایش سختی (Difficulty) شبکه، قدرت محاسباتی بیشتری برای استخراج ارزهای دیجیتال موردنیاز است. افزایش قدرت محاسباتی برای یک ماینر تنها، به دلیل هزینه بالای انرژی و دستگاه‌های مخصوص پردازش بسیار پرهزینه است. بدین منظور ماینرها قدرت پردازشی خود را در محلی به نام (استخر) جمع می‌کنند تا بتوانند هزینه‌های مربوط به این پردازش را کاهش دهند.

اگرچه استخرهای استخراجی وجود دارند که فقط یک ارز دیجیتال را استخراج می‌کنند، اما استخرهای استخراج چندگانه به کاربران این قابلیت را می‌دهند که ارزهای دیجیتال مختلفی را با توجه به سودشان در زمان مختلف تغییر دهند. بدین منظور برای تعیین سودآورترین ارز دیجیتال جهت استخراج در زمان معین، یک استخر استخراج چندگانه موارد زیر را حساب می‌کند:

- سختی استخراج در ارز دیجیتال
- نرخ تبادل ارزهای مختلف
- زمان ساخت بلاک
- نرخ هش Hash Rate یا قدرت هش

استخرهای چندگانه برای کاربرانی که در یک زمان مشخص از استخراج ارز دیجیتال خاصی مطمئن نیستند، می‌تواند بسیار مفید باشد. هرچند که ارزهای دیجیتالی که استخراج می‌شوند معمولاً بلافاصله در صرافی به یکدیگر تبدیل می‌شوند، همین امر باعث تغییر قیمت آن‌ها شده و ممکن است در پایان نیز، قیمت کوین استخراج شده کمی کاهش پیدا کند.

پاداش استخرها

پرداخت به ازای هر سهم (PPS): به‌عنوان یکی از اساسی‌ترین ساختار پاداش، PPS روش پرداخت فوری به ازای سهمی (هش ریت) است که ماینر در حل مسئله رمزنگاری داشته است. پرداخت از میزان موجودی استخرها انجام می‌شود.

پرداخت کامل به ازای هر سهم (FPPS): علاوه بر تقسیم پاداش هر بلاک بین اعضای استخر، روش FPPS ماینرهای شرکت‌کننده در استخر را از کارمزد تراکنش‌ها نیز بهره‌مند می‌کند. کارمزد تراکنش‌ها در دوره‌ی زمانی خاصی محاسبه شده و به پاداش بلاک افزوده می‌شود. درنهایت این پاداش بر اساس مدل PPS بین ماینرها توزیع می‌گردد.

مزایا و معایب استخرهای ارزهای دیجیتال

- درآمد باثبات‌تر
- کاهش بالقوه‌ی هزینه‌های استخراج
- پتانسیل افزایش درآمدزایی

معایب استخرهای استخراج شامل موارد زیر است:

- رنج بردن استخرهای استخراج از مزاحمت‌ها (حملات هکری)
- پاداش بلاک باید به اشتراک گذاشته شود.
- ساختار بالقوه نامطلوب پاداش استخر

استخراج ترکیبی Merged Mining

Cryptojacking چیست؟

Cryptojackingاستفاده‌ی غیرمجاز از کامپیوترها، به منظور ماین کردن ارزهای دیجیتال است.

هکرها Cryptojacking را از طریق روش‌های زیر انجام می دهند:

- از طریق ارسال لینک مخرب به ایمیل افراد (کد ماینینگ ارزهای دیجیتال بر روی کامپیوتر بارگذاری می شود)
- نفوذ به وبسایت‌ها
- ایجاد آگهی‌های تبلیغاتی آنلاین با استفاده از زبان برنامه نویسی جاوا اسکریپت

بنابراین، هکرها از طریق روش‌های گفته شده، کد ماینینگ ارزهای دیجیتال را به دست می آورند .تنها تفاوتی که ممکن است بین کد هکرها و کاربر اصلی وجود داشته باشد این است که شاید این کدها دیر اجرا شوند یا عملکرد کم تری داشته باشند.

چرا Cryptojacking در حال افزایش است؟

هیچ کس نمی داند که چقدر ارز دیجیتال می توان از طریق Cryptojacking ماین کرد اما هیچ سوالی هم وجود ندارد که چرا این اقدام انقدر رایج شده است؟

Cryptojacking مبنی بر مرورگر، به سرعت در حال افزایش است.در نوامبر سال گذشته، براساس گزارشAdguard ، Cryptojacking مبنی بر مرورگر، حدود ۳۱٪ نرخ رشد داشته است. طبق تحقیقات صورت گرفته حدود ۳۳۰۰۰ وبسایت در حال اجرای اسکریپت‌های Cryptojackingبرای ماینینگ ارزهای دیجیتال هستند. وبسایت‌های مورد نظر، ماهیانه حدود یک میلیارد بازدید کننده دارند.

براساس گزارش Bad Packets در ماه فوریه سال ۲۰۱۸ میلادی، حدود ۳۴.۴۷۴ سایت از سرویس Coinhive استفاده می کنند. همچنین ماینرهای جاوااسکریپت نیز، برای انجام فعالیت‌های قانونی ماینینگ خود از Coinhive استفاده می کنند. براساس گزارش Check Point Software Technologiesدر ماه جولای سال ۲۰۱۸ میلادی، حدود چهار بدافزار از ۱۰ بدافزار موجود، مربوط به سرویس ماینینگ ارزهای دیجیتال Coinhive و Cryptoloot بوده‌اند. محققان دریافتند که بیش از نیمی از دستگاه‌های ماینینگ، به خصوص در کشورهای روسیه، هند و تایوان به وسیله‌ی بوت نت ماینینگ Smominru مختل شده‌اند . بوت نت مورد نظر، سرورهای ویندوز را برای ماین رمزارز مونرو هدف قرار داده و براساس آمار شرکت سایبری Proofpoint ، حدود ۳.۶ میلیون دلار از طریق ماین ارز دیجیتال مونرو، نصیب هکران شده است. برای انجام فرآیندCryptojacking ، داشتن مهارت‌های فنی لازم نیست. ابزار لازم برای انجام فرآیند Cryptojacking، در فضای دارک وب با قیمت ۳۰ دلار موجود است.

Cryptojackingچگونه کار می کند؟

هکران دو روش اصلی برای به دست آوردن کامپیوترهای غیرمجاز، برای ماین مخفی ارزهای دیجیتال دارند. اولین روش، تحریک کاربران برای بارگذاری کدهای کریپتوماینینگ خود روی کامپیوترهایشان است. این کار از طریق تکنیک‌های فیشینگ مانند ارسال لینک مورد نظر به ایمیل کاربر و تحریک او برای کلیلک روی لینک مربوطه است. لینک مورد نظر کدی را اجرا کرده و اسکریپت کریپتوماینینگ را روی کامپیوتر قرار می دهد.

روش دوم این است که بر روی یک وبسایت یا تبلیغ، اسکریپت قرار می دهند و اسکریپت مورد نظر به چندین وبسایت ارسال می شود. هنگامی که کاربران از وبسایت بازدید کنند یا پاپ آپ مورد نظر به مرورگرشان نفوذ کند، اسکریپت به صورت خودکار انجام می شود. همچنین هیچ گونه کدی بر روی کامپیترهای هک شده، ذخیره نمی شود. بنابراین، اگر از هر یک از روش‌های گفته شده استفاده شود، درنهایت کدهای ارسال شده به سرور مورد نظر، تحت کنترل هکران قرار می گیرد. گاهی اوقات هکران به منظور افزایش بازگشتی خود از هر دو روش استفاده می کنند. برای انجام حملات سایبری به کامپیوترها، هکران از بدافزارهای قدیمی برای ارسال نرم افزارهای مورد اعتماد استفاده می کنند. برخلاف بدافزارهای موجود، اسکریپت‌های Cryptojacking هیچ گونه آسیبی به کامپیوترهای نفوذی و اطلاعات کاربران وارد نمی کند. اسکریپت‌های Cryptojacking تنها منابع پردازش CPU را سرقت می کنند. بنابراین اگر کامپیوترهای کاربران معمولی مورد هدف قرار داده شود، آن‌ها فقط از کندی اجرای برنامه‌های کامپیوتری خود رنج می برند. اما برای سازمان‌های بزرگ، اسکریپت‌های Cryptojacking دردسرساز و هزینه بر خواهند بود.

کریپتوجکرها افراد باهوشی هستند و برای انجام اقدامات خود، از برنامه‌های طراحی شده استفاده می کنند .بدافزارهای مورد نظر جدید نیستند و اکثرا مشتقاتی از بدافزارهایی مانند ransomware و adware هستند.

بدافزارهای:Cryptojavking

- PowerGhost
- MinerGate
- BadShell
- rTorrent

ماینینگ انفرادی یا Solo Mining به چه معنا است؟

Solo Miningانجام فرآیند ماینینگ در طی سال‌های گذشته در صنعتِ ارزهای دیجیتال، به نوعی به روشی برای کسب درآمد در این صنعت، تبدیل شده است .این مفهوم، دنیایِ گسترده‌ای را در بر می گیرد. مفهومِ "Solo Mining" به چه معنا است؟

متاسفانه، این کار غیرممکن است که بگوییم کدام یک از روش‌های فرآیندِ ماینینگِ ارزهای دیجیتال، کاملا سودآور خواهد بود. فرآیند و روندِ ماینینگِ ارزهای دیجیتال درست مانندِ بازارهای آن، ناپایدار بوده و کسبِ سود، به فاکتورهای متعددی بستگی دارد. با این تفاسیر، ماینینگ انفرادی یاSolo Mining ، یک جستجویِ کاملا مستقلی برایِ ماینِ بلاک‌ها و کسبِ پاداش برای انجامِ این کار است. به عبارتی دیگر، ماینینگ انفرادی به معنایِ انجامِ فرآیند ماین و استخراج به صورتِ مستقل و انفرادی است. هر فردی با داشتنِ دستگاه‌ها و تجهیزاتِ مربوطه، توانایی انجام فرآیند ماینینگ به صورتِ مستقل و انفرادی را خواهد داشت. بنابراین، کاربران و ماینرهای ارزهای دیجیتال، به جایِ پیوستن به گروه‌ها و استخرهای ماینینگ ، این فرآیند را به صورتِ مستقل و انفرادی انجام می دهند. همچنین، لازم به ذکر است که انجامِ فرآیند ماینینگ به روشِ انفرادی، وابسته به سیستم‌های شخص ثالث نیست!

مزایا و معایب انجامِ فرآیند ماینینگ به صورتِ انفرادی:

بی شک، یکی از بهترین مزیت‌های انجام فرآیند ماینینگ به صورت انفرادی، کسبِ پاداش به صورتِ کامل است. به عبارتی دیگر، ماینر مورد نظر با استخراجِ بلاک‌ها، به طور کامل، سود مورد نظر را به دست خواهد آورد. در حال حاضر، ماینِ هر بلاکِ بیت کوین، ۱۲.۵ BTC پاداش به دنبال خواهد داشت! بنابراین، ماینینگ انفرادی، سببِ کسبِ مقدار زیادی پول نقد خواهد شد. با این تفاسیر، شاید این مزیت، تنها مزیتِ موجود برای انجام فرآیند استخراج به صورتِ انفرادی خواهد بود (البته به استثنایِ افزایشِ زمانِ کار در این روش).

انجام فرآیند ماینینگ به صورت انفرادی معیابی را هم شامل می شود

به عنوانِ مثال، شاید یک ماینر بر روی ماینِ یک بلاک، به مدتِ یک ماه کار انجام دهد، این در حالی است که ماینرِ دیگری به سرعت، بلاک مورد نظر را ماین می کند؛ در نتیجه، سود مورد نظر به ماینری تعلق خواهد داشت که بلاک مورد نظر را ماین کرده باشد و در این مورد، سود و پاداش به ماینر دوم خواهد رسید! به دلیلِ اینکه، قدرتِ تجهیزاتِ ماینینگِ ماینر دوم، بیشتر از ماینر اول بوده است، ماینر دوم به راحتی توانسته، بلاک مورد نظر را ماین کند. بنابراین، این گونه می توان نتیجه گیری کرد که کسبِ درآمد در ماینینگِ انفرادی به صورتِ نامنظم بوده و زمانِ ماینِ یک بلاک نیز به طور دقیق، مشخص نیست.

در نهایت، در ماینینگ انفرادی، زمانِ زیادی از دست می رود و ماینر مورد نظر، بایستی به صورتِ تکی و مستقل به انجامِ این فرآیند بپردازد (مشخص نخواهد بود که ماینر چه زمانی بتواند، بلاک مورد نظر را ماین کند). پس در این صورت، کسب درآمد به صورتِ گروهی (پیوستن به استخرِ ماینینگ) بیشتر و سودآورتر خواهد بود! امروزه، انجام فرآیند ماینینگ به صورت انفرادی، ایده‌ی مناسب و خوبی نیست.

واقعیت این است که به دلیلِ وجودِ تعدادِ بی شماری شرکت کننده، پیچیدگیِ شبکه‌های رمزارزهای محبوبی مانند بیت کوین به یک سطحِ غیرواقعی رسیده است. بنابراین، انجام این روش، ایده‌ی مناسبی به شمار نخواهد آمد زیرا بر این اساس، ماینرها باید زمان و انرژی بیشتری را صرفِ ماینِ ارزهای دیجیتالِ مورد نظر خود بکنند. با این شرایط، اگر هزینه‌های مصرف شده بیش از سود به دست آمده شود، ماینر مورد نظر دچارِ ضرر مالی خواهد شد.

با این شرایط، کدام روش بهتر خواهد بود solo :یاpool ؟! برای کاربران و ماینرهایی که سرمایه‌های چند میلیونی ندارند، بهترین گزینه‌ی پیش رو برای آن‌ها، پیوستن به استخرهای ماینینگ (pool mining) خواهد بود! علاوه بر این‌ها، با گذشتِ زمان، پیچیدگیِ شبکه‌های ارز دیجیتال افزایش پیدا می کند در نتیجه بهترین کار پیوستن به استخرِ ماینینگ است. با تمام این تفاسیر، به دلیل اینکه در فرآیند ماینینگ به صورت گروهی، سرعتِ کار و پیدا کردنِ بلاک‌ها افزایش پیدا می کند و ماینرها، اطلاعاتِ مورد نظر را با یکدیگر در میان می گذارند، این روش

گزینه‌ی خوبی خواهد بود. همانگونه که گفته شد، با توجه به افزایشِ پیچیدگیِ شبکه‌ی ارزهای دیجیتال، استخر ماینینگ، روشِ معقول تری به نظر می رسد، حتی با این شرایط که باید سود به دست آمده را با ماینرهای دیگر به اشتراک گذاشت.

نتیجه گیری

به طور کلی، افراد می توانند با تجهیزاتِ نسبتا ضعیف خود به انجام فرآیندِ ماینینگِ کوین‌های تقریبا ناشناخته، به صورتِ انفرادی بپردازند (جایی که هنوز، پیچیدگی شبکه غالب نشده است). علاوه بر این، این واقعیت را نیز باید در نظر گرفت که چنین کوین‌هایی، ارزشِ زیادی نخواهند داشت و بنابراین، سودِ خوبی از آن‌ها به دست نخواهد آمد. همچنین، اگر ماینری بخواهد سودی زیادی از طریقِ ماینِ رمزارز بیت کوین به صورت انفرادی به دست آورد باید سرمایه گذاریِ قابل توجهی بر روی آن انجام دهد. در نهایت، برای ماینِ کوین‌های پرسود و قابل توجه، ماینرها به استخرهای ماینینگ پیوسته و توانایی‌های خود را برای ماینِ یک بلاک، ترکیب می کنند سودِ به دست آمده را با توجه به سهمِ هر یک از ماینرها در این فرآیند، تقسیم بندی می کنند.

داستان اولین و قدیمی ترین استخر ماینینگ بیتکوین

در اواخر سال ۲۰۱۰ میلادی، بیت کوین اولین انقلاب صنعتی خود را تجربه کرد، زمانی که چندین ماینر تصمیمی مبنی بر ترکیب قدرت هش ریت خود گرفتند .در آن موقعیت (آن لحظه)، تاریخی برای رمزارز بیت کوین ایجاد شد که سبب شد این رمزارز در سال‌های آتی محبوبیت فراوانی به دست آورد .این ایده، در تاریخ ۲۷ ماه نوامبر سال ۲۰۱۰ میلادی توسط Slush ارائه و مطرح شد.

Slushاظهار داشت" :زمانی که برای اولین بار، مردم شروع به انجام فرآیند ماینینگ با استفاده از کامپیوترهای مبنی بر GPU کردند، انجام این فرآیند برای افراد دیگر پیچیده و سخت شد .من به شخصه حدود سه هفته در تلاش بودم تا بتوانم رمزارز بیت کوین ماین کنم، اما نتوانستم هیچ بیت کوینی را ماین کنم."

Slushدر ادامه توضیح داده است:

"اگر کاربر یا ماینری کامپیوتر ضعیف تری داشته باشد، انجام فرآیند ماینینگ، حدود چند هفته یا شاید حدود چند ماه ممکن است، طول بکشد. اگر این روند به این صورت ادامه پیدا کند، کاربران و ماینرها، بیت کوین‌های کمتری را ماین و استخراج خواهند کرد. به نظر من، بهترین کار برای تقویت اقتصاد رمزارز بیت کوین، همگام سازی در طول کل شبکه‌ی بیت کوین به جهتِ انجام فرآیند ماینینگ است!!"

اظهار نظر درمورد ایده‌ی !Slush (برخی موافق و برخی مخالف بودند). Slush بعد از ارائه و مطرح کردن ایده‌ی خود، واکنش‌ها و نظرات مختلف و متفاوتی را دریافت کرد. برخی از کاربران و ماینرها با پیشنهاد Slush موافق بودند، در حالی که برخی دیگر، واکنش‌های شدیدی نسبت به این ایده، نشان دادند. یکی از کاربران در پاسخ گفت: "آیا تو یک کمونیسم هستی و همکاری برای انجام فرآیند ماینینگ نیز از این منبع سرچشمه می گیرد؟! از نظر من، این ایده بی فایده است و نمی توان چنین فرآیند سختی را انجام داد."

با این تفاسیر، Slushناامید نشد و مصمم به کار خود ادامه داد. Slushسه هفته پس از مطرح کردن ایده خود، شروع به راه اندازی پیشنهاد خود مبنی بر انجام "همکاری برای انجام فرآیند ماینینگ" کرد. در نهایت، او استخر ماینینگ خود به نام "Slush Pool " را راه اندازی کرد. Slush Poolدر زمان راه اندزی با "Jeff Garzik's bitcoin CPU " و GPU اولیه ماینرها سازگار و همگام بود.

در حال حاضر، حدود ۹.۳٪ از قدرت هش ریتِ شبکه‌ی بیت کوین تحت کنترل Slush Pool قرار دارد. Slush Poolاز سال ۲۰۱۰ میلادی حدود یک میلیون رمزارز بیت کوین ماین کرده و قدرت هش ریتِ این استخر از ۵ EH/s نیز بیشتر است. امروزه حدود ۸.۵۰۰ ماینر در استخر ماینینگ "Slush Poo " مشغول به کار هستند!

کیف پول Wallet

کیف پول ارز رمزگذاری شده (cryptocurrency wallet) یک نرم‌افزار است که کلید خصوصی و کلید عمومی کاربر را ذخیره کرده و با انواع بلاک چین ارتباط برقرار می‌کند تا به این ترتیب کاربر بتواند ارز دیجیتال خود را برای کاربر مورد نظر ارسال و یا از او دریافت و نیز موجودی حساب خود را مشاهده کند. امکان استفاده از ارز دیجیتال بدون بهره‌گیری از کیف پول وجود ندارد.

همه کیف ها به دو نوع گرم یا سرد طبقه بندی می شوند. نوع اولی به اینترنت متصل و آنلاین است که به آن کیف پول "گرم" گفته می شود. دومین نوع کلی کیف پول، به اینترنت متصل نیست و آفلاین است که به آن کیف پول "سرد" گفته می شود. برای مبالغ بالا کیف پول سرد بهترین گزینه نگهداری ارزدجیتال است. اما کیف پول گرم برای نظم دادن و جلوگیری از گم شدن بیت کوین ها روش معمول تری بین مردم است. (پیش از استفاده از هر کیف چول در رابطه با امنیت آن و قابل استفاده بودن توسط ایرانیان تحقیق کنید)

کیف پول دسکتاپDesktop wallet

این کیف پول ها برای دانلود و استفاده در لپ تاپ ها و رایانه های شخصی طراحی شده اند. آنها حتی وقتی که کامپیوتر به اینترنت متصل نیست، قابل دسترسی هستند. این کیف پول ها برای سیستم عامل های مختلف مانند ویندوز، سیستم عامل مک و اوبونتو در دسترس هستند. کیف پول Armoryبهترین کیف پول دسکتاپ است، به خصوص با توجه به ویژگی های امنیتی آن. انواع دیگر کیف پول دسکتاپ که مناسب هستند عبارتند از: Atomic wallet, Coinomi, Exodus و ...

کیف پول های موبایلی Mobile wallet

امرزه که برای اکثر کارهای روزمره از تلفن همراه استفاده می کنیم ، استفاده از کیف های بیت کوین برای گوشی های هوشمند شما بسیار راحت است. کیف پول های Myceliumو Blockchainهر دوبرای پلتفرم های اندروید و IOS در دسترس هستند. برای بلک بری، Bittoin Walletمناسب ترین کیف پول در این سیستم عامل است. شاید یکی از ویژگی های مفید در کیف های موبایل، به جز ویژگی های امنیتی پیشرفته، قابلیت کد QR است. این کد امکان پرداخت های فوری را میسر می سازد.

کیف پول های آنلاین Online wallet

این خدمات توسط شرکت های خدمات کیف پول شخص ثالث در سرویس های ابری ارائه می شود. دسترسی به این کیف پول، تنها از طریق اتصال به اینترنت امکان پذیر استCoinbase ،. Circleو blockchainچند مورد از ارائه دهندگان این خدمات هستند. همچنین کیف پول Bitgoاز نوعی الگوریتم امنیتی برای قفل کردن حساب ها استفاده می کند.از سوی دیگر، کیف پول Coinkite، امکان ایجاد حساب های چند کاربره را فراهم می کند.

کیف پول های کاغذی Paper wallet

استفاده از کیف پول کاغذی برای ذخیره ارز دیجیتال بسیار ساده است و در عین حال از سطح امنیت بالایی نیز برخوردار است. عبارت کیف پول کاغذی به معنای نسخه فیزیکی (کاغذی) و یا پرینت شده از کلیدهای عمومی و خصوصی است و در عین حال به نرم‌افزارهایی نیز اشاره دارد که برای ایجاد کلید عمومی و کلید خصوصی و سپس پرینت آنها مورد استفاده قرار می‌گیرد. استفاده از کیف پول کاغذی بسیار ساده است. انتقال بیت کوین و یا هر نوع ارز دیجیتال دیگر به حساب شما از طریق انتقال این مقدار پول از کیف پول نرم‌افزاری به نشانی عمومی مندرج بر روی کاغذ پرینت شده صورت می‌گیرد. اگر هم قصد خارج کردن پول را داشته باشید،کافی است آن را از کیف پول کاغذی‌تان به کیف پول نرم‌افزاری منتقل کنید. این فرآیند که گاهی (سوییپینگ) (Sweeping) نیز نامیده می‌شود، می‌تواند به صورت دسترسی (با وارد کردن دستی کلید خصوصی) و یا با اسکن کردن کیوآرکد (QR code) مندرج روی کیف پول کاغذی صورت گیرد.

کیف پول های سخت افزاری Hardware wallet

این نوع کیف پول ارز دیجیتال با کیف پول نرم‌افزاری تفاوت دارد، زیرا کلیدهای خصوصی کاربر در آن بر روی یک سخت‌افزار نظیر یپاس‌بی ذخیره می‌شود. با وجود اینکه کیف پول سخت‌افزاری تراکنش مورد نظر (انتقال ارز دیجیتال) را به صورت آنلاین انجام می‌دهند، اطلاعات مربوط به ارز دیجیتال را به صورت آفلاین ذخیره می‌کنند که همین امر سبب افزایش امنیت آن می‌شود. کیف پول سخت‌افزاری با برخی رابط‌های تحت وب سازگار بوده و می‌تواند ارزهای مختلفی را در خود جای دهد. افزون بر این، انجام تراکنش با این نوع کیف پول آسان است. کافی است کاربر کیف پول خود را به رایانه (یا مشابه آن) متصل به اینترنت وصل کند و سپس رمز خود را وارد و مقدار مورد نظر از ارز دیجیتال را ارسال کند. کیف پول سخت‌افزاری امکان ذخیره ارز دیجیتال به صورت آنلاین و حفاظت از آن دربرابر خطرات فضای آنلاین را در اختیار کاربر قرار می‌دهد(Ledger و Trezor دو نمونه از این نوع کیف های پول هستند).

کیف پول چندامضاء Multi-Signature

Multi-signatureیا Multisig یک نوع پیکربندی از کیف پول‌های دیجیتالی بوده که برای تایید معاملات، حداقل به دو کلید نیاز دارد .به طور معمول از کیف پول های چند گانه در صرافی‌های رمزارز، برای جلوگیری از جا به جایی سرمایه‌های ذخیره شده توسط کارمندان صرافی، استفاده می شود .همچنین این کیف پول‌ها، دارای اپلیکیشن‌هایی برای کاربران نهایی نیز هستند .بنابراین، اگر کاربری بخواهد امنیت کیف پول بیت کوین خود را به طور قابل توجهی افزایش دهد، استفاده از کیف پول های چند گانه گزینه‌ی مناسبی است.

تلاش برای ایجاد امنیت بیشتر!

گزینه‌ای برای محافظت کامل از کیف پول بیت کوین وجود ندارد .کیف پول سخت افزاری ممکن است تحت ایجاد شرایطی، باز شود .کیف پول کاغذی ممکن است از بین برود. کیف پول موبایلی امکان دارد، گم شود .اما با این شرایط، گزینه‌ای وجود دارد که ترکیبی از عنصرهای کارآمد و مناسب تر است (کیف پول های چند گانه) .کیف پول چند گانه، برای تایید معاملات مورد نظر، حداقل به دو کلید نیاز دارد .استفاده از این نوع کیف پول‌ها باعث افزایش ایمنی وجوه سرمایه گذاری شده می شود.

P2SHآدرس استانداردی است که به طور معمول، در کیف پول های چند گانه یا چند امضایی بیت کوین استفاده می شود .ارائه دهندگان کیف پول‌های دیجیتالی از این نوع آدرس پشتیبانی کرده است و اطلاعات مفصلی نیز درمورد نحوه‌ی استفاده از نرم افزار مورد نظر، برای راه اندازی کیف پول چندگانه ارائه می دهند.

- دامنه‌های مختلفی از کلیدها وجود دارد که هر کدام برای بخشی مناسب اند:
- دامنه ۱تا۲: امضای معاملات توسط هر یک از طرفین معامله
- دامنه ۲تا۳: استفاده در خدمات سپرده گذاری مانندLocalbitcoins
- دامنه ۳تا۵: استفاده توسط صرافی‌های رمزارز به منظور محافظت بیشتر از کیف پول‌های گرم و سرد

چند کیف پول چندگانه

Electrumکیف پول دسکتاپ بیت کوین، یک کیف پول اوپن سورس بوده و چند سالی است که کاربران می توانند از آن استفاده کنند . Electrumاز کیف پول‌های سخت افزاری Ledger و Trezor پشتیبانی کرده است و آموزشی مبنی بر ایجاد کیف پول چند گانه‌ی ۲ of2را نیز ارائه می دهد .کیف پول Electrum به وسیله‌ی Jonald Fyookball توسعه یافته است.

Armoryکیف پول دسکتاپِ اوپن سورس بیت کوین بوده که از امضاهای چندگانه‌ی ۷ of7پشتیبانی می کند Armory .ایده‌ای برای کیف پول‌های چند گانه بوده که ارزهای دیجیتال را مانند روش ذخیره سازی سرد، به مدت طولانی ذخیره کرده و امکان دسترسی به آن کم است.

Casaگزینه‌ی دیگری برای کیف پول های چند گانه است. این کیف پول خدماتی مانند Keymaster را ارائه می دهد. کیف پول چند منظوره‌ی Casa برای افرادی که میزان زیادی ارز دیجیتال نگهداری می کنند، بسیار مناسب است.

چرا باید از کیف پول Full node استفاده کنیم؟

استفاده از یک کیف پول فول نود بهترین راه برای استفاده از یک کوین می‌باشد؛ زیرا برای استفاده‌ی از آن از تمام قوانین شبکه باید استفاده شود برای مثال بیت‌کوین‌هایی خرج می‌شوند که متعلق به شما نیستند به‌طور خلاصه بیت‌کوین شما از حمله‌ی دوبار خرج کردن در امان می‌ماند؛ همچنین تمام قوانین مربوط به‌سختی شبکه و مدت ساخت بلاک به روند دقیق پیش می‌رود. فول نودها بهترین راه شخصی برای استفاده از بیت کوین هستند که در شبکه هیچکس نمی‌فهمد کدام آدرس متعلق به شماست. به‌طورکلی کیف پول‌های فول نود از بسیاری از حملاتی که کیف پول‌های (لایت) رنج می‌برند در امان هستند.

استحکام اقتصادی

این مهم‌ترین دلیل نیاز به فول نودها است؛ هرچند که درکش شاید سخت باشد.

همان‌طور که قبلاً گفته شد فول نودها قوانینی که از قبل برایشان تعریف شده را انجام می‌دهند و مهم نیست که این قوانین چه باشد. در حالی که نودهای لایت (Lightweight Node) آن‌چیزی را که قدرت اصلی ماینرها دیکته می‌کند را انجام می‌دهند. برای مثال اگر ماینرها پاداش ساخت بلاک را افزایش دهند نودهای سبک کورکورانه آن‌ها را دنبال می‌کنند و اگر این اتفاق بیفتند شبکه مجزا می‌شود و لایت نودها و فول نودها مسیرشان از هم جدا می‌شود و هر یک از لایت نودها شبکه‌ی مجزای خود را می‌سازند و هر یک واحد پول دیجیتال خود را دارند. درنتیجه افرادی که از لایت نودها استفاده می‌کنند قادر به استفاده از فول نودها نیستند. اگر همه‌ی کاربران از گره‌ی کامل استفاده کنند در این صورت این مشکل به وجود آمدن شبکه‌های متعدد مشکل بزرگی نخواهد بود؛ کاربران لایت نود متوجه خواهند شد که با کاربران دیگر که

از فول نودها استفاده می‌کنند نمی‌توانند مبادله کنند درنتیجه آن‌ها از لایت نود استفاده نخواهند کرد تا ماینرهای مخرب دست از غلبه‌ی خود بردارند که پاسخ مناسبی به اقدام شیطانی آنهاست. البته اگر در این شرایط هر فرد اقدام به استفاده از لایت نودها کند درنتیجه این افراد می‌توانند با یکدیگر مبادله کنند و ماینرهای بد به مقصود بدشان می‌رسند.

در عمل، سناریوی فوق تحقق نیافتنی است زیرا فول نودها بسیار زیاد و شایع هستند و ماینرها برای صرف چنین قدرتی پول بسیار زیادی را باید خرج کنند. ولی اگر افراد زیادی از لایت نود استفاده کنند قطعاً ماینرها برای تغییر قوانین شبکه انگیزه پیدا خواهند کرد. تنها استفاده‌ی منطقی از لایت نود موجّه است زیرا بار اقتصادی بیت‌کوین بر روی فول نودها می‌باشد. بنابراین برای بیت کوین فول نودها بسیار حیاتی و لازم هستند؛ می‌توانیم بگوییم اقتصاد بیت‌کوین برپایه‌ی فول نودها است و لایت نودها نقشی ندارند. شرکت‌هایی که حجم معاملاتی بالایی دارند حتماً باید از فول نودها استفاده کنند. برای افزایش (استحکام اقتصادی) شبکه‌ی بیت‌کوین شما باید برای تراکنش‌های خود از یک فول نود استفاده کنید (یا از لایت نودی که اطمینان داشته باشید که از فول نود استفاده می‌کند.)

حریم خصوصی

بهترین راه برای داشتن کیف پول بیت کوین، داشتن اطلاعات در کامپیوتر است. بیشتر کیف پول‌های لایت باعث درز اطلاعات شما می‌شوند به دلیل اینکه سرور ثالثی اطلاعات شما مانند احراز هویت و آدرس شما را می‌خواهند. سرور الکتروم (Electrum) می‌تواند بفهمد کدام یک از آدرس‌ها برای شماست و آن‌ها را به هم مربوط کند.

امنیت

در لایت نودها امکان فریب وجود دارد؛ ممکن است لایت نود تراکنشی را تائید کند که واقعاً تایید نشده است. این امر می‌تواند آسیب مالی جدی به اعتبار بعضی از سایت‌ها بزند. در مقابل لایت نودها، فول نودها بیشترین ضریب امنیت را دارند؛ برای همین توصیه می‌شود که چه برای کاربردهای تجاری و روزمره از فول نودها استفاده شود.

خدمات شبکه

فول نودها می‌توانند خدماتی به دیگر شبکه‌ها و سایت‌ها ارائه کنند؛ که این خدمات برای لایت نودها هم مفید است. ازجمله این خدمات به موارد ذیلمی توان اشاره کرد:

- لایت نودها برای ساخت تراکش از فول نودها استفاده می‌کنند؛ پس باوجود فول نودها، یک لایت نود برای ساخت تراکنش نیاز ندارد که دفتر کل را دانلود کند.
- بلاک‌های جدیدی که ساخته‌شده را در اختیار نودهایی که برای مدتی آفلاین بوده است می‌دهند.
- تراکنش‌ها را از کاربران به استخراج‌کننده‌گان انتقال می‌دهند.
- تراکنش‌هایی که توسط استخراج‌کننده‌گان ساخته‌شده است را به نودهای دیگر انتقال می‌دهند.

کیف پول Hierarchical Deterministic

از زمان پیدایش بیت کوین و دیگر ارزهای دیجیتالی، کیف پولهای بسیار متنوعی به وجود آمده اند .کیف پولها مهمترین و اساسی ترین رابط هایی هستند که از طریق آنها یک کاربر دارایی دیجیتالی خود را مدیریت و حفاظت می کند. به عنوان مثال، با یک کیف پول ساده بیت

کوین شما می توانید بانک خود باشید و دارایی خود را در تمامی نقاط دنیا بدون هیچ مساله ای همراه داشته باشید. اما این امکان در روزهای ابتدایی پیدایش بیت کوین و در حقیقت پیش از ظهور کیف پول اچ دی ، محقق نبود.

به طور معمول، در کیف پولهای بیت کوین، آدرس خصوصی / عمومی (یا کلید) به طور تصادفی تولید می شود و مستلزم این است که شما هر بار پس از ایجاد آدرس جدید یک نسخه پشتیبان یا در اصطلاح بکاپ بگیرید. اگرچه ممکن است در ابتدا احساس کنید که این یک روند ساده و آسان است. اما رفته رفته با توجه به افزایش تعداد تراکنش های شما کنترل و بکاپ گرفتن از آدرس ها امری پر زحمت و پیچیده تر می شود.

علاوه بر این، اگر فردی هستید که برای مساله حریم خصوصی مالی اهمیت ویژه ای قائلید و تراکنش های زیادی را انجام می دهید، بنابراین شما نیازمند ایجاد آدرسها و کلیدهای خصوصی فراوانی هستید. از سوی دیگر، به منظور جلوگیری از تلفات، برخی از کیف پولها از همان آدرس بیت کوین برای تمامی تراکنشهای خود دوباره استفاده می‌کنند. این عمل خیلی درست و صحیح نیست و می تواند حریم شخصی شما را به خطر بیندازد. و به همین دلیل است که کیف پول های اچ دی تحت نشان Bitcoin Improvement Proposal) ۳۲ (توسعه داده شد.

کیف پولهای اچ دی چیست؟

تصور کنید که چقدر آسان خواهد بود اگر مکانیسمی، الگویی ایجاد کند که از طریق آن کلیدهای خصوصی و عمومی بدون دشواری بکاپ گرفتن و همچنین بدون امکان کشف این رمزها تولید شوند. به این کیف پولها، کیف پولهای اچ دی می گویند.

همه کیف پول های اچ دی از کلید های سید (seed)که از ۱۲ کلمه تشکیل شده اند استفاده می کنند. هر بار این seed در انتها، توسط یک مکانسیم شمارشی اضافه می شود و برای ایجاد آدرسهای نامحدود بیت کوین استفاده می شود.

چه اتفاقی در داخل یک کیف پول اچ دی رخ می دهد؟

کیف پول های اچ دی یک ساختار سلسله مراتبی مانند یک درخت ایجاد می کند که این درخت از کلید seed اصلی مبتنی بر BIP ۳۲ شروع می شود. هنگامی که شما یک کیف پول اچ دی را با استفاده از کلید seed بازیابی می کنید، این کیف پول جستجو را آغاز کرده و تمام کلیدهای خصوصی این درخت را که از BIP ۳۲ استفاده کرده اند را می یابد و به محض اینکه اسکن کردن کلیدها بر روی شبکه به اتمام برسد شما دارایی خود را بازیابی کرده اید. هنگام استفاده از کیف پول اچ دی، بکاپ گرفتن از کلید seed و نگهداری آن در یک محیط امن امری اجباری و واجب است زیرا تنها از طریق آن شما می توانید اطلاعات از دست رفته کیف پول خود را بازیابی کنید. تنها یک بار بکاپ گرفتن به این معنی است که تمام آدرس های بعدی بر اساس محاسبات ریاضی الگوریتم این کیف پول دوباره ایجاد شوند. کیف پول های اچ دی از یک الگوریتم هش یک طرفه-SHA ۲۵۶ استفاده می کند تا حتی اگر ورودی یا کلید seed یکسان باشد بدون هیچ گونه خطایی این درخت کلید ها را تولید می کند.

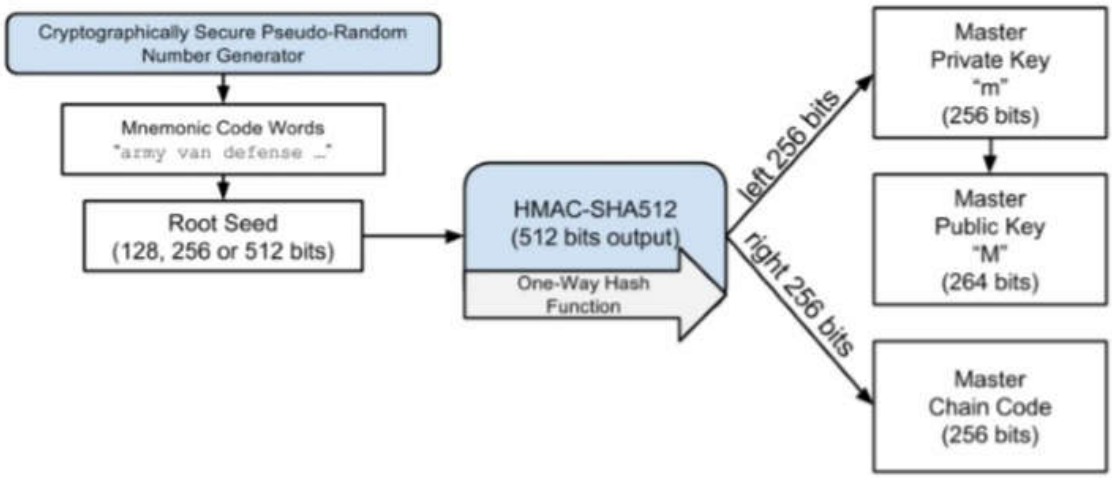
مزایای کیف پولهای اچ دی

- شما فقط باید از یک کلید بکاپ بگیرید. این تنها باری است که شما نیازمند چنین عملی هستید.
- شما هر زمان که بیت کوین دریافت می کنید، می توانید آدرسهای دریافتی زیاد و متفاوتی بسازید.
- شما می توانید حریم خصوصی مالی خود را حفظ کنید.
- از آنجا که شما هر دفعه یک آدرس جدید دریافت می کنید می توانید کاربران جدید را گمراه کنید.

استخراج کیف پول HD از سید چگونه انجام می‌شود؟

کیف پول‌های HD از یک سید ریشه (root seed)بوجود می‌آیند که یک عدد اتفاقی ۱۲۸، ۲۵۶ یا ۵۱۲ بیتی است. معمولا هر سید از یک یادآور به وجود می‌آید.هر کلید موجود در کیف پول اچ دی به طور قطعی از سید ریشه استخراج می‌شود و امکان استخراج مجدد کل کیف پول اچ دی را از سید ریشه و در هرگونه کیف پول سازگار ممکن می‌سازد. این ویژگی امکان بک‌آپ، بازیابی، ارسال و دریافت کیف پول اچ دی را فراهم می‌کند. هر کیف پول اچ دی می‌تواند دارای هزاران و حتی میلیون‌ها کلید باشد و به وسیله انتقال یادآوری که سید ریشه از آن استخراج شده، بازیابی شود.

تصویر پایین روند ایجاد کلیدهای اصلی و چین کد را برای یک کیف پول اچ دی به نمایش گذاشته است:



سید ریشه در الگوریتم HMAC-SHA512قرار می‌گیرد و هش حاصل شده برای استخراج یک کلید شخصی اصلی (m) و یک چین کد اصلی (c)به کار می‌رود. کلید شخصی اصلی یا مادر(m) ، سپس یک کلید اصلی عمومی متناظر (M) را با استفاده از یک ضرب منحنی بیضوی m * Gاستخراج می‌کند. چین کد (c) برای معرفی آنتروپی به تابعی که کلیدهای کوچک را بوجود می‌آورد، استفاده می‌شود. در قسمت بعد بیشتر راجب این موضوع صحبت شده است.

استخراج کلیدهای شخصی کوچک(Private child key derivation)

کیف پول اچ دی از یک تابع به نام CKD (child key derivation) برای استخراج کلیدهای کوچک از کلیدهای اصلی (parent keys)استفاده می‌کند. این توابع استخراج کلیدهای کوچک بر اساس یک تابع هش بوجود می‌آید که این موارد را با هم ترکیب می‌کند:

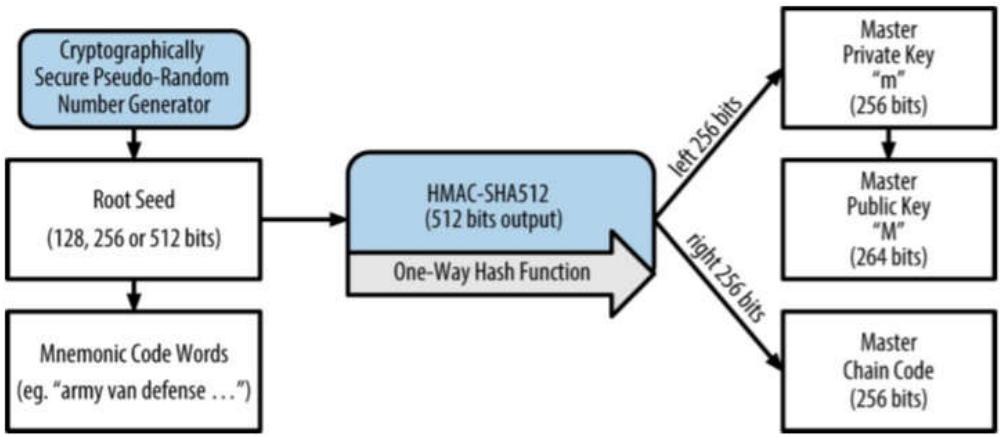
- یک کلید خصوصی یا عمومی اصلی) که به آن کلید بازشده ECDSA گفته می‌شود(
- یک سید که به آن چین کد گفته می‌شود (۲۵۶ بیت)
- یک عدد شاص (۳۲ بیت)

چین کد برای معرفی دیتای اتفاقی قطعی (deterministic) به این روند معرفی می‌شود. بنابراین دانستن کلید کودک و عدد شاخص برای استخراج دیگر کلیدهای کوچک کافی نیست. دانستن کلیدهای کوچک امکان پیدا کردن کلیدهای همتا را ممکن نمی‌کند مگر این که چین

کد را نیز بدانید. سید چین کد اولیه (در ریشه درخت) از سید به وجود می‌آید در حالیکه کلیدهای کوچک بعدی از چین کدهای اصلی یا مادر خودشان به وجود می‌آیند.

این سه آیتم یعنی کلیدهای اصلی، چین کد و عدد شاخص با هم ترکیب می‌شوند و برای استخراج کلیدهای کوچک ترکیب می‌شوند و الی آخر. کلید عمومی اصلی (parent public key)، چین کد (chain code)و عدد شاخص (index number) با هم ترکیب می‌شوند و با الگوریتم HMAC-SHA512 برای تولید یک هش ۵۱۲ بیتی، ترکیب می‌شوند. این هش ۵۱۲ بیتی به دو هش نیمه ۲۵۶ بیتی تقسیم می‌شود. نیمه سمت راست ۲۵۶ بیتی، تبدیل به چین کد برای کلید کوچک می‌شود. هش ۲۵۶ بیتی سمت چپ و عدد شاخص به کلید خصوصی اصلی یا مادر اضافه شده و کلید خصوصی کوچک را تولید می‌کند.

در تصویر پایین می‌بینیم که چگونه از عدد شاخص ۰ برای تولید صفر کلید کوچک از کلیدهای اصلی استفاده می‌شود.



تغییر شاخص باعث افزایش کلیدهای اصلی و تولید کلیدهای کوچک در نسل‌های بعدی می‌شود. به عنوان مثال کلید کوچک ۰، ۱ و ۲ و الی آخر. هر کلید اصلی میتواند ۲,۱۴۷,۴۳۸,۶۴۷(۲^۳۱) (کودک را به وجود آورد (۲^۳۱ (نیمی از کل طیف(۲^۳۲)موجود است چرا که نیمه دوم آن برای نوع خاصی از استخراج به کار می‌رود. با تکرار این روند در قسمت پایین درخت، هر کلید کوچک می‌تواند به یک کلید اصلی تبدیل شده و کلیدهای کوچک خود را در نسل‌های بی انتها بسازد.

استفاده از کلیدهای کوچک (child keys) استخراج شده

کلیدهای کوچک خصوصی از کلیدهای اتفاقی (nondeterministic)قابل تمییز نیستند. کلید کوچک نمی‌تواند در جهت یافتن کلیدهای اصلی مورد استفاده قرار بگیرد چرا که تابع استخراج، یک تابع یک طرفه است. اگر شما کلید کوچکn ام را داشته باشید، نمی‌توانید همتایانش مانند n-1 یا n+1 یا هر کلید کوچکی که قسمتی از این توالیست را پیدا کنید. فقط کلیدهای اصلی و چین کد می‌توانند همه کلیدهای کوچک را استخراج کنند. بدون داشتن چین کد کلید کوچک، کلید کوچک نمی‌تواند برای تولید کلیدهای نسل بعد مورد استفاده قرار بگیرد. شما برای ایجاد شعبات بعدی و کلیدهای کوچک نسل بعدی نیاز به کلیدهای شخصی کوچک و چین کد کوچک دارید. حالا سوال اینجاست که پس کلیدهای شخصی کوچک چه فایده‌ای دارند؟ این کلیدها را می‌توان برای ایجاد کلیدهای عمومی و آدرس بیت کوین استفاده کرد. علاوه بر این، چنین کلیدی می‌تواند برای امضای معاملات به منظور خرج هرآنچیزی که به آدرس مدنظر ارسال شده استفاده شود.

کلیدهای توسعه یافته(Extended keys)

همانگونه که می‌دانیم، تابع استخراج کلید می‌تواند برای ایجاد کلید کوچک در هر سطحی از درخت مورد استفاده واقع شود و این استخراج بر اساس سه ورودی یعنی یک کلید، یک چین کد و یک عدد شاخص برای کلید کوچک مدنظر انجام می‌شود. دو عنصر اصلی در این روند، کلید و چین کد هستند و ترکیب اینها، کلید توسعه یافته را به وجود می‌آورد. عبارت کلید توسعه یافته همچنین می‌تواند به نام کلید قابل توسعه نیز شناخته شود چرا که این نوع کلید می‌تواند برای استخراج کلیدهای کوچک به کار گرفته شود.

کلیدهای توسعه یافته، ذخیره شده و در واقع به عنوان مبدلی برای تبدیل کلید ۲۵۶ بیتی و چین کد ۲۵۶ بیتی به یک توالی ۵۱۲ بیتی مورد استفاده واقع می‌شوند. یک کلید عمومی توسعه یافته، شامل یک کلید عمومی و یک چین کد است که می‌تواند برای ایجاد کلیدهای عمومی کوچک مورد استفاده واقع شود. کلید توسعه یافته را به عنوان ریشه یک شاخه در ساختار درختی کیف پول اچ دی در نظر بگیرید. به کمک ریشه این شاخه، شما می‌توانید بقیه شاخه‌ها را استخراج کنید. کلید خصوصی توسعه یافته می‌تواند یک شاخه کامل ایجاد نماید در حالی که یک کلید عمومی توسعه یافته می‌تواند فقط یک شاخه از کلیدهای عمومی را ایجاد کند.

کلیدهای توسعه یافته با استفاده از Base58Check کدگذاری می‌شوند تا بتوانند به راحتی بین کیف پول‌های سازگار BIP-32 وارد و خارج شوند. در کدگذاری Base58Check کلیدهای توسعه یافته از یک نسخه عددی خاص استفاده می‌شود که نتیجه آن ایجاد یک پیشوند "xprv" و "xpub" برای کدگذاری کاراکترهای Base58 به منظور شناسایی راحت آنهاست. به دلیل وجود کلیدهای توسعه یافته ۵۱۲ یا ۵۱۳ بیتی، این نوع Base58Check از دیگررشته های کدگذاری شده Base58Check طولانی‌تر است.

در اینجا مثالی از یک کلید توسعه یافته خصوصی با کدگذاری در Base58Check آورده شده است:

xprv9tyUQV64JT5qs3RSTJkXCWKMyUgoQp7F3hA1xzG6ZGu6u6Q9VMNjGr67Lctvy5P8oya
YAL9CAWrUE9i6GoNMKUga5biW6Hx4tws2six3b9c

در اینجا کد کلید عمومی توسعه یافته متناظر را مشاهده می‌کنید که در Base58Check کدگذاری شده است:

xpub67xpozcx8pe95XVuZLHXZeG6XWXHpGq6Qv5cmNfi7cS5mtjJ2tgypeQbBs2UAR6KECe
eMVKZBPLrtJunSDMstweyLXhRgPxdp14sk9tJPW9

استخراج کلید کوچک عمومی(Public child key)

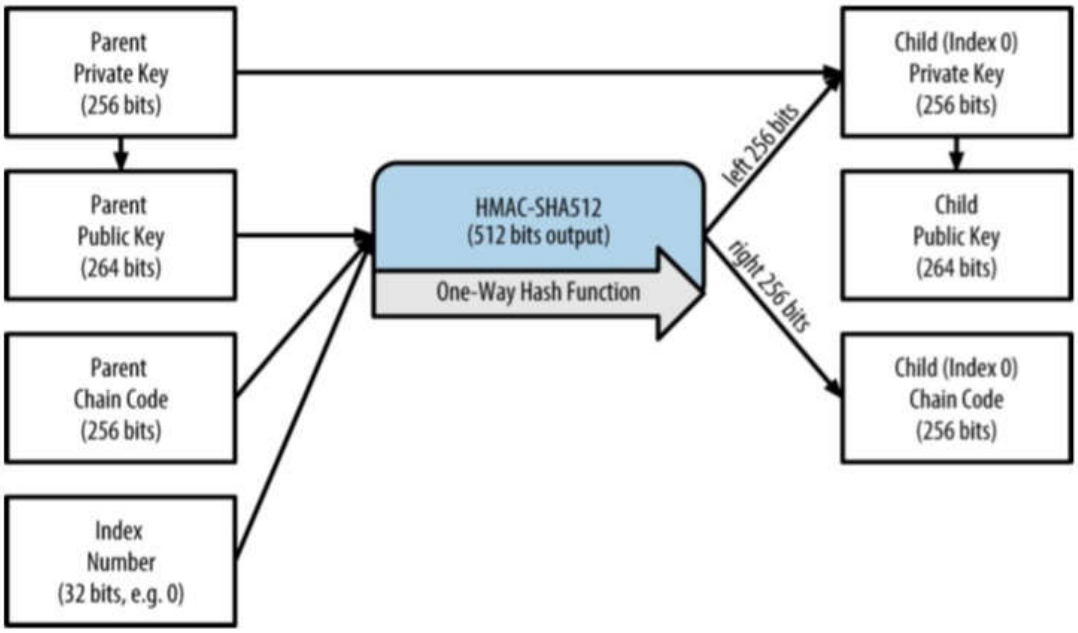
همانگونه که اشاره شد یکی از ویژگی‌های مفید کیف پول‌های اچ دی، توانایی استخراج کلیدهای کوچک عمومی از کلیدهای اصلی عمومی بدون داشتن کلید خصوصی است. این ویژگی به ما دو راه استخراج کلید عمومی کوچک را می‌دهد: یکی از کلید خصوصی کوچک و یکی از کلیدهای اصلی عمومی. بنابراین یک کلید اصلی عمومی توسعه یافته می‌تواند برای استخراج همه کلیدهای عمومی (و تأکید می‌کنیم فقط کلیدهای عمومی) در همان شاخه ساختار کیف پول اچ دی مورد استفاده قرار بگیرند.

این میانبر می‌تواند برای استخراج یک کلید عمومی بسیار امن به کار رود یعنی آرایشی که در آن یک سرور و یا اپلیکیشن، یک کپی از کلید عمومی توسعه یافته را داشته و هیچ کلید خصوصی را شامل نشود. این نوع آرایش می‌تواند تعداد نامحدود کلید عمومی و آدرس بیت کوین بسازد اما نمی‌تواند هیچ پولی را در آن آدرس‌ها خرج کند. در همین حال و در یک سرور امن دیگر، کلید توسعه یافته خصوصی می‌تواند همه کلیدهای خصوصی متناظر را برای امضای معاملات و پرداخت پول استخراج کند

یکی از کاربردهای مهم این روش، نصب یک کلید توسعه یافته عمومی بر روی یک سرور وب برای استفاده در تجارت الکترونیک است. سرور وب از یک تابع استخراج کلید عمومی برای ایجاد یک آدرس جدید بیت کوین برای معاملات استفاده می‌کند (به عنوان مثال کارت خرید مشتری). سرور وب هیچ کلید خصوصی که نسبت به سرقت آسیب‌پذیر باشد را نخواهد داشت. بدون کیف پول اچ دی، تنها راه انجام این کار استخراج هزاران آدرس بیت کوین بر روی سرورهای امن جداگانه و پیش بارگذاری آن روی سرور تجارت الکترونیک است. این روش غلط بوده و نیازمند مراقبت مداوم است تا این اطمینان حاصل شود که کلیدهای سرور خالی نشده باشد.

کاربرد دیگر این روش برای محفظه سرد یا کیف پول های سخت‌افزاریست. در این موضوع، کلیدهای خصوصی توسعه یافته می‌تواند بر روی یک کیف پول کاغذی و یا یک دستگاه سخت افزاری مانند ترزور (Trezor)ذخیره شده و کلیدهای عمومی توسعه یافته به صورت آنلاین با امنیت بالا نگهداری شوند. کاربر می‌تواند یک آدرس دریافت (receive) را در هر زمانی که بخواهد ایجاد نماید در حالیکه کلیدهای خصوصی به صورت امن و آفلاین ذخیره شده اند. برای خرج پول، کاربر می‌تواند از یک کلید شخصی توسعه یافته برای امضای آفلاین بیت کوین یا امضای معاملات در یک دستگاه کیف پول سخت‌افزاری استفاده کند.

تصویر پایین نشان دهنده مکانیزم توسعه کلیدهای اصلی عمومی برای استخراج کلیدهای کوچک است.



BIP32

BIP39

some of CRYPTOCURRENCY

BIP44

BIP77

ICO به چه معناست؟

ICOدر لغت به معنای عرضه اولیه پول یا همان Initial Coin Offering است. در عمل به فرایندی گفته می‌شود که در آن کمک‌های مالی جمع‌آوری می‌شود. پول در این جمع آوری به صورت یک توکن ایجاد شده و فروخته می‌شود. این توکن در بستر یک بلاکچین پیاده می‌شود که امروزه اکثر توکن‌های موجود از بلاکچین اتریوم برای این کار استفاده می‌کنند. در سراسر دنیا بسیاری از شرکت‌ها یا حتی گروه کوچکی از افراد به دنبال راه‌اندازی یک کسب و کار برای خود هستند، ایده جالب و خلاقانه‌ای هم در سر دارند، اما سرمایه اولیه اینکار را ندارند. امروزه آنها می‌توانند به صورت غیر متمرکز و با اعلام ICO خود، از همه مردم در هر جای دنیا سرمایه جذب کنند.

بجز توکن‌های پایه اتریوم (Ether_Base) توکن‌های دیگری مثلEOS ، NEO، ICONو کاردانو که روی یک بلاکچین جدا پیاده شدند، وارد بازار شده‌اند و برنامه‌های غیرمتمرکز زیادی روی آنها انجام می‌شود.

در این روش، یک سرمایه‌گذار توسط یک قرارداد هوشمند که روی بستر بلاکچین نوشته شده است، درخواست توکن مورد نظر برای سرمایه‌گذاری را ارسال می‌کند. در مقابل، شرکت مقداری از توکن را به نسبت قیمت ارز خریداری‌شده توسط سرمایه‌گذار برای او میفرستد. برخی از پارامترهای سرمایه‌گذاری سنتی مانند مقدار حداقلی و حداکثری بودجه مورد نیاز برای جمع‌آوری و تعیین مقداری بودجه برای پاداش در قراردادهای هوشمند نیز رعایت شده است.

تاریخچه پیدایش ICO

اولین ICO در ۳۱ جولای ۲۰۱۳ توسط پروژه Mastercoin برگزار شد. این پروژه به رهبری براک پیرس و اسکات واکر به طور رسمی با یک اعلام عمومی برای جمع‌آوری بودجه راه‌اندازی شد که در آن هر کس می‌توانست با ارسال بیت کوین به یک آدرس کیف پول خاص، سهام یا همان توکن Mastercoins را بخرد. با به بار نشستن پروژه و بالا رفتن ارزش سهام این تیم، سرمایه گذاران می‌توانستند توکن خود را در بازار بفروشند و از این طریق به سود برسند. در این پروژه ۵۰۰ نفر شرکت کردند و چیزی حدود ۴۷۰۰ بیت کوین جمع‌آوری شد که معادل با ۵ میلیون دلار در آن زمان بود. قیمت بیت کوین در دسامبر همان سال از ۱۰۰ دلار به ۱۰۰۰ دلار افزایش پیدا کرد.

ICOکه جهان را تغییر داد توسط بنیانگذار اتریوم، ویتالیک بوترین در سال ۲۰۱۴ رهبری شد. براساس گزارش خبرگزاری کوین‌تلگراف، حدود ۱۲ ساعت پس از آغاز شروع فروش توکن، ۷.۴ میلیون اتر فروخته شد که در آن زمان معادل حدود ۳،۷۰۰ بیت کوین یا ۲.۳ میلیون دلار بود. گزارش‌ها حاکی از آن است که او بیش از ۱۵ میلیون دلار برای راه‌اندازی پروژه جمع‌آوری کرد و شروع به گسترش پلت‌فرم خود کرد. پروتکل ERC۲۰ اتریوم، تحول عظیمی روی ICO ایجاد کرد و باعث شد اتریوم به بستری برای برگزاری ICO تبدیل شود و مدل سنتی آن را به کلی تغییر داد.

تفاوت‌های ICO با سیستم‌های سنتی جمع آوری بودجه

با این وجود کهICO ها به زودی به طور کامل جایگزین سرمایه‌گذاری‌های سنتی نخواهند شد، اما مطمئنا دسترسی غیر متمرکز به سرمایه، مدل‌های جمع‌آوری کمک‌های مالی سنتی را مختل می‌کند. یکICO ، تکنولوژی پایه آن و قراردادهای هوشمند، اساسا شبیه Kickstarter یا Indiegogoاست. فرض کنید یک شرکت پروژه‌ای دارد که می‌خواهد آن را اجرا کند و بودجه لازم را ندارد، در گزارشی تحت عنوان وایت پیپر، جزئیات پروژه خود، زمان شروع و اتمام کار، مقدار بودجه مورد نیاز، ایده مورد نظر و تیم تشکیل دهنده را به صورت عمومی اعلام می‌کند. معمولا در وبسایت رسمی یا شبکه های مجازی این وایت پیپر منتشر شده و همه مردم در سراسر دنیا می‌توانند به آن دسترسی داشته باشند. اما Kickstarter یا Indiegogo صندوق‌هایی هستند که شرکت‌ها می‌توانند به صورت وام بودجه را تامین کنند.

در روش های سنتی بودجه مورد نیاز برای یک پروژه توسط نهادهای مرکزی تامین می‌شد. این یعنی بعد از بازدهی و سوددهی پروژه، درآمد حاصل بین شرکت و سرمایه‌گذار متمرکز تقسیم می‌شد، اما به روش ICO هرکس در هر جای دنیا می‌تواند در یک پروژه سهیم شود و از درآمد حاصل آن سود ببرد. از طرفی به روش های سنتی این احتمال وجود دارد که در بودجه مورد نیاز تقلب یا تخلفی رخ دهد (برای مثال همه پول مورد نیاز به شرکت اهدا نشود)، اما با ICO چون پول مستقیما توسط قرارداد هوشمند از مردم به تیم پروژه انتقال می‌یابد، نهاد واسطه‌ای در این بین وجود ندارد که شاهد تخلف احتمالی باشیم. مدتی پیش گزارش شد که Indiegogo نیز یک بلاکچین ایجاد کرده تا سیستم جمع‌آوری بودجه نوین را پیاده سازی کند. این نشان می‌دهد که سیستم های سنتی متوجه ویژگی‌های کاربردی ICO شده‌اند و تمایل دارند از آن استفاده کنند.

ارتباط اتریوم باICO

در سال ۲۰۱۷، بلاکچین اتریوم تبدیل به بستری برای برگزاری ICO شد. تا پایان ۲۰۱۷، ٪۹۰ توکن‌های ایجاد شده برایICO ها روی اتریوم پیاده شد. این آمار طبق لیست کوین‌مارکت‌کپ اعلام شده که معتبرترین منبع قیمت و حجم معاملات ارزهای موجود در بازار است. در اینجا به دلایلی اشاره می‌کنیم که چرا اتریوم توانست چنین قابلیت گسترده‌ای داشته باشد:

۱. قابلیت نوشتن قرارداد هوشمند روی بستر اتریوم که باعث شد توسعه‌دهندگان به راحتی بتوانند برنامه‌های غیرمتمرکز خود را روی آن بنویسند و اجرا کنند.
۲. محبوبیت پروتکلERC ۲۰ اتریوم که این مزیت را برای اکسچنج‌ها ایجاد می‌کرد تا به راحتی بتوانند توکن‌های جدید را به پلت فرم خود اضافه کنند.
۳. سرمایه‌گذارانی که در پروژه اتریوم شرکت کردند، در همین چند سال سود زیادی بردند و علاقه شدیدی به گسترش سرمایه‌گذاری های خود روی توکن‌های دیگر پیدا کردند.

همه این عوامل دست در دست هم داد تا اتریوم سال به سال جذاب‌تر و محبوب‌تر شود. البته این حجم از توکن‌های موجود روی بستر اتریوم و گستردگی جهانی، آن را با مشکل مقیاس‌پذیری مواجه کرده و شاید چالش‌های زیادی پیش پای توسعه‌دهندگان و برنامه نویسان این پروژه قرار دهد.

با به بلوغ رسیدن مدلICO ، نیاز به انطباق و تکامل آن با بازار بیشتر احساس می‌شود. تخلفات رخ داده در این مدت، هک و کلاهبرداری ها و مقررات دولتی نیاز به مدیریت بهتر و اصلاحاتی دارد. در ماه دسامبر، ویتالیک بوترین وJason Teutsch ، بنیانگذار پروژه بلاکچینی TrueBit، یک وایت پیپر ۱۵ صفحه‌ای را با توصیف نوع جدیدی از ICO به نام عرضه تعاملی پول معرفی کردند. مشکل اصلی که آن‌ها امیدوارند با این طرح جدید حل شود، محدود کردن تاثیراتی است که تبلیغات و حواشی می تواند روی ICO بگذارد. در حقیقت هدف کاهش اثر پامپ و دامپ قیمت توکن است که منجر به نوسانات شدید در قیمت‌گذاری ICO های اخیر شده‌است. آن‌ها امیدوارند که این کار را به دو طریق انجام دهند:

۱. حذف کردن حداکثر میزان بودجه .این موضوع تا به امروز باعث شده سرمایه گذاران از ترس اینکه نتوانند توکن مورد نظر خود را خریداری کنند، برای خرید هجوم آورند و در عرض چند دقیقه قیمت توکن به شدت افزایش پیدا کند یا اصطلاحا پامپ شود.
۲. به سرمایه گذاران اجازه داده شود تا خرید خود را لغو کنند .این کار باعث می شود زمانیکه قیمت به شدت افزایش پیدا کرده، اگر کسی در زمان خرید منصرف شده باشد، خرید خود را لغو کند و اجازه دهد تا دیگران در صورت تمایل خرید کنند. طبق وایت پیپر منتشر شده: اکثر کاربران معمولا بر اساس رفتارهای دیگر خریداران به بازار وارد یا خارج می‌شوند. با این روش می‌توان ارزش‌گذاری را به سمت تعادل در بازار حرکت دهیم.

اخیرا، ویتالیک مقاله دیگری را در مورد گسترش مفهوم و آینده ICO منتشر کرده که یک سیستم خودمختار غیرمتمرکز را با ICO ترکیب کرده و نام آن را DAICO گذاشته است. او ادعا می‌کند که این کار پیچیدگی و ریسک مرتبط باICO ها را با توزیع قدرت به حداقل می‌رساند. برای مثال، این کار مانع از کلاهبرداری صندوق‌های بزرگ می‌شود. موارد زیادی را در این مدت مشاهده کردیم که بعد از جمع‌آوری بودجه، پروژه عملی نشده و پول جمع شده در حقیقت دزدی شده است. این مکانیزم طوری تعریف شده که اگر پروژه در مرحله اجرا قرار گرفت، سرمایه‌گذاران با رسیدن به یک اجماع اجازه دسترسی به بودجه را به تیم پروژه می دهند و در صورت اتمام پروژه مطمئن می شوند که سود به آنها باز خواهد گشت. اگر چه سیستم‌های رای‌گیری هم از هر نوع، همیشه مستعد دستکاری هستند، اما مفهوم در اینجا به حفاظت سیستم در مقابل کلاهبرداری کمک خواهد کرد.

چه جایگزین‌هایی برای ICO وجود دارد؟

راه‌های دیگری نیز وجود دارند که بتوان توکن‌ها را توزیع کرد. به عنوان مثال، یک پروژه بلاکچین تصمیم می‌گیرد که توکن‌های خود را به صورت رایگان توزیع کند. این توزیع را بین کاربران یک جامعه (مثلا جامعه بیت کوین) انجام می‌دهد. در حقیقت یک تیم با این کار، بجای اینکه هزینه تبلیغات بپردازد، توکن‌هایش را رایگان به کاربران می‌دهد و این انگیزه را در آنها ایجاد می‌کند تا در گسترش و افزایش استفاده پلت فرم مشارکت کنند. این روش تقریبا به نوعی جمع‌آوری بودجه شبیه است و به آن ایردراپ می‌گویند.

تقلب، دروغ و ناامیدی

مانند هر ابزار دیگری، افرادی در اکوسیستم هستند که نقاط ضعف سیستم را پیدا کرده و از آنها به سود خودشان بهره می‌برد، ICO نیز از این امر مستثنی نیست. افرادی سودجو، با ساختن داستان‌های دروغین راجع به راه‌اندازی پروژه‌هایشان، توکن خود را به مردم غالب کرده و ارزش آن را برای همیشه تسخیر کرده‌اند. دیدگاهی وجود دارد که می‌توان ICOهای بد را از طریقICOهای خوب شناسایی نمود.

آیا قانون از سرمایه‌گذاران محافظت نمی‌کند؟ پاسخ در شرایط فعلی خیر می‌باشد. بیشتر iCOها ارائه‌دهنده‌ی توکن‌های کاربردپذیر و با ارزش هستند. این توکن‌ها برای استفاده بر روی یک پلتفرم دیگر طراحی می‌شوند. از این رو مفاهیم امنیت و قانون برای آنها کارساز نیست. برخی معتقدند نبودن قوانین و محدودیت، مفید بوده و نوآوری و توسعه را تسریع می‌کند. با اینکه این استدلالی معتبر است اما به دزدان نیز این فرصت را می‌دهد تا از سرمایه‌گذارانی که خیلی با نحوه‌ی کار ICOها آشنا نیستند کلاه‌برداری کنند. البته ICOهایی هم وجود دارند که اقدامات نظارتی نسبت به فروش توکن‌های خود پیش گرفته‌اند. به عنوان مثال می‌توان اینطور تعیین کرد که اگر سرمایه‌ی کافی برای اجرای پروژه‌ی مورد نظر جمع‌آوری نشد، مبالغ جمع شده به صاحبان آن بازگردانده شود.

آینده ICO

دسترسی غیر متمرکز به سرمایه به عنوان یک نیروی محرک در مرحله اولیه آغاز سرمایه‌گذاری، مفهومی اساسی و البته الزامی برای دنیای امروز است. با ظهور پلت‌فرم های جدید نظیر EOS و شروع به گرفتن سهم بازار از اتریوم، این تکنولوژی روز به روز بالغ‌تر خواهد شد و رشد خواهد کرد.

STO چیست؟

عرضه توکن های اوراق بهادار که به آن STO گفته می شود، به طور روز افزون در میان مشتاقان ارز دیجیتال محبوبیت می یابد. در حالی که ابهامات زیادی در مورد ICO ها موجود است، STOها تا حدودی تردیدهای این فضا را رفع می کنند و انتظار می رود که به شیوه ای قانونی، دسترسی آزاد به سرمایه افراد سرمایه گذار را فراهم کنند.

توکن های اوراق بهادار معرف اوراق بهادار مالی مانند بورس، اوراق قرضه و اشکال مختلف دارایی ها به صورت دیجیتال هستند. به عنوان مثال اگر سهام بورس را در نظر بگیریم، زمانی که سرمایه گذار سهام شرکتی را می خرد، این سهام نماینده درصد مالکیت سهام دار در آن شرکت می باشد. این مالکیت معمولا یک سری حقوق مالی مانند حق رای و حق دریافت سود سهام را برای فرد سرمایه گذار به همراه می آورد.

فرآیند STO را هم می توان به همین شیوه در نظر گرفت با این تفاوت که در اینجا سرمایه گذار توکنی که معرف مالکیت او در شرکت مورد نظر است را خریداری می کند. تفاوت برجسته و عمده آن است که STO ها از فناوری بلاک چین برای ثبت تراکنش ها استفاده می کنند که این تراکنش ها معرف انتقال مالکیت از فردی به فرد دیگر می باشند. در این حالت هر گونه پرداخت سود سهام نیز می تواند بر روی بلاک چین ثبت شود.

تفاوت STOو ICO

شباهت STO و ICO در این است که در هر دو فرآیند توکن عرضه می شود. تفاوت اصلی این دو فرآیند ریشه در طبقه بندی توکن های صادر شده دارد. توکن های صادر شده در ICO ها، معمولا به عنوان توکن های کاربردی طبقه بندی می شوند که این توکن ها دسترسی به خدمات و یا محصولات صادر شده توسط شرکت را فراهم می آورند. به عنوان مثال Augur را در نظر بگیرید؛ سرمایه گذاران این پروژه در آگوست ۲۰۱۵ در راه اندازیICO ، توکن این پلتفرم یعنی REP را در عوض دریافت بیت کوین یا اتر عرضه کردند. سرمایه گذاران این پروژه تا زمانی که شبکه اصلی این ارز دیجیتال در ماه جولای ۲۰۱۸ عرضه شد قادر نبودند که از این توکن برای مشارکت در شبکه استفاده کنند. توکن های REPبه کاربران اجازه می دهد تا به ترید، گزارش و مباحثه در مورد نتیجه رویداد ها بپردازند.

در مقابل، افرادی که در STO ها مشارکت می کنند، عمدتا سرمایه گذار هستند و نه کاربر معمولی. یکی از STO های مشهور اخیر tZERO است که یک شرکت تابعه از شرکت آمریکایی Overstock می باشد tZERO .قصد دارد تعدادی از ناکارآمدی های بازار های مالی سنتی را از طریق اعمال بلاک چین های خصوصی حل کند. این STO در مجموع مبلغ ۱۳۴ میلیون دلار را جمع آوری کرد و سپس به مدت ۹۰ روز بنا به دلایل قانونی، توکن ها را توقیف کرد و این توقیف توکن در ۱۰ ژانویه ۲۰۱۹ پایان یافت. یکی از طرح های تشویقی برای دارندگان توکن tZEROاین است که دارندگان این توکن هر سه ماه یک بار، ده درصد از درآمد ناخالص تعدیل شده را دریافت می کنند.

STOها یک مزیت کلیدی دارند که آنها را تبدیل به یک مکانیزم نویدبخش برای جذب سرمایه می کند که در آینده کار آفرینان و شرکت ها آن را انتخاب خواهند کرد زیرا در این شیوه در مقایسه با مکانیسم های دیگر، دسترسی به سرمایه افراد سرمایه گذار بسیار آسان تر فراهم می آید. کار آفرینان می توانند تا جایی که قوانین اجازه دهد به صدور توکن هایی بپردازند که ارائه دهنده درصد مالکیت در سرمایه گذاری آنها باشد. تفاوت اصلی بین این فرآیند و تب داغ ICO سال ۲۰۱۷ در این است که توکن های صادر شده در STO ها نمایان گر سهام واقعی از شرکت های مورد نظر می باشند.

اقدامی که اخیرا توسط انتشارات رسانه ای مشهور ارز دیجیتال هکر نون (Hacker Noon) برای جذب سرمایه صورت گرفت، نمونه ای عالی از مدل جذب سرمایه توسط STO است که می توان آن را اعمال کرد. این پروژه در حال حاضر مشغول تکمیل کردن فرآیند جمع آوری سرمایه خود می باشد و در این فرآیند سرمایه گذاران در عوض سرمایه گذاری اوراق بهادار را به صورت توکن Hacker Noon دریافت می کنند. STOها در صدد آزاد کردن فرآیند جمع آوری وجوه مورد نیاز پروژه ها به شیوه ای مطابق قانون می باشند که ICO ها از انجام آن ناکام ماندند. دیجیتال کردن اوراق بهادار مزیت هایی اساسی مانند افزایش نقدینگی و زمان تصفیه سریعتر معاملات را به ارمغان می آورد.

انفجار و ازدیاد ICO ها در سال ۲۰۱۷ در ظهور STO ها نقش مهمی داشت و امکان به وجود آمدن یک اقتصاد توکنی را به همگان آموزش داد STO .ها پتانسیل تحقق کامل چنین دیدگاهی را دارا می باشند.

IEO چیست؟

عرضه اولیه پول توسط صرافی ها (IEO) اخیرا بسیار مورد توجه قرار گرفته است و به نظر می رسد که صرافی های اصلی ارز دیجیتال از پروژه های معینی حمایت می کنند و در حال شکل دادن به یک مدل جمع آوری پول موفق می باشند. این مدل سبب می شود که تلاش های بلاک چین محور، منابع مورد نیاز را دریافت کنند و سودآوری قابل ملاحظه ای نیز برای سرمایه گذاران داشته باشند IEO .منافع زیادی دارد مثلا توسط صرافی که یک منبع مورد اعتماد است، مدیریت می شود. اما وقتی روند جدیدی مانند این مدل جمع آوری سرمایه ظاهر می شود،

امنیت

صرافی های ارز دیجیتال همیشه هدف شیرینی برای هکر ها بوده اند و این قضیه در موقعیت های متعددی برای ما ثابت شده است. در خلال فرآیند های فروش توکن مانند IEO ها، وجوه زیادی در صرافی ذخیره خواهد شد که در مدت زمان نسبتا کوتاهی انتقال داده خواهند شد. این عامل باعث می شود که صرافی هدف نهایی گستره ای از تلاش های مختلف از جمله حملات فیشینگ برای هک باشد.

علاوه بر این، اکثر صرافی های ارز دیجیتال برای نگهداری حجم زیادی از توکن ها طراحی نشده اند. به عبارت دیگر، افرادی که می خواهند واجد شرایط شرکت در IEO باشند، لازم است که توکن بومی صرافی را برای مدت خاصی نگه دارند. مسئله اینجاست که این توکن باید در صرافی نگهداری شود. به عنوان مثال صرافی بایننس (Binance) کاربرانش را تشویق می کند تا ۵۰۰ BNB را که در حال حاضر معادل حدود ۹۰۰۰ دلار است به منظور برخوردار شدن از قرعه کشی های IEO نگهداری کنند. هکر ها این را می دانند و حالا این امر شفاف تر از همیشه برای آنها محرز شده است.

تاثیر بر ارزش توکن

بر خلاف ICO های سنتی که در ۲۰۱۷ و ۲۰۱۸ شکوفا شد، ارزش توکن IEO شدیدا تحت تاثیر توکن صرافی قرار خواهد گرفت زیرا این توکن بومی صرافی تنها ابزار برای شرکت در فروش است. بنابراین نوسانات در قیمت توکن بومی صرافی به طور جدی بر ارزش واقعی توکن فروخته شده در IEO تاثیر خواهد گذاشت. به عنوان مثال KCS که توکن صرافی Kucoin است، به دنبال اولین IEOخود یعنی MultiVAC شدیدا افت کرد.

محدودیت های استفاده

استفاده توکن نیز تا حدودی توسط صرافیی که در آن فروخته می شود، محدود خواهد شد. بسیاری از توکن های مبتنی بر صرافی که در حال حاضر در بازار معامله می شوند در درجه اول برای تخفیف کارمزد فراهم شده اند. توکن های فروخته شده در IEO تا حدود زیادی وابسته به آن صرافی ارز دیجیتال میزبان خواهند بود و این توکن ها کاربرد مهمی به جز حضور در صرافی فراهم نخواهند کرد. بنابراین اگر اتفاق غیر منتظره ای برای صرافی بیافتد، ارزش توکن نیز احتمالا افت خواهد کرد و این قضیه تنها

محدود به هک صرافی ها نیست بلکه تلاش های قانونی را هم شامل می شود که قوانین وضع شده برای صرافی ها قطعا بر این توکن ها هم تاثیر گذار خواهد بود.

صرافی های متمرکز: معاملات ناشناخته و نهنگ ها

تقریبا همه صرافی ها و مخصوصا آنهایی که حجم ترید بالایی دارند، متمرکز هستند. این یعنی همه IEO ها توسط سازمان های متمرکز انجام می شود. بله، این شرکت ها یا صرافی ها کنترل کامل بر پروژه های فروش توکنی دارند که این مدل جمع آوری وجه را انتخاب می کنند. حتی ممکن است چیز هایی ناشناخته و مخفی برای عموم موجود باشد که این فرآیند را تحت تاثیر قرار دهد. علاوه بر متمرکز بودن، صرافی ها نیز می توانند شدیدا ارزش توکن فروخته شده در IEO را تحت تاثیر قرار دهند. در نهایت باید گفت که به نفع صرافی هاست که موفقیت این مدل جدید را اثبات کنند.

مقررات و مسائل قانون گذاری

قانون گذاران بررسی های دقیق و موشکافانه خود را در مورد ICOها افزایش داده اند و این قضیه را که توکن با توجه به مکانیسم صدور خود جز اوراق بهادار است یا نه را نیز مورد بازرسی دقیق قرار می دهند. در این اواخر بود که کمسیون بورس و اوراق بهادار آمریکا (SEC) راهنمایی را بیرون داد و پاره ای از ابهامات را کنار زد.

با این وجود، متمرکز بودن صرافی های ارز دیجیتال بار دیگر خود را نشان می دهد زیرا قطعا قانون گذاران آسان تر می توانند IEO ها را لغو کنند. قانون گذاران صرافی ها را دنبال می کنند و آنها را مجبور به تبعیت از قوانین خود می کنند. این فرآیند نه تنها بر توکن های مورد نظر تاثیر خواهد گذاشت بلکه به طور کلی بر صرافی و هر کسی که از آن استفاده می کند نیز تاثیر خواهد گذاشت.

البته هیچ یک از موارد ذکر شده در این مقاله بدین معنی نیست که IEO اقدام بدی است بلکه در این مقاله تنها تعدادی از مشکلات احتمالی آینده مطرح شده است و براستی این گونه موضوعات ارزش فکر کردن را دارد.

Hardcap و Softcap

Hardcap در ICO به میزان حداکثر سرمایه محتملی اشاره دارد که در مورد یک رمزارز جمع آوری خواهد شد .بیشتر پروژه های رمزنگاری شده در طول مراحل اولیه راه اندازی، محدودیت ها را افزایش می دهند بنابراین هاردکپ های این چنینی به سختی قابل دستیابی خواهند شد. اگرچه وابستگی زیادی به محبوبیت و استقبال از ICO نیز خواهد داشت چنانچه تبلیغات صحیحی صورت بگیرد می تواند به راحتی به اهداف مورد نظر دست پیدا کرد.

Hardcap به حداکثر بودجه ی موردنیاز برای راه اندازی یک کسب و کار خاص اشاره دارد .هنگامی که یک رمزارز به بازار معرفی می شود مقدار هاردکپ یکی از عوامل موثر بر ارزش آتی آن خواهد بود .درکنار هاردکپ می توان مقدار عرضه و تقاضاهای موجود در بازار را برای تخمین قیمت آینده ی یک رمزارز موثر دانست.

Softcap درICO به حداقل مقدار سرمایه ی اضافه شده اشاره دارد که موفقیت یک پروژه را تعیین می کند و به همان اندازه به سرمایه گذاری برای پیشرفت آن کمک خواهد کرد. اغلب پروژه ها به سافت کپ ICO می رسند، زیرا پیشنهاد اولیه ی سکه یا همانICO ها یک راه عالی برای شروع سرمایه گذاری جدید است. اگرچه هرگز تضمینی برای رسیدن به سافت کپ در پروژه ای وجود نخواهد داشت.

- چنانچه یک پروژه به سافت کپ ICO نرسید به طور کامل بسته خواهد شد
- تمام پول ها به سرمایه گذاران برگردانده خواهد شد.

اکثر پروژه ها بدون توجه به اینکه سافت کپ آنها به درستی تنظیم شده یا خیر به کار خود ادامه می دهند. سرمایه گذاران در قبال پروژه های معرفی شده در ICOباید اطمینان پیدا کنندکه مقدار هاردکپ و سافت کپ ها برمبنای اعداد و ارقام و آمارهای واقعی ارائه شده است. بدین منظور و برای جلب اعتماد جامعه ی کاربران نیاز است تا شفافیت های لازم از سوی شرکت ها اعمال شود.

انشعاب FORK چیست

اطلاعات ثبت شده در بلاک چین قابل تغییر نیستند و وقتی یک بلاک چین فعالیت خود را آغاز می‌کند، تا زمانی که کاربران آن را بپذیرند، هیچ کس نمی‌تواند جلوی کار آن را بگیرد. در هر کدام از ارزهای دیجیتال یک سری قوانین که اصطلاحا به آن پروتکل می‌گوییم توسط برنامه نویسان تعیین شده است و یک بلاک چین براساس همان پروتکل و قوانین تا ابد به کار خود ادامه می‌دهد. مثلا برای بیت کوین چنین قوانینی تعریف شده: زمان هر بلاک ۱۰ دقیقه باشد – هر بلاک ۱ مگابایت ظرفیت داشته باشد و...

اما اگر کسی با قوانین بیت کوین یا هر ارز دیجیتال دیگری مخالف بود چه؟ اگر در شبکه یک ارز دیجیتال، یک اتفاق بد رخ دهد چه؟ راه‌حل ساده است. به‌روزرسانی یا ایجاد بلاک چین جدید که اصطلاحا به آن فورک می‌گویند. وقتی گروهی از برنامه نویسان از شرایط و قوانین یک ارز دیجیتال ناراضی باشند یا اینکه شبکه با مشکلاتی مواجه باشد که حل آن ضروری است، راه‌حلی به نام فورک پیش روی این افراد است.

واژه فورک یا انشعاب از پروژه‌های برنامه‌نویسی ریشه گرفته است. در حقیقت با کپی کد منبع یک پروژه و ایجاد تغییراتی در آن، برنامه‌ای جدید از دل برنامه قبلی بیرون می‌آید. از این رو فورک در ارزهای دیجیتال نیز با مفهومی یکسان و با برخی پیچیدگی‌های خود به کار می‌رود.

فورک یا انشعاب معمولاً به‌نوعی، آپدیت یا به روزرسانی یک نرم‌افزار گفته می‌شود که می‌تواند به روشی سازگار با قبل (backward-compatible) و یا ناسازگار با قبل (backward-uncompatible) باشد. به‌طور خلاصه، واژه فورک یا انشعاب فقط یک اصطلاح برای زمانی است که یک نرم‌افزار یا یک پروتکل، آپدیت می‌شود. در حوزه‌ی ارزهای دیجیتال و بلاک چین فورک زمانی اتفاق می‌افتد که شبکه به دو بخش تقسیم شود.

اصلی ترین سناریوهایی که موجب رخ دادن فورک می شود:

- راه‌حلی برای اختلافات فنی : بیت کوین کش یکی از فورک‌های بیت کوین است که به دلیل اختلاف نظرهای گسترده درباره مقیاس‌پذیری بیت کوین انجام شد. گروهی از توسعه دهندگان و ماینرهای بزرگ بیت کوین که از سرعت و کارمزد تراکنش‌ها راضی نبودند، با تغییرات گسترده در قوانین بیت کوین و افزایش سایز بلاک، بلاک چین و نسخه ای جدید از پروتکل را ارائه دادند.
- برای برگشت دادن مبالغ از دست رفته : در سال ۲۰۱۶، فقط یک اتریوم وجود داشت اما بعد از رخ دادن هک DAO و از دست رفتن میلیون‌ها دلار از سرمایه کاربران، جامعه اتریوم مجبور به ارائه فورک شد تا بتواند اعتماد مردم را به دست آورد. اتریوم فورک شد، اکثر جامعه به شبکه جدید نقل مکان کردند. نام اتریوم قبلی به اتریوم کلاسیک تغییر یافت و اتریوم جدید شد همین که اکنون در بازار خرید و فروش می‌شود.
- برای اضافه کردن ویژگی و قابلیت‌های جدید : یک شبکه بلاک چینی در طول زمان نیازمند به‌روزرسانی‌های فنی است تا شبکه را از خطرات پیش رو حفظ نماید. بطور کلی دو نوع انشعاب وجود دارد : Soft fork و Hard fork

انشعاب نرم Soft fork

سافت فورک یک بروزرسانی در نرم افزار بوده که با نسخه‌های قدیمی سازگار (backwards compatible) است. این بدین معناست که شرکت‌کنندگانی که نرم‌افزار خود را آپدیت نکرده باشند نیز می‌توانند در اعتبارسنجی (Validation) و تایید (Verification) تراکنش‌ها شرکت کنند. پیاده‌سازی سافت فورک به نسبت آسان‌تر بوده چراکه تنها نیاز است اکثریت شرکت‌کنندگان نرم‌افزار خود را آپدیت کنند. همه‌ی

شرکت‌کنندگان چه نرم‌افزار خود را آپدیت کرده و چه نکرده باشند، می‌توانند بلاک‌های جدید را تشخیص دهند و فعالیت‌هایشان با شبکه سازگار است. نکته‌ی قابل تامل این است که عملکرد شرکت‌کننده‌ای که نرم‌افزار خود را آپدیت نکرده تحت تاثیر قرار می‌گیرد.

یک مثال برای سافت فورک این است که مثلا سایز بلاک‌ها از ۱ مگابایت به ۸۰۰ کیلوبایت تغییر پیدا کرده است. نودهایی از شبکه که نرم‌افزار خود را آپدیت نکرده‌اند در سافت فورک می‌توانند تراکنش‌های جدید را ببینند. مشکل زمانی به وجود می‌آید که ماینری که نرم‌افزار خود را آپدیت نکرده است، بخواهد بلاک جدیدی را ثبت نماید و بلاک او توسط شبکه رد می‌شود. از این رو سافت فورک یک مکانیزم ارتقاء تدریجی را نشان می‌دهد که افرادی که نرم‌افزار خود را آپدیت نکرده‌اند با محدود شدن قابلیت‌هایشان، انگیزه‌ی کافی برای اینکار را پیدا کنند.

BIP66: یک سافت فورک برای اعتبارسنجی امضای شبکه‌ی بیت کوین بود.

P2Sh: یک سافت فورک برای اضافه کردن قابلیت آدرس‌های چند امضایی بر روی شبکه‌ی بیت کوین بود.

انشعاب سخت Hard fork

هاردفورک مربوط به تغییرات نرم‌افزاری است که که با نسخه‌های قدیمی سازگار نیست .(not backwards compatible) در این فورک تمامی شرکت‌کنندگان باید نرم‌افزار خود را به روزرسانی کنند تا قادر باشند در تایید تراکنش‌ها و اعتبارسنجی آنها شرکت کنند. نودهایی که به روزرسانی را انجام نداده باشند از شبکه جدا شده و نمی‌توانند تراکنش‌های جدید را تایید کنند. این فورک موجب انشعاب دائمی بلاک‌چین می‌شود و تا زمانی که کاربرانی در زنجیره‌ی قدیمی حضور داشته باشند، دو بلاک‌چین به صورت جداگانه و همزمان وجود خواهند داشت.

هاردفورک برنامه‌ریزی شده (Planned Hard Forks)

هاردفورک برنامه‌ریزی شده، یک بروزرسانی در پروتکل است که از ابتدا در نقشه‌ی راه (Roadmap) پروژه در نظر گرفته می‌شود. از آنجایی که این بروزرسانی در راستای قابلیت‌ها و ویژگی‌های بلاک چین می‌باشد، تمامی شرکت‌کنندگان به رهبری توسعه‌دهندگان اصلی به زنجیره‌ی جدید رفته و نرم‌افزار خود را بروزرسانی می‌کنند چراکه این تغییرات در سطح کدنویسی پایه‌ی شبکه صورت می‌پذیرند. در این فورک زنجیره‌ی قبلی از بین می‌رود و دلیلی نیز برای حمایت از آن وجود ندارد. در این فورک، کوین جدیدی به وجود نخواهد آمد.

مثال‌های این نوع هاردفورک فورک:

اتریوم: هاردفورک های موجود در نقشه راه اتریوم از این نوع هستند. به عنوان مثال بیزانس (Byzantium)، فاز اول بروزرسانی مربوط به اتریوم ۲ بود. این فورک در اکتبر ۲۰۱۷ به وقوع پیوسته و هدف آن بهبود مقیاس‌پذیری اتریوم و یکپارچه‌سازی تراکنش‌های خصوصی است.

مونرو : در ژانویه‌ی ۲۰۱۷، هاردفورکی در شبکه‌ی اتریوم جهت اضافه شدن ویژگی جدیدی به نام حلقه‌ی معاملات محرمانه (RCT) برای بهبود حریم خصوصی و امنیت شبکه، به وقوع پیوست.

هاردفورک بحث‌برانگیز (Contentious Hard Forks)

هاردفورک بحث‌برانگیز به علت اختلاف نظر بین اعضای شبکه اتفاق می‌افتد و موجب می‌شود بخشی از شرکت‌کنندگان، زنجیره‌ی جدیدی که از نظر خودشان بهتر است را با تغییرات عمده‌ای در کد ایجاد کنند.

مثال های هارفورک بحث برانگیز:

بیت کوین کش (Bitcoin Cash): هاردفورکی بود که توسط گروهی که می‌خواستند مقیاس‌پذیری بیت کوین را با افزایش سایز بلاک از ۱ مگابایت به ۸ مگابایت افزایش دهند، ترتیب داده شد. این کار باعث شد که شبکه بتواند تراکنش‌های بیشتری را پردازش کند، کارمزد شبکه کاهش پیدا کرده و همچنین تنگنای شبکه‌ی بیت‌کوین با افزایش استفاده از آن بهبود داده شده است. این هاردفورک منجر به پیدایش ارز جدیدی به نام بیت کوین کش گردید.

اتریوم کلاسیک (Ethereum Classic): اتریوم نیز برای خنثی کردن تاثیر هکی که در یکی از برنامه‌های کاربردی‌اش به نام سازمان خودکار غیرمتمرکز (DAO) اتفاق افتاد، دچار هاردفورک شد. توسعه‌دهندگان اصلی اتریوم و اکثریت شرکت‌کنندگان شبکه،با هاردفورک موافقت کردند و تنها تعداد معدودی از مواضع خود کوتاه نیامده و نرم‌افزار خود را آپدیت نکردند که بلاک‌چین آنها به اتریوم کلاسیک (ETC) معروف است.

سکه های مشتق شده (Spin-off Coins)

از آنجایی که پروتکل بیت کوین منبع باز است، هر فردی می‌تواند به کد پایه‌ی آن دسترسی داشته، آن را تغییر دهد و ارز جدیدی را با ویژگی‌های مختلفی به وجود آورد. مثلا لایت کوین (Litecoin)، فورکی از بیت کوین بود که با تغییرات زیر به وجود آمد:

- زمان ایجاد یک بلاک: زمان ساختن یک بلاک در لایت کوین ۵/۲ دقیقه است. این زمان برای بیت کوین نزدیک به ۱۰ دقیقه می‌باشد.
- الگوریتم: لایت کوین از الگوریتم اسکریپت(Scrypt) به جای SHA256 استفاده می‌نماید.
- بیشینه سکه‌های موجود(Max Supply): این رقم برای لایت کوین ۸۴ میلیون بوده در حالی که برای بلاک چین بیت کوین ۲۱ میلیون می‌باشد.

برخی از سکه‌هایی که از بلاک‌چین بیت کوین مشتق شده‌اند:.Namecoin, Peercoin, Litecoin ,Dogecoin ,Auroracoin

انواع ارزهای دیجیتال

ارزهای دیجیتال به چند دسته تقسیم می شوند:

۱- پول‌ها : معروف ترین نوع ارزهای دیجیتال بوده و به ارزهای دیجیتالی مانند بیت کوین اشاره دارد که عمدتا نقش ذخیره ارزش، ابزار معامله، یا واحد پولی را در بازار ایفا می کنند. چیزی شبیه به ارز فیات (دلار، یورو و ...) .بیت کوین به خودی خود به عنوان یک کالا یا روش پرداختی، ارزش ذاتی محدودی دارد، و در عوض مردم به آن ارزش می بخشند.

۲- کاربردپذیرها : ارزهای دیجیتال کاربردپذیر، مفهوم تازه ای را به بازار عرضه می کنند. این دسته از ارزهای دیجیتال یک زیرساخت و بستر را ایجاد می کنند، مثل اتریوم که امکان ساخت قراردادهای هوشمند را برای توسعه دهندگان فراهم کرده است. (قرارداد هوشمند به کدی گفته می شود که به کمک آن تراکنش ها بدون نیاز به وجود فرد واسطه یا شخص ثالث، اجرا می شوند.) پلتفرم این ارز دیجیتال برای اپلیکیشن های غیر متمرکز یک بستر فراهم کرده است. فایل کوین (Filecoin) یک نمونه ارز دیجیتال کاربردپذیر دیگر است. فایل کوین یک شبکه ذخیره سازی غیرمتمرکز را برای توسعه دهندگان به ارمغان آورده است، یک روش جدید برای ذخیره سازی و بازیابی داده ها.

۳- برنامه‌ای یا /پلتفرمی‌ها : به خودی خود یک اپلیکیشن یا پلتفرم نیستند، و در عوض در بستر ارزهای دیجیتال کاربردپذیر مثل اتریوم ایجاد می شوند. برای نمونه ارز دیجیتال Augur، یک بازار پیش بینی غیرمتمرکز مبتنی بر اتریوم است، که کاربران می توانند در آن روی نتایج رویدادها سرمایه گذاری کنند (مثلا نتیجه انتخابات ریاست جمهوری یا یک مسابقه ورزشی)، و در ازای پیش بینی پاسخ صحیح پاداش بگیرند. پروژه ۰x نیز، یک پلتفرم مبتنی بر اتریوم برای ایجاد صرافی های غیر متمرکز از هر نوع است.

گروه (پول ها)

بیت کوین اولین ارز دیجیتال این گروه می باشد، که با مشکلاتی اعم از مقیاس پذیری و پرایوسی مواجه است. از این رو سکه های جدیدی با هدف رفع این مشکلات پا به گروه (پول ها) گذاشته اند.

- مشکل مقیاس پذیری

انجام تراکنش های بیت کوین در شبکه با محدودیت هایی روبروست. سایز بلاک بیت کوین یک مگابایت است، و بدین ترتیب در هر ثانیه قابلیت تایید هفت تراکنش را دارد. استخراج هر بلاک در شبکه میانگین ۱۰ دقیقه زمان می برد؛ بنابرین شبکه قادر به تایید بیشتر از ۳.۳ الی ۷ تراکنش در ثانیه نیست.

مقیاس پذیر بودن، برای یک ارز دیجیتال ویژگی مهمی به شمار می رود. ارزهای دیجیتال باید مقیاس پذیر باشند تا بتوانند در خدمت تبادلات مالی استفاده شوند. با این حال، وجود این ویژگی برای اینکه یک چیز (ذخیره ای از ارزش) باشد، ضرورت ندارد.

فورک های مختلف، در پروتکل اصلی یکسری تغییر به وجود می آورند. فورک به عنوان یک راه حل برای رفع مشکل مقیاس پذیری به شبکه معرفی شده است. ارزهای دیجیتال دیگری هم هستند که با همین هدف ساخته شده اند: مثل لایت کوین litecoin و بیت کوین کش bitcoin cash.

لایت کوین، سعی دارد مشکل مقیاس پذیری بیت کوین را حل کند، هر ۲٫۵ دقیقه تمام تراکنش های تایید شده لایت کوین در بسته های دیجیتالی به نام بلاک قرار می‌گیرند. این بلاک ها به بلاک چین اضافه می‌شوند. برخلاف بیت کوین که فقط ۲۱ میلیون از آن قابل تولید شدن است، لایت کوین تا ۸۴ میلیون واحد استخراج خواهد شد. این تعداد محدود رقابت میان ماینرها و در نتیجه میزان کارمزدها را کاهش می دهد:

در مقابل، بیت‌کوین‌کش انشعاب یا (فورکی) از پروتکل اصلی بیت کوین است و سعی دارد با افزایش سایز بلاک از ۱ به ۸ مگابایت، و خالی کردن فضای اضافه از SegWit یا Segregated Witness (راهی برای جدا کردن امضاهای معامله) مشکل مقیاس پذیری را در آن حل کند.

این فورک بحث و جنجال به پا کرد. زیرا با بزرگتر شدن سایز بلاک، عمل استخراج برای ماینرهای کوچک سخت تر، و قدرت در استخرهای استخراجی بزرگ متمرکز می شود. این تمرکزِ قدرت، ماهیت دیرینه ی بیت کوین یعنی (غیر متمرکز بودن) آن را تضعیف می کند.

- حریم خصوصی

خلق (پرایوسی کوین) یکی از اقدامات مهمی است که در این فضا صورت گرفته. پرایوسی کوین ها عملکرد اقتصادی مشابهی نسبت به بیت کوین دارند: (ذخیره ارزش، ابزار معاملاتی، واحد پولی) ولی در مقایسه با آن از یک لایه پرایوسی (حریم خصوصی) دیگر نیز بهره مند هستند.

آدرس کیف پول های بیت کوین ناشناس هستند، یعنی به یک شخص خاص در دیتابیس پیوند نشده اند. با این حال دارایی ها و تراکنش های هر کیف پول در یک دفتر کل توزیع شده و قابل مشاهده هستند.

از لحاظ قانونی مشخص نیست که آیا به وجود یک لایه پرایوسی دیگر نیاز یا حتی تمایل داریم یا خیر.

عده ای نگران هستند که مبادا پرایوسی کوین ها در خدمت معاملات بازار سیاه باشند. (پیرامون این مسأله بحث وجود دارد: آیا خصوصی سازی به نفع عاملان خبیث در بازار است یا خیر)

چند خط بالاتر گفته شد که دارایی ها و تراکنش های هر کیف پول بیت کوین در یک دفتر کل توزیع شده و قابل مشاهده هستند. مونرو از این جهت با بیت کوین فرق دارد!

در مورد مونرو، نمی توان میزان ثروت ذخیره شده در یک کیف پول خاص را از روی یک دفتر کل توزیع شدهخواند. در عوض، مونرو اطلاعات تراکنش ها را با ایجاد آدرس های موقتی و یکبار مصرف برای انتقال سکه ها، رمزنگاری می کند. با این کار حریم خصوصی فرستنده و گیرنده در تراکنش های مونرو حفظ می شود. با این حساب، امکان انتقال پول به یک آدرس عمومی وجود دارد، اما اطلاعات دارایی ذخیره شده در آن آدرس کاملا محرمانه خواهد بود. در واقع، تراکنش های مونرو به طور پیش فرض، (خصوصی) هستند.

یکی از امکانات دش، انجام معامله به صورت خصوصی است. قابلیت (ارسال به صورت خصوصی) در دش، اطلاعات تراکنش و هویت کیف پول را به حالت در هم ریخته و رمزی در می آورد. سیستم شبکه دش بر خلاف بیت کوین که در همه حال فعالیت آن به ماینرها بستگی دارد، دو ردیفه یا (Two-tier) است. در این معماری دو ردیفه، کارکردهای مربوط به استخراج بلاک جدید در شبکه توسط ماینرها انجام می‌شود و مَسترنودها (Masternodes) مسئول پردازش حالت‌های ارسال خصوصی (Privatesend) و ارسال فوری (Instantsend) و همچنین کارکردهای نظارتی هستند.

با استناد به توضیحات ویکی پدیا، مسترنودها برای جلوگیری از حملات سایبری Sybil، باید ۱۰۰۰ دش را وثیقه بگذارند. در ضمن این وثیقه را می توان در هر زمان استفاده و خرج کرد، اما مسترنودی که این کار را انجام بدهد، از شبکه حذف می شود. از آنجایی که عملکرد مسترنود در شبکه حیاتی است، پاداش بلاک میان ماینرها و مسترنودها تقسیم شده و به هر گروه ۴۵ درصد از پاداش استخراج بلاک پرداخت می شود. البته ۱۰ درصد از هر پاداش به عنوان بودجه در خزانه توسعه دش ذخیره می شود.

زی کش، از یک سیستم اثبات دانش صفر تحت عنوان zk-snark استفاده می کند. پرداخت های زی کش در یک بلاک چین عمومی ذخیره شده اند، اما این امکان برای کاربران وجود دارد که مشخصات فرستنده، گیرنده، و مبلغ ارسال شده را مخفی نگه دارند.

به نقل از ویکی پدیا؛ در زی کش امکان (افشای انتخابی) برای معامله‌گران خصوصی وجود دارد که کاربر می تواند برای اهداف حسابرسی از آن استفاده نماید. یک از دلایل وجود چنین قابلیتی در زی کش این است: معامله‌گران بتوانند تراکنش های خصوصی را با مقررات ضد پولشویی یا مالیات مطابقت دهند.

گروه (کاربردپذیرها)

معروف ترین ارزهای دیجیتالی که در این گروه دسته بندی می شوند، اتریوم و فایل کوین هستند. بنابر توضیحاتی که در Ethereum documentation قید شده است، اتریوم یک پلتفرم غیر متمرکز است که قراردادهای هوشمند به عنوان نوعی اپلیکیشن در بستر آن اجرا می شوند. این اپلیکیشن ها به برنامه ای که برای آنها نوشته شده، پایبند هستند، یعنی بدون هیچ گونه از کار افتادگی، سانسور، تقلب، یا دخالت شخص ثالثی اجرا شده و در شبکه کار خود را انجام می دهند.

فعالیت قراردادهای هوشمند در بستر یک بلاک چین سفارشی ساز صورت می گیرد. این بلاک چین، یک زیرساخت جهانی، توزیع شده و قدرتمند است که انتقال و جابجایی ارزش را ممکن ساخته، و حق مالکیت دارایی را به نمایش می گذارد. این موضوع به توسعه دهندگان اجازه ایجاد بازار، ثبت بدهی و وعده ها، انتقال سرمایه طبق دستورات قبلی (مثل یک وصیت نامه یا قرارداد آتی)، و کارهای بسیار دیگری را می دهد که هنوز اختراع نشده اند؛ تمام این کارها بدون ریسک مرد میانی یا شخص واسطه، ممکن است. از طرف دیگر، فایل کوین یک فضای ذخیره دیجیتال متکی بر بلاک چین است. فایل کوین روش بازیابی اطلاعاتی است که از طریق یک سیستم کریپتوکارنسی و پرداختی، اجرا و تشویق می شود.

فایل کوین همانطور که در گزارش اولیه آن ذکر شده، یک شبکه ذخیره سازی غیرمتمرکز است، که فضای ابری را به یک بازار الگوریتمی تبدیل می کند. فعالیت های فایل کوین در بستر یک بلاک چین و با استفاده از توکن با پروتکل بومی (به نام فایل کوین)، صورت می گیرد. برای استخراج فایل کوین، احتیاجی به صرف قدرت محاسباتی بسیار زیادی نیست و تنها لازم است که ماینرها داده های کاربران را در شبکه ذخیره کنند. به بیانی دیگر، کاربران به ماینرها فایل کوین پرداخت می کنند، تا داده هایشان در شبکه توزیع یا ذخیره شود. ماینرهای فایل کوین هم مثل ماینرهای بیت کوین، بر سر استخراج بلاک جدید و دریافت پاداش با یکدیگر رقابت دارند. اما قدرت استخراج فایل کوین با ذخیره سازی فعال در شبکه -که خدمات مفیدی را به کاربران عرضه می کند- متناسب است. (برعکس استخراج بیت کوین که کاربرد آن منحصرا حفظ اجماع در بلاک چین است). این موضوع ماینرها را به ذخیره هر چه بیشتر داده ها، تشویق کرده و انگیزه آنها را برای ادامه کار بالا می برد.

گروه (برنامه‌ای یا پلتفرمی‌ها)

پروژه های جالب بسیاری بر بستر ارزهای دیجیتال کاربردپذیر مثل اتریوم متولد شده اند. دو نمونه از این پروژه های امیدوارکننده Augur و ۰x هستند. در آینده زیرساخت های کاربردپذیر پیشرفت کرده و با پذیرش گسترده (گروه پول ها) در میان کاربران، مدل های تجاری جدیدی روی کار خواهند آمد. از این جهت، در سال های آتی شاهد توسعه برنامه های این چنینی و تولد پروژه های بیشتر در این زمینه خواهیم بود.

همانطور که در گزارش اولیه Augur آمده، آگِر یک پیشگوی غیرمتمرکز، بی نیاز از اصل اعتمادسازی و در واقع پلتفرمی برای بازارهای پیش بینی است. دارندگان توکن های REP، نتیجه این بازارها را مشخص می کنند. آن ها توکن های خود را در نتیجه ای که فکر می کنند درست است، سرمایه گذاری می کنند و در آخر، اگر نتیجه آن رویداد را درست پیش بینی کرده باشند، برنده می شود و پاداش می گیرند.

ساختار انگیزشی آگِر (Augur)، صحت و صداقت گزارشات را تضمین می کند. یعنی در سیستم آگِر نتیجه یک اتفاق از یک منبع خاص گزارش نمی شود، بلکه توسط گروه بزرگی از دارندگان توکن REP اعلام شده، و بسیار دقیق تر و صادقانه تر از جوابی است که از یک نفر پرسیده شود. دارندگان این توکن ها می توانند به مراتب سهم بزرگتری را در سیستم پیش بینی بگذارند. در صورتی که ارزش هر سهم در پلتفرم به حد مشخصی برسد، برای هر یک از نتایج احتمالی در بازار پیش بینی یک اعتبار تعیین می شود. بدین ترتیب هر یک از شرکت کنندگان می تواند با پرداخت توکن REP، نتیجه مورد نظر خود را انتخاب کند.

گزینه های دور از واقعیت بی ارزش هستند، افراد همواره بین بازارهای پیش بینی گزینه ای را انتخاب می کنند که نتیجه آن از همه بهتر و مطمئن تر است. بنابرین، دارندگان توکن REP پیوسته بر روی نتیجه ای سرمایه گذاری می کنند که می دانند همواره ارزشمند است: یعنی، نتیجه ای که چندان بعید و دور از نتیجه واقعی آن اتفاق نیست.

در گزارش اولیه ۰x نوشته شده است که پروتکل آزاد و بدون محدودیت آن، انتقال همتا به همتای توکن های ERC20 را در بلاک چین اتریوم تسهیل می بخشد. پروتکل ۰x به عنوان یک استاندارد باز و یک واحد سازنده، اپلیکیشن های غیرمتمرکز (dApps) که قابلیت جابجایی و انتقال در آنها وجود دارد را تعامل پذیرمی کند.

معاملات در بستر اتریوم و از طریق یک سیستم قراردادهای هوشمند انجام می شوند. این سیستم به طور عمومی قابل دسترس است، استفاده از آن رایگان است، و تمام dAppها می توانند با آن ارتباط برقرار کنند. اپلیکیشن های غیرمتمرکزی که با تکیه بر پروتکل ۰x ایجاد شده اند، به استخرهای نقدینگی عمومی دسترسی داشته و امکان خلق نقدینگی و تعیین کارمزد بر اساس حجم نهایی برایشان وجود دارد. پروتکل ۰x به کاربران خود هزینه ای را تحمیل نمی کند، یا خودسرانه و به نفع چند کاربر، از بقیه پول نمی گیرد. بروزرسانی ها با مدیریت غیر متمرکزی که ۰x دارد، به طور مداوم و ایمن در بستر این پروتکل اعمال می شوند؛ بدون آنکه خللی در کار dApps یا کاربران نهایی ایجاد شود.

AirDrop

Trading

صرافی Exchange

صرافی‌های ارز دیجیتال مکانی مجازی برای خرید و فروش ارزهای دیجیتال هستند. نرخ و قیمت یک ارز دیجیتال توسط همین عرضه و تقاضا در صرافی‌ها به دست می‌آید. بدیهی‌ست هر چقدر تقاضای خرید یک ارز بیشتر باشد، قیمت آن نیز افزایش می‌یابد و بالعکس. البته عوامل مصنوعی دیگری هم می‌تواند در قیمت‌ها تاثیرگذار باشد.

صرافی‌های ارز دیجیتال می‌توانند از نظر امکانات و عملکرد با یکدیگر متفاوت باشند. در اکثر موارد، صرافی‌های ارز دیجیتال واسطه‌ای برای خریداران و فروشندگان هستند. عملکرد آن‌ها به این گونه است که صرافی وظیفه بهم‌رسانی سفارشات خرید و فروش بین کاربران را انجام می‌دهد و از هر معامله انجام شده کمیسیون دریافت می‌کند. این نوع صرافی‌ها برای ارزهای پشتیبانی شده در سایتشان، کیف پول قرار می‌دهند تا کاربر بتواند ارزهای دیجیتال مختلف را به صرافی وارد یا آن را برای معاملات بعدی ذخیره کند.

نوع دیگر صرافی ارز دیجیتال وجود دارد که کاربران با مالکان سایت خرید و فروش می‌کنند. این صرافی‌ها اغلب محلی هستند و به کاربران کشور یا منطقه خاصی سرویس می‌دهند.

ارزهای دیجیتال بصورت جفت ارز مبادله و قیمت گذاری می شوند. یک تعداد ارز پایه وجود دارد که ارزهای دیگر بر پایه آنها خرید و فروش می شوند مثلا BTC/ADA که قیمت توکن کاردانو را بر اساس قیمت بیت کوین نمایش می دهد نوع دیگر معاملات خرید و فروش و قیمت گذاری بر حسب ارزهای فیات مانند دلار است که در این صورت یک طرف معامله ارز فیات خواهد بود برای مثال قیمت هر بیت کوین ۴۰۸۹ دلار است که برای خرید این ارز ۴۰۸۹ دلار باید پرداخت و در ازای فروش آن کمی کمتر از ۴۰۸۹ دلار با توجه به کارمزد آن صرافی بدست خواهد آمد.

به دلیل اینکه صرافی‌های ارز دیجیتال به طور جداگانه فعالیت دارند، نسبت به عرضه و تقاضا و خرید و فروش‌های انجام شده در هر صرافی قیمت متفاوت است و قیمت‌های جهانی از برایند قیمت‌های مختلف در صرافی‌ها به دست می‌آیند. البته تفاوت قیمت در صرافی‌ها بسیار ناچیز است زیرا در صورت وجود یک اختلاف قیمت بالا، معامله گران زیادی برای کسب سود به آن صرافی حجوم خواهند برد و دوباره قیمت متعادل می‌شود.

همانطور که در بالا اشاره کردیم، در هر صرافی، قیمت بیت کوین و ارزهای دیجیتال نسبت به حجم معاملات و عرضه و تقاضا محاسبه می‌گردد. این بدان معنی است که هر چه یک صرافی بزرگتر باشد، قیمت مناسب و واقعی تری نسبت به قیمت جهانی به دست می‌آید. برای بیت کوین و سایر ارزهای دیجیتال مشابه با آن قیمت ثابت معنایی ندارد و در هر لحظه می‌تواند تغییر کند.

صرافی متمرکز

صرافی غیر متمرکز

آربیتراژ Arbitrage چیست؟

به کسب سود از طریق اختلاف قیمت در دو بازار مختلف آربیتراژ می‌گویند. این اختلاف می‌تواند از لحاظ زمانی باشد مثل بازار نقد و آتی، و هم از نظر مکانی مثل تفاوت نرخ در دو بازار در مکان‌های جغرافیایی متفاوت باشد. یکپارچگی بازارهای مالی امکان آربیتراژ به علت اختلاف در مکان بازار را تقریبا به صفر رسانده است.

آربیتراژ به صورت آکادمیک به مجموعه تراکنش های مالی اطلاق می شود که در هیچ حالتی باعث زیان نشده و حداقل در یک حالت باعث سود شود به عبارتی آربیتراژ به طور ایدآل یک معامله بدون ریسک (Risk Free) است. این نوع آربیتراژ در بازارهای کالایی به علت وجود هزینه نگهداری و حمل و نقل و... که باعث ایجاد قیمت‌های متفاوت برای یک کالا می‌شود، اتفاق می‌افتد. اما اختلاف به علت تفاوت در زمان، فرصت آربیتراژی را برای هم بازارهای مالی و کالایی از طریق قرارداد آتی ایجاد می‌کند. آربیتراژ در بازار آتی سهام زمانی اتفاق می‌افتد که فرد با حذف ریسک نوسانات قیمت در طول زمان سهم پایه را در یک بازار (نقد و آتی) خریده و در بازار دیگر به فروش برساند .اگر قیمت‌های بازار آتی بالاتر از نقد باشد: آربیتراژگر می‌تواند سهم پایه را در بازار نقد خریده و به طور همزمان در بازار آتی با قیمت مشخص به فروش برساند.

آربیتراژ به زبان ساده یعنی شما کالایی را از جایی به قیمت ارزان‌تر بخرید و در جای دیگر همان کالا را با همان کیفیت بفروشید. یا این‌که کالایی را در بازار خریداری کنید و آن را در بازار برای تحویل در آینده به فروش برسانید. مثلاً طلا را در بازار تهران خریداری کنید و تعهد بدهید که آن طلا را در روز یا ماه‌های آتی به قیمت مشخص به فروش برسانید. مثلاً ۳۰ گرم طلا را از قرار هر گرم ۱۳۰ هزار تومان در بازار تهران خریداری کنید و به فرد یا افرادی تعهد بدهید که ۳۰ گرم طلا را از قرار ۱۴۰ هزار تومان در هر گرم برای یک روز یا حتی چند ماه آینده تحویل دهید. این اتفاق در داخل ایران عمدتاً در بازار آتی سکه می‌افتد.

سود آربیتراژی به سه دسته تقسیم می‌شود:

- آربیتراژ ساده (Simple arbitrage): زمانی که ارزهای دیجیتال در بیشتر از یک صرافی مبادله بشوند، آربیتراژ رخ می‌دهد. زیرا امکان خرید و فروش یک ارز دیجیتال در چند صرافی وجود خواهد داشت.
- آربیتراژ مثلثی (Triangular arbitrage): آربیتراژ مثلثی در نتیجه یک اختلاف قیمت بین سه ارز خارجی شکل می‌گیرد. یعنی زمانی که نرخ مبادله ارزها دقیقا با یکدیگر برابر نیستند. فرصت‌های آربیتراژ مثلثی انگشت شمارند و خیلی رایج نیستند. در آربیتراژ مثلثی، معامله گرها سه ارز را انتخاب می‌کنند (مثلا بیت کوین، دلار و یورو)، مقداری از جفت ارزی (بیت کوین/ دلار) را با یک نرخ مشخص مبادله و سپس جفت ارز را جابجا می‌کنند (بیت کوین/ یورو). در نهایت آن را به ارز پایه تغییر می‌دهند (دلار/ یورو)، و با پرداخت اندکی کارمزد برای انجام این تبادلات، به یک میزان سود خالص دست پیدا می‌کنند. مثلاً یک معامله گر با یورو اتریوم می‌خرد، آن را در ازای دریافت ین می‌فروشد و در نهایت با ین دریافتی یورو خریداری می‌کند. او از راه مبادله این سه ارز به سود آربیتراژی دست می‌یابد.
- آربیتراژ پوشش نرخ بهره (Price convergence arbitrage): قیمت ارزهای دیجیتال در بازارهای مختلف، در نتیجه آربیتراژ به سمت همگرایی می‌رود. برای نمونه، اگر صرافی کراکن اتریوم را ارزان‌تر از صرافی بیت استمپ بفروشد، مسلما آن دسته از معامله گرهایی که طرفدار سود آربیتراژی هستند، از کراکن خرید می‌کنند، و اتریوم‌های خریداری شده را در بیت استمپ می‌فروشند. در بسیاری از موارد تحت تاثیر این همگرایی، بازار به سمت برابری قیمت‌ها سوق داده می‌شود. در اینجا سود معامله گر از همگرایی قیمت‌ها حاصل می‌شود.

در آربیتراژ چه ریسک‌هایی معامله را تهدید می‌کند؟

- ریسک اجرایی (Execution Risk)

به طور حتم، امکان بستن دو یا چند معامله به طور همزمان وجود ندارد. زمانی که بخشی از یک معامله بسته شود، حرکت سریع قیمت‌ها در بازار، بستن معامله دیگر در یک قیمت سودآور را غیر ممکن می‌کنند.

علاوه بر آن، اگر یک معامله گر تصمیم بگیرد از اختلاف قیمت بیت کوین در دو صرافی ارز دیجیتال کراکن و بیت استمپ سود آربیتراژی به دست بیاورد، شاید بلافاصله به هدف خود نرسد. ممکن است او برای این کار از صرافی کراکن مقدار قابل توجهی بیت کوین بخرد، اما در بیت استمپ موفق به فروش آن‌ها نشود.

- ریسک طرف مقابل (Counterparty Risk)

ریسک طرف مقابل به ریسک آربیتراژی گفته می‌شود که در آن یک طرف نمی‌تواند وظایف خود را نسبت به طرف مقابل خود در قرارداد انجام بدهد. این یک مشکل جدی است! زیرا اگر فردی با آن شخص یک معامله یا چند معامله داشته باشد و او در انجام وظایف خود شکست بخورد، یک بحران مالی برای طرف مقابل خود به وجود می‌آورد. شکست یکی از طرفین قرارداد، یک تهدید جدی به شمار می‌رود. زیرا طرفین باید برای اینکه از تفاوت‌های قیمتی کوچک سود ببرند، مقادیر قابل توجهی را معامله کنند.

برای اینکه یک معامله گر بتواند استراتژی آربیتراژ خود را پیاده کند، باید سکه‌هایش را در صرافی نگه دارد. یک قانون اصلی و مهم در حفظ امنیت دارایی دیجیتال این است: دارایی دیجیتال خود را از صرافی خارج کنید. این نکته بارها تکرار شده است، اگر سرمایه‌تان را در صرافی نگه می‌دارید باید بدانید که در هر لحظه امکان هک شدن صرافی و از دست رفتن سرمایه‌تان وجود دارد.

شاید یک راه حل برای این مشکل وجود داشته باشد: استفاده از صرافی های غیر متمرکز. اما اگر از زاویه آربیتراژ به صرافی های غیر متمرکز نگاه کنیم متوجه می‌شویم که نقدشوندگی هنوز در آن ها پایین است.

- ریسک نقدشوندگی (Liquidity Risk)

این ریسک مالی زمانی پیش می‌آید که یک معامله گر نتواند دارایی خاصی مثل ارز دیجیتال را به اندازه کافی سریع و بدون تحت تاثیر قرار دادن قیمت بازار مبادله کند.

برای اجرای استراتژی آربیتراژ، باید از بابت نقدشوندگی بازار اطمینان حاصل کنید. اگر بازار نقدینگی نداشته باشد، ممکن است هنگام کسب سود آربیتراژی از فرصت موجود ضرر کنید.

- ریسک انتقال دارایی (Asset Transfer Risk)

انتقال دارایی از یک صرافی به صرافی دیگر به منظور کسب سود آربیتراژی، بدون ریسک نیست. زمانی که متوجه فرصت آربیتراژ می‌شوید، لازم است دارایی‌هایی که از یک صرافی خریده‌اید را به صرافی دیگری منتقل کنید. دلایل زیادی وجود دارد که می‌تواند این انتقال را به وقفه انداخته و به نوعی آن را با مشکل مواجه کند. این کاستی منجر به از دست رفتن فرصت آربیتراژ می‌شود.

کاربران مشکلات مختلفی را هنگام انتقال وجه از صرافی به صرافی دیگر گزارش کرده‌اند.

۱. ممکن است بلاک چین از دسترس خارج بشود و انتقال دارایی موفقیت آمیز نباشد.
۲. ممکن است انجام تراکنش چند روز طول بکشد. تراکنش هایی که کارمزد پایین تری بابت تایید آن ها پرداخت می شود، در اولویت کار ماینرها قرار ندارند.
۳. ممکن است کیف پول ها از دسترس خارج بشوند، و قادر به همگام سازی با بلاک چین نباشند.

- ریسک کاهش بها (Risk of depreciation)

کاهش قیمت ارز دیجیتال یک ریسک به حساب می‌آید. برای مثال، اگر شما از راه ترید ارز دیجیتال سود آربیتراژی کسب کنید و بعد قیمت بیت کوین شروع کند به پایین آمدن، بازار چیزی بیشتر از سود شما را خواهد بلعید!

نکاتی که در این نوع آربیتراژ وجود دارد، استفاده از ربات‌های تریدر برای این منظور است؛ چرا که تمامی سفارشات باید در کسری از ثانیه صورت گیرد و علاوه بر آن میزان وجود کارمزد نیز در سودمند بودن یا نبودن معاملات دخیل شود. در این صورت ربات با تصمیم‌گیری درست می‌تواند معامله و سود بی‌دردسری به دست آورد. این نوع آربتراژ در صرافی‌های با کارمزد مانند بایننس کمتر اتفاق می‌افتد، چرا که کارمزد هر سفارش معمولاً بیشتر از فرصت آربیتراژ به وجود آمده می‌شود و امکان انجام این عمل از بین می‌رود.

نمونه ساده ای از آربیتراژ بیت کوین

قیمت بیت کوین در کوین بیس حدود ۶۵۰ دلار و قیمت بیت کوین در اکسچنج BTC-E حدود ۶۳۶ دلار است. تفاوت بین این دو قیمت ۱۴ دلار می‌باشد و این امر تقریبا فرصت مناسبی برای آربیتراژ است. در نظر بگیرید که شما ۱۰۰ بیت کوین از BTC-E خریده اید که هر یک با نرخ ۶۳۶ دلار می‌باشد. شما هر یک از آنها را در کوین بیس با نرخ ۶۵۰ دلار می‌فروشید و برای هر بیت کوین ۱۴ دلار سود بدست می‌آورید.

بنابراین می‌توان دید که با آربیتراژ بیت کوین فرصت مناسبی برای ایجاد درآمد انفعالی خواهید داشت، اما این کار با موانع و محدودیت هایی مواجه است.

موانع آربیتراژ بیت کوین

۱. زمان لازم برای تأیید هر تراکنش (خرید و فروش) ممکن است افزایش یابد و نرخ اکسچنج در آن زمان تغییر کند.
۲. بسیاری از اکسچنج ها برای معامله تعداد زیادی بیت کوین به تاییدیه های بسیاری نیاز دارند.
۳. واریز ارز فیات می‌تواند فرایند زمان بری باشد (بسته به روش پرداختی شما ممکن است تا ۱۰ روز طول بکشد).
۴. بسیاری از اکسچنج ها کارمزد دارند که در مثال بالا آن را در نظر نگرفتیم. شما باید این هزینه را در نظر داشته باشید.
۵. به حجم تراکنش در هر اکسچنج توجه کنید زیرا ممکن است شما نتوانید تمام بیت کوینی که از اکسچنج ارزانتر خریده اید را بفروشید.
۶. تفاوت قیمت به اعتبار و شهرت اکسچنج نیز برمی‌گردد. به عنوان مثال این روزها نرخ اکسچنج BTC-E پایین می‌باشد زیرا مردم اعتماد ندارند که این اکسچنج به طور صحیح پول های آنها را مدیریت و نگهداری می‌کند. اعتماد کمتر = خریدار کمتر= نرخ پایین اکسچنج. چنین اتفاقی چند روز پیش برای اکسچنج Mt.Gox افتاد و قیمت بیت کوین در این اکسچنج کمتر و کمتر می‌شد زیرا مردم به اکسچنج اعتماد نداشتند و اجازه برداشت پول را نمی‌دادند.

کارمزدهای آربیتراژ بیت کوین

حال بیایید که مثال ملموسی بزنیم و تمام کارمزدهای متفاوت دخیل در آربیتراژ را در نظر بگیریم. این کارمزدها شامل موارد زیر می باشد:

- کارمزدهای واریز فیات
- کارمزدهای برداشت فیات
- کارمزدهای واریز بیت کوین
- کارمزدهای برداشت بیت کوین

- کارمزدهای تراکنش

تمام این اقدامات بیان می‌کنند که آربیتراژ بیت کوین عملی کاملا دشوار است. اگر کمی با اعداد سروکار داشته باشید متوجه خواهید شد که اگر پراکندگی (اختلاف بین ارزش خرید و ارزش فروش) به مقدار کم افزایش یابد به سودآوری می‌رسید. اما در وضعیت کنونی با انجام این فرآیند پول از دست می‌دهید .هرچند اگر بیشتر دقت کنید متوجه خواهید شد که ۱۰ روز طول می‌کشد تا اکسچنج BTC-E واریز شما را دریافت کند. طی این مدت پراکندگی می‌تواند تغییر کند. بنابراین بهترین روش، نگهداری مقداری ارز فیات در اکسچنج و انتخاب زمان مناسب برای اجرای آربیتراژ خواهد بود.

آیا باید آربیتراژ بیت کوین را امتحان کنیم؟

اگر بیت کوین یا پول اضافی دارید، پس خودتان دست به کار شوید. مادامی که محتاط هستید و قوانین محکمی در خصوص چه زمان و چگونه انجام دادن این اقدام مشخص می‌کنید، در این فرآیند حضور خواهید داشت. بر خلاف سرمایه‌گذاری با ریسک، معاملات مارجین و سایر فعالیت هایی که می‌توان به آن ها به عنوان روش‌های دستکاری در بازار نگاه کرد، آربیتراژ فرآیندی مثبت است.

قیمت بیت کوین در اکسچنج های مختلف نباید فرق داشته باشد، مخصوصا با توجه به اینکه دسترسی به تمام اکسچنج ها از یک رایانه امکان پذیر است. آربیتراژ اکسچنج ها را به یک قیمت میانگینی می‌رساند. با رشد بازار بیت کوین، شکاف بین اکسچنج ها کاهش خواهد یافت زیرا میزان آربیتراژ افراد افزایش می‌یابد. حجم کنونی بیت کوین می‌تواند به افراد کمک کند که به سود خوبی دست یابند اما هنوز برای شرکت های بزرگ مالی ارزش ندارد که مستقیما وارد آربیتراژ بیت کوین شوند.

آربیتراژ بیت کوین در کل می‌تواند فرصتی برای درآمدزایی باشد اما در عین حال خطرات خود را دارد. به علاوه، تقریبا تمام اکسچنج ها API دارند و این نکته می‌تواند باعث موفقیت شما شود. استفاده از این API ها به شما ابزار مورد نیاز برای ایجاد یک ربات آربیتراژ یا استخدام فرد دیگر برای انجام این کار را خواهد داد. تا هنگامی که دقیق تر بررسی کنید و اطمینان حاصل کنید که معاملات همزمان انجام می‌دهید، اقدام به آربیتراژ می‌تواند بسیار سودمند باشد .نظر بسیاری از افراد این است که اگر بخواهید سود خوبی از آربیتراژ کسب کنید باید در این حوزه حرفه ای باشید. احتمالا در اولین یا دومین اقدام خود نخواهید توانست آربیتراژ موفقی انجام دهید. مانند هر عمل دیگری، آربیتراژ نیز به تمرین، صبر و تجربه نیاز دارد.

Leverage در معاملات Bitcoin

Leverage به معنای استفاده از سرمایه‌ای است که از یک کارگزاری به عنوان وام گرفته شده است .گاهی اوقات سرمایه گذاران از Leverageبه عنوان یک استراتژی در سرمایه گذاری خود استفاده می کنند .که بتوانند به وسیله آن با کمترین میزان سرمایه بیشترین سود را به دست آورند .چند ضلع سرمایه گذاری مانند ۲ ...x, 5xبرای این فرایند در نظر گرفته شده است .از Leverage در خرید (بلند مدت) و فروش (کوتاه مدت) استفاده می شود .علاوه بر این‌ها از Leverage در معاملات سهام، ارزهای دیجیتال، ETFS، کالا و شاخص‌ها نیز استفاده می شود .هر کدام از این معاملات دارای مقررات و محدودیت‌هایی هستند.

Leverage در معاملات بیت کوین

یکی از موارد جذاب در ترید کردن بیت کوین استفاده از Leverage است .فرایند ذکر شده این امکان را به تریدکنندگان می دهد که با سرمایه‌های کم، سرمایه گذاری‌های بزرگی را انجام دهند .در این زمینه، بخش تجاری معاملات بیت کوین بسیار شبیه به بخش تجارت جهانی

فارکس است که هر دو گزینه‌های مشابهی را برای تریدکنندگان ارائه می دهند .درواقع، Leverageیک نوع اهرم در انجام معاملات است . فارکس، بازار جهانی ارزهای خارجی برای تجارت غیرمتمرکز و غیرمستقیم آن‌ها است .این بازار نرخ جهانی ارزها را تعیین می کند .به عنوان مثال فارکس Leverage 50:1 را برای انجام معاملات در نظر گرفته است این بدین معنی است که یک سرمایه گذار توانایی انجام یک سرمایه گذاری به ارزش ۵۰ برابری سرمایه واقعی خود دارد .زمانی استفاده از این فرایند بازده بالایی خواهد داشت که در موارد ضرر نیز از آن استفاده شود.

به دلیل نوسانات قیمت ارز بیت کوین، استفاده از Leverage بسیار ریسک بالایی خواهد داشت. همانطور که می دانید تریدکنندگان روزانه، سرمایه گذاران جدی نیستند. در طول سال‌های اخیر قیمت بیت کوین نوسانات بسیار شدیدی داشته و گاهی اوقات از کمترین قیمت به بیشترین قیمت رسیده است یا برعکس. بنابراین سرمایه گذاران در این شرایط حاضر به سرمایه گذاری‌های بلند مدت نیستند زیرا احتمال نابودی سرمایه شان وجود دارد. این شرایط برای ترید کنندگان روزانه مناسب است.

در یک دوره زمانی این تریدکنندگان از Leverage در معاملات خود استفاده کردند و به جای تمرکز بر روی بازده برگشت بر روی مدیریت خطرات کوتاه مدت تمرکز کردند. بعد از مدتی متوجه شدند که نوسانات قیمت رمزارز بیت کوین بر روی Leverage تاثیر می گذارد و باعث ضرر به آن‌ها می شود. در ۱۴ تا ۱۸ ماه آگوست سال ۲۰۱۴ میلادی، قیمت بیت کوین در هر معامله تقریبا ۱۰۰ دلار کاهش قیمت پیدا کرد که این رویداد به عنوان رویداد flash crash شناخته شده است. بسیاری از کارشناسان دلیل سقوط قیمت بیت کوین را تجارت حاشیه‌ای margin tradingدانستند.

تجارت حاشیه‌ای بخشی از سیستم Leverage است. بسیاری از تریدکنندگان با سرمایه کم می توانند تجارت حاشیه‌ای با استفاده از این فرایند انجام دهند که بدون نیاز به سرمایه زیاد می توانند سرمایه خود را به طور فزاینده‌ای افزایش دهند. تجارت حاشیه ای بسیار ریسک پذیر است و انجام آن به همه توصیه نمی شود. برای مثال تجارت حاشیه‌ای Leverage 2x به این معنی است که به جای افزایش ۱۰٪ دارایی، ۲۰٪ افزایش می یابد. اما تجارت‌های استاندارد با Leverage 1x انجام می شوند.

در حالی که تجارت با این فرایند بسیار سودمند بوده در عین حال نیز ممکن است زیان‌های زیادی را به دنبال داشته باشد. ترید کنندگان زمانی که متوجه ضرر شدند باید دست از ادامه معامله بردارند و سود خود را مبنی بر نرخ یا پولی که سرمایه گذاری کرده‌اند، بگیرند.

کارگزاری‌های Leverage در معاملات بیت کوین

Whale Club : کارگزاری آنلاینی است که به تریدکنندگان اجازه ترید با Leverage 40:1 را می دهد. علاوه بر این، این امکان را به تریدکنندگان می دهد که دارایی‌هایی مانند Blue Chip و ارزهای دیگر را با استفاده از بیت کوین به عنوان ارز اصلی با هزینه‌های معاملاتی صفر، ترید کنند.

1Broker : کارگزاری بیت کوین فارکس و پلتفرم CFD است که هدف آن اتصال بیت کوین به بازارهای جهانی است. همچنین سهام ارزهای دیگر را با استفاده از بیت کوین به عنوان ارزپایه، به فروش می رساند.

eToro : پلتفرم معاملاتی تجاری پیشرو در بازار است. این کارگزاری به کاربران خود اجازه‌ی تعیین قیمت برای ارز بیت کوین را می دهد.

IG Group : کارگزاری آنلاینی در بریتانیا است. همچنین یک پلترم معاملاتی CFD است. اخیرا نیز بیت کوین را به عنوان دارایی به معاملات خود اضافه کرده است.

Plus 500 : کارکزاری آنلاینی در انگلستان بوده و دارای پلتفرم CFD است و امکان تجارت با Leverage 10:1 را به تریدکنندگان می دهد. علاوه بر این کارگزاری‌ها، کارگزاری‌های دیگری مانند فارکس و BitMEX نیز امکان ترید با این فرایند در معاملات بیت کوین را می دهد.

some of CRYPTOCURRENCY

امنیت ارزهای دیجیتال

آیا ممکن است که آدرس کیف پول دیجیتالی دو کاربر مختلف، یکی باشد؟

سوالی که برای اکثر کاربران و افرادِ دنیای ارزهای دیجیتال وجود دارد، این است که آیا این احتمال وجود دارد که آدرسِ کیف پولِ کاربری با آدرس کاربر دیگر، یکی باشد!؟؟ برای پاسخ به این سوال، به مثالِ کیف پول دیجیتالی MyEtherWallet توجه کنید :اولین نکته‌ی مهمی که باید به آن اشاره کرد، این موضوع است که کیف پول دیجیتالی "MEW " هیچ کلید خصوصی و یا آدرسِ عمومی‌ای ایجاد نمی کند MEW ! یا هر کیف پول دیجیتالی دیگر (برای ذخیره‌ی رمزارز اتریوم) به صورت تصادفی، برای کاربرانی که کیف پول دیجیتالی جدیدی ایجاد می کنند؛

یک جفت آدرس عمومی و کلید خصوصی تولید می کند. هر آدرس رمزارز اتریوم با '۰x' شروع شده و به وسیله‌ی ۴۰ کاراکتر هگزادسیمال (برای مجموعا ۴۲ کاراکتر) دنبال می شود. کاراکترهای هگزادسیمال (Hexadecimal characters) می توانند کاراکترهایی بین محدودهای 'a – f' و '۹ – ۰' باشند. این بدین معنی است که حدود ۱۶^۴۰ آدرسِ احتمالی رمزارز اتریوم وجود دارد که این میزان، همان ۲^۱۶۰ است!! به عبارت دیگر، حدود ۱,۴۶۱,۵۰۱,۶۳۷,۳۳۰,۹۰۲,۹۱۸,۲۰۳,۶۸۴,۸۳۲,۷۱۶,۲۸۳,۰۱۹,۶۵۵,۹۳۲,۵۴۲,۹۷۶ آدرسِ احتمالی برای انتخاب وجود دارد!!!

با این شرایط، کلیدها برداشت (انتخاب) نمی شوند!

علتِ تصافی بودنِ این فرآیند، بسیار سخت وپیچیده می باشد زیرا مغز ما توانایی درک آن را ندارد! هیچ کدام یک از ما، با انتخاب‌هایی که می کنیم، توانایی رسیدن به آمارهای تصادفی واقعی را نداریم! این نکته را در نظر بگیرید که، اگر کاربری کلید خصوصی‌ای برای خود انتخاب کند، تنها توانایی دسترسی به کیف پول دیجیتالی را دارد (به وسیله‌ی انتخابی که کرده است). با این وجود، اگر شخصِ دیگری نیز همان کلید خصوصی را انتخاب کند، این به این معنی است که به تمام اطلاعات و سرمایه‌ی کاربر اول، دسترسی خواهد داشت! بنابراین، این خود ما هستیم که به وسیله‌ی تکنولوژی‌ها، چنین آدرس‌هایی (پیچیده و غیرقابل درک) تولید و ایجاد می کنیم (برای ایجادِ آنتروپی واقعی).

با تمام این تفاسیر، به این نتیجه گیری می توان رسید که اگر در هر ثانیه، حدودِ 1.6 10^31 x بار، آدرس عمومی، برای کاربران ارزهای دیجیتال ایجاد شود این میزان، تنها نیمی از آدرس‌های احتمالی ایجاد شده در زمانِ مشخص شده، خواهد بود! به عبارت دیگر، در هر ثانیه، حدود ۱۶ nonillion (عدد یک با ۵۴ صفر) آدرس عمومی تولید می شود که این عدد فقط نیمی از آدرس‌های احتمالی است که ایجاد می شوند. بنابراین، احتمالِ یکی بودنِ آدرس‌های عمومی کیف پول‌های دیجیتالی، "صفر" خواهد بود.

با اطمینان کامل می توان گفت که اگر از تکنولوژی بلاک چین، هزاران سال نیز استفاده شود، شانس و احتمالِ دریافتِ یک " آدرس کیف پول تکراری " عملا صفر خواهد بود!!!

کامپیوترهای کوانتومی؛ تهدید بزرگی برای بلاک چین و ارزهای دیجیتال !

با وجود اینکه شبکه‌های بلاک چین طراحی شده‌اند تا ایمن و تغییرناپذیر باشند، مقاله پژوهشی جدیدی که توسط دانشگاه کرنل (Cornell) منتشر شده، نشان می‌دهد که این شبکه‌ها در مقابل حمله رایانه‌های کوانتومی قدرتمند، آسیب‌پذیرند. بر اساس مقاله‌ای که در ۲۱ نوامبر توسط وب‌سایت گیزمودو منتشر شده است، نگرانی روزافزونی در رابطه با توسعه رایانه‌های کوانتومی وجود دارد که در نهایت می‌توانند رمزنگاری کلیدهای عمومی و کدهایی که شبکه بلاک چین را پایدار نگه داشته است، در هم بشکنند.

رایانه های کوانتومی چگونه عمل می کنند؟

اساس کار رایانه‌های کوانتومی با رایانه‌هایی که ما امروزه در حال استفاده از آنها هستیم، متفاوت است. در محاسبات کوانتومی، ذرات زیراتمی می‌توانند در آن واحد، بیش از یک حالت را به خود بگیرند. این رفتار خاص ذرات باعث می‌شود که انجام عملیات مختلف و حل مسائل و وظایف پیچیده با رایانه‌های کوانتومی، به‌صورت قابل‌توجهی سریع‌تر از رایانه‌های معمولی باشد.

در رایانه‌های معمولی، هر بیت فقط می‌تواند یکی از دو حالت ۰ یا ۱ را به خود بگیرد. اما رایانه‌های کوانتومی، به جای بیت از کیوبیت‌ها (qubit) استفاده می‌کنند که قادرند بیش از دو حالت را به خود بگیرند. برخلاف بیت‌های سنتی که در رایانه‌های معمولی به‌کار می‌روند، کیوبیت‌ها می‌توانند مقادیر بسیار بیشتری از ۰ و ۱ را در خود ذخیره کنند زیرا به‌عنوان ترکیبی از همه احتمالات موجود، قادرند که در چینش‌های مختلفی جای بگیرند. داشتن توانایی پردازش عملیات جدید، امکان حل عملیات پیچیده‌ای مانند ایجاد هوش مصنوعی پیشرفته، مدل‌سازی واکنش‌های شیمیایی و حتی شکستن قفل ایجاد شده توسط رمزنگاری در کلیدهای عمومی را فراهم می‌سازد.

در حالی که به‌نظر می‌رسد محاسبات کوانتومی راه درازی در پیش دارند، وب‌سایت Nature با انتشار مقاله‌ای در ماه مارس ۲۰۱۷ اعلام کرد که گوگل، این غول موتور جستجوی اینترنتی تصمیم دارد تا ۵ سال آینده، فناوری کوانتوم را تجاری‌سازی نماید که البته میزان احتمال دستیابی گوگل به این هدف، هنوز مشخص نیست. با این حال، نگرانی‌هایی در مورد رشد سریع محاسبات کوانتومی وجود دارد که اگر به همین منوال ادامه یابد، فناوری بلاک چین را در معرض خطر بزرگی قرار خواهد داد زیرا رایانه‌های کوانتومی در نهایت قادر خواهند بود تا کدهای بلاک چین را درهم بشکنند.

(الکساندر لووفسکی) فیزیک‌دان تجربی دانشگاه آکسفورد، در این‌باره گفت: رایانه‌های کوانتومی، همه سیستم‌هایی که از (رمزنگاری کلید عمومی) بهره می‌گیرند را در معرض خطر قرار می‌دهند.

وی افزود: به دلیل اینکه سیستم‌های بلاک چین کاملاً ناشناس هستند، از این رو در معرض خطر ویژه‌ای قرار دارند. این سیستم‌ها تنها از طریق رمزنگاری کلید عمومی محافظت می‌شوند در حالی‌که سیستم بانکداری مجهز به تحویل‌داران انسانی، کارت‌های پلاستیکی عابر بانک‌ها و خودپردازها هستند. حضور فیزیکی افراد یکی از ملزومات استفاده از خدمات بانکی می‌باشد اما در مورد بلاک چین، این‌گونه نیست.

شبکه‌های بلاک چین چگونه در معرض خطر قرار می‌گیرند؟

زمانی که در مورد داده‌های شبکه‌های این چنینی سخن می‌گوییم، باید در نظر داشته باشیم که داده‌ها، گرایش به رمزنگاری یک‌طرفه دارند. تابع یک‌طرفه عملکردی است که در آن، دو ورودی به‌راحتی باهم ترکیب می‌شوند اما معکوس کردن این عملیات و حل کردن آن، کار بسیار دشواری است. یک مثال عالی برای درک این مفهوم، ضرب اعداد اول بزرگ به یکدیگر است. در حالی که رایانه‌ها به راحتی می‌توانند اعداد اول بزرگ را در یکدیگر ضرب کنند، عکس این عمل یعنی حدس زدن اعداد اول ضرب شده در یکدیگر بر اساس حاصل‌ضرب، بدون در اختیار داشتن اطلاعات کافی، عملیاتی چالش‌برانگیز برای رایانه خواهد بود.

این توابع رمزنگاری‌شده استاندارد، به‌صورت اعجاب‌انگیزی امن هستند زیرا شکستن آنها مستلزم در اختیار داشتن میزان قابل‌توجهی از منابع محاسباتی می‌باشد که به‌صورت کلی در دسترس نیستند.

فناوری بلاک چین برای ایجاد امضاهای دیجیتالی بر روی دفتر کل که جعلشان بسیار دشوار است به این توابع رمزنگاری‌شده استاندارد وابسته هستند. متأسفانه، شبکه‌های بلاک چین تنها متکی بر این امضاها هستند زیرا هیچ‌گونه نظارت انسانی برای تقویت سیستم دفاعی این شبکه‌ها وجود ندارد. با وجود اینکه توابع یک طرفه با در نظر گرفتن تکنولوژی عصر حاضر، بسیار ایمن هستند اما رایانه‌های کوانتومی احتمالاً این توابع یک طرفه را درهم شکسته و شبکه‌های بلاک چین را بسیار آسیب‌پذیر خواهند کرد.

اگر رایانه‌های کوانتومی به‌دست متخلفان و خرابکاران بیفتند، قادر خواهند بود تا از الگوریتم شُر (Shor) برای جعل امضای دیجیتالی و هویت کاربر استفاده کرده و دارایی دیجیتال قربانیان را به سرقت ببرند. و به دلیل اینکه امضای دیجیتال، تنها راه محافظت کاربران از اطلاعاتشان بوده، از این رو توابع یک طرفه تنها خط دفاعی شبکه است. بر اساس استدلال انجام شده توسط وب‌سایت Nature با توسعه محاسبات کوانتومی، زیرساخت‌های مالی موجود مانند بانک‌ها لایه‌های امنیتی مطمئن‌تری برای کاربران خود خواهند داشت زیرا نظارت و بررسی‌های انسانی مانند احراز هویت، کارت‌های پلاستیکی خودپردازها، سوالات امنیتی و صندوق‌داران انسانی در این فرآیند دخیل هستند. با این حال، تخمین میزان تهدید از سوی رایانه‌های کوانتومی و توانایی آنها برای سرنگونی فناوری بلاک چین، آسان نیست. محاسبات کوانتومی در مقایسه با رایانه‌های سنتی که در حال حاضر از آنها استفاده می‌کنیم، هنوز در طی مراحل اولیه خود است. به هر حال کسب آمادگی لازم برای رویارویی با این پدیده، بسیار مهم است. گرچه شاید با آن دسته از رایانه‌های کوانتومی که قادر به شکستن رمزنگاری یک طرفه باشند، چندین دهه فاصله داشته باشیم اما نگرانی‌هایی وجود دارد که در این صورت، محاسبات کوانتومی با سرعتی بیش از حد انتظار رشد خواهند کرد.

(نیک فرینا) مدیرعامل شرکت سخت‌افزاری کوانتوم EeroQ که استارت‌آپی در زمینه محاسبات کوانتومی می‌باشد، در این خصوص اظهار داشت: درست همانند سخت‌افزارهای کوانتوم امروزی که هنوز به بلوغ نرسیده‌اند، الگوریتم‌هایی که بتوانند رمزنگاری را در کوتاه‌مدت تهدید کنند نیز به بلوغ نرسیده‌اند. اما به‌سرعت در حال پیشرفت هستند.

وی افزود: راه‌حل این است که وحشت‌زده نشویم اما باید توسعه جوانب محاسبات کوانتومی را با دقت تحت نظر قرار داده و زودتر از چیزی که شما برنامه‌ریزی کرده‌اید، نگاهی نیز به امنیت (پساکوانتومی) داشته باشیم.

امکان شروع زودهنگام

(رابرت سوتور) نائب رئیس تیم تحقیقاتی شرکت آی.بی.ام (IBM) که مسئول برنامه تحقیقاتی کوانتومی این شرکت است، تأیید کرد که هم‌اکنون برای شروع بررسی اقدامات امنیتی موردنیاز در مقابل محاسبات کوانتومی، زود نیست. وی خاطرنشان کرد که تقریباً همه فعالان حاضر در عرصه علوم، تحقیقات و فناوری بر این باورند که بررسی نسل بعدی پروتکل‌های رمزنگاری، امری ضروری است زیرا این فرآیند بایستی به روش استانداردی برای حفاظت از اطلاعات همه سازمان‌ها و عملیات امنیتی سایبری تبدیل شود.

برای کوتاه‌مدت، هم‌اکنون دانشمندان در حال توسعه الگوریتم‌های امنیتی پساکوانتومی هستند. حل این الگوریتم‌های یک طرفه، برای رایانه‌های سنتی و کوانتومی، دشوار خواهد بود. با این حال، گیزمودو معتقد است که پیشرفت تکنولوژی کوانتوم از اینترنت گرفته تا پردازنده‌ها، می‌تواند منجر به ارائه فناوری‌های رمزگشایی جدیدی شود. با این حال، لووفسکی با سوتور هم‌عقیده بوده و خاطرنشان کرد که با وجود اینکه هنوز فرصت باقی است، اما بایستی اقدامات لازم را زودتر شروع کنیم. وب‌سایت technologyreview.com یک گام فراتر نهاده و اشاره کرده است که دانشمندان بسیاری پیشنهاد داده‌اند که رمزنگاری کوانتومی برای تضمین امنیت بلاک چین، به آن افزوده شود. با این حال، (دل راجان) و (مت ویسر) از دانشگاه ویکتوریای نیوزیلند معتقدند که افزودن یک لایه کوانتومی به پروتکل استاندارد بلاک چین، محافظت کافی را برای آن فراهم نخواهد کرد. در عوض، آنها بر این باورند که ساخت بلاک چین جدید بر پایه پدیده کوانتوم، می‌تواند بهترین رویکرد برای توسعه آن باشد.

داستان هک صرافی Mt.Gox

در اوایل سال ۲۰۱۴، صرافی ژاپنی Mt.Gox بزرگ‌ترین صرافی بیت کوین در جهان به شمار می‌رفت و کنترل بیش از ۷۰ درصد از معاملات بیت کوین جهان را در دست داشت. در اواخر فوریه (اسفند) همان سال، این صرافی ورشکسته شد.

صرافی بیت کوین MT.Gox قربانی یک هک بزرگ بود و حدود ۷۴۰٬۰۰۰ بیت کوین (۶٪ بیت کوین‌های موجود آن زمان) را از دست داد که ارزشش در آن موقع، معادل ۴۶۰ میلیون یورو و در اکتبر ۲۰۱۷ معادل ۳ میلیارد دلار بود. به‌علاوه، ۲۷ میلیون دلار نیز از حساب‌های بانکی این شرکت دزدیده شد. با اینکه ۲۰۰٬۰۰۰ بیت کوین دزدیده‌شده بازیابی شدند، اما ۶۵۰٬۰۰۰ بیت کوین دیگر هرگز پیدا نشدند.

پیدایش صرافی Mt.Gox

این صرافی در سال ۲۰۱۰ توسط یک برنامه‌نویس آمریکایی به نام جد مک کلاب (Jed McCaleb) که کمی بعدریپل را پایه‌گذاری کرد، شروع به کار نمود. یک توسعه‌دهنده‌ی فرانسوی و یکی از علاقه‌مندان به بیت کوین به نام مارک کارپلس (Mark Karpelés) در مارس ۲۰۱۱، MT.Gox را خرید. این صرافی به‌سرعت رشد کرده و به محبوب‌ترین صرافی بیت کوین در جهان تبدیل شد. همچنین، جالب است بدانید که Mt.Gox با نام کامل Magic The Gathering Online Exchange نیز شناخته می‌شود.

در ژوئن ۲۰۱۱ این صرافی هک شد. به نظر می‌رسد این اتفاق، به علت وجود آسیب‌پذیری در کامپیوتر یکی از حسابداران شرکت به وجود آمد. در این حادثه، هکر با دسترسی به صرافی، ارزش اسمی بیت کوین را به‌طور مصنوعی تا ۱ سنت کاهش داد و حدود ۲۰۰۰ بیت کوین را از حساب‌های کاربران صرافی بالا کشید و آنها را فروخت. علاوه بر آن، حدود ۶۵۰ بیت کوینی که توسط مشتریان Mt.Gox به علت کاهش مصنوعی قیمت خریداری شد، هیچ یک بازگردانده نشدند. درنتیجه این هک، صرافی Mt.Gox تصمیم به اتخاذ چند معیار امنیتی جدید گرفت که شامل ذخیره‌ی مقدار قابل‌توجهی از بیت کوین‌های خود به صورت آفلاین و در کیف‌پول‌های سرد بود.

علی‌رغم هک Mt.Gox در ژوئن ۲۰۱۱، این صرافی موفق به کسب عنوان بزرگ‌ترین صرافی بیت کوین جهان در سال ۲۰۱۳ شد. این موضوع موجب علاقه‌مندی افراد به بیت کوین به‌عنوان یک ارز ارزشمند و افزایش قیمت آن شد. (از ۱۳ دلار در ژانویه ۲۰۱۳ به بیش از ۱۲۰۰ دلار رسید)

کشمکش‌های پشت پرده

با وجود اینکه Mt.Gox به‌سرعت توانست در سال ۲۰۱۳ به لقب بزرگ‌ترین صرافی بیت کوین جهان دست یابد، اما در پشت پرده همچنان تنش‌هایی در جریان بود. از زمان فروپاشی و هک قبلی این صرافی، بعضی از کارمندان این شرکت راجع به اینکه این صرافی چطور کار می‌کند؛ با ایجاد تصویری از یک سازمان بی‌نظم و متضاد، بهره‌گیری از روش‌های امنیتی ضعیف، وجود مشکلات جدی در سورس کد سایت صرافی و چندین مشکل در حال رشد دیگر که عملیات تجاری شرکت را تحت تأثیر قرار می‌داد، سبب تخریب چهره‌ی صرافی شدند.

در تاریخ ۵ می ۲۰۱۳، یکی از شرکای تجاری Mt.Gox به نام کوین لب (Coinlab) با ادعای نقض قرارداد، Mt.Gox را به پرداخت غرامت ۷۵ میلیون دلاری محکوم کرد. این دو شرکت توافق‌نامه‌ای را امضا کردند که تحت آن، ارائه سرویس به مشتریان آمریکایی Mt.Gox بر عهده شرکت کوین لب قرار می‌گرفت. اما با توجه به طرح دعوی مطرح شده توسط شرکت کوین لب، این معامله به دلیل زیر پا گذاشتن یک بند از قرارداد توسط صرافی Mt. Gox نقض شده بود.

به‌علاوه، طبق بررسی‌های انجام شده توسط آژانس امنیت ملی ایالات‌متحده، یکی از شرکت‌های آمریکایی تابع Mt.Gox، بدون داشتن مجوز و به‌عنوان یک شرکت انتقال پول ثبت نشده در حال فعالیت بود. بنابراین با ادامه این تحقیقات، مبلغ ۵ میلیون دلار از حساب بانکی این شرکت توسط دولت آمریکا کشف و ضبط شد.

درنتیجه تحقیقات دولت آمریکا، صرافی Mt.Gox اعلام کرد که به‌طور موقت اقدام به تعلیق قابلیت برداشت دلار از حساب کاربری مشتریان خود خواهد کرد. پس از این اتفاق، در حالی که اکثر منابع رسمی، مدت تعلیق در برداشت از حساب‌ها را تنها یک ماه عنوان کرده بودند، بسیاری از کاربران تا ۳ ماه نمی‌توانستند پول خود را از این صرافی برداشت کنند و تنها برخی از برداشت‌های دلاری از حساب‌ها موفقیت آمیز

بود. مجموع این تاخیرها در ارائه خدمات سبب کاهش مقام Mt.Gox به‌عنوان بزرگ‌ترین صرافی بیت کوین جهان به رتبه‌ی سوم تا پایان سال ۲۰۱۳ شد. با این حال، آن‌طور که پیداست موارد ذکر شده تنها بخش کوچکی از مسائل آنان را تشکیل می‌دادند و در زیرپوشش این شرکت، Mt. Gox مشکلاتی بسیار بزرگ‌تر از تصور خود داشته است. به نظر می‌رسد که این صرافی برای بیش از دو سال قربانی یک هک دنباله‌دار بوده است.

هک بزرگ Mt.Gox

در تاریخ ۷ فوریه ۲۰۱۴، Mt.Gox تمام درخواست‌ها و قابلیت برداشت بیت کوین را صرفاً با ادعای بازنگری فنی و بررسی دقیق فرایند این ارز، متوقف کرد. درنهایت و پس از چند هفته بلاتکلیفی، در ۲۴ فوریه ۲۰۱۴ این صرافی تمام معاملات را مسدود کرده و وب‌سایت این شرکت از دسترس خارج شد. در همان هفته و به‌واسطه‌ی یک سند درز کرده از شرکت مشخص شد که هکرها با حمله به این صرافی، تعداد ۷۴۴٬۴۰۸ بیت کوین متعلق به مشتریان Mt.Gox به‌علاوه ۱۰۰٬۰۰۰ بیت کوین متعلق به خود صرافی را به سرقت برده‌اند که درنتیجه این اتفاق، شرکت اعلام ورشکستگی کرده است. در ادامه نیز این صرافی در در تاریخ ۲۸ فوریه و ۱۲ مارس در ژاپن و آمریکا به‌طور رسمی اعلام ورشکستگی کرد.

تحقیقات بعدی در رابطه با هک بزرگ Mt.Gox نشان داد که اولین حملات ناشی از این هک بسیار قبل‌تر و از سپتامبر ۲۰۱۱ آغاز شده بود. بنابراین، پیداست که این صرافی در حالی به فعالیت خود ادامه داده است که از دو سال پیش‌تر ورشکسته بوده و عملاً تمام بیت کوین‌هایش را تا میانه‌سال ۲۰۱۳ از دست داده است. به‌علاوه، شواهد و مدارک نشان دادند Mt.Gox بیش از ۸۰٬۰۰۰ بیت کوین را نیز پیش از خرید آن توسط Mark Karpelés در ۲۰۱۱ از دست داده است.

اگرچه با ادامه تحقیقات، حقیقت همچنان در هاله‌ای از ابهام قرار دارد اما بر طبق یک فرضیه، اکثر بیت کوین‌ها از کیف پول‌های آنلاین (یا کیف پول گرم) این صرافی به سرقت رفته‌اند که شامل ارزهایی که به‌واسطه‌ی نفوذ در کیف پول آنلاین از کیف پول های سرد دزدیده شده نیز می‌شوند. کیف پول های آنلاین،کیف پول های مبتنی بر وب هستند که برای ذخیره‌ی کدهای دیجیتالی ایمن استفاده می‌شوند. این کدها که کلید خصوصی (Private Key) نام دارند، برای اثبات مالکیت کلید عمومی (Public Key) یا کدهای دیجیتالی عمومی مورد استفاده قرار می‌گیرند و در صورت تأیید مالکیت می‌توان از آن‌ها برای دسترسی به آدرس ارز و اطلاعات مربوط به آن در کیف پول استفاده کرد. تا پیش از سپتامبر ۲۰۱۱، کلیدهای خصوصی Mt. Gox به دلیل عدم رمزگذاری به‌راحتی قابل‌مشاهده بودند که توسط یک هکر و یا شاید یکی از کارمندان داخلی شرکت در قالب یک فایل Wallet.dat دزدیده شدند.

پس از هک شدن این فایل، هکر(ها) به‌تدریج و به‌واسطه‌ی کلیدهای خصوصی Mt.Gox توانستند بدون شناسایی شدن هک به بیت کوین‌های رمزنگاری شده در حساب‌های مرتبط با این شرکت دست یابند. ظاهراً، از آنجایی که سپرده‌های این شرکت به‌واسطه‌ی سیستم تفسیر نقل و انتقالات در حال ارجاع به یک آدرس ایمن‌تر بودند، این صرافی نسبت به استفاده مجدد کلیدواژه مشترک موجود در فایل کپی شده خود که به معنی وقوع یک سرقت است، بی‌توجه بوده. همچنین به علت آنکه بیش از ۴۰٬۰۰۰ بیت کوین به چندین حساب کاربری مختلف فرستاده‌شده بود، سیستم‌های Mt.Gox تنها زمانی می‌توانستند این دزدی را تشخیص دهند که کیف پول شرکت کاملاً خالی شده باشد.

پیامدها

در مارس ۲۰۱۴، Mt.Gox با انتشار گزارشی در سایت خود به یافتن ۲۰۰٬۰۰۰ بیت کوین موجود در کیف پول‌های دیجیتال قدیمی خود که مربوط به استفاده تا پیش از ژوئن ۲۰۱۱ بودند اشاره کرد. این بیت کوین‌ها در حالی برای حفظ اعتماد طلبکاران نگهداری شدند که شرکت همچنان تحت قوانین حفاظت از ورشکستگی قرار داشت.

مارک کارپلس نیز در آگوست ۲۰۱۵ و در ژاپن به جرم تقلب و اختلاس بازداشت شد، در حالی که هیچ‌یک از اتهام‌های وی مستقیماً به موضوع سرقت مرتبط نبودند. او تا ماه جولای ۲۰۱۶ در زندان بود و پس از آزادی به قید وثیقه، درخواست بازنگری نسبت به اتهامات وارد شده به خود را داد که محاکمه وی تا این لحظه همچنان ادامه داشته است. Mt. Gox در حالی تحت حفاظت قوانین مرتبط با ورشکستگی قرار گرفته که تحقیقات در رابطه با این شرکت همچنان ادامه دارد. به‌علاوه، دعوی قضایی Coinlab نیز همچنان ادامه دارد و تا پایان حل این پرونده امکان توزیع حقوق بستانکاران امکان‌پذیر نخواهد بود.

سرانجام پول‌ها چه شد؟

درنتیجه هک Mt.Gox، همچنان ۶۵۰،۰۰۰ بیت کوین بی‌اعتبار وجود دارد. در حال حاضر چندین نظریه مختلف در اینترنت عنوان‌شده که می‌توانند پاسخی برای محل سکه‌های گم شده باشند. برخی از آن‌ها احتمال می‌دهند که ادعای Mt. Gox مبنی بر داشتن این تعداد بیت کوین هرگز واقعی نبوده و آقای Karpelés برای بزرگ‌نمایی در تعداد بیت کوین‌های موجود در این صرافی، اعداد را دست‌کاری کرده است.

با ادای احترام به توانایی هکر در دستیابی به بیت کوین‌های نگهداری شده در کیف‌پول‌های سرد Mt. Gox، نظریه‌های محدودی برای این موضوع عنوان شده است که برخی از آن‌ها از احتمال به خطر انداختن فضای ذخیره‌سازی توسط فردی با دسترسی به سایت صحبت می‌کنند و در نظریه‌ای دیگر گمان می‌شود زمانی که حجم پول کیف پول گرم کاهش پیدا می‌کرد تا سکه‌های کیف‌پول سرد متناوباً به‌عنوان سپرده جدید به سیستم صرافی وارد شوند، به دلیل عدم مسئولیت‌پذیری کارمندان هیچ‌کس از خالی شدن تدریجی حساب توسط هکرها مطلع نمی‌شد.

در جولای ۲۰۱۷، یک فرد روسی به نام الکساندر وینیک (Alexander Vinnik) توسط ایالات‌متحده در یونان و به اتهام شستشوی بیت کوین‌های دزدیده‌شده از Mt.Gox بازداشت شد. به‌علاوه، Vinnik توسط مقامات یونانی به شستشوی ۴ میلیون دلار بیت کوین دیگر نیز متهم شد. گفته می‌شود که این فرد یکی از افراد مرتبط با صرافی BTC-e است که در پول‌شویی بیت کوین‌های به سرقت رفته از Mt.gox نقش داشته و در طی انجام تحقیقات توسط پلیس فدرال آمریکا (FBI) موردحمله قرار گرفته است. سایت BTC-e نیز به‌طور کامل متوقف شد و نام دامنه آن نیز توسط FBI ضبط گردید. این نخستین بار است که ایالات‌متحده یک صرافی خارجی در کشورd دیگر را مصادره می‌کند. پس از بررسی‌های انجام شده توسط تیم Wizsec (یک تیم متشکل از متخصصان امنیتی بیت کوین) مشخص شد که وینیک صاحب کیف پول هایی از بیت کوین‌های انتقال داده شده است که بسیاری از آن‌ها در صرافی BTC-e به فروش رفته بودند.

با وجود ادامه‌ی محاکمه‌ی مارک کارپلس و اتهام وارد شده به Vinnik، به نظر می‌رسد که سرنخ‌های تحقیقات بر روی هک Mt. Gox در نهایت به یکدیگر مرتبط شده‌اند. حتی اگر تمام این اتفاقات بتوانند سبب بازیابی تمام یا بخشی از بیت کوین‌های دزدیده شده شوند بازهم به نظر نمی‌رسد بتوانیم در آینده‌ای نزدیک شاهد جزئیات بیشتری در رابطه با هک صرافی Mt. Gox باشیم.

آیا دوباره اتفاق خواهد افتاد؟

در جواب کوتاه باید گفت، می‌تواند اتفاق بیافتد. در حال حاضر صرافی‌های بیت کوین زیادی وجود دارند که برخی از آن‌ها نسبت به دیگران از اعتبار بیشتری برخوردارند. صرافی‌های محبوبی چون کوین بیس و بایننس در رابطه با عملیات خود نسبتاً شفاف هستند، همچنین ارائه سپرده‌های بیمه‌شده و حمایت مالی سرمایه‌گذاران معتبر نیز از سایر مزیت‌های این صرافی‌ها است. با این حال، این صرافی‌ها در حال تبدیل به اهداف هکرهای خبره‌ای هستند که با پیدا کردن حفره‌های امنیتی خشنود می‌شوند.

به‌علاوه، در حال حاضر تعداد زیادی از صرافی کوچک‌تر وجود دارند که اطلاعات واضحی از نحوه کارکرد آنها وجود ندارد. البته این موضوع به معنی هک شدن این صرافی‌ها و بی‌اعتبار بودن آنان نیست. اما وقتی صحبت از خریدوفروش ارزهای دیجیتال به میان می‌آید، برای آرامش ذهن خودتان هم که شده، از صرافی‌های معتبر در این حوزه استفاده کنید و در صورتی که قصد استفاده از یک صرافی کوچک را دارید، از قانونی بودن آن برای تضمین مبادلات خود اطمینان حاصل کنید.

اگر با مطالب گفته شده، همچنان ترسی در استفاده از این صرافی‌ها ندارید، به‌عنوان آخرین نکته به شما توصیه می‌کنم که هرگز از صرافی‌ها برای ذخیره بیت کوین‌های خود استفاده نکنید.

هفت هک بزرگ تاریخ ارزهای دیجیتال

تا به امروز هک‌های بسیاری را در رابطه ارزهای دیجیتالی دیده‌ایم. در ادامه قصد داریم تا به هفت مورد از بزرگ‌ترین هک‌های تاریخ ارزهای دیجیتالی اشاره‌کنیم و آنها را در ابعاد مختلف مورد برسی قرار دهیم؛ هک‌هایی که دنیای ارزهای دیجیتالی را لرزاندند و بازار را تا سر حد نابودی پیش بردند. در این مقاله قصد بر ترساندن شما نداریم و تنها می‌خواهیم دلایل به وقوع پیوستن این اتفاقات را برای شما عنوان کنیم، با ارز دیجیتال همراه باشید.

هک Mt.Gox

در سال ۲۰۱۳ (مکس کارپلس) در صدر تمام اخبار دنیا قرار داشت. شرکت او در ژاپن بانام Mt.Gox (Magic The Gathering Online Exchange) با اختلاف بسیار نسبت به رقبا، بزرگ‌ترین صرافی بیت کوین در تمام دنیا بود به‌طوری‌که بیشتر از هفتاد درصد معاملات بیت کوین در دنیا از طریق این صرافی صورت می‌پذیرفت. اوضاع برای کارپلس به بهترین شکل پیش می‌رفت و قرار بود تا ایده‌های جالبی همچون (کافه بیت کوین) نیز توسط این شرکت به اجرا دربیاید؛ اما اوضاع در زیر پوسته این شرکت بسیار شکننده بود.

مشکل Mt.Gox

قبل از هک سال ۲۰۱۴ نیز مشکلاتی گریبان آنها را گرفته بود که به دلیل مدیریت ضعیف، فرصت پیگیری آنها پیش نیامد. اتفاقات فاجعه‌بار بسیاری در شرف به وقوع پیوستن بود. یک شرکت که در توکیو کار می‌کرد، به دنبال فرصتی برای کار کردن با Mt.Gox بود که با دیدن اوضاع آنها وحشت شده شد.

مشکل شماره یک: نبود VCS

اول از همه باید گفت که VCS یا (نرم‌افزار کنترل نسخه)، یکی از لازمه‌هایی است که هر شرکت مرتبط با توسعه نرم‌افزارها باید از آن به دلایل بی‌شماری استفاده کند.

یک VCS به شما این امکان را می‌دهد که تمام تغییرات را در یک کدبیس ردیابی کنید. با استفاده از این قابلیت نه تنها می‌توانید مشاهده کنید که در چه زمانی چه تغییراتی در یک کد خاص اتفاق افتاده، بلکه به شما این امکان داده می‌شود که بفهمید چه کسی این تغییرات را انجام داده است. VSC همچنین امکان برگرداندن تغییرات را نیز به شما می‌دهد.

یکی دیگر از فواید VCS، استفاده همزمان چندین کاربر از یک کد خاص بدون وارد شدن نگرانی به توسعه‌دهنده‌ها یا برنامه‌نویس‌ها بابت همپوشانی کدهایی است که در یک زمان‌بر روی آن کار می‌کنند.

این قابلیت برای شرکتی همچون Mt.Gox بسیار سودمند است چرا که همیشه چندین برنامه‌نویس بر روی یک کد خاص کار می‌کردند.

مشکل شماره دو: فقدان یک سازوکار آزمایش‌کننده

اطلاعات هشداردهنده دیگری نیز به این توسعه‌دهنده نرم‌افزار رسیده بود؛ فقدان سازوکاری آزمایش‌کننده که تا همین چند وقت اخیر نیز در این شرکت به‌کار گرفته نشده بود. کمی فکر کنید، بزرگ‌ترین صرافی بیت کوین در دنیا چنین سازوکاری را نداشته! درواقع آنها کدهای تست نشده را در اختیار کاربران قرار می‌دادند! اوضاع بدتر از اینها هم خواهد شد!

مشکل شماره سه: همه‌چیز در انتها به یک جا ختم می‌شد

بعدها مشخص شد که در Mt.Gox همه اطلاعات درنهایت باید از یک گذرگاه خاص عبور می‌کردند. تمام تغییرات در کدها باید به‌وسیله شخص مدیرعامل تأیید می‌شدند. کارپلس آخرین مرحله و نقطه پایان تمام سیستم بود که تمام ناشی از مدیریت بد می‌شد. مدیرعامل شرکت هیچ‌گاه نباید همه اطلاعات را از یک کانال خاص عبور می‌داد، این همان کاری بود که انجام گرفت!

مشکل شماره چهار: فقدان مدیریت مناسب

اگر بخواهیم در یک کلام تمام مشکلات بالا را جمع‌بندی کمی تنها یک عبارت به ذهنمان خواهد رسید. مدیریت بد و بچگانه. (آندریاس آنتونوپولوس) در نقدی می‌نویسید:

Mt.Gox یک ریسک سیستماتیک برای بیت کوین است، تله‌ای مرگ‌بار برای تبادل کنندگان و کسب‌وکاری که توسط یک آدم بی‌تجربه اداره می‌شود.

کلماتی رک و تلخ اما کاملاً درست و واقعی. مسئله اینجاست که کارپلس بیشتر یک برنامه‌نویس ایده آل بود تا یک مدیر. در همان زمان که مشغول کد نویسی بود، نمی‌توانست هوش لازم برای مدیریت شرکت را داشته باشد، و متأسفانه به همین دلیل فاجعه بزرگی در شرف وقوع بود؛ اما هیچ‌کس از آمدنش خبر نداشت.

هک سال ۲۰۱۱: نشانه‌ای از اتفاقاتی که قرار است بیافتند.

نهم ژوئن سال ۲۰۱۱، اتفاق عجیبی افتاد. ارزش بیت کوین در Mt.Gox به یک سنت رسید!

در میان دقیقاً چه اتفاقی افتاد که منجر به کاهش قیمت شد؟

مهاجم، با هک کردن و ورود به رایانه تنظیم‌کننده Mt.Gox و استفاده از آن برای انتقال مقدار قابل‌توجهی بیت کوین به‌حساب خود استفاده نمود. آنها به استفاده از یک نرم‌افزار تبدیل تمام بیت کوین‌ها را فروختند و باعث ایجاد کرنش‌هایی در سیستم شدند که درنتیجه آن قیمت بیت کوین با افت شدیدی مواجه شد.

باوجود اینکه قیمت بیت کوین بعد از چند دقیقه دوباره به حالت عادی برگشت اما آسیب‌ها خیلی قبل‌تر به سیستم زده‌شده بودند. تمام حساب‌های کاربری با موجودی بالای هشت میلیون و هفت‌صد پنجاه‌هزار دلار صدمه‌دیده بودند. Mt.Gox به دنبال ترمیم صدمات حاصل از این فاجعه بود ولی هیچ کاری برای فاجعه‌ای که در شرف وقوع قرار داشت، کارساز نبود.

هک سال ۲۰۱۴: دزدی ۴۷۳ میلیون دلاری

در سال ۲۰۱۴، همه از تأخیر در خدمات Mt.Gox شکایت داشتند. درواقع این مسئله از چوب لای چرخ گذاشتن‌های سیستم بانکداری آمریکا به‌منظور مشکلات آئین‌نامه‌ای برای این شرکت ناشی می‌شد. در تاریخ هفتم فوریه ۲۰۱۴، شرکت تمام فرایندهای فروش بیت کوین را به‌منظور بازنگری‌های فنی و فهمیدن منشأ مشکلات و تأخیرها، متوقف کرد. این شرکت با انتشار بیانیه‌ای نوشت: مشتری‌های عزیز شرکت

Mtgox در پی تلاش‌های ما در رابطه با مشکل فروش بیت کوین، مشخص شد که این مشکل به دلیل بالا بودن ترافیک فروش مانع از کارهای فنی ما برای اصلاح می‌شود. از همین رو و برای برسی های بهتر سیستم از دسترس خارج خواهد شد. به‌منظور حل مشکل لازم است تا تمام تراکنش‌های مرتبط با فروش متوقف شوند و تمام فرایندهای حال حاضر بازبینی گردند. بابت اطلاع سریع و بدون هماهنگی از شما عذرخواهی می‌کنیم اما تمام فرایندهای فروش بیت کوین متوقف خواهند شد و فروشندگان در صف قرار خواهد گرفت و به‌محض رفع مشکل می‌توانند دوباره اقدام به انجام عملیات‌های خود کنند. تبادلات در پلتفرم طبق روال عادی قابل انجام است. تیم ما طی روزهای آخر هفته کار بر روی مشکل را انجام خواهد داد و در روز یکشنبه به‌روزرسانی‌ای از کارهای انجام‌شده اعلام می‌شود. دوباره بابت مشکلات به وجود آمده عذرخواهی می‌کنیم و کمال تشکر را از صبر و شکیبایی و پشتیبانی‌های شما داریم.

کمال احترام، تیم MtGox

طی برسی ها، آنها دریافتند که در معرض یک حمله ناشی از انعطاف‌پذیری سیستم هستند.

انعطاف‌پذیری تراکنش چیست؟

قبل از اینکه مفهوم آن را بفهمید، باهم به برسی یک کد ساده از تراکنش بیت کوین می‌پردازیم. اگر یک تراکنش بیت کوین را به‌صورت کد دربیاوریم به شکل زیر خواهد بود. فرض کنید آلیس می‌خواهد ۰٫۰۰۱۵ بیت کوین را به باب بفرستد، برای انجام این کار باید مقدار ۰٫۰۰۱۵۷۷ بیت کوین را وارد کندکه همان نام تراکنش یا همان (hash) میزان ورودی و ارزش خروجی است.

Vin_sz میزان داده‌های ورودی است. ازآنجایی‌که آلیس تنها از یکی از تراکنش‌های قبلی خود استفاده می‌کند، عدد واردشده یک است. Vout_sz به این دلیل که تنها خروجی باب است، عدد دو را شامل می‌شود.

این هم داده‌های خروجی است: آلیس تنها از یک تراکنش ورودی استفاده می‌کند، به همین دلیل vin_sz عدد یک است. اولین بخش این داده‌های نشان‌دهنده این است که باب ۰٫۰۰۱۵ بیت کوین دریافت خواهد کرد. بخش دوم نیز نشان می‌دهد آلیس ۰٫۰۰۰۰۵۱۲ بیت کوین را به‌عنوان باقی‌مانده دریافت می‌کند. حالا، به یاد دارید که داده‌های ورودی ۰٫۰۰۱۵۷۷ بیت کوین بود؟ این عدد از (۰٫۰۰۱۵+۰٫۰۰۰۰۱۵۲) بیشتر است. کسر این دو مقدار همان کارمزد تراکنش است که ماینرها آن را برمی‌دارند. این ساختار یک تراکنش ساده بود.

قبل از اینکه بفهمید انعطاف‌پذیری یک تراکنش چیست، نکته دیگری را باید در نظر داشته باشد: بلاک چین به‌منظور تغییرناپذیری ایجادشده است، که از طریق عملکرد Hash به‌دست می‌آید. این موضوع یعنی اگر اطلاعاتی در بلاک چین وارد شود هیچ‌گاه قابل‌تغییر نیستند. از همین رو ارزهای دیجیتالی مبتنی بر بلاک چین امنیت فوق‌العاده بالایی را دارند. در این میان اما، راه گریزی نیز وجود دارد. اگر دست‌کاری اطلاعات پیش از ورود آنها به بلاک چین رخ دهد چطور؟ حتی اگر نسبت به وقوع آنها نیز آگاهی پیدا کنید، بعد از ورود آنها به بلاک چین هیچ راه برگشتی برای آنها وجود نخواهد داشت. این موضوع همان انعطاف‌پذیری تراکنشی است.

امضای داده‌های که به همراه داده‌های ورودی، وارد می‌شوند را می‌توان تغییر داد، که به این وسیله می‌توان شناسه تراکنش را نیز عوض کرد. درواقع می‌توان کاری کرد که تراکنش به‌نوعی نشان داده شود که گویی اصلاً انجام‌نشده است. در مثال بالا به این‌گونه خواهد بود که: فرض کنید باب می‌خواهد آلیس ۳ بیت کوین را به او ارسال کند. آلیس ۳ بیت کوین را به آدرس عمومی باب می‌فرستند و منتظر تأیید ماینرها می‌شود. در همین حین باب با بهره‌گیری از انعطاف‌پذیری تراکنش، امضای آلیس را تغییر داده و شناسه تراکنش را عوض می‌کند. حالا این شانس وجود دارد که تراکنش دستکاری‌شده زودتر از تراکنش آلیس تأیید شود که در این صورت موجب بازنویسی تراکنش آلیس می‌شود. وقتی‌که باب سه بیت کوین خود را دریافت می‌کند، به‌راحتی به آلیس می‌گوید که آنها را دریافت نکرده است. آلیس نیز با دیدن تراکنش ناموفق سرویس را مجاب به بازفرستادن بیت کوین‌ها می‌کند. درنتیجه باب، به‌جای سه بیت کوین، شش بیت کوین را دریافت می‌کند. این

اتفاق دقیقاً اتفاقی است که در مورد Mt.Gox رخ داد. به دلیل مدیریت بد و نبود برنامه‌های مقابله‌ای، چیزی در حدود ۴۷۳ میلیون دلار بیت کوین که ۷ درصد تمام بیت کوین‌های دنیا را شامل می‌شود از سیستم به سرقت رفت.

پیامدها

زمان وقوع این حمله به Mt.Gox بسیار بد بود؛ چراکه بیت کوین به‌آرامی داشت اعتماد جریان اصلی را به سمت خود جلب می‌کرد. این ترس وجود داشت که حمله به Mt.Gox باعث ناامیدی و سلب اطمینان مردم نسبت به بیت کوین طی چهار الی پنج سال شود. کمی بعد از حمله ارزش بیت کوین به‌شدت افت کرد. این افت در نمودار پایین قابل‌مشاهده است. Mt.Gox اعلام ورشکستگی کرد و کمی بعد دریافت که پول‌های به‌دست‌آمده از طریق صرافی دیگری بانام BTC-e پول‌شویی شده است. مالک این صرافی (الکساندر وینیک) در یونان دستگیر شد و به جرم پول‌شویی پول‌هایی که از طریق Mt.Gox به‌دست‌آمده بود به ایالات‌متحده آمریکا تحویل داده شد. در صورت اثبات این اتهام او باید ۵۵ سال را در زندان سر کند. اقدامات پول‌شویی از طریق دیگر صرافی این فرد بانام Tradehill انجام‌گرفته بود. خوشبختانه بیت کوین این اتفاق را پشت سر گذاشت و از آن زمان به روند صعودی خود ادامه می‌دهد.

هک DAO

حالا که راجع به بزرگ‌ترین حمله هکرها به بیت کوین صحبت کردیم، نوبت اتریوم و بزرگ‌ترین حمله به این ارز دیجیتالی است. این حمله و عواقبش به حدی بزرگ بود که توسعه‌دهندگان آن مجبور شدند به‌منظور دفع و پیشگیری از حملات مشابه، این ارز دیجیتالی را دوباره بسازند. قبل از توضیح در موردحمله، بهتر است تا چند پیش‌زمینه تاریخی را برای شما تشریح کنیم.

ترکیب DAO

تمام اکوسیستم اتریوم بر پایه قراردادهای هوشمند کار می‌کند. درواقع قراردادهای هوشمند روشی است که در اکوسیستم اتریوم، اعمال مختلف صورت می‌پذیرند. به عبارت ساده‌تر، قراردادهای هوشمند، قراردادهایی خودکار هستند که مفاد قرارداد را خودشان تعیین می‌نمایند.

(سازمان مستقل غیرمتمرکز) یا به‌اختصار DAO، قراردادی پیچیده و هوشمند است که قرار بود به‌وسیله آن تمام سیستم اتریوم زیرورو شود. درواقع DAO قرار بود تا سرمایه را مستقل سازی کند و در آینده‌ای نزدیک تمام اپلیکیشن های مبتنی بر خود را تأمین مالی نماید. سازوکار آن نیز بسیار ساده بود. اگر می‌خواستید به هر شکلی اپلیکیشن مستقل خود را تأمین مالی نمایید، آنگاه باید توکن های DAO باارزش مشخص اتریوم می‌خریدید. درواقع به این وسیله و با خرید توکن ها شما به‌طور رسمی عضوی از سیستم DAO می‌شدید.

حالا، این اپلیکیشن ها چگونه تأیید و ساخته می‌شدند؟ ابتدا باید توسط سازندگان گواهی‌های عدم آلودگی به ویروس‌ها و برنامه‌های مخرب را دریافت می‌کردید. این سازندگان درواقع مقامات اصلی اتریوم به‌حساب می‌آمدند. سپس می‌بایست توسط دارندگان توکن های DAO رأی اعتماد دریافت می‌کردید. اگر رأی ۲۰ درصد از این افراد کسب می‌شد، اجازه تأمین مالی پروژه به شما اعطا می‌شد. پتانسیل‌های DAO به همراه انعطاف‌پذیری، کنترل و شفافیت کاملی که ارائه می‌کرد، به نحوی بی‌سابقه بود و با استقبال کم‌سابقه مردم مواجه شد. طی ۲۸ روز بعد از تأسیس، چیزی در حدود ۱۵۰ میلیون دلار جمع‌آوری شد. در آن زمان، این مقدار ۱۴ درصد از تمام توکن های اتریوم را شامل می‌شد.

شاید این سؤال برای شما پیش‌آمده باشد که باوجوداین همه مزیت چطور یکی از این سیستم بیرون رفت؟ یا اگر پروژه‌ای که شما چندان مایل به شراکت در آن نیستید، تأیید می‌شد، چطور می‌شد از شراکت صرف‌نظر کرد؟ به این منظور، راه خروجی بانام (عملکرد جداگانه) ایجاد شد. به این وسیله می‌توانستید از پروژه بیرون روید و اترهای خود را نیز دریافت کنید، و حتی DAO جدیدی برای خود ایجاد نمایید. این DAO های جدید بانام (DAO نو رس) شناخته می‌شدند. به این وسیله شما و تعدادی دیگر از دارندگان توکن که مایل به شرکت در یک پروژه خاص نبودند، با ایجاد سیستمی جدید پذیرای پروژه‌های دیگر می‌شدید.

یک شرط نیز در قرارداد وجود داشت که بر اساس آن، در صورت استفاده از عملکرد جداگانه، باید ۲۸ روز اترهای خود را نگه می‌داشتید و سپس آن‌ها را خرج می‌کردید. تا اینجا همه‌چیز درست و بر اساس برنامه است، به‌جز یک چیز؛ مشکلی بسیار کوچک. بسیاری از مردم این مشکل را به‌صورت شکافی بالقوه می‌پنداشتند. خالقان DAO نیز به آنها اطمینان دادند که هیچ مشکل بزرگی گریبان آنها را نخواهد گرفت. مشکل همین‌جا بود. دقیقا مشکل بزرگی گریبانشان را گرفت. مشکلی که بعدها باعث تمایز میان اتریوم و اتریوم کلاسیک شد.

حمله DAO

در ۱۷ ژوئن ۲۰۱۶، فردی از این شکاف استفاده کرد و باعث از دست رفتن یک‌سوم سرمایه DAO شد. مبلغی بالغبر ۵۰ میلیون دلار. شکافی که هکرها از آن استفاده کرده بودند بسیار ساده و ابتدایی بود. اگر فردی تمایل داشت تا از DAO خارج شود باید درخواستی را ارسال می‌کرد. پروسه خروج نیز طی دو مرحله انجام می‌گرفت: برگرداندن اتریوم های فرد در قبال توکن های DAO ، ثبت تراکنش و به‌روزرسانی موجودی توکن ها در داخل سیستم. کاری که هکرها انجام داده بودند، شامل یک عملکرد برگشتی در درخواست می‌شد که پروسه مذکور را تغییر می‌داد. بر این اساس: گرفتن توکن های DAO از کاربر و برگرداندن اتریوم های درخواستی قبل از ثبت تراکنش، عملکرد برگشتی، باعث می‌شد تا کد به‌عقب برگشته و اترهای بیشتری را برای توکن های مشابه انتقال دهد. این کار تا مرز ۵۰ میلیون دلار پیش رفت و اترهای جمع‌آوری‌شده در یک DAO نورس ذخیره شدند. شعله‌های این آتش در تمام جامعه اتریوم نفوذ کرد. لازم به ذکر است که هک به دلیل مشکلی در DAO اتفاق افتاد نه به خاطر مشکل در اتریوم. اتریوم در پس‌زمینه کار می‌کند و DAO مبتنی بر آن.

(گاوین وود)، از بنیان‌گذاران اتریوم در اظهارنظری اعلام کرد: (مثل این است که بگوییم هرگاه وب‌سایتی از دسترس خارج می‌شود، باید بگوییم تمام اینترنت خراب‌شده است!)

عواقب: طی اجماع جامعه اتریوم، در پایان، تصمیمی اتخاذ شد که بر پایه آن، ارائه یک سافت فورک راه‌حل کار است. با این کار نه تنها می‌توان از قابلیت برگردان جانبی در مورد اتریوم بهره برد، بلکه باعث از یاد رفتن حمله DAO نیز می‌شود. بااین‌حال توسعه‌دهندگان دریافتند که با ارائه یک سافت فورک احتمال حملات DDOS بیشتر خواهد شد. در پایان این اتفاق منجر به جداسازی دو نوع اتریوم شد. یکی اتریوم اصلی که با نام اتریوم کلاسیک از آن یاد می‌شود و دیگری اتریوم جدید.

هک بیت فاینکس

هک پلتفرم تبدیل ارزهای دیجیتالی، بیتفاینکس، دومین هک بزرگ تاریخ بیت کوین است. این صرافی که در هنگ کونگ قرار دارد، در ۲ آگوست سال ۲۰۱۶ اعلام کرد که ۱۲۰ هزار بیت کوین که در آن زمان ارزشی معادل ۷۲ میلیون دلار را داشتند، به سرقت رفته‌اند. پیش از بررسی ابعاد مختلف این حمله ذکر چندین نکته ضروری است.

این هک چگونه اتفاق افتاد؟

این مشکل از نیاز بیتفاینکس به ارتقای سطح امنیتی و قابلیت تبدیل به پول‌های رایج برای کاربرانش، سرچشمه می‌گرفت. بیشتر تراکنش‌ها در بستری اینترنتی انجام می‌شدند که احتمال قرار گرفتن در معرض حملات هکرها را افزایش می‌دهد. بیتفاینکس و بیتگو در سال ۲۰۱۵ تفاهم‌نامه همکاری را به امضا رساندند و سیستم ایجاد کردند که به‌وسیله آن کیف پول‌ها چند امضایی، برای تمام کاربران در دسترس بود. در این کیف پول‌ها، کلیدها میان تعدادی از صاحبان پخش‌شده بود تا بتوان ریسک‌های احتمالی را کنترل کرد.

بیتفاینکس در بیانیه‌ای اعلام کرده بود: دوران درهم‌آمیختگی مشتری‌های بیت کوین و تمام خطرات امنیتی آن به‌پایان رسیده است.

در پایان همین اقدامات امنیتی بود که باعث هک شدنشان شد. همان‌طور که پیش‌تر گفتیم، یک کیف پول چند امضایی دارای کلیدهایی است که بین چندین نفر از دارندگان پخش‌شده. به‌منظور انجام یک تراکنش امضا و تأیید تمام این افراد نیاز است. در مورد بیتفاینکس، دو کلید در اختیار خودشان و یک کلید توسط بیتگو نه داری می‌شد. از همین رو، بیتگو به‌عنوان یک لایه امنیتی اضافی و به‌نوعی مهر تأییدی بر تراکنش‌های بیتفاینکس تلقی می‌شد. به دلیل همین لایه امنیتی جدید، بیتفاینکس، میزان حافظه‌های سرد خود را کاهش داد و شروع به ذخیره پول‌های مشتری‌ها خود در کیف پول‌های چند امضایی گرم نمود. این ایده به‌منظور سهولت در تبدیل ارزها به پول، بدون به خطر انداختن امنیت آنها، صورت گرفته بود. در هنگام حمله هکرها، آنها نه تنها امضای بیتفاینکس را برای خروج بیت کوین‌ها در تراکنش‌ها استفاده می‌کردند، بلکه گاهی با دور زدن موانع امنیتی بیتگو، امضای آنها را نیز در تراکنش مورداستفاده قرار می‌دادند.

نظریه‌های بسیاری در مورد اینکه دقیقاً چه اتفاقاتی افتاده وجود دارد. از تئوری‌های مرتبط با توطئه تا نظریاتی صرفاً مضحک. اما طی معتبرترین نظریه، سیستم راه‌اندازی بیت فاینکس دچار نقص بوده به‌طوری‌که بیتگو همان کاری را با سرمایه‌ها می‌کرده که بیتفاینکس به آن گفته بود. درنتیجه این کیف پول چند امضایی اصلاً چند امضایی نبوده است! در این میان تنها یک نقطه به‌عنوان اشکال وجود داشته و آن‌هم سرورهای بیتفاینکس بوده‌اند. البته باید به یاد داشته باشیم که بیتگو به‌صورت عمومی اعلام کرد که سرورهای آنها به‌هیچ‌وجه مورد هجوم و رخنه هکرها قرار نگرفته بودند.

عواقب :قیمت بیت کوین با کاهش شدیدِ بیست درصد مواجه شد. پیش از آنکه بیت کوین بتواند دوباره روی پای خود بیستد قیمت آن تا هر بیت کوین ۴۸۰ دلار نیز افت نمود. بازیابی بیتفاینکس هم به‌نوعی ستودنی است. آنها در ابتدا توکن های BFX را میان مشتری‌ها خود تقسیم کردند که نوعی فته طلب به شمار می‌رفت. البته شایعه‌هایی هم وجود دارند که طبق آنها، این کار بیتفاینکس خریدن زمان بیشتر برای بازپرداخت بدهی‌های خود به کاربرانش بوده. اول سپتامبر، به‌منظور کاهش اضطراب‌ها و ترس‌های مرتبط با بیت کوین، ۱،۰ درصد توکن ها را بازخرید کردند. بیتفاینکس با اضافه کردن سازوکارهای (Pairs trade) موجب سریع‌تر شدن انجام فروش‌ها و ایجاد OTC برای تبادلات بزرگ‌تر شد که درنهایت به جذب کسب‌وکارهای بزرگ و در نتیجه پرداخت سریع‌تر قرض‌ها شد. در تاریخ سوم آوریل سال ۲۰۱۷، بیتفاینکس تمام تبادلات BFX را متوقف کرد و شروع به‌نقد کردن این توکن ها با مبلغ یک دلار برای هر توکن نمود.

هک BitStamp

در اواسط سال ۲۰۱۵، صرافی محبوب BitStamp مورد یک حمله بزرگ قرار گرفت. طی این حمله ۱۹،۰۰۰ واحد بیت کوین از فضای کیف پول سرد این صرافی به سرقت رفت. بیت‌استمپ در آن زمان بزرگ‌ترین صرافی اروپا بود که پس از فروپاشی MtGox افراد زیادی به آن روی آورده بودند. پس از این اتفاق کلیه فعالیت های سایت برای چند ماه به حالت تعلیق در آمد. سرقت از کیف پول های سرد که به اینترنت متصل نبودند، بسیاری از کاربران را به اعتراض وا داشت که احتمالا این سرقت کار افراد داخلی در این صرافی بوده است. اما مانند بیت فینکس این صرافی هم تمام مبالغ به سرقت رفته را آرام آرام به کاربران بازگرداند.

پیامد ها

این حمله رشد صعودی بیت کوین را برای دو ماه متوقف کرد. این هک یه فضای انتقادی بزرگ برای بیت کوین ایجاد کرد و منتقدان نسبت به ماهیت و عدم قانونگذاری آن بسیار معترض بودند. البته پس از بازگشت پول ها به کاربران،اعتماد ها کمی بهبود یافت و رشد قیمت بیت کوین بازهم شروع شد.

به باد رفتن سرمایه‌ها در Parity!

اگرچه ازلحاظ فنی این مورد، جزو هک‌های بزرگ در تاریخ ارزهای دیجیتالی به شمار نمی‌رود ولی ذکر کردن آن خالی از لطف نیست. چقدر پیش می‌آید که ببینید کسی ۱۵۰ میلیون دلار را به باد بدهد؟ این دقیقاً همان کاری است کاربر (devops199) انجام داد. او این کار را با نابود کردن قرارداد x863df6bfa4469f3ead0be8f9f2aae51c91a907b4۰ صورت داد.

۲۰ جولای، به دلیل نقصی که پیش از آن رخداده بود، نسخه جدید کیف پول قرارداد Parity منتشر شد. متأسفانه، عیب عجیبی در کدهای جدید وجود داشت. بعدها مشخص شد که طی این نقص ممکن است، کیف پول با استفاده از قابلیت initWallet به یک کیف پول چند امضایی تبدیل شود.

Parity تمام کیف پول‌های چند امضایی خود را به یک کتابخانه قراردادها (library contract) متصل می‌کند که این کار را به‌منظور عاملیت خود انجام می‌دهد. به‌طور خلاصه، تمام کیف پول‌های چند امضایی Parity دارای یک نقطه نقص بوده‌اند و آن نقطه در سالیدیتی کد قرار داشته است:

constant _walletLibrary = 0x863df6bfa4469f3ead0be8f9f2aae51c91a907b4

بر طبق نوشته‌های یکی از کابران سایت Reddit بانام (ItsAConspiracy)، این کار به‌منظور صرفه‌جویی در وقت و انرژی صورت گرفته است. درواقع به‌جای کپی و پیست کردن یک کد در هر کیف پول چند امضایی، آنها اقدام به استفاده از یک کتابخانه کرده‌اند؛ از همین رو به‌جای داشتن یک کد که در هر کیف پول تکرار می‌شده، یک مکان مشخص که در آن هر کیف پول می‌توانسته عملکردهایی را به انجام برساند، وجود داشته.

پس کاربر می‌توانسته از کتابخانه به‌صورت یک کیف پول استفاده کند و تمام قابلیت‌های صاحب آن را نیز در اختیار داشته باشد که این قابلیت‌های شامل از بین بردن کامل آن‌هم می‌شده.

تمام قراردادها دارای ساختاری (از بین برنده) هستند. برای فهم این موضوع به نمونه پایین دقت کنید :از این قابلیت برای پایان بردن قرارداد و انتقال باقی‌مانده توکن ها به خالق آن استفاده می‌شود. درواقع باعث اتمام قرارداد می‌شود. پس، وقتی یک کاربر کیف پول را از بین ببرد، درواقع کیف پول و کتابخانه و تمام عملکردهای لگاریتمی مرتبط را نیز از بین برده. از همین رو، تمام کیف پول‌ها متصل به این کتابخانه بی‌مصرف شده و تقریباً ۳۰۰ میلیون دلار بربادرفته!

عواقب

Parity در مورد این اتفاق در توییتر نوشت: همچنان تمام دارایی‌ها غیرقابل دسترسی هستند. ازآنجایی‌که اتریوم غیرقابل دست‌کاری است، این کار نیز قابل‌برگشت نیست. تنها می‌توان از طریق یک هاردفورک سرمایه‌های ازدست‌رفته را بازگرداند.

جامعه اتریوم نیز نسبت به این موضوع دوگانه‌اند. در بسیاری از نظرسنجی ها توییتری، میزان موافقان و مخالفان هارد فورک ۵۰-۵۰ است. همین حالا و در حال نگارش این مطلب، چیزی در حدود ۳۰۰ میلیون دلار به‌صورت اتریوم در فضایی قرارداد که هیچ‌کس نمی‌تواند ادعای مالکیت آنها را داشته باشد.

هک (نایس هَش)

ششم دسامبر ۲۰۱۷، در ساعت ۱۸دقیقه بامداد، شرکت اسلوونیایی نایس هش هک شد و ۴۷۰۰ بیت کوین به ارزش ۸۰ میلیون دلار به سرقت رفت. (مارکو کوبال) مدیر اجرایی نایس هش، در ویدیویی زنده در فیس‌بوک در مورد نگرانی‌های موجود در مورد این حمله صحبت کرد. او تنها به گفتن ورود هکرها به رایانه‌های کارکنان که منجر به سرقت شد، بسنده کرد. مهاجمین با استفاده از هویت کارکنان این شرکت،

توانستند از سیستم نایس هش سرقت کنند. کوبال در ویدیوی خود گفت :باوجود پیچیدگی سیستم‌ها در اینجا، به نظر می‌رسد این حمله به‌صورت گسترده‌ای برنامه‌ریزی‌شده و دارای جنبه‌های فوق پیچیده است.

نایس هش، ۲۴ ساعت را برای چک کردن و آنالیز جنبه‌های مختلف این هک از دسترس خارج شد. در مصاحبه مطبوعاتی این شرکت اعلام شد :سیستم پرداخت ما دچار مشکل شد و با رخنه بر آن، محتویات کیف پول‌های بیت کوین به سرقت رفتند. ما در حال کار بر روی میزان دقیق بیت کوین‌ها هستیم. واضح است که اهمیت این موضوع بسیار است و ما به‌سختی در حال کاربر روی برطرف کردن آن در روزهای پیش رو هستیم. به‌منظور تسریع امور، تمام اطلاعات در اختیارات مقامات و مراجع امنیتی قرارگرفته است و ما در حال همکاری با آنها برای رفع هر چه سریع‌تر مشکل هستیم.

هک Youbit

هک شدن این صرافی کره ای خیلی اتفاق بزرگی نبود اما اینکه در یک سال دوبار مورد حمله قرارگرفته است، در نوع خود جالب است . روز ۱۹ (۲۹ دی ماه)، این تجارتخانه بزرگ ارزهای دیجیتال که در آوریل هم مورد حجوم قرارگرفته بود، هک شد. هکرها با به سرقت بردن ۱۷ درصد از سرمایه های این سایت، آن را تا مرز ورشکستگی پیش بردند.

این صرافی مبالغ سرقت رفته از کیف پول های گرم را اعلام نکرده است اما کیف پول های سرد از این حمله در امان ماندند. این شرکت کره ای قول داده است که تمام مبالغ به سرقت رفته کاربران را رفته رفته پرداخت کند. در آوریل سال جاری هم که اسم این صرافی Yapizon بود،حدود ۳۱۰۰ بیت کوین از این صرافی سرقت رفت که اکنون بالای ۶۰ میلیون دلار ارزش دارد.

پیامدها

هک شدن دوباره این صرافی باعث شد تا دولت کره جنوبی با برگزاری جلساتی درباره قوانین ارزهای دیجیتال تصمیم گیری کند. همچنین اعتماد کاربران زیادی نسبت به این سایت از بین رفته است.

نتیجه‌گیری

از مقیاس بزرگ هک Mt.Gox گرفته تا ضعف مدیریتی و عواقب وخیم هک شدن DAO و فاجعه تصادفی Partity برای شما گفتیم تا بتوانید درک درستی از حملات هکر به دنیای ارزهای دیجیتالی پیدا کنید. ولی بیتفاینکس نشان داد که باوجود تمام اتفاقات می‌شود دوباره روی پای خود ایستاد. به‌طورکلی، به یاد داشته باشید بالا بردن اطلاعات خود نسبت به خطرات دنیای ارزهای دیجیتالی باعث می‌شود تا بفهمید، همیشه راه خروجی برای مشکلات وجود دارد. ارزهای دیجیتالی نیز مانند سیستم‌های مالی و بانکداری دارای نواقص فراوانی هستند و هیچ‌کس نیز نمی‌تواند منکر این حقایق باشد.

کیف پول‌های چند امضایی چه نوع کیف پول‌هایی هستند؟

برای درک بهتر عملکرد کیف پول‌های دیجیتالی چند امضایی، آنها را مانند گاوصندوقی در نظر بگیرید که برای باز شدن به چندین کلید نیاز دارند. این نوع کیف پول‌ها برای دو کاربرد مناسب‌اند:

۱. برای ایجاد امنیت بیشتر در رابطه با خطاهای انسانی.
۲. به‌منظور ایجاد کیف پولی با پیروی از دموکراسی که می‌تواند برای یک یا چند کاربر مورداستفاده قرار گیرد.

حالا یک کیف پول چند امضایی چگونه ما را از خطاهای انسانی مصون می‌دارد؟ با مثال از بیتگو، یکی از اصلی‌ترین کیف پول‌هایی که از قابلیت چند امضایی بهره می‌برد به این سؤال پاسخ می‌دهیم. این کیف پول از سه کلید شخصی استفاده می‌کند. یکی توسط خود شرکت نگه‌داری می‌شود، یکی توسط کاربر و دیگری کلیدی است که به‌عنوان کلید پشتیبان از آن یاد می‌شود و می‌توان به‌وسیله آن شخص سوم را به‌عنوان صندوق‌دار یا هر عنوان دیگری به سیستم اضافه کرد. برای انجام هر تراکنش وجود دو کلید از سه کلید اشاره‌شده لازم است. در این صورت، باوجود تهدید هکرها، امکان دست‌یابی آنها به دو کلید مشکل است. از طرف دیگر در صورت گم‌شدن یکی از کلیدها به هر دلیلی، می‌توان از کلید یدکی که به دوست خود داده‌اید استفاده کنید.

حالا، چطور این کیف پول‌ها باعث ایجاد محیطی دموکراتیک می‌شوند؟ تصور کنید که شما در شرکتی کار می‌کنید که از ده نفر، رضایت هشت نفر برای انجام تراکنش حیاتی است. با استفاده از نرم‌افزاری مثل (الکتروم) ایجاد کیف پولی با ده کلید کار بسیار راحتی است. به این وسیله می‌توانید تراکنش‌هایی را بر پایه دموکراسی در شرکت خود انجام دهید.

باوجود تمام این مسائل، این کیف پول از نوع مبتنی بر اینترنت و آنلاین است، از همین رو باید از آن برای مقاصد اقتصادی استفاده کنید. در مورد هک بیتفاینکس، این اتفاق علیرغم وجود امنیت چند امضایی رخ داد. به‌علاوه در پایان، شرکتی که از کیف پول آن استفاده می‌کنید، یکی از کلیدهای شخصی را در اختیار دارد. استفاده از سرمایه شما توسط آنها کاملاً به مسائل اخلاقی‌شان برمی‌گردد.

چند توصیه امنیتی برای کیف پول ارز دیجیتال

از کیف پول خود نسخه پشتیبان بگیرید

بهتر است فقط مقدار اندکی از ارز دیجیتال را برای استفاده روزمره آنلاین خود بر روی رایانه و یا گوشی خود نگه دارید و بیشتر دارایی خود از ارز دیجیتال را در محیطی با امنیت بالاتر حفظ کنید. گزینه‌های موجود برای ذخیره سرد (یا آفلاین) نظیر لجر نانو اس و یا کاغذ می‌تواند موجودی شما را از مشکلات ناشی از خرابی رایانه حفظ کرده و امکان بازیابی کیف پول را در صورت گم‌شدن و یا سرقت فراهم سازد. واقعیت این است که کیف پول آنلاین همیشه ریسک‌هایی بیشتری به همراه دارد.

نرم‌افزار خود را به‌روزرسانی کنید

نرم‌افزار خود را به روز نگه دارید تا بیشترین میزان امنیت را در اختیار داشته باشید. نه تنها باید نرم‌افزار کیف پول خود را به روز کنید، بلکه باید نرم‌افزار روی رایانه یا گوشی نیز باید به روز شود.

لایه‌های امنیتی بیشتری اضافه کنید

هر قدر کیف پول ارز دیجیتال شما لایه‌های بیشتری داشته باشد، بهتر است. تعیین گذرواژه طولانی و پیچیده و اطمینان حاصل کردن از اینکه برای هر برداشتی نیاز به وارد کردن گذرواژه است، پیش نیاز به شمار می‌رود. از کیف‌های پولی استفاده کنید که از اعتبار خوبی نزد کاربران برخوردارند و لایه‌های امنیتی بیشتری نظیر تایید دومرحله‌ای هویت را داشته باشند. شاید هم بخواهید از کیف‌پولی استفاده کنید که امکان

تراکنش را با تایید یک یا چند کاربر دیگر فراهم کنند. این کیف‌های پول در اصطلاح multising نامیده می‌شوند که مخفف عبارت (چند امضایی((multi signature) است. دو کیف پول آرموری (Armory) و کوپی (Copay) از جمله آنها به شمار می‌روند.

پنج مورد از خلاقانه ترین حمله های ۵۱ درصد در دنیای ارز دیجیتال!

یک حمله ۵۱ درصد زمانی می تواند صورت بگیرد که مهاجم کنترل بیش از ۵۰ درصد میزان هش شبکه را در دست بگیرد. (کل قدرت استخراجی که برای اعتبار بخشی به تراکنش ها بر روی شبکه مورد استفاده قرار می گیرد) زمانی که یک مهاجم ۵۰ درصد و یا بیشتر از میزان هش یک شبکه را داشته باشد، این مهاجم می تواند تراکنش ها را از اعتبار ساقط کند و حتی به خرج کردن دوباره کوین ها بپردازد که این باعث بی اعتبار شدن تغییر ناپذیری و امانت یک بلاک چین می شود.

اجرای حملات ۵۱ درصد در بلاک چین هایی که با قدرت استخراج بیشتری پشتیبانی می شوند، پر هزینه تر و مشکل تر می باشد. به طور ساده باید گفت که کنترل نصف شبکه ای با میزان هش بیشتر پر هزینه تر می باشد. به عنوان مثال crypto51.com تخمین می زند که اجرای یک حمله ۵۱ درصد بر شبکه بیت کوین ۳۸۰۰۰۰ دلار در ساعت هزینه خواهد داشت. برعکس تنها ۸۱۰۰ دلار برای حمله به بیت کوین SV در همان دوره زمانی لازم است. در حال حاضر، بیت کوین میزان هش 38000PH/Sرا در مقایسه با ۸۶۰ PH/Sکوین BSV دارد.

تمرکز استخراج نیز عاملی در این زمینه است، زیرا یک استخر استخراج با بیش از ۵۰ درصد از میزان هش یک بلاک چین می تواند حمله ۵۱ درصد را انجام دهد. به عنوان مثال، وقتی که BTC.TOP که یک استخر استخراج است، کنترل ۵۰.۲ درصد از میزان هش بیت کوین کش را در خلال مدتی در ژانویه ۲۰۱۹ در دست گرفت، نگرانی ها افزایش پیدا کرد.

کوین هایی که از این گونه حملات رنج برده اند

بیت کوین گلد(Feathercoin (FTC) ، (Vertcoin (VTC، BTG)، اتریوم کلاسیک و ورج (Verge) همگی از حمله ۵۱ درصد رنج برده اند. همه این ارز های دیجیتال ذکر شده نسبتا میزان هش پایینی در مقایسه با کل مقدار هش موجود در خانواده الگوریتمی خود دارند و این عامل آنها را مستعد حمله کرده است.

نمودار پایین میزان هش بیت کوین، بیت کوین کش، Vertcoinو Bitcoin Gold را در سال گذشته مورد مقایسه قرار می دهد. میزان هش بالاتر بیت کوین آن را کمتر در معرض حمله ۵۱ درصد قرار می دهد.

- Feathercoin۵

این ارز دیجیتال شبیه لایت کوین است و مانند لایت کوین زمان بلاک ۲.۵ دقیقه ای و الگوریتم استخراج اسکریپت دارد. این آلت کوین در حال حاضر در رده ۴۶۱ لیست قیمت ها قرار دارد Feathercoin .امروزه کمتر توجه کسی را جلب می کند اما در زمانی که از حمله ۵۱ درصد رنج برد، جز ارز های دیجیتال برجسته بود.

حمله هشتم ژوئن به شبکه Feathercoin با یک افزایش برجسته در میزان هش شبکه آغاز شد. گمان می شد که این قدرت استخراج اضافی از جانب ماینر ها از استخر های مبتنی بر الگوریتم Scrypt آمده باشد. بر طبق گفته بنیان گذارFeathercoin ، ماینر ها در جستجوی منفعت بردن از سودآوری افزایش یافته در استخراج Feathercoin به علت تغییر سختی بودند.

در حمله ابتدایی کلا ۸۰ بلاک مجزا شدند .بلاک های اورفان Orphaned بلاک های معتبری در شبکه هستند که بعدا جایگزین می شوند زیرا یک زنجیره طولانی تر با گواه اثبات کار بزرگتر اولویت دارد. این یعنی تراکنش های تایید شده FTC در آن حمله معکوس شدند. بعضی از ماینر ها نیز در نهایت با تلاش بی حاصل برای استخراج بلاک هایی مواجه شدند که در نهایت بر روی زنجیره جایگزین شده بودند.

زمانی که وبسایت رسمی Feathercoin تقریبا در همان زمان با حمله DDoS مواجه شد، مشکلات تشدید شدند. بنا به اظهارات Tradeblock، در آن زمان صرافی ها مجبور به افزایش نیازمندی های تایید تراکنش های Feathercoin بودند تا تضمین حاصل کنند که تنها تراکنش های معتبر در زنجیره درست پردازش شده است. ویژگی Checkpointing پیشرفته هم توسط تیم Feathercoinپیشنهاد شد تا از حملات ۵۱ درصد در آینده جلوگیری شود. با این وجود، این حمله اعتماد به FTC را از میان برد و این ارز دیجیتال از آن زمان به بعد در شک و ابهام قرار گرفت.

4-بیت کوین گلد(Bitcoin Gold)

این ارز دومین فورک بیت کوین بود که در نوامبر ۲۰۱۷ راه اندازی شد (در میان چند موضوع فنی که قبل از راه اندازی روی داد). اگرچه این کوین به عنوان ارز دیجیتالی تبلیغ می شد که از استخراج غیر متمرکز از طریق الگوریتم استخراج مقاوم در برابر ASICپشتیبانی می کند اما منتقدان آن را بدست آوردن سریع پول نامیدند. با این وجود، کوین BTG به بسیاری از افراد نگه دارنده بیت کوین داده شد و بسیاری به ورود پول رایگان خوشامد گفتند.

در یک پست وبلاگ در یازدهم ماه می، تیم Bitcoin Gold دارندگان این کوین را از تلاش برای حمله به شبکه Bitcoin Gold آگاه کرد. از صرافی ها خواسته شد که در برابر این حمله مقاومت کنند زیرا مهاجمان احتمال داشت که از خرج کردن دوباره کوین ها در تراکنش های صرافی سود ببرند. این پست وبلاگ در ۲۴ می به روز رسانی شد و اعلام کرد که یک حمله ۵۱ درصد سهمناک به شبکه در بین ۱۶ و ۱۹ ماه می ۲۰۱۸ روی داده است. حمله به Bitcoin Gold همچنین شامل قدرت هش اجاره شده از جانب سرویس های کلود ماینینگ بود.

Bitcoin Goldکه تقریبا یکی از بد عملکرد ترین ارز های دیجیتال در سال ۲۰۱۸ بوده است حتی بعد از این حمله با مشکلات بیشتری هم مواجه شد. صرافی Bittrex این کوین را از لیست خارج کرد که دلیل آن امتناع تیم آن از پرداخت غرامت ۱۲۳۷۲ کوین BTG بود. صرافی هایی مانندBittrex ، Binance، Bithumb، Bitinkaو Bitfinex تخمین زده می شود که به ارزش ۱۸ میلیون دلار از این کوین را به دلیل حمله خرج کردن دوباره از دست داده باشند Bittrex .تیم BTG را برای اهمال سرزنش کرد و برای در لیست نگه داشتن این کوین خواستار پرداخت غرامت شد.

تیم این کوین در جواب اعلام کردند که حملات ۵۱ درصد ریسکی شناخته شده در این اکوسیستم هستند. آنها همچنین ابراز داشتند که سازمان BTG مسئول این حمله نیست زیرا به دلیل نقص در بلاک چین یا کد Bitcoin Gold روی نداده است. علاوه بر این، تیم BTG هشدار های خود قبل از حمله و مساعدت با صرافی برای دفاع از خودشان را خاطرنشان کرد.

تیم BTG همچنین ادعا کرد که ارتقای شبکه در جولای ۲۰۱۸ انجام گرفته و احتمال حمله ای دیگر به شبکه را کاهش خواهد داد Bittrex .در نهایت این کوین را از لیست خارج کرد و بسیاری دیگر نیز همین کار را کردند Bitcoin Gold .هنوز هم به عنوان سی امین کوین در رده بندی باقی مانده است.

- Vertcoin۳

حمله ۵۱ درصد در شبکه Vertcoin بین اکتبر و دسامبر ۲۰۱۸ روی داد Coinmonks .تخمین می زند که کلا ۱۰۰۰۰۰ دلار از کوین های این ارز دیجیتال توسط یک مهاجم در هشت سازماندهی مجدد بلاک چین Vertcoin دوباره خرج شدند. سازماندهی مجدد یک زنجیره زمانی روی می دهد که ماینری با بیش از ۵۰ درصد میزان هش، یک سابقه تراکنش جایگزین را با ایجاد افزونه ای از هر زنجیره ارائه دهد و در نهایت تاریخچه تراکنش شبکه را جایگزین کند.

در این حمله، تراکنش ها در تعدادی از بلاک هی مجزا شده در تاریخچه تراکنش پذیرفته شده نهایی دوباره خرج شده اند. در این حمله کلا ۷۱۰۰۰ کوین VTC دوباره خرج شد. متعاقب آن وحشت در بازار حکمفرما شد و قیمت هر کوین VTC از ۰.۷ دلار به ۰.۳ دلار کاهش پیدا کرد.

Gert-Jaap Glasbergenاز توسعه دهندگانVertcoin ، آن حمله را به وجود سرویس های کلود ماینینگ و بیرون دادن سخت افزار استخراج اختصاصی برای Vertcoin نسبت داد. سرویس های کلود ماینینگ مانند NiceHash اجاره کردن قدرت استخراج به قیمت پایین تر را برای مهاجمان آسان تر کردند (خرید و نصب کردن سخت افزار استخراج برای همین منظور گران تر می باشد).

Vertcoinاز آن به بعد الگوریتم استخراج خود را به Lyra2REV3 به روز رسانی کرد تا سخت افزار استخراج اختصاصی را برای استخراج Vertcoin نا کارآمد کند. در Verthash نیز توسعه در حال انجام است و الگوریتم جدیدی که به کلی استفاده از سخت افزار استخراج اختصاصی را در شبکه Vertcoin از میان بردارد، ایجاد خواهد شد. این الگوریتم جدید Verthash انتظار می رود که مشکل افزایش میزان هش به دلیل کارت گرافیک اجاره شده را حل کند Vertcoin .تا سپتامبر ۲۰۱۸ در رده ۱۳۸ ارز های دیجیتال بود اما امروزه به رده ۱۶۲ تنزل پیدا کرده است.

۲ -اتریوم کلاسیک

اتریوم کلاسیک نسخه اورجینال اتریوم می باشد که بعد از اینکه تیم اصلی یک فورک را با معکوس کردن هک ننگین DAO بر روی شبکه اتریوم ایجاد کرد، باقی ماند. طرفداران اتریوم کلاسیک از حفظ یک تاریخچه تراکنش غیر قابل مداخله حمایت می کردند. اما در نهایت اتریوم کلاسیک محبوبیت کمتری از نسخه دیگر پیدا کرد.

Cryptoslateبه طور گسترده ای ۱.۱ میلیون دلار سرقت اتریوم کلاسیک را که در حمله ۵۱ درصد به بلاک چین اتریوم کلاسیک روی داد، پوشش داد. این واقعه در ابتدا توسط کوین بیس (Coinbase) در یک پست وبلاگ در هفتم ژانویه گزارش شد. در این گزارش آشکار شد که کلا ۲۱۹۵۰۰ کوین اتریوم کلاسیک به ارزش ۱.۱ میلیون دلار در ۱۱ سازمان دهی مجدد بلاک چین آن دوباره خرج شده بود و این کار از پنجم ژانویه آغاز شده بود. کوین بیس و Kraken سریعا در نتیجه این امر، ترید اتریوم کلاسیک را متوقف کردند.

به دنبال این حمله قیمت اتریوم کلاسیک کاهش پیدا کرد اما بعد از آن بهبود پیدا کرد. نمودار زیر قیمت اتریوم کلاسیک را از روز حمله تا به امروز نشان می دهد.

به دنبال این حمله، تیم اتریوم کلاسیک نا کافی بودن میزان هش و ماینر بدکاری را که به عنوان Private Pool 0xccc8f74 شناخته شده بود، مورد سرزنش قرار داد و آنها را دلیل حمله دانست. بار دیگر تیم تصمیم گرفت که حمله را معکوس نکند. لیستی از اقدامات برای جلوگیری از حملات ۵۱ درصد در آینده نیز در اختیار عموم قرار گرفت که از جمله آنها ایجاد یک سیستم هشدار و نظارت برای کشف سریعتر حملات را می توان نام برد. تغییر الگوریتم گواه اثبات کار (Proof of Work) برای به حداقل رساندن حملات اجاره ای NiceHash نیز پیشنهاد داده شد.

۱ -ارز دیجیتال ورج(Verge)

Justin Sunerokبنیان گذار ورج در مصاحبه ای با CryptoSlate این ارز دیجیتال را به عنوان "یک کوین حریم خصوصی که برای استفاده روزمره طراحی شده است" توصیف کرد. این کوین حریم خصوصی از پنج الگوریتم استخراج مختلف استفاده می کند. ماینر های این ارز دیجیتال مجبورند که از الگوریتم متفاوتی برای هر بلاک استفاده کنند تا احتمال کنترل اکثریت میزان هش در شبکه توسط یک موجودیت خاص کاهش پیدا کند. این سیستم چند الگوریتمی به طور جالبی برای تعمیر حمله قبلی ایجاد شد که در سال ۲۰۱۶ این شبکه را رنج داده بود.

در آپریل ۲۰۱۸، یک مهاجم از اشکال موجود در کد ورج سوء استفاده کرد و حداقل ۲۰ میلیون کوین ورج را دزدید که تقریبا ارزشی معادل ۱۷۰۰۰۰ دلار داشت. همچنان که توسط یکی از کاربران فورم Bitcointalk بنام ocminer توضیح داده شد، این باگ به ماینر بدکار اجازه داد تا بلاک های استخراج شده با برچسب زمانی جعلی را ارائه دهد. این مهاجم سپس چندین بلاک را در فواصل یک ثانیه ای با بهره برداری از یکی از پنج الگوریتم استخراج، استخراج کرد.

تیم ورج در تلاش برای حل این مشکل هارد فورکی را اجرا کرد که مشکلات جدیدی را در مورد کیف پول ها به وجود آورد. علی الرغم این مرمت، ورج یک ماه بعد از حمله مشابهی رنج برد.

Justin Sunerokدر مصاحبه CryptoSlate خود ابراز داشت که این مجموعه حمله ها به شبکه ورج اعتماد به این پروژه را تحت تاثیر قرار نخواهد داد. او همچنین افزود که جامعه ورج مانند همیشه پر طراوت است. از آپریل ۲۰۱۸ به بعد، ورج از جایگاه ۲۶ خود در بازار ارز های دیجیتال سقوط کرده و هم اکنون در جایگاه ۵۰ قرار دارد.

ارزهای مهم بازار

بیت کوین BITCOIN

به زبان ساده، بیت کوین، یک ارز و پول دیجیتال و همچنین یک شبکه برای پرداخت‌های مستقیم و بدون واسطه است. در سال ۲۰۰۸، درست کمی پس از بحران اقتصادی بزرگ آن زمان، یک مفهوم جدید از پول و دارایی به نام بیت کوین ارائه شد که به عقیده بسیاری از اقتصاددانان می‌تواند آینده اقتصاد جهان را متحول کند و یا حداقل شروع کننده این جریان باشد. چیزی که بیت کوین را از دیگر پول‌های پیش از خود متمایز می‌کند، غیر متمرکز بودن آن است. غیرمتمرکز بودن یعنی اینکه هیچ‌کس نمی‌تواند به تنهایی کنترل شبکه را در دست داشته باشد و هیچ کس مالک اصلی آن نیست. هیچ بانک، موسسه، نهاد یا دولتی بیت کوین را کنترل نمی‌کند. در حقیقت کنترل بیت کوین به دست تمام کاربران آن است. در روش‌های سنتی برای انتقال پول، شما نیاز اعتماد به واسطه‌ها و موسساتی مثل بانک دارید اما با بیت کوین می‌توانید بدون نیاز به اعتماد به هیچ موسسه و نهادی، به تمام جهان و به صورت مستقیم و همتا به همتا پول (بیت کوین) ارسال کنید. این نکته را به یاد داشته باشید که بیت کوین هیچگونه شکل و فرم فیزیکی ندارد و فقط به صورت دیجیتالی منتقل می‌شود. از بیت کوین می‌توان همانند پول‌های رایج برای خرید کالا، تبادل و انتقال پول و همچنین مانند طلا برای سرمایه‌گذاری استفاده کرد. واحد اختصاری ارز بیت کوین، BTC است.

چند ویژگی عمده از بیت کوین که آن را با پول‌های رایج متمایز می‌کند:

- تمرکززدایی

مهمترین مشخصه بیت کوین غیرمتمرکز بودن آن است. همانطور که گفتیم، هیچ فرد حقیقی یا حقوقی خاصی کنترل شبکه بیت کوین را در دست ندارد. بیت کوین توسط هرکسی که به شبکه وصل شود، کنترل می‌شود. هر کس در هر جای دنیا می‌تواند با کامپیوتر خود به شبکه بیت کوین متصل شود و برای کنترل شبکه حق رای خواهد داشت. این ویژگی باعث شد تا افرادی که به نهادهای مالی اعتماد ندارند، جذب بیت کوین شوند.

در روش سنتی، بانک یا نهاد مالی وظیفه تایید تراکنش‌ها را بر عهده دارد و این یعنی که امکان جلوگیری و کنترل تراکنش‌ها توسط آن نهاد محتمل است اما در بیت کوین از هیچ تراکنش صحیحی جلوگیری به عمل نخواهد آمد.

بیت کوین مشکل (دوبار خرج کردن) (که در آن دارایی‌های دیجیتال می‌توانستند کپی و دوباره خرج شوند) را با استفاده از تکنیک‌های پیچیده رمزنگاری حل کرده است. در سیستم‌های الکترونیکی سنتی، مشکل دوبار خرج کردن توسط بانک‌ها حل شده است اما در بیت کوین که یک شبکه کاملا باز است، تراکنش‌ها توسط تمام کاربرانی که به این شبکه متصل هستند، انجام می‌شوند.

- محدودیت واحدهای بیت کوین

برخلاف پول‌های رایج (فیات – بدون پشتوانه) مانند دلار و یورو که به تعداد نامحدود چاپ و توسط دولت‌ها صادر خواهند شد، تعداد واحدهای بیت کوین بیت کوین محدود است. در پروتکل بیت کوین مشخص شده است که بیت کوین‌ها محدود باشند و تعداد آن‌ها فقط ۲۱ میلیون واحد خواهد بود. از آنجایی که هر کسی که شبکه بیت کوین متصل می‌شود، پروتکل و قوانین را می‌پذیرد، پس از رسیدن بیت کوین‌ها به عدد ۲۱ میلیون واحد، دیگرهیچ بیت کوینی استخراج نخواهد شد. این مسئله از نظر ریاضیات اثبات شده است.

واحدهای بیت کوین توسط سازمان متمرکز خاصی تولید و صادر نمی‌شوند. افرادی به نام استخراج‌کننده یا به اصطلاح ماینر (miner) می‌توانند سخت افزارهای قدرتمند خود را برای حفظ امنیت شبکه بیت کوین به کار بگیرند. طی این فرایند بیت کوین تولید می‌شود و به عنوان پاداش به ماینرها تعلق می‌گیرد.

محدود بودن واحدهای بیت کوین موجب کمیابی، عدم تورم و ارزشمندی آن در طول زمان خواهد شد. به دلیل این ویژگی بیت کوین، افراد زیادی بیت کوین را به عنوان ابزاری برای سرمایه‌گذاری و ذخیره ارزش (مانند طلا) خریداری و نگهداری می‌کنند.

- نیمه‌ناشناس بودن بیت کوین

در سیستم‌های پرداخت الکترونیکی سنتی، مشتریان معمولا نیاز به ثبت نام یا افتتاح حساب با مشخصات شناسایی خود دارند. اما در بیت کوین کاربران به نوعی نیمه ناشناس هستند. برای ارسال بیت کوین نیاز به ارائه مشخصات کاربری یا حتی ایمیل نیست. پروتکل بیت کوین به‌گونه‌ای طراحی شده که برای تایید تراکنش‌ها شبکه نیاز به دانستن اطلاعات هویتی کاربران ندارد. در بیت کوین هرکاربر با کیف پول خودش شناسایی می‌شود.

تراکنش‌های بیت کوین شفاف هستند یعنی هرکس که بخواهد می‌تواند یک تراکنش را پیگیری کند اما نه به این معنی که اطلاعات هویتی افراد مشخص شود و تنها می‌توان آدرس‌های هر کیف پول را مشاهده کرد.

با این حال صرافی‌های بیت کوین، برای جلوگیری از فعالیت‌های مجرمانه اقدام به احراز هویت از کاربران خود می‌کنند تا در صورت بروز هرگونه جرم با بیت کوین ها خریداری یا فروخته شده، بتوان آن را از طریق مراجع قانونی پیگیری کرد. به همین جهت بیت کوین روش خوبی برای جرائم یا پولشویی نخواهد بود.

- تغییرناپذیری

هنگامی که یک تراکنش بیت کوین انجام شود، دیگر قابل برگشت نیست. در سیستم‌های سنتی می‌توان تراکنش‌ها را دستکاری کرد اما زمانی که یک تراکنش در بیت کوین ثبت شد، آن تراکنش برای تمام اعضای شبکه ارسال می‌شود و به عنوان ثبت شده قرار می‌گیرد. از این رو دیگر هیچ کس نمی‌تواند آن تراکنش را برگشت بزند.

- بیت کوین (BTC) یک ارز دیجیتال است که به صورت الکترونیکی منتقل و استفاده می‌شود. بیت کوین یک ارز فیزیکی و لمس پذیر نیست نیست.
- بیت کوین یک شبکه همتا به همتا و غیرمتمرکز است که هیچ نهاد یا سازمان مرکزی آن را کنترل نمی‌کند.
- تعداد واحدهای بیت کوین محدود به ۲۱ میلیون واحد است و تنها ۲۱ میلیون واحد بیت کوین وجود خواهد داشت.

نحوه کار – فناوری زیرساختی و استخراج بیت کوین

بیت کوین روی یک پایگاه داده غیرمتمرکز به اسم بلاک چین فعالیت می کند. برای کسب اطلاعات بیشتر درباره بلاک چین می توانید به مقاله (فناوری بلاک چین چیست؟) مراجعه کنید اما به زبان ساده، بلاک چین یک دفترچه یادداشت دیجیتال است که اطلاعات می‌توانند روی آن به صورت توزیع شده و غیرقابل تغییر، ثبت شوند. این اطلاعات هر چیزی می‌توانند باشند اما در بیت کوین، اطلاعاتی روی بلاک چین ثبت می‌شوند، تاریخچه تراکنش‌ها هستند. تاریخچه تمام تراکنش‌های بیت کوین روی یک دفتر دیجیتال به نام بلاک چین ثبت می‌شود. هر کسی که به شبکه بیت کوین متصل می‌شود (که اصطلاحا نود – node نام دارد) یک کپی کامل از بلاک چین را دریافت می‌کند. هر تراکنشی که به بیت کوین ارسال می‌شود توسط این کامپیوترهای متصل به شبکه بررسی می‌شود و هر کامپیوتر به آن تراکنش رای می‌دهد. گروهی تراکنش را تایید می‌کنند و گروهی آن را غیرمعتبر می‌دانند. در نهایت با رای اکثریت مشخص خواهد شد که تراکنش معتبر است یا خیر.

اگر تراکنش توسط کامپیوترهای متصل به شبکه تایید شود روی برگه‌ای به نام بلاک ثبت می‌شود و سپس بعد از گذشت یک زمان مشخص، این بلاک‌ها به هم متصل می‌شوند و از بهم پیوستگی بلاک‌ها، بلاک چین (در معنای لغوی به معنای زنجیره‌ای از بلاک‌ها) پدید می‌آید.

استخراج بیت کوین چیست؟

از آنجا که بیت کوین یک ارز غیرمتمرکز است و برای ادامه بقا نیاز به توزیع و تایید تراکنش ها به صورت غیرمتمرکز دارد. استخراج یک نوع فرایند رقابتی است که در پروتکل بیت کوین به منظور ایجاد انگیزه برای پایداری شبکه و تولید بیت کوین جدید طراحی شده است. در این عملیات برای ثبت یک بلاک در بلاک چین، کامپیوترهای ماینر باید طی فرایند ریاضی پیچیده، معادلات ریاضی را حل کنند و هر کس که زودتر به جواب برسد، بیت کوین تولید شده و به عنوان پاداش به او تعلق می‌گیرد. این کار نیازمند داشتن سیستم‌های سخت افزاری قدرتمند و برق است.

به منظور حفظ شبکه و تاخیر در تولید واحدهای جدید بیت کوین، استخراج بیت کوین به مرور زمان سخت تر و سخت‌تر می‌شود و پاداش استخراج کم‌تر می‌شود. در حال حاضر هر ده دقیقه ۱۲.۵ بیت کوین تولید می‌شود. تاکنون بیش از ۱۷ میلیون واحد بیت کوین استخراج شده است. پیش‌بینی می‌شود که استخراج تمام واحدهای بیت کوین تا سال ۲۱۴۰ طول بکشد.

چه کسی بیت کوین را ساخته است؟

در اواخر سال ۲۰۰۸، ابتدا گزارش عملکرد (WhitePaper) بیت کوین ارائه شد و سپس در سال ۲۰۰۹ رسما شبکه بیت کوین آغاز به کار کرد. در گزارش عملکرد بیت کوین، نام مستعاری به نام ساتوشی ناکاموتو (Satoshi Nakamoto) به عنوان سازنده این پروتکل به چشم می‌خورد. با این وجود، اکنون که بیش از ۱۰ سال از تولد بیت کوین می‌گذرد، هنوز هویت واقعی ساتوشی ناکاموتو مشخص نیست و فقط یک سری حدس و گمان نه چندان معتبر درباره آن وجود دارد.

ساتوشی ناکاموتو می‌تواند یک فرد حقیقی، یک گروه برنامه نویسی، یک دولت یا هر چیز دیگری باشد. گفته می‌شود که در زمان ساخت بیت کوین، ساتوشی ناکاموتو در اولین روزهای استخراج این ارز دیجیتال برای خود حدود ۱ میلیون واحد بیت کوین برداشته است که با قیمت فعلی این ارز دیجیتال، رقم به شدت قابل توجهی است. با این میزان دارایی، اگر هویت او مشخص بود، امروزه به عنوان یکی از ثروتمندترین افراد جهان در نظر گرفته می‌شد.

چه چیزی ارزش بیت کوین را تعیین می‌کند؟

قیمت بیت کوین مانند هر کالا یا پول دیگری با عرضه و تقاضا بالا و پایین می شود. با افزایش تقاضا برای بیت کوین، قیمت آن هم افزایش می‌یابد و با کاهش تقاضا، از قیمت آن کم می‌شود. بیت کوین ها به تعداد محدود ۲۱ میلیون واحد وجود خواهند داشت به همین دلیل کمیابی آن نقش به‌سزایی در افزایش تقاضا دارد که با کمبود عرضه همراه است.

نوپایی بازار بیت کوین و عدم وجود قانون‌گذاری درست تا این زمان، موجب شده است تا این بازار به شدت پرنوسان و پرریسک باشد. نوساناتی که طی یک سال در بازار سهام رخ می‌دهد می‌توانند در یک روز برای بیت کوین انجام شود. همچنین امکان دستکاری مصنوعی در بازار بیت کوین وجود دارد که ریسک سرمایه‌گذاری را دو چندان می‌کند.

بیت کوین ها را در کجا ذخیره کنم؟

در بحث ارزهای دیجیتال برای ذخیره ارز نیازی به افتتاح حساب در بانک‌ها یا شرکت‌های متمرکز ندارید. در این فضا خودتان بانک خودتان هستید. یک کیف پول ارز دیجیتال، ابزاری برای ذخیره، ارسال و دریافت ارزهای دیجیتال است. کاربران بیت کوین می‌توانند از انواع مختلف کیف پول بیت کوین استفاده کنند.

برای بیت کوین نسبت به نیاز کاربران، انواع مختلف کیف پول وجود دارد. کیف پول‌های موبایل، کیف پول‌های دسکتاپ، کیف پول‌های تحت وب، کیف پول‌های کاغذی و کیف پول‌های سخت افزاری مهمترین انواع کیف پول هستند. کیف پول‌های موبایل، دسکتاپ، تحت وب و کاغذی رایگان هستند و کاربران می‌توانند آن‌ها را به راحتی دانلود و نصب کنند. اما کیف پول‌های سخت افزاری به دلیل فیزیکی بودن، باید خریداری شوند.

کلاینت و کیف پول رسمی بیت کوین، بیت کوین کور (Bitcoin Core) نام دارد که کاربران را مستقیما به بلاک چین بیت کوین متصل می‌کند. استفاده از این کیف پول نیازمند دانلود بیش از ۱۲۰ گیگ اطلاعات و مشخصات قدرتمند سخت افزاری است که برای کاربران تازه‌کار پیشنهاد نمی‌شود. در عوض گزینه‌های ساده‌تر و بسیار کم حجم‌تری برای کاربران تازه‌کار وجود دارد که پیشنهاد می‌شود از آن‌ها استفاده کنید. شما می‌توانید با مراجعه به سایت رسمی بیت کوین، معتبرترین کیف پول‌های بیت کوین را نسبت به دستگاه خود (موبایل، دسکتاپ یا تحت وب) به صورت رایگان دانلود و نصب کنید. برخی از نرم افزارهای کیف پول هم می‌توانند به صورت همزمان، چند ارز دیجیتال مختلف را ذخیره کنند.

توجه داشته باشید که تراکنش‌های بیت کوین بدون برگشت هستند و شبکه بیت کوین زیر نظر هیچ سازمانی قرار ندارند. به همین دلیل، حتما از کیف پول خود نسخه پشتیبان یا همان بک‌آپ تهیه کنید تا در صورت بروز هرگونه مشکل برای دستگاهی که کیف پول روی آن نصب است، بتوانید مبالغ خود را روی دستگاه دیگری بازیابی کنید. همچنین به هیچ عنوان رمزعبور یا کلید خصوصی کیف پول خود را در اختیار شخص دیگری قرار ندهید.

چگونه بیت کوین بخرم؟

خرید بیت کوین از سایت‌های فروشنده بیت کوین و یا به‌طور مستقیم از طریق افراد دیگر انجام می‌پذیرد. شما می توانید با روش‌های مختلفی مانند کارت‌های اعتباری، حساب‌های اینترنتی و یا حتی با سایر ارزهای دیجیتال، از سایت‌ها یا افراد حقیقی، بیت کوین خریداری نمایید.

برای خرید بیت کوین فرایند زیر را باید در نظر بگیرید:

- نصب کیف پول بیت کوین
- پیدا کردن فروشنده معتبر بیت کوین (سایت یا فرد حقیقی)
- انتقال پول به فروشنده و دادن آدرس کیف پول برای دریافت بیت کوین‌های خریداری شده (بعضی از سایت‌ها خودشان دارای کیف پول هستند)
- انتقال بیت کوین از فروشنده به کیف پول شما

بیت کوین قانونی است؟

تاکنون دولت های زیادی از جلمه ایران درباره بیت کوین موضوع روشنی از خود بروز نداده‌اند اما به صورت یک عرف، بیت کوین غیرقانونی نیست. بعضی از دستگاههای قضایی مانند چین و روسیه، ارزهای دیجیتالی را قانونی نمی‌دانند اما از نظر اجرایی عموم مردم می‌توانند از بیت کوین استفاده کنند. البته به دلیل ماهیت خاص بیت کوین، به احتمال زیاد در آینده قوانین جامعه برای این حوزه تعیین خواهد شد.

بیت کوین نوعی پول است و پول هم مانند کالاهای دیگر، می‌تواند برای فعالیت‌های مجرمانه مانند پولشویی یا خرید و فروش کالاهای غیرقانونی مورد استفاده قرار گیرد. با این حال پیگیری جرائم انجام شده با بیت کوین غیرممکن نیست. یکی از نمونه‌های موفق در این زمینه، کشور ژاپن است. در ژاپن که حجم معاملات میلیارد دلاری بیت کوین و ارزهای دیجیتال در آن صورت می‌گیرد، دولت توانسته با ثبت صرافی‌ها و ارسال بخشنامه‌های مالی به آن‌ها از بروز پول‌شویی و کلاهبرداری جلوگیری کند.

طبق تحقیقات موسسه بزرگ آسیا نیکی (Nikkei Asian)، پرونده‌های مشکوک به پول‌شویی مربوط به ارزهای دیجیتال در ژاپن، نسبت به پول‌شویی با ارزهای سنتی، مانند سوزنی در انبار کاه است. به گزارش این بنیاد، طبق آمار رسمی اداره پلیس ژاپن، از آوریل تا دسامبر ۲۰۱۷، صرافی‌های ارزهای دیجیتال، ۶۶۹ مورد مشکوک به پول‌شویی را گزارش داده‌اند. این در حالی که است که در سال ۲۰۱۷ جمعاً حدود ۴۰۰,۰۰۰ گزارش پول‌شویی با ارزهای رایج، توسط پلیس بررسی شده است.

در کشورهای زیادی از جمله ایران قوانین مشخصی برای بیت کوین تعریف نشده است اما استفاده از بیت کوین برای مردم تقریبا در هیچ جای جهان به عنوان جرم مشخص نشده است مگر در فعالیت‌های مجرمانه. در چند کشور مانند ایالات متحده، کره جنوبی، ژاپن ، هنگ‌کنگ و مالزی صرافی‌های بیت کوین به صورت قانونی و رسمی در حال فعالیت هستند. برای کسب اطلاعات بیشتر در مورد وضعیت قانونی بیت کوین در ایران می‌توانید به مقاله (بیت کوین در ایران قانونی است؟) مراجعه کنید. همچنین پیشنهاد می‌کنیم با مراجعه به بخش (امنیت) سایت ارزدیجیتال از راهکارهای حفظ امنیت در فضای ارزهای دیجیتال آگاهی یابید.

آیا بیت کوین هک می‌شود؟ امنیت بیت کوین چگونه است؟

از دیدگاه تئوری هر شبکه ای یک راه نفوذ وجود دارد که بیت کوین هم از این قاعده مستثنی نیست. روی کاغذ، هر نوع رمزنگاری قابل شکستن است. اما می‌توان گفت که هک کردن شبکه و دوبار خرج کردن در بیت کوین با توجه به گستردگی فعلی آن تقریبا غیرممکن است. شبکه اصلی بیت کوین تاکنون هک نشده است و دوبار خرج کردن تاکنون در بیت کوین اتفاق نیفتاده است و احتمالا این اتفاق تا ابد رخ نخواهد داد. کیف پول‌ها و صرافی‌های بیت کوین می‌توانند هک شوند و تا به حال چندین هک بزرگ در این زمینه رخ داده است اما خود شبکه بیت کوین تاکنون هیچگونه مشکلی از بابت امنیت نداشته است. این موضوع را می‌توان با اینترنت مقایسه کرد. هک شدن یک وب‌سایت روی اینترنت به معنای هک شدن خود اینترنت نیست.

چند راه محتلف برای هک کردن شبکه بیت کوین وجود دارد که مهمترین آن حمله ۵۱ درصد است. این حمله نیاز به تجهیزات ماینینگ قدرتمند دارد به طوری که بتوان بیش از ۵۰ درصد از قدرت پردازش شبکه را تصاحب کرد. به دلیل گستردگی شبکه بیت کوین و هزینه بالای حمله دوبار خرج کردن، هیچ انگیزه‌ای برای این کار وجود ندارد و می‌توان آن را تقریبا غیرممکن دانست.

قیمت بیت کوین

یکی از دلایل اصلی توجه مردم به بیت کوین، رشد قیمت شدید این ارز دیجیتال در طول عمر ۱۰ ساله خود بوده است. اگر در سال ۲۰۱۰ که قیمت هر واحد بیت کوین حدود ۱۰ سنت (۰.۱ دلار) ارزش داشت، معادل ۱,۰۰۰ دلار بیت کوین می‌خریدید، امروز بیش از ۴۰ میلیون دلار سرمایه داشتید. آگاهی عمومی درباره بیت کوین در سال ۲۰۱۷ که قیمت این ارز دیجیتال به ۲۰,۰۰۰ دلار رسید، تا حد بسیار بالایی افزایش یافت. با نگاهی به تاریخچه قیمت بیت کوین متوجه می‌شوید که در طول ۱۰ سال از پیدایش بیت کوین، این ارز دیجیتال همواره اوج‌گیری‌های بزرگی داشته و از سوی دیگر دچار سقوط‌های بزرگی هم شده است. از این رو سرمایه‌گذاران باید همواره در مقابل ریسک‌های زیاد سرمایه‌گذاری در بیت کوین آگاه باشند. مسائلی مانند شرایط قانون‌گذاری، کاربردی شدن (پذیرش)، مسائل فنی، دستکاری بازار، پاداش استخراج و ... می‌توانند باعث تغییرات قیمت بیت کوین شوند.

سگویت Segwit

بیت کوین به عنوان ارز دیجیتال پرسروصدای این روزها مشکلاتی دارد که از مهم‌ترین آنها می‌توان به مساله‌ی مقیاس‌پذیری (Scalability) اشاره کرد. در سال‌های اخیر راهکارهایی برای امکان افزایش سایز بلاک بیت کوین ارائه شده که از میان آنها می‌توان به سگویت و

یا Segregated Witness اشاره کرد. این سافت فورک بیت کوین در سال ۲۰۱۷ اجرا شد. مکانیزم آن به گونه‌ای بود که داده‌های مربوط به امضای دیجیتال را از داده‌های دیگر تراکنش‌ها جدا می‌کرد که در نتیجه‌ی این امر، فضای خالی در هر بلاک بیشتر شده و می‌توان تراکنش‌های بیشتری را روی آن ثبت نمود.

بیش از یک سال از فعال‌سازی فورک سگویت (SegWit) می‌گذرد، با این وجود تنها ۳۶ درصد از تمام تراکنش‌های بیت کوین واقعا از آن استفاده می‌کنند. چرا نرخ پذیرش آن تا این اندازه پایین بوده است؟ عمدتا به این علت که درست مانند هر بروزرسانی سازگار با نسخه‌های قدیمی (backward-compatible) یا به عبارتی سافت فورک دیگر، سگویت نیز به تمامی نودهای شبکه‌ی بیت کوین، حتی نودهایی که نرم‌افزار خود را به روز نکرده باشند نیز امکان می‌دهد شبکه را تحت قوانین محدود کننده‌ی مختصری دنبال کنند. در نتیجه، حتی با وجود مزیت کمتر بودن کارمزد آن به هنگام ارسال پرداخت‌های بیت کوین نیز، برخی از کسب‌وکارهای مبتنی بر بیت کوین و صرافی‌ها، آپدیت نرم افزار خود برای فعالسازی سگویت به تعویق انداخته‌اند.

برخی از شرکت‌های سرمایه‌گذاری خطرپذیر نیز اهمیت چندانی به پرداخت کارمزد بیت کوین نمی‌دهند. روستی راسل (Rusty Russell) توسعه دهنده‌ی بلاک چین از شرکت بلاک استریم (Blockstream) در این خصوص گفت: این شرکت‌ها (VCها)، می‌توانند در یک هفته، یک میلیون دلار را در تراکنش‌های بیت کوین از دست بدهند و واقعا کسی بدان توجه نمی‌کند و تنها چیزی که بدان توجه می‌شود، رقم‌های مربوط به پذیرش یک محصول بین کاربران است.

راسل، سوئیچ به سگویت برای بهینه‌سازی عملیات را تصمیمی در سطح مهندسی خوانده و پیشتر در ماه دسامبر در گزارش خود با کوین دسک اعلام کرده بود که با توجه به کاهش قابل توجه کارمزد تراکنش‌های بیت کوین از ابتدای سال ۲۰۱۸، اولویت امروز استارتاپ‌ها بهینه‌سازی در راستای پیشرفتشان بوده و پیاده‌سازی یک فناوری جدید چندان اهمیتی ندارد.

راسل و ارن لشر (Aaron Lasher)، مدیر استراتژی ارشد شرکت کیف پول بیت کوین BRD، هردو مظنون هستند که در صورت بالا رفتن قیمت بیت کوین، فشار برای پذیرش سگویت بر روی کسب و کارها بیشتر می‌گردد.

لشر در نوامبر گذشته به کوین دسک گفت: ما اکنون فشاری برای پیاده‌سازی سگویت احساس نمی‌کنیم چراکه تفاوت زیادی ایجاد نمی‌کند اما در دور بعدی افزایش قیمت بیت کوین، تفاوت زیادی را ایجاد خواهد کرد. نمی‌دانم این افزایش قیمت یک سال، سه سال و یا پنج سال بعد اتفاق می‌افتد اما کاملا مطمئن هستم که بالاخره اتفاق خواهد افتاد.

لشر تایید کرد که تغییر کد بکاِند برای شناسایی، ارسال و دریافت تراکنش‌های سگویت به هیچ وجه کار ساده‌ای نبوده است: جنبه‌های فنی زیادی وجود دارند که باید در نظر گرفته شوند. مساله، پول افراد است و در چنین مواقعی پیش فرض لازم این است که کاری انجام ندهید چراکه شبکه همچنان کار می‌کند و شما سرمایه‌ی مشتریان خود را به خطر نمی‌اندازید.

به گفته‌ی لشر، تایلر وینکلواس (Tyler Winklevoss)، مدیرعامل صرافی جمینی، در یک فروم پرسش و پاسخ مربوط به سایت ردیت (Reddit) در اوایل این ماه اعلام کرده بود که بازسازی کیف‌پول‌های این صرافی برای پشتیبانی از سگویت کار بسیار پرریسکی بود و نیاز به ساخت یک کیف پول گرم از ابتدا داشت. با اینکه خبر رسمی‌ای در این خصوص منتشر نشده اما وینکلواس قول داده که جابه‌جایی به سمت یک کیف پول جدید در سه ماه نخست امسال اتفاق خواهد افتاد.

راسل که به کسب و کارها و صرافی‌ها توصیه می‌کند پویا فکر کنند معتقد است هرچه این اتفاق زودتر بیفتد بهتر است. او به کوین دسک گفته است: صادقانه بگویم در زمانی که کارمزدها افزایش می‌یابند، اگر کسب و کارهایی وجود داشته باشند که از سگویت پشتیبانی نکنند، نارضایتی مردم از کارمزدها منجر به انتقال کسب وکارشان به بستر پلتفرم‌هایی می‌شود که از سگویت پشتیبانی می‌کنند.

انگیزه های استخراج کنندگان

پس از انتشار سگویت در آگوست ۲۰۱۷، اختلافات بنیادینی منجر شد تا حزب‌های رقیب، کاربردهای متفاوتی را برای نخستین ارز دیجیتال در جهان پیش‌بینی کنند. در حقیقت از سال ۲۰۱۷، بخشی از جامعه‌ی بیت کوین که آپدیت سگویت را رد کرده بود، تمرکز خود را بر روی یک ارز دیجیتال جایگزین به نام بیت کوین کش گذاشتند، (بیت کوین کش در زمان انتشار این مقاله در اثر انشعاب زنجیره، در برخی صرافی‌ها با نام‌های بیت کوین ABC و بیت کوین SV شناخته می‌شود)

با وجود آنکه شرکت‌های ماینینگ بیت کوینی وجود دارند که رسما به صورت واضح مخالفت خود را با آپدیت سگویت اعلام کردند، اما اقدام شرکت بیت مین غول سخت افزار دنیا و قرار دادن مشوق‌های مالی برای ماینرهایی که تراکنش‌های سگویت را تایید می‌کنند، امری انکارناپذیر است. حدود ۴۰ درصد از شبکه‌ی بیت کوین، سگویت را بر روی تراکنش‌های خود فعال کرده‌اند. این بدان معنی است که تراکنش‌هایی که عمدتا به دلایل ایدئولوژیکی تایید نمی‌شوند، مجموع پاداش‌هایی را که به ماینرها در ازای تایید یک بلاک جدید تعلق می‌گیرد را کاهش می‌دهد.

دیوید اشتینبرگ (David Steinberg)، معاون رئیس شرکت رندم کریپتو (Random Crypto)، شرکت تحلیلی‌ای که ماشین حسابی ساخته که قادر است سودآوری ماینینگ را نشان می‌دهد با اشاره به این مساله که اینها تفاوت‌های ایدئولوژیک هستند در مصاحبه‌ی قبلی خود با کوین دسک به بیان دیدگاه خود پرداخته است: سگویت چند قانون به بیت کوین اضافه کرده و یک قانون را حذف می‌کند. قانون حذف شده این است که شما فقط می‌توانید پولی را که صاحب آن هستید خرج کنید. البته این بدین معنا نیست که این قانون را اجرا نکند بلکه آن را به صورت متفاوتی اجرا می‌کند که بسیاری افراد از جمله من آن را از نظر امنیتی ضعیف‌تر می‌بینیم.

اشتینبرگ با لشر بر سر اینکه اختلاف نظرها بر سر سگویت، مساله‌ای نیست که مانع از پذیرش آن شده باشد، هم عقیده است. حداقل از نقطه‌ی قوت جامعه‌ی ماینینگ بیت کوین او اعتقاد دارد: دلیل منطقی‌تری که چرا ماینرها مایلند تراکنش‌های سگویت را رد کنند، ایسیک بوست (AsicBoost) است.

یک حدس خیلی خوب

ایسیک بوست که به عنوان یک حقه‌ی ریاضی شناخته می‌شود، یک میان افزار ماینینگ است که به ماینرهای بیت کوین امکان می‌دهد تا محاسبات ضروری برای ایجاد بلاک‌های جدید و تایید تراکنش‌های بلاک چین را را ۲۰ درصد سریع‌تر از سرعت متوسط انجام دهند.

این فناوری توسط تیمو هنک (Timo Hanke) و سرگیو دمیان لرنر (Sergio Demian Lerne) در سال ۲۰۱۴ به ثبت رسیده و به تازگی برای تمامی ماینرها تحت لایسنس DPL فراهم شده است. برای استفاده از این میان افزار بدون لایسنس، ماینرها می‌بایست از نسخه‌ی جایگزین این فناوری به نام (covert AsicBoost) استفاده کنند. نسخه‌ی جایگزین به علت نحوه‌ی درج شدن پرداخت‌ها و چینش مجدد بلاک‌ها با سگویت سازگار نیست. بدین ترتیب در اواخر اکتبر ۲۰۱۸، زمانی که استخر استخراج انت‌پول (Antpool) تراکنش‌های سگویت را تقریبا به مدت یک هفته حذف کرد، برخی هواداران جامعه بیت کوین به اتهامات خود علیه بیت مین شرکتی که Antpool را اداره می‌کند و تلاش او برای نصب مخفیانه این میان‌افزار اشاره کردند.

پیتر تاد (Peter Todd)، توسعه دهنده سابق هسته بیت کوین و مشاور رمزنگاری این را (عدم پذیرش سگویت به علت عدم پشتیبانی پلتفرم AsicBoost) یک حدس خوب دانسته و می‌گوید دلیل قطعی هنوز مشخص نیست. او در مصاحبه‌ی پیشین خود با کوین دسک اظهار کرد: شما می‌توانید راجع به آن فرضیه بسازید، شما واقعا نمی‌دانید. ماینرها ممکن است کاری بسیار متفاوت‌تر از آنچه که فکر می‌کنید انجام دهند و هر آن چیزی که می‌بینید تنها خروجی یک فرایند است.

اشتینبرگ همچنین اظهار داشت که به نظر او ، استفاده از هر نوآوری‌ای در این حوزه (ماینینگ)، در یک استخر استخراج و ماهیت غیرمتمرکز بیت کوین و بلاک چین، عادلانه خواهد بود. او در این خصوص می‌گوید: پردازنده‌های جدیدتری از ساخت تراشه‌ها به وجود می‌آیند و مردم با نحوه‌ی کار این تجهیزات آشناتر می‌شوند و من فکر می‌کنم این مزیت‌ها (AsicBoost و غیره) کاملا منصفانه هستند.

انواع سگویت

با توجه به تعداد روزافزون تراکنش‌های سگویت، به نظر نمی‌رسد تراشه‌های covert AsicBoost و نوآوری‌های سخت‌افزاری دیگری که با سگویت سازگار نیستند، برای ماینرها سودآور باقی بمانند.

راسل توسعه‌دهنده‌ی بلاک استریم (blockstream)، پذیرش انبوه سگویت را به عنوان یک حقیقت کند اما اجتناب‌ناپذیر قبول داشته و در این خصوص به کوین دسک اینچنین توضیح می‌دهد: این تکنولوژی در ظرف ۱۰ تا ۲۵ سال آینده توسعه می‌یابد و هنوز برای پذیرش سگویت زود است.

لشر و دیگر مدیران BRD در سپتامبر گذشته، وبسایتی را با عنوان WhenSegwit راه‌اندازی کرده که نامه‌ای متن‌باز برای افرادی که به بیت کوین علاقه دارند در آن نوشته شده است. در این نامه از کسب وکارها و کاربران خواسته شده تا سرویس‌های بهینه‌سازی سگویت را اولویت‌بندی کرده و پذیرش آن را به ۱۰۰ درصد برسانند. لشر پذیرش کند سگویت را مشکلی انگیزشی دانسته و به کوین دسک می‌گوید که هدف اصلی سایت WhenSegwit، ترویج پذیرش بهترین نسخه‌ی سگویت است. با توجه به اینکه سگویت بر روی سایز تراکنش‌ها تاثیر می‌گذارد، کسب و کارها و صرافی‌ها باید به نحوی نرم‌افزار خود را به روز رسانی کنند که کاربران بتوانند تراکنش‌هایی را که سگویت در آنها فعال است از یک رشته‌ی ۲۶ الی ۳۵ کاراکتر شامل حروف و اعداد ارسال و یا دریافت نمایند.

این کار به دو طریق امکان‌پذیر است، نخست به روزرسانی قدیمی‌تری که از سال ۲۰۱۲ تاکنون در دسترس بوده و P2SH نام دارد. به روزرسانی P2SH در حقیقت به عنوان روشی برای فشرده‌سازی پرداخت‌ها در شرایط پیچیده در نظر گرفته شده بود که به تراکنش‌های بیت کوین متصل می‌شد بود اما بعدا توسعه‌دهندگان طوری آن را تغییر دادند که برای اطمینان از قابلیت همکاری بین آدرس‌هایی است که از تراکنش‌های سگویت پشتیبانی نمی‌کنند و آدرس‌هایی که از سگویت پشتیبانی می‌کنند به کار رود. نسخه‌ی دیگری که لشر آن را نسخه‌ی بهتر سگویت می‌نامد منحصرا، با کسب و کارها و کاربرانی که نرم افزار خود را برای خواندن یک آدرس با فرمت سگویت آپدیت کرده باشند، سازگار است. این نسخه توسط توسعه‌دهندگان بیت کوین ،پیتر وول (Pieter Wuille) و گریگ مکسول (Greg Maxwell) مدیر ارشد فناوری شرکت بلاک استریم توسعه یافته و Bech32 نام دارد.

با زبان سگویت سخن بگویید

Bech32 کمی پیچیده است. به گفته‌ی بیت کوین ویکی تا زمانی که نرم‌افزارهای بیشتری از آن پشتیبانی کنند، استفاده از آن پیشنهاد نمی‌شود. این نسخه، پیاده‌سازی سخت‌تری از سگویت بوده و از P2SH، کاراتر است. این بدین علت است که بر خلاف Bech32، که درفوریه گذشته پیاده‌سازی شد، P2SH بروزرسانی‌ای در سال ۲۰۱۲ با هدف باز طراحی پروژه‌ای بود که ذاتا برای پشتیبانی از سگویت ایجاد نشده بود. P2SH تراکنش‌ها را در مقایسه با Bech32 در مدل غیرمستقیم‌تری پردازش می‌کند.

راسل در این خصوص توضیح می‌دهد: استفاده از Bech32 می‌تواند خیلی راحت‌تر باشد. در این صورت دیگر به P2SH برای استفاده از سگویت نیازی ندارید. این خیلی بهینه‌تر است. وگرنه زمانی که از P2SH استفاده می‌کند، گام اضافه‌تری به مراحل شما افزوده می‌شود.

لشر معتقد است ناسازگاری Bech32 با برنامه‌های پیشین (backward-incompatibile) مثبت بوده و صرافی‌ها و کسب و کارها را وادار می‌کند تا نرم‌افزارشان را به روزرسانی کنند.

لیشر می‌گوید: تصور کنید که یک صرافی هستید و نیمی از مشتریان فقط به شما این آدرس عجیب (Bech32) را داده و هیچ چیز دیگری نمی‌دهند. آنها می‌گویند اگر کسب و کار آنها را میخواهید باید از Bech32 پشتیبانی کنید. در این صورت شما حاضر هستید این کار را انجام دهید.

لشر این فرآیند را مانند یادگیری یک زبان جدید همچون یونانی دانسته و اینچنین استدلال می‌کند: چالش ناسازگاری در جایی که هر فردی نیاز دارد یاد بگیرد یونانی صحبت کند مشابه چالشی است که از پذیرش سگویت به صورت گسترده جلوگیری می‌کند.

او در انتها نتیجه گرفت: همه می‌دانند که باید اینکار را انجام دهند (آپدیت سگویت) اما اینکه شما اولین نفری باشید که اینکار را انجام می‌دهد هیچ کمکی به شما نمی‌کند. علاقه شما به این است که نفر آخری باشید که این کار را انجام می‌دهید.

شبکه لایتنینگ Lightning Network

به دلیل این که بلاکچین ها، کند هستند. و درنتیجه، پرهزینه. اگر تعدادی بیت کوین ارسال شود، چندین ساعت بعد آن ها دریافت خواهند شد و هزینه ی بسیار سنگینی (کارمزد) برای تراکنش پرداخته می شود پس بلاک چین ها با چنین شهرت و اعتباری، چگونه جهان را تصاحب خواهند کرد؟ هر ایده ای که بتواند مشکل مقیاس پذیر نبودن بلاکچین ها را حل کند، ارزش توجه، زمان گذاشتن بر روی آن و تلاش را دارد. Lightning Network یکی از این ایده هاست. اما قبل از این که این راه حل را درک کنیم، باید ابتدا مشکل را درک کنیم. اگر از مشکل آگاهی دارید پس می توانید مستقیماً به بخش بعدی بروید.

شبکه لایتنینگ (LN) دومین لایه موجود بر شبکه بلاک چینی بیت کوین است. گفته می شود که این شبکه در تحول بیت کوین نقش مهمی را ایفا می کند. زمانی که لایتنینگ در سرتاسر شبکه و بر تمام نودها (nodes) گسترش پیدا کند، سرعت پردازش تراکنش ها در شبکه افزایش پیدا کرده و کارمزد انجام هر یک کاهش می یابد.

از ابتدای سال میلادی جاری، سرعت اجرا و گسترش این فناوری افزایش یافته است. در زمان نوشتار این مقاله ۹۷۷ نود، در حال اجرای ۱۸۲۷ کانال در شبکه لایتنینگ بودند. (بر اساس آمار bitnodes.earn.com در آن زمان تقریبا ۱۱۸۱۰ نود در شبکه موجود بود.) علی رغم تعداد کم نودهای لایتنینگ، نشریات از این فناوری به عنوان ناجی بیت کوین یاد کرده اند. باید در انتظارات بالای خود تجدید نظر کنیم. این فناوری با توجه به استانداردهای موجود، همچنان در ابتدای راه، در حال توسعه، و در دست تعمیر است!

تادوس دریجا، در نگارش وایت پیپر اصلی شبکه لایتنینگ همکاری کرده است. او در مصاحبه ای با Investopedia گفته است که لایتنینگ هنوز آمادگی کافی این را ندارد که در سطوح گسترده مورد استفاده قرار بگیرد. به گفته تادوس دریجا، مفهوم شبکه لایتنینگ تا حد زیادی اثبات شده است، اما او فعلا قصد ندارد از این فناوری به طور گسترده در سطح بلاک چین بیت کوین استفاده کند.

چرا بلاکچین ها کند هستند؟

یک بلاکچین را به صورت یک رجیستر (ثبت شده) در نظر بگیرید. این رجیستر شامل صفحات (بلوک های) متعددی است که هر صفحه دارای تراکنش های متعددی است. به محض این که صفحه با تراکنش ها پر شد، باید قبل از شروع به ثبت و ضبط تراکنش ها در صفحه ی بعد، به رجیستر اضافه شود. قبل از این که صفحه (بلوک) بتواند به رجیستر (زنجیره) اضافه شود، پردازش هایی باید انجام شود تا اطمینان حاصل شود که همه با محتویات داخل آن، موافق هستند. این فرآیند برای هر بلوک، حدوداً ۱۰ دقیقه (برای بلاکچین بیت کوین) طول می کشد. تصور

کنید، شما ۱ بیت کوین (BTC) برای دوستتان به نام حامد ارسال می کنید. این تراکنش، چیزی شبیه به این روند است. در میان سایر موارد، یک تراکنش حاوی اطلاعاتی درباره فرستنده، گیرنده، مبلغ و کارمزد تراکنش است.

کارمزد تراکنش

بله، یک هزینه ی اضافی به نام کارمزد وجود دارد. شما می توانید این کارمزد را پرداخت کنید تا ماینرها تشویق شوند تراکنش شما را هر چه سریع تر در یک بلوک قرار دهند. هیچ قیمت مشخصی برای کارمزد وجود ندارد و کاملاً به خود شما بستگی دارد که حاضر هستید برای سرعت بخشیدن به روند، چه مبلغی بپردازید. به ازای کارمزدهای بالاتر، تراکنش شما سریع تر انجام خواهد شد. در هر لحظه از زمان، تراکنش های متعددی وجود دارند که باید در صفحه ی فعلی ثبت شوند.

ماینرها، یعنی کامپیوترهایی که در حال کار در شبکه ی بلاکچین هستند، باید تصمیم بگیرند که کدام یک از تراکنش های موجود باید در بلوک فعلی قرار گیرند. آن ها برای تصمیم گیری بهتر، نگاه می کنند ببینند کدام یک از تراکنش ها انعام بیشتری می پردازند، یعنی تراکنش های با کارمزد بالاتر، اول انجام می شوند. اگر تراکنش های با کارمزد بالاتر از کارمزدی که شما می خواهید بپردازید به اندازه ی کافی وجود داشته باشد که بلوک را پر کند، تراکنش شما در صف در حالت انتظار می ماند. این انتظار ممکن است از حداقل چند دقیقه باشد تا چندین ساعت، و در برخی مواقع، چندین روز. هرچه کارمزد بیشتری بپردازید، تراکنش شما سریعتر پردازش می شود. به همین دلیل بلاکچین ها برای افرادی که می خواهند آغاز به کار کنند، کُند و در نتیجه پرهزینه هستند. در حالت ایده آل، پذیرش بلاکچین به این معنی خواهد بود که تراکنش های بیشتری انجام شوند، اما با بالا رفتن تعداد تراکنش ها، شبکه، کند می شود و این خود مانعی برای پذیرش می گردد. چه تناقضی! شبکه ی لایتنینگ (LN) یک راه حل بالقوه برای این مشکل است.

شبکه ی لایتنینگ (Lightning Network) چیست؟

(Lightning Network یا شبکه ی صاعقه، به دلیل سرعت بالای انجام تراکنش ها در آن به این عنوان نامیده شده) ایده ی نهفته در پس LN این است که نیازی نیست تمام تراکنش ها در بلاکچین ، ثبت شوند. تصور کنید من و شما چندین بار میان خودمان داد و ستد داشته ایم. در چنین موردی، می توانیم از ثبت تراکنش ها بر روی بلاکچین صرف نظر کرده و آن ها را خارج از زنجیره انجام دهیم. به بیان ساده تر، نحوه ی کار بدین صورت است، ما چیزی به نام یک کانال پرداخت(payment channel) میان خودمان باز می کنیم و بازگشایی کانال را در بلاکچین ، ثبت می کنیم. اکنون، من و شما می توانیم هر چند بار که بخواهیم از طریق این کانالِ پرداخت، با هم داد و ستد کنیم و این کانال می تواند برای ساعت ها، روزها، هفته ها یا حتی دهه ها باز بماند. تنها زمانی که ما مجدداً با بلاکچین سروکار داریم، زمانی است که بخواهیم کانال را ببندیم. سپس، وضعیت نهایی تراکنش هایی که از طریق این کانال بر روی بلاک چین انجام شده اند را ثبت می کنیم. با استفاده از ایده ی کانال پرداخت، می توانیم شبکه ای از کانال های پرداخت اینجاد کنیم به گونه ای که به ندرت نیاز باشد تراکنشی بر روی بلاکچین انجام شود. فرض کنید، سه نفر به نام های سارا، حامد و سعید وجود دارند. اگر حامد و سارا یک کانال پرداخت باز شده میان خودشان و سارا و سعید نیز یک کانال پرداخت باز شده میان خودشان داشته باشند پس حامد می تواند از طریق سارا برای سعید پول ارسال کند. فرض کنید حامد بخواهد ۲ بیت کوین برای سعید ارسال کند، سارا ، ۲ بیت کوین به سعید ارسال می کند و حامد ، ۲ بیت کوین به سارا بازپرداخت می کند (جبران می کند). ایده ی نهفته در پس شبکه ی لایتنینگ، این است. به دلیل این که شما اغلب با بلاکچین سروکار ندارید، تراکنش ها، بسیار بسیار سریع (به سرعت برق) انجام می شوند. از آنجا که احتمالاً تاکنون تمام وقایع سحرآمیزی که در کانال های پرداخت رخ می دهند را حدس زده اید. پس بیایید، ترفند سحرآمیزی را بیاموزیم.

کانال های پرداخت، چیستند؟

این کانال ها مانند یک گاوصندوق هستند که دو نفر مبلغ یکسانی را در آن گذاشته اند و هر کدام یک قفل به آن می زنند. این سپرده گذاری مبالغ یکسان در یک صندوق مشترک، در بلاکچین به صورت یک "تراکنش بازگشایی"(Opening Transaction) ثبت می شود و پس از آن یک کانال پرداخت میان این دو نفر باز می شود. ایده ی نهفته در پس قفل زدن به چنین صندوقی این است که هیچکس نتواند پول موجود در صندوق را بدون اجازه ی دیگری خرج کند. پس پول موجود در این صندوق برای داد و ستد میان یکدیگر مورد استفاده قرار می گیرد. فرض کنید، حامد و سارا هر کدام ۱۰ بیت کوین در یک صندوق مشترک ذخیره می کنند. حالا، اگر حامد بخواهد ۲ بیت کوین برای سارا ارسال کند، چگونه می تواند این کار را انجام دهد؟ برای انجام این کار، حامد تعهد می دهد مالکیت دو بیت کوین اش که در صندوق مشترک موجود است را به سارا واگذار کند. پس از این انتقال تعهد مالکیت، اگر صندوق باز باشد (قفل نباشد)، حامد قادر خواهد بود ۸ بیت کوین از صندوق بردارد و سارا نیز می تواند، ۱۲ بیت کوین مطالبه کند.

اما آن ها، درِ صندوق را باز نخواهند کرد زیرا می خواهند به داد و ستدهای میان خودشان ادامه دهند. زیبایی این شبکه در همین نظم و ترتیب اش است. حالا، اگر در روز بعد، سارا ، ۱ بیت کوین برای حامد ارسال کند می تواند همان کار را انجام دهد یعنی تعهد دهد مالکیت ۱ بیت کوین خودش را به حامد واگذاری می کند. پس از انجام این دو تراکنش، اگر صندوق، باز شده باشد، حامد می تواند ۹ بیت کوین و سارا نیز ۱۱ بیت کوین مطالبه کند

به طور خلاصه، کانال پرداخت، چیزی نیست جز تلفیق شریک شدن با یکدیگر و سپس واگذاری تعهد مالکیت پول های جمع آوری شده به نحوی که توافق شده است. در صورتی که حامد یا سارا بخواهند کانال را ببندند، می توانند این کار را انجام دهند. مفهوم بستن کانال نیز به سادگی گشودن صندوق و دریافت پول داخل آن است. بازگشایی صندوق، دربلاکچین اتفاق می افتد و این چه کسی مالک چه مبلغی از موجودی صندوق است، به صورت پیوسته و تا ابد ثبت می شود.

نحوه ی کار کانال های پرداخت بدین نحو بود. اما این، حتی به تعریف پتانسیل واقعی آن ها هم نزدیک نیست. نیرو و قدرت واقعی آن ها هنگامی که دو یا تعداد بیشتری کانال پرداخت به صورت یک شبکه- Lightning Network- با هم کار کنند، آزاد می شود.

پس متوجه شدید این شبکه در حقیقت چگونه کار می کند؟

LN به وسیله ی انتقال ارزش مالک بیت کوین ها به تعهدنامه ی مالکیت بیت کوین ها، کار می کند. این تغییر، بسیار بزرگ است. مثل همیشه، برای درک این موضوع از مثال استفاده می کنیم. فرض کنید سه نفر به نام های حامد، سارا و سعید وجود دارند به گونه ای که یک کانال پرداخت میان حامد و سارا و کانال پرداخت دیگری میان سارا و سعید وجود دارد. توجه داشته باشید که حامد و سعید هیچ کانال پرداختی بین خودشان ندارند. در چنین وضعیتی، اگر حامد بخواهد ۲ بیت کوین برای سعید ارسال کند، می تواند از کانال پرداخت میان سارا و سعید استفاده کند. این کار چطور انجام می شود؟ حامد از سارا می خواهد انتقال ۲ بیت کوین به سعید از طریق کانال پرداخت سارا-سعید را متعهد شود و سپس او(حامد) ۲ بیت کوین به سارا از طریق کانال حامد-سارا ، بازپرداخت می کند.

به وسیله ی چنین شبکه ای متشکل از کانال های پرداخت، بخش عظیمی از تراکنش ها را می توان از بلاکچین خارج کرد تا خارج از زنجیره انجام شوند، در نتیجه، فضای پهنای باند زنجیره، آزاد می شود. با استفاده از شبکه ی کانال های پرداخت، میلیون ها تراکنش و حتی خیلی بیشتر از آن می توانند بدون پرداخت هزینه های تراکنش (کارمزد) سنگین انجام شوند.

مشکلات شبکه لایتنینگ

۱- مشکل کارمزد تراکنش‌های بیت کوین را کاملا حل نمی‌کند

معمولا از لایتنینگ به عنوان یک راه حل یاد می شود. راه حلی که می تواند مشکل افزایش هزینه انجام تراکنش ها در شبکه بیت کوین را رفع کند. طرفداران و دنبال کنندگان این ارز دیجیتال می گویند که کارمزد تراکنش‌ها با کندی و شلوغی شبکه رابطه مستقیم دارد و زمانی کاهش پیدا می‌کند که تراکنش‌ها خارج از بلاک چین اصلی، انجام شوند. اما شلوغی شبکه بیت کوین تنها یکی از چند عاملی است که در کارمزد تراکنش ها تاثیر دارند. علاوه بر این، کارمزد تراکنش های بیت کوین، به خودی خود مولفه بزرگی از هزینه های کلی در شبکه لایتنینگ است. به بیان دقیق تر، هزینه های کلی در شبکه لایتنینگ به دو بخش تقسیم می شوند: بخش اول شامل هزینه هایی است که با کارمزد تراکنش های بیت کوین برابرند و به باز و بسته شدن کانال ارتباطی بین اشخاص تخصیص داده می شوند. علاوه بر آن، یک هزینه روتینگ جداگانه هم به انتقال پرداخت ها میان کانال ها تعلق می گیرد. در حال حاضر این هزینه دومی در حد صفر است، زیرا نود (node)های کمی از لایتنینگ استفاده می کنند. بنابر پیش بینی تادوس دریجا این هزینه برای یک مدت زمان طولانی پایین خواهند ماند، چرا که شبکه لایتنینگ کاملا مقیاس پذیر است.

با این حال به گفته او، احتمال افزایش کارمزدهای بیت کوین به دلایلی فراتر از حد شبکه لایتنینگ وجود دارد: ممکن است کارمزدهای بیت کوین دوباره افزایش پیدا کند، و میزان اتخاذ شبکه لایتنینگ در میان تریدرها با کاهش روبرو شود.

او در ادامه گفته است: این مشکل با رویکردی که در دیگر ارزهای دیجیتال برای افزایش کاربرد لحاظ شده، در تضاد است. برای نمونه،ارز دیجیتال دَش پلاگین های نرم افزاری رایگانی را در اختیار کاربرانش قرار می دهد. به گفته مدیر عامل این شرکت، ویژگی غیر انتقاعی مذکور برای تریدرهایی که از دش به عنوان یک روش پرداختی استفاده کنند، هزینه های ناشی از انجام این کار را جبران می کند.

۲- نودهایی که همواره آنلاین هستند، حساس‌ترند.

نودها (node) در شبکه لایتنینگ بیت کوین باید همیشه آنلاین باشند تا پرداخت ها را ارسال و دریافت کنند. ذخیره سازی سکه ها در فضای سرد، یکی از امن ترین روش های نگه داری ارز دیجیتال است. البته، استفاده از این روش در شبکه لایتنینگ امکان پذیر نیست. به گفته برخی از افراد، الزام حضور مداوم در شبکه، آنها را بیشتر در معرض هک و دزدی قرار می دهد. در شبکه لایتنینگ آفلاین بودن هم مشکلات خاص خودش را دارد. دریجا می گوید ممکن است یکی از طرفین معامله در زمان نبود طرف مقابل خود کانال پرداختی را بسته و سرمایه را به جیب بزند. به این کار، بستن متقلبانه کانال پرداختی گفته می شود. البته برای بسته شدن هر کانال یک وقفه زمانی در نظر گرفته می شود، اگر فرد مقابل تا پایان آن بازه زمانی تعیین شده آنلاین نشود، کانال به طور خودکار بسته می شود.

موقعیت آفلاین می تواند شبکه را نیز از دسترس خارج کند. به گفته مدیر عامل دش بزرگترین مشکل شبکه لایتنینگ این است که سرمایه به طور فزاینده ای در میان چند نود خاص در شبکه متمرکز شده است. به بیان دقیق تر، در صورتی که یکی از نودهای شبکه لایتنینگ آفلاین بشود، سرمایه کاربران توقیف می شود. یک قطعی ساده در سرور، می تواند به طور قابل ملاحظه ای در سرتاسر شبکه اختلال ایجاد کرده، و باعث شود سرمایه کاربران برای مدت چند روز غیر قابل پرداخت یا به اصطلاح frozen باقی بماند.

۳- ممکن است نتواند مشکلات ناشی از تاثیرات شبکه بیت کوین را حل کند.

شبکه لایتنینگ به بیت کوین در انجام تراکنش های روزانه هم کمک می کند. بیت کوین می تواند در تراکنش های روزانه مورد استفاده قرار بگیرد. کاربران می توانند با شرکت ها یا افرادی که معمولا با آنها معامله می کنند، یک کانال پرداختی باز کنند. یعنی مثلا با صاحب خانه خود، یا فروشگاه اینترنتی محبوبشان یک کانال پرداختی ایجاد کرده و از طریق آن با استفاده از بیت کوین به معامله بپردازند. اما هنوز برای تحقق این مساله، یک راه طولانی در پیش روی بیت کوین است. طی چند ماه اخیر حجم معاملات بیت کوین به دلیل افزایش حجم تراکنش ها بالا رفته و شاهد یک رشد قابل توجه بوده است. بدین ترتیب، تاثیر کلی شبکه لایتنینگ در کاهش کارمزدهای شبکه بیت کوین، احتمالا محدود است.

دکتر گریک هایلمن، اقتصاددان و بنیان گذار Mosaic (یک ارز دیجیتال برای ایجاد انگیزه در تحقیقات علمی) در این خصوص گفته است: حتی اگر شبکه لایتنینگ سرعت انجام تراکنش ها را افزایش بدهد، باز هم یک سوال مطرح است: این شبکه در چه حد قابل استفاده است؟

او در ادامه می گوید: نوسانات قیمتی بازار بیت کوین نسبت به دارایی های دیگر تقریبا بیشتر است، بنابرین احتمال آن کمتر است که مردم پول کرایه خانه شان را در قالب بیت کوین نگهداری کنند.

به گفته هایلمن، مشکل دیگر بیت کوین این است که در حال حاضر تنها عده کمی از افراد هستند که در قالب ارز دیجیتال حقوق می گیرند. افراد بیشتر به ارزهای دیجیتال به چشم یک نوع سرمایه گذاری نگاه می کنند تا پول رایج.

شبکه لایتنینگ چطور بیت کوین را تغییر می‌دهد؟

آیا مشکلاتی که تا اینجا به آن اشاره شد، پیشاپیش شکست شبکه لایتنینگ را به ما نشان می دهند؟ نه کاملا. مشکل ارزیابی های کنونی لایتنینگ، ناقص بودن آنها است. به گفته دریجا، این تصور که شبکه لایتنینگ یک روز جایگزین ویزا خواهد شد و در سرتاسر جهان گسترش پیدا خواهد کرد، اشتباه است: اگر قرار باشد یک میلیارد نفر به طور همزمان از این فناوری در تراکنش های روزمره خود استفاده کنند، کارمزدها به سرعت سر به آسمان می گذاشتند. او می گوید که شبکه لایتنینگ در حل مشکل مقیاس پذیری بیت کوین نقش مهمی دارد، اما در عین حال به چیزهای دیگری مثل SegWit، و امضای دیجیتال Schnorr هم احتیاج است.

در این میان، تیم توسعه این فناوری کاربردهای تازه ای را به شبکه افزوده و مشغول جستجوی ویژگی های تازه دیگری است. یک نمونه از موارد استفاده دلگرم کننده ای که قرار است در شبکه پدیدار شود، مربوط بهصرافی ارزهای دیجیتال است. طبق گفته های دریجا، کانال های پرداختی لایتنینگ می توانند در خدمت تسهیل ترید های میکرو میان صرافی ها باشند. (به جای پرداخت های میکرو در تراکنش های روزمره) بدین ترتیب، کاربران می توانند با استفاده از اکانت های مجهز به فناوری لایتنینگ، در صرافی های سرشناسی مثل Coinbase و Kraken، اقدام به خرید و فروش ارز دیجیتال کنند.

تحقیقات دیگر بر روی پر کردن شکاف های موجود در سیستم حاضر متمرکز است. برای نمونه، می توانید به نودهای دیگر نشان بدهید که طرف مقابلتان دروغ گفته و با این کار از بسته شدن متقلبانه کانال پرداختی جلوگیری کنید. اگر آن ها حرف شما را باور کنند، تمام سکه های موجود در کانال به شما واگذار خواهد شد. در صورتی که یک نود در شبکه آفلاین شود نیز نودهای دیگر از کانال پرداختی مراقبت خواهند کرد تا تقلبی رخ ندهد. درست مثل یک (برج مراقبت)!

نتیجه گیری

شبکه لایتنینگ یک مفهوم امیدوار کننده است و در بلاک چین بیت کوین تغییر بسزایی را به وجود خواهد آورد. اما لایتنینگ، یک گلوله نقره ای نیست، که بتوانیم با استفاده از آن مشکلات فعلی بیت کوین را ریشه کن کنیم. (اشاره به سریال supernatural، که در آن برای مقابله با افسونگری و سایر هیولاها از گلوله نقره ای استفاده می کردند) و حتی ممکن است منجر به بروز مشکلات جدیدی در اکوسیستم این ارز دیجیتال بشود. حل مشکلات حاضر تا حد زیادی به پیشرفت قابلیت های لایتنینگ و توسعه تحقیقاتی بستگی دارد که در حوزه آن شکل می گیرند.

نخستین خرید با بیت کوین

اتریوم Ethereum

وب‌سایت رسمی اتریوم آن را اینگونه تعریف می‌کند: اتریوم یک پلتفرم غیرمتمرکز است که قراردادهای هوشمند را اجرا می‌کند: هیچ‌گونه احتمال از کارافتادگی، سانسور، تقلب یا دخالت افراد شخص ثالث برای برنامه‌هایی که روی اتریوم اجرا می‌شوند، وجود ندارد.

در ساده ترین جمله، اتریوم یک پلتفرم آزاد مبتنی بر فناوری بلاک چین است که توسعه دهندگان را قادر می سازد تا برنامه های غیرمتمرکز خود را روی آن پیاده سازی کنند. این برنامه‌ها تحت کنترل و نظارت هیچ سازمان و نهادی نخواهند بود و تراکنش‌ها و معاملات روی اتریوم به صورت کاملا مستقل از بانک‌ها یا نهادهای دیگر پولی انجام می‌شوند. ارز دیجیتال این شبکه هم اتر نام دارد و واحد اختصاری آن ETH است.

هر کسی قادر است با استفاده از اتریوم برنامه غیرمتمرکز خود را توسعه دهد. همچنین توسعه دهندگان می‌توانند بدون نیاز به ساخت بلاک چین جدید، با استفاده از اتریوم برای برنامه‌های خود ارز دیجیتال مستقل بسازند که به آن‌ها توکن می‌گویند. در واقع توکن، ارز برنامه‌های غیرمتمرکزی هستند که خودشان بلاک چین خصوصی ندارند و از بلاک چین های دیگر مثل اتریوم استفاده می‌کنند. تا قبل از پیدایش اتریوم، برنامه‌نویسان بلاک چین برای ساخت ارز دیجیتال خود از ابتدا مجبور به ساخت یک بلاک چین جداگانه بودند اما امروزه بلاک چین اتریوم میزبان هزاران هزار توکن است.

تیم اتریوم دلیل ساخت این شبکه را اینگونه عنوان می‌کنند: اتریوم ایجاد شد تا ما برای انجام کارهایمان به هیچ بانک، شرکت و نهاد دیگری به جز خودمان نیاز نداشته باشیم. هدف اتریوم تبدیل شدن به یک کامپیوتر جهانی است. یک کامپیوتر برای همه کارها

تفاوت‌های بیت کوین و اتریوم

آیا اتریوم شبیه بیت کوین است؟ هم بله هم نه. اتریوم هم مانند بیت کوین می‌تواند به عنوان ارز دیجیتال دسته‌بندی شود، مورد معامله قرار بگیرد و آن را به عنوان روش پرداخت پذیرفت اما اتریوم تفاوت‌های زیادی با بیت کوین دارد. مانند بیت کوین، اتریوم هم یک بلاک چین توزیع شده عمومی دارد. اگر چه تفاوت های فنی زیادی بین این دو وجود دارد اما مهمترین تفاوت، اهداف و قابلیت هاست.

در واقع بیت کوین برای اولین بار با هدف یک سیستم پرداخت جهانی، همتا به همتا و غیرمتمرکز خلق شد اما اتریوم به دنبال حذف تمرکز از تمام فرایندهاست. در حالی که بلاک چین بیت کوین برای رهگیری مالکیت پول دیجیتال (بیت کوین) استفاده می‌شود، بلاک چین اتریوم برای اجرای کد برنامه‌های غیرمتمرکز طراحی شده است. اتریوم هم مانند بیت کوین مبتنی بر الگوریتم اجماع اثبات کار یا همان ماینینگ (استخراج) بوده اما قرار است که سمت به اثبات سهام حرکت کند. در اثبات سهام، ماینینگ صورت نمی‌گیرد و افراد بر اساس میزان دارایی خود در شبکه، به تایید تراکنش‌های می‌پردازند و پاداش دریافت می‌کنند.

در حالی که تعداد واحدهای بیت کوین محدود به ۲۱ میلیون واحد است برای اتریوم هنوز سقف مشخصی تعیین نشده است اما احتمالا در ادامه مسیر سقف تعداد کوین تعیین خواهد شد یا حداقل برای آن حد تولید سالانه در نظر گرفته می‌شود تا تورم آن کنترل شود. سرعت تراکنش‌های اتریوم به مراتب سریع‌تر از بیت کوین است و به مراتب کارمزد کمتری نسبت به بیت کوین دارد. نمی‌توان به طور دقیق گفت که بیت کوین بهتر است یا اتریوم زیرا این دو شبکه اهداف یکسان ندارند و هر کدام کاربرد و ویژگی منحصر به فرد خاص خودش را دارد.

مزایای پلتفرم‌های غیرمتمرکزی مانند اتریوم چیست؟

از آنجا که برنامه های غیرمتمرکز در بلاک چین اجرا می شوند، لذا از تمام ویژگی های بلاک چین نیز می توانند استفاده کنند.

- غیر قابل تغییر بودن : واسطه ها و افراد ثالث نمی تواند هیچ تغییری در داده ها ایجاد کنند. غیرقابل دستکاری و نفوذ – برنامه ها بر اساس اجماع شبکه فعالیت می کنند. بنابراین امکان سانسور، نفوذ به شبکه یا حذف داده ها نیست.
- امن : بدون نهاد مرکزی و تضمین شده توسط رمزنگاری.
- همیشه فعال : برنامه‌های غیرمتمرکز هرگز متوقف نمی شوند و هیچ کس قادر به جلوگیری از فعالیت آن ها نیست.

هر خدمت متمرکزی می تواند توسط اتریوم غیرمتمرکز شود. خدمات بزرگی مثل پرداخت ها، بیمه، رای گیری و بسیاری از خدماتی که اکنون توسط واسطه ها انجام می شوند، با بلاک چین غیرمتمرکز خواهند شد. با استفاده از پلتفرم‌هایی مانند اتریوم، شرکت‌ها و خدمات گوناگون می‌توانند اعتمادسازی در کار خود را به حداکثر برسانند و به کسب و کار خود اعتبار ببخشند. در دنیایی که داده‌ها بسیار ارزشمند هستند، تمرکززدایی اجتناب‌ناپذیر خواهد بود

مروری بر تاریخچه اتریوم تا به اینجا

خالق اصلی و ایده‌پرداز اتریوم یک نابغه روسی به نام ویتالیک بوترین است. او که اکنون (سال ۲۰۱۹) حدود ۲۴ سال سن دارد، در سال ۲۰۱۳ در حالی که فقط ۱۸ الی ۱۹ سال سن داشت، وایت‌پیپر (گزارش کار شبکه) اتریوم را منتشر کرد. در همان زمان نزدیک به ۳۰ نفر از توسعه دهندگان مطرح برای بحث و گفتگو پیرامون این موضوع با ویتالیک گرد هم آمدند. بوترین منتظر انتقادات بود و بقیه نیز به اشتباهات اساسی که در مفهوم آن وجود داشت، اشاره می‌کردند. حتی در آن دوران مفهوم اتریوم محوریت بیشتری درباره یک ارز داشت. طی دیدار و مباحثه با افرادی که این ایده را داشتند، گذشت زمان آن را تغییر داد و شکل جدیدی به آن بخشید. پس از اینکه به زبان برنامه‌نویسی مدنظر دست یافتند، هر هفته روش‌های جدیدی برای استفاده از آن به کار می‌بردند. در اواخر ژانویه ۲۰۱۴، تیم پروژه دریافت که ایجاد فضای ذخیره‌سازی فایل در بستری غیرمتمرکز نسبتاً آسان است و مفاهیمی مانند رجیستری نام (Name Registery) را تنها با چندخط کد می‌توان به وجود آورد. با روی هم انباشته‌شدن موارد استفاده‌های جدید، ایده ویتالیک آرام‌آرام تغییر شکل داد و به اتریومی که امروز می‌بینیم، تبدیل شد.

اعلان عمومی در سال ۲۰۱۴ : در ژانویه سال ۲۰۱۴، به صورت رسمی آغاز به کار توسعه پلتفرم اتریوم اعلام شد. اعضای تیم اولیه توسعه پلتفرم ویتالیک بوترین، میهای آلیسی، آنتونی دی‌لوریو و چارلز هاسکینسون بودند.

تاسیس بنیاد اتریوم در سال ۲۰۱۴ : در ژوئن سال ۲۰۱۴ بنیاد غیرانتفاعی اتریوم برای کمک بیشتر در توسعه پلتفرم تاسیس شد. مقر این بنیاد هم‌اکنون در کشور سوئیس است.

جمع‌سپاری و جذب سرمایه در سال ۲۰۱۴ :در ماه‌های ژوئن و آگوست ۲۰۱۴، در طول فروش جمعی که اتر در ازای بیت کوین فروخته شد، تیم اتریوم بیش از ۳۱،۰۰۰ بیت کوین از جامعه ارزهای دیجیتال جمع‌آوری کرد. ارزش آن بیت کوین‌ها در آن زمان چیزی نزدیک به ۱۸ میلیون دلار بود. در زمان فروش جمعی بیت کوین در محدوده ۶۵۰ دلار معامله می‌شد، اما پس از گذشت زمان قیمت بیت کوین سقوط شدیدی تجربه کرد و تیم پروژه باید با زیان از دست دادن میلیون‌ها دلار روبرو می‌شد.

راه‌اندازی شبکه آزمایشی اتریوم در سال ۲۰۱۵ : المپیک (Olympic) نام شبکه آزمایشی اتریوم بود که در ماه مه ۲۰۱۵ راه‌اندازی شد. بسیاری از کاربران تاریخ انتشار اتریوم را به انتشار المپیک نسبت می‌دهند. این شبکه اجازه آشنایی توسعه دهندگان با پلتفرم را می‌داد.

پیاده‌سازی هارد فورک فرانتیر (Frontier) در سال ۲۰۱۸ : روند توسعه اتریوم به چهار مرحله تقسیم شد تا توسعه دهندگان بتوانند خود را با آن وفق دهند. فرانتیر (Frontier) اولین مرحله از این روند توسعه شبکه بود و اساس کلی اتریوم در آن ارائه شد. در این نسخه کاربران می‌توانستند اتریوم خرید و فروش کنند، به استخراج اتریوم بپردازند و قرارداد هوشمند و برنامه‌های غیرمتمرکز بسازند. فرانتیر رسما در تاریخ ۳۰ جولای ۲۰۱۵ منتشر شد.

پیاده‌سازی هارد فورک هوم‌استد (Homestead) در سال ۲۰۱۵ : هوم‌استد اولین نسخه پایدار از اتریوم است که در تاریخ ۱۰ مارس ۲۰۱۶ روی بلاک شماره ۱,۱۵۰,۰۰۰ پیاده‌سازی شد. در هارد فورک هوم‌استد تضمین شد که شبکه اتریوم واقعا امن است و یک‌سری به‌روزرسانی‌های کلی روی آن اعمال شد.

هک دائو (DAO Hack) و پیدایش اتریوم کلاسیک در سال ۲۰۱۶ : یکی از ویژگی‌های جالب بلاک چین‌ها، سازمان‌های خودگردان غیرمتمرکز (DAOs) است. به بیان ساده یک DAO قرارداد هوشمندی است که با آن می‌توان یک فرایند سیستماتیک را به طور خودکار و بدون واسطه‌ها انجام داد. برای ساخت DAO ابتدا گروهی از برنامه‌نویسان با کدهایشان مشخص می‌کنند که سازمان چگونه باید کار کند. زمانی که قرارداد هوشمند اجرا شد مردم می‌توانند با خرید توکن‌ها که نشان دهنده سهام آن‌ها در سازمان است، در تعیین سرنوشت آن نقش داشته باشند. قرارداد هوشمند DAO شامل کدی است که چگونگی تصمیم‌گیری در آن را مدیریت می‌کند و توکن DAO ارز دیجیتال یا نرم‌افزاری است که به کاربران DAO اجازه رای دادن می‌دهد. به نوعی بیت کوین را می‌توان اولین DAO موجود دانست زیرا کاربران قادر خواهند بود در این شبکه به تایید تراکنش‌ها رای بدهند.

یک استارتاپ آلمانی به اسم Slock.it، یک قرارداد هوشمند DAO روی شبکه اتریوم ساخت که مردم را قادر می‌ساخت دارایی خود را به صورت غیرمتمرکز به اشتراک بگذارند. این پروژه وقتی به مرحله‌ی فروش توکن رسید، تبدیل به موفق‌ترین کمپین جمع‌آوری سرمایه اولیه دنیا شد و توانست ۱۵۰ میلیون دلار جذب کند. کد پایه‌ی DAO، عالی نبود؛ ضمن اینکه متن باز بوده و برای همه قابل رویت بود. در ۱۷ ژوئن، یک هکر ناشناس و یا گروهی از هکرها، باگی در سیستم پیدا کرده و شروع به جمع‌آوری پول از DAO و انتقال آن به یک DAO کپی کردند. پیش از اینکه جلوی او گرفته شود، ۵۰ میلیون دلار اتر دزدیده شد. با وجود اینکه تنها یک باگ در کد موجب این از دست رفتن سرمایه شد، شهرت اتریوم و مفهوم DAO زیر سوال رفت. با انتشار این خبر عده کثیری از افراد در جامعه اتریوم تصمیم به ایجاد نوعی هارد فورک گرفتند تا به این وسیله اعتبار از دست‌رفته را بازگردانند. هارد فورک، شکاف و انشعابی در بلاک چین یک ارز دیجیتال است که به طور کلی قوانین یک ارز را تغییر میدهد و بلاک چین جدیدی به وجود می‌آید. یک هارد فورک به‌نوعی جدا شدن یک رویکرد توسط اعضای یک جامعه است که تصمیم می‌گیرند، دیگر پروتکل‌های قبلی را در همان بلاک چین دنبال کنند. به‌عبارت‌دیگر یک نسخه جدید از بلاک چین قبلی، هارد فورک نام دارد.

بدین ترتیب در بلاک ۱۹۲۰۰۰۰، یک هارد فورک برای اتریوم اتفاق افتاد. تا بدین‌وسیله بتوان سرمایه‌های از دست رفته سرمایه گذاران را به جیبشان بازگردانند. به سبب این هارد فورک، شبکه اتریوم جدیدی به وجود آمد و شبکه قبلی اتریوم کلاسیک نام گرفت.

پیاده‌سازی تنجرین ویسل (Tangerine Whistle) در سال ۲۰۱۶ : در تنجرین ویسل مفهوم گس (Gas) و بالا پایین شدن آن، برای پرداخت کارمزدها و هزینه‌های شبکه مطرح شد. همچنین توسعه دهندگان با بالا بردن هزینه برخی از فعالیت‌های سنگین، توانستند با حملات دیداس (DDoS) به طرز فوق‌العاده‌ای مقابله کنند. این به‌روزرسانی در بلاک شماره ۲,۴۶۳,۰۰۰ مصادف با ۱۸ اکتبر ۲۰۱۶ انجام شد.

پیاده‌سازی اسپیریوس دراگون (Spurious Dragon) در سال ۲۰۱۶ : اسپریوس دراگون دومین فورک اتریوم برای مقابله با حملات دیداس بود. در این هارد فورک که ۲۲ نوامبر ۲۰۱۶ پیاده‌سازی شد، آسیب‌پذیری شبکه اتریوم در مقابل حملات دیداس تقریبا به صفر رسید.

پیاده‌سازی هارد فورک متروپلیس (بیزانس و قسطنطنیه) در سال ۲۰۱۹ : هارد فورک متروپلیس به دو هارد فورک بیزانس و قسطنطنیه تقسیم می‌شود اما اصلی‌ترین بخش، قسطنطنیه است.

هارد فورک بیزانس (byzantium) که در اکتبر سال ۲۰۱۷ اجرا شد، با ۹ تغییر روی پلتفرم اتریوم همراه بود و سختی شبکه اتریوم را کاهش داد. همچنین راه برای پیاده‌سازی قسطنطنیه و تکمیل متروپلیس باز کرد.

هارد فورک قسطنطنیه (کُنستانتینوپول – Constantinople) مهمترین هارد فورک اتریوم طی سال‌های گذشته خواهد بود که بعد از چند بار تعویق، قرار است نهایتا در ۲۷ فوریه ۲۰۱۹ پیاده‌سازی شود. این به‌روزرسانی برای شبکه اتریوم و توسعه دهندگانی که قصد کوچ کردن از الگوریتم اثبات کار (ماینینگ) به اثبات سهام را دارند، قدم بزرگی خواهد بود. در این به‌روزرسانی بزرگ که در نقشه راه اتریوم تعریف شده است، علاوه بر بهبود شبکه، پاداش بلاک از ۳ به ۲ کم خواهد شد و بمب سختی اتریوم به تاخیر خواهد افتاد.

به طورکلی پس از پیاده‌سازی قسطنطنیه و تکمیل هاردفورک مترو پلیس بهبودها و تغییرات زیر در شبکه اتریوم حاصل خواهد شد:

- بهبود حریم خصوصی تراکنش‌ها
- بهبود امنیت قراردادهای هوشمند
- به تاخیر انداختن بمب سختی اتریوم
- کاهش پاداش استخراج اتریوم

پیاده‌سازی هارد فورک سرینتی (Serinity) یا همان اتریوم ۲.۰۰ در زمان نامعلوم

ویتالیک بوترین، خالق اتریوم، در کنفرانس Devcon4 که ۳۱ اکتبر ۲۰۱۸، در شهر پراگ برگزار شد، از نقشه راه نسخه دوم اتریوم (Ethereum 2.0) رونمایی کرد و آن را یکپارچه خواند.

اتریوم ۲ نسخه‌ای کاملا متفاوت از اتریوم فعلی خواهد بود. این نسخه از اتریوم شامل کسپر (Casper) برای رفتن به اثبات سهام، شاردینگ (Sharding) برای مقیاس پذیری (تراکنش‌های سریع و ارزان) و ای‌وازم (eWASM) برای بهبود ماشین مجازی اتریوم و در نتیجه بهبود شبکه است. اتریوم ۲ در واقع همان مرحله سرینتی (Serinity) است که در نقشه راه اولیه اتریوم تعریف شده بود.

اتریوم چگونه کار می‌کند؟

پیشنهاد می‌کنیم برای درک بهتر نحوه کار اتریوم ابتدا مقاله چگونگی کارکرد بیت کوین را مطالعه فرمایید اما در این قسمت به زبان ساده نحوه کار اتریوم را بررسی می‌کنیم. همانطور که گفتیم، اتریوم پلتفرمی برای اجرای قراردادهای هوشمند است. قراردادهای هوشمند برنامه‌هایی هستند که توسط برنامه‌نویسان نوشته می‌شوند و به صورت غیرمتمرکز و بدون توقف، یک فرایند را به صورت هوشمند انجام می‌دهند. زبانی که با آن قراردادهای هوشمند را می‌نویسند، زبان برنامه نویسی سالیدیتی (Solidity) است.

قراردادهای هوشمند روی بلاک چین اتریوم پیاده‌سازی و اجرا می‌شود. اتریوم مانند بیت کوین، بلاک چین مخصوص خودش را دارد. مثل بیت کوین، در اتریوم هم شاهد یک بلاک چین عمومی هستیم یعنی همه اعضای شبکه اتریوم در تایید تراکنش‌ها نقش دارند.

دفترکل بلاک چین روی کامپیوترهای هر کسی که به شبکه متصل شود، نگهداری می‌شود با این تفاوت که در بیت کوین فقط تاریخچه تراکنش‌ها ذخیره می‌شود اما در اتریوم نودها از وضعیت قراردادهای هوشمند هم نگهداری می‌کنند. نودها همچنین چیزی به نام ماشین مجازی هم اجرا می‌کنند.

ماشین مجازی اتریوم چیست؟

ماشین مجازی اتریوم (EVM)، یک نرم افزار کاملا تورینگ است و روی شبکه نودهای اتریوم اجرا می‌شود. این سیستم صرف نظر از زبان برنامه نویسی، به هر میزان که کاربر بخواهد زمان و حافظه در اختیارش قرار می دهد. ماشین مجازی اتریوم روند ایجاد برنامه های بلاک چینی را بسیار آسان تر و کارآمد تر از همیشه می‌کند. به جای اینکه برای هر برنامه یک بلاک چین ایجاد کنید می توانید از بلاک چین اتریوم برای هزاران برنامه استفاده کنید.

اتر چیست؟

اتر (Ether) نام ارز دیجیتال اصلی شبکه اتریوم است. یکی از کاربردهای اتر استفاده به عنوان دارایی و انجام پرداخت‌های آنلاین می‌باشد اما هدف اصلی از ساخت این ارز ایجاد انگیزه برای فعالیت شبکه بوده است. مثل بنزین که سوخت خودروهاست، اتر هم سوخت شبکه اتریوم است و اگر نباشد هیچ‌انگیزه‌ای برای فعالیت شبکه وجود نخواهد داشت.

هزینه‌های شبکه مثل کارمزد تراکنش‌ها با استفاده از اتر پرداخت می‌شود و ماینرها در ازای ساخت بلاک به عنوان پاداش اتر دریافت می‌کنند. اتر دارای ارزش بوده و در صرافی‌ها خرید و فروش می‌شود.

قیمت اتریوم

در سال ۲۰۱۷، سال شکوفایی ارزهای دیجیتال، قیمت اتریوم ۱۰,۰۰۰ درصد رشد داشت. بله درست است یعنی ۱۰۱ برابر. یعنی ۱۰۰ دلار در ابتدای ۲۰۱۷، و برداشت ۱۰,۰۰۰ دلار در انتهای ۲۰۱۷. اتفاقی که شاید هر قرن یکبار رخ دهد. در سال ۲۰۱۶ ارزش هر اتر کمتر از یک دلار بود. پس از ژانویه ۲۰۱۸، قیمت اتریوم به روند نزولی شدیدی افتاد و امروز (۲۷ بهمن) که در حال نگارش این مقاله هستیم، اتریوم از بالاترین قیمتش در ۱۵۰۰ دلار، بیش از ۸۹ درصد سقوط کرده است. ارزش کل این ارز دیجیتال در اوایل سال ۲۰۱۷ به شدت به بیت کوین نزدیک شد و حتی برخی پیش‌بینی می‌کردند که این ارز دیجیتال بتواند در جدول ارزها از بیت کوین عبور کند. هم‌اکنون هر واحد اتریوم با قیمت حدود ۱۲۰ دلار معامله می‌شود. این رقم نشان دهنده این است که اگر اتریوم دوباره بتواند به بالاترین قیمت قبلی خود یعنی ۱۵۰۰ دلار برسد، حدود ۱۵ برابر رشد کرده است.

اتر یک ارز کاربردی است. بدیهی ست که هر چقدر کاربرد و پذیرش آن بیشتر شود، قیمت هم افزایش خواهد یافت. از اتریوم می توان برای هوشمند سازی فرایندها نهایت استفاده را برد. هر میزان که قراردادهای هوشمند اتریوم بیشتر مورد پذیرش نهادها قرار بگیرند، محبوبیت و کاربرد بیشتر و در نتیجه قیمت هم افزایش خواهد یافت.

کسپر FFG

کسپر FFG (یا Friendly Finality Gadget) نام یک پروتکل جدید برای تأیید بلاک است که نشان می‌دهد اتریوم به‌جای اثبات کار (PoW) از اثبات سهام (PoS) استفاده خواهد کرد. سازگاری با اثبات سهام علاوه بر اینکه گامی به‌سوی مقیاس‌پذیری است، احتمالاً مزایای بیشتری مانند حل مشکل مصرف بالای انرژی، تمرکزگرایی استخرهای استخراج و نظایر آن را به ارمغان خواهد آورد.

کسپر چیز جدیدی نیست، اولین نسخه از آن در سپتامبر ۲۰۱۴ نوشته‌شده است. ویرایش‌های متعددی تاکنون روی آن صورت گرفته است و آخرین نسخه از آن در نوامبر ۲۰۱۷ منتشر شد. بااین‌حال، کسپر باید به‌طور کامل آزمایش شود و باید کاملاً با نسخه‌های قبلی اتریوم سازگاری پیدا کند، در غیر این صورت، بهباردفورک نیاز خواهد بود. به همین دلیل است که سازگاری با چنین پروتکلی تا حدودی به آهستگی صورت می‌گیرد.

اتریوم چگونه تحت کسپر FFG کار می‌کند؟

در کسپر فرایندهای اثبات کار و اثبات سهام به‌صورت موازی اجرا می‌شوند. اثبات کار برای پیشنهاد بلاک و اثبات سهام برای تأیید آن است. در شرایط عادی، انتظار داریم این سازوکار پیشنهادکننده (اثبات کار) به‌طورمعمول بلاک‌ها را یکی پس از دیگری در یک فهرست پیوسته ارائه

دهد (به‌عنوان‌مثال، هر بلاک مادر، فقط و فقط یک بلاک فرزند داشته باشد). اما در صورت تأخیر شبکه یا حملات عمدی، این سازوکار پیشنهادکننده به شکل اجتناب‌ناپذیر گاهی اوقات چند بلاک فرزند برای یک بلاک مادر تولید خواهند کرد. نقش کسپر این است که از هر بلاک مادر فقط یک فرزند انتخاب کند و بنابراین از درختِ بلاک‌ها فقط یک زنجیره متعارف انتخاب می‌شود.

ماینرها (اثبات کار) و اعتبارسنج‌ها (اثبات سهام) نقش اساسی در امنیت سامانه دارند و بنابراین برای ایفای این نقش به مشوق نیاز دارند.

- ماینرها پاداش معمول بلاک‌ها را پس از استخراج یک بلاک دریافت می‌کنند. بااین‌حال پاداش بلاک‌های فعلی سه اتر است که به ۶/۰ اتر تقلیل خواهد یافت.
- اعتبارسنج‌ها پاداشی به شکل اتر دریافت می‌کنند که به‌عنوان سپرده به آنها داده می‌شود. اگر آنها از این موضوع سوءاستفاده کنند (به‌عنوان‌مثال رأی نادرست بدهند یا از شبکه غیبت کنند) جریمه می‌شوند. تیم اتریوم هنوز سیستم پاداش‌دهی و جریمه را نهایی نکرده است. پیشنهاد اولیه این است که فرض کنیم اگر ۱۰ میلیون اتر به‌عنوان سپرده قرار داده‌شده باشد، پاداش حضور در شبکه و رأی دادن از ۰ درصد تا ۵ درصد در سال باشد (با توجه به مقدار سپرده متغیر باشد) ولی مبلغ جریمه برای غیبت مکرر از شبکه از ۵ درصد تا ۱۰ درصد در سال باشد و یا اینکه شرایط سخت‌تری در نظر گرفته شود. جریمه برای رأی مخالف از ۱ درصد تا ۱۰۰ درصد است و خروج از شبکه را به دنبال دارد.

کسپر با چند مفهوم جدید معرفی می‌شود:

نقاط بررسی (چک پوینت): بلاک جنسیس یا بلاک صفر، یک نقطه بررسی است و هر بلاک که ارتفاع آن (یا شماره آن) در درخت بلاک‌ها دقیقاً مضربی از ۱۰۰ باشد نیز یک نقطه بررسی خواهد بود. بنابراین اگر ارتفاع یک بلاک $100 \times k$ باشد (ارتفاع نقطه بررسی) آن بلاک به‌اندازه k است. کسپر فقط زیر درخت نقاط بررسی را در نظر می‌گیرد که درخت کل را تشکیل می‌دهند.

پیوند اکثریت قاطع (supermajority link): زوج مرتب‌هایی از نقاط بررسی به‌صورت (a, b) هستند، به‌طوری‌که حداقل دو سوم از اعتبارسنج‌ها (بر اساس میزان سپرده‌شان) رأی‌هایشان را با منبع a و باهدف b منتشر کرده باشند. نقطه بررسی c را نقطه تعدیل‌شده می‌نامیم؛ درصورتی‌که یک پیوند اکثریت قاطع از نقطه بررسیِ تعدیل‌شده و c موجود باشد. نقطه بررسی c را نهایی شده می‌نامیم؛ درصورتی‌که تعدیل‌شده باشد و یک پیوند اکثریت قاطع به شکل $c \rightarrow c'$ وجود داشته باشد که در آن c' فرزند مستقیم c باشد.

اعتبارسنج‌ها باید از این دو فرمان اساسی پیروی کنند:

۱. اعتبارسنج نباید دو رأی متمایز برای یک هدف منتشر کند.

۲. اعتبارسنج نباید در محدوده سایر آرا رأی دهد

هر اعتبارسنجی که هر یک از این فرامین را نقض کند سپرده‌شان کاهش خواهد یافت. می‌توان ثابت کرد که دو نقطه بررسی متناقض، غیرممکن است که بتوانند با رأی دو سوم از اعتبارسنج‌هایی که یکی از دو فرمان کسپر را نقض می‌کنند نهایی شوند. قانون انتخاب انشعاب این است: باید زنجیره‌ای را دنبال کنید که حاوی نقطه بررسی تعدیل‌شده از بالاترین ارتفاع باشد. برای اینکه برخی از اعتبارسنج‌ها بتوانند از شبکه خارج شوند، اعتبارسنج‌های جدید ملحق شوند و در این میان از برخی حملات جلوگیری به عمل آید، یک تأخیر در برداشت سپرده به‌اندازه ۴ ماه وجود دارد. اگر در این مدت اعتبارسنج بخواهد هر یک از فرامین را نقض کند دیگر به سپرده‌اش دست نخواهد یافت.

ویژگی مهم این پروتکل:

۱. مسئولیت‌پذیری

قدرت رأی یک گره برابر است با سهم آن از کل سپرده‌ای که در دست سامانه قرار دارد و در معرض ریسک است. اگر اعتبارسنج از قانون سرپیچی کند، ما می‌توانیم این سرپیچی را تشخیص دهیم و بفهمیم که کدام اعتبارسنج مرتکب این خطا شده است. به دلیل مسئولیت‌پذیری می‌توانیم اعتبارسنج‌های متخلف را جریمه کنیم و مشکل (ایمنی) که بلای جان اثبات سهام در زنجیره شده است را حل کنیم (برخلاف اثبات کار که در آن خود استخراج هم هزینه‌بر است). ازآنجایی‌که امنیت اثبات سهام به مقدار جریمه بستگی دارد و می‌تواند طوری تنظیم شود که تا حد زیادی از پاداش‌های به‌دست‌آمده از استخراج بیشتر شود، انگیزه‌های امنیتی قوی‌تری نسبت به اثبات کار فراهم می‌کند.

۲. قطعیت

یکی از ویژگی‌های مهم کسپر قطعیت آن است. در سیستم اثبات کار، هر بلاک که روی بلاک حاوی تراکنش شما قرار دارد سبب می‌شود بازنویسی تاریخچه و نامعتبر کردن تراکنش شما سخت باشد. بااین‌حال، اهمیتی ندارد که چقدر منتظر بمانید؛ بلاک هرگز ۱۰۰ درصد قطعی نخواهد شد. کسپر از قطعیت بلاک اطمینان حاصل می‌کند و مطمئن است که هرگز بلاکتان نمی‌تواند برگشت بخورد. اهمیتی هم ندارد که قدرت حمله‌کننده چقدر است.

چگونه کسپر اتریوم را مقیاس‌پذیرتر می‌کند؟

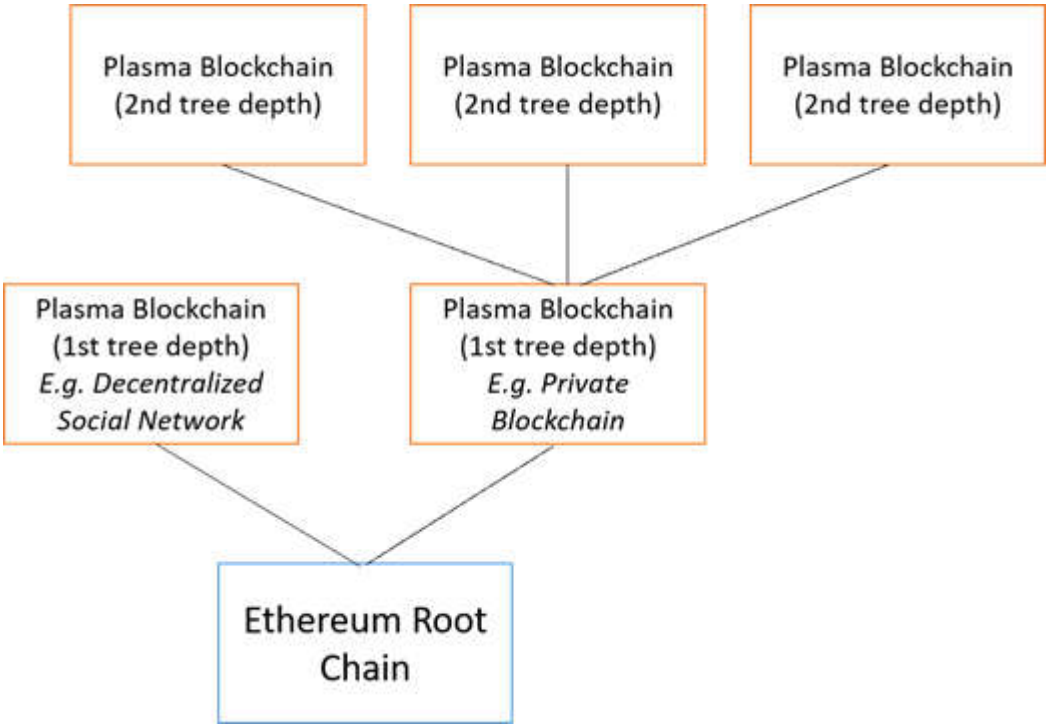
کسپر واقعاً پیچیده است؛ بااین‌حال این پروژه امیدوارکننده است و می‌خواهد مقیاس‌پذیری را به اتریوم ارائه دهد و بر تمام جنبه‌های آن تأثیر بگذارد. درباره مقیاس‌پذیری باید به نکات زیر توجه کرد:

- اثبات کار می‌تواند زمانی را که برای تأیید بلاک لازم است به کمترین مقدار کاهش دهد؛ زیرا نسبت به اثبات کار آسان‌تر انجام می‌شود.
- شاردینگ (چند شاخه کردن یا انشعاب درست کردن که در این مطلب از شارد کردن استفاده می‌کنیم) را ممکن می‌سازد.

ویتالیک بوترین این موضوع را این‌طور بیان می‌کند: کسپر هنوز ناتمام است.به‌عنوان‌مثال، سازوکار پیشنهاد بلاک اجازه نمی‌دهد کسپر بلاک‌های جدید را نهایی کند و باید این مشکل حل شود. کسپر یک پیشرفت اساسی امنیتی مبتنی بر اثبات سهام برای هر زنجیره‌ای است که از اثبات کار استفاده می‌کند. مشکلاتی که کسپر به‌طور کامل حل نمی‌کند (مخصوصاً در ارتباط با حملات ۵۱ درصدی) را می‌توان با استفاده از فورک‌های نرم فعال‌شده توسط کاربران اصلاح کرد. پیشرفت‌های آینده بی‌تردید امنیت کسپر را بهبود خواهد بخشید و پس‌ازآن دیگر نیاز چندانی به فورک‌های نرم فعال‌شده توسط کاربر نخواهد بود. حتی اگر اولین اجرای کسپر بتواند فقط یک (اثبات سهام ترکیبی) را به‌عنوان سازوکار پیشنهاد بلاک (که هنوز از قید اثبات کار آزاد نیست) پیشنهاد کند، اتریوم قطعاً درنهایت به سازوکار اثبات سهامِ محض خواهد رسید. البته هنوز اجرای عملی آن ممکن نشده است.

پلاسما

پلاسما (یا راه‌حل خارج از زنجیره یا مقیاس‌گذاری لایه دوم) طرحی است که ادعا می‌کند قادر است بلاک چین‌های ایمن را روی بلاک چین اصلی اتریوم ایجاد کند. پلاسما مانند کانال‌های پرداختی در شبکه لایتنینگ بیت کوین روشی برای انجام تراکنش‌های خارج از زنجیره است، اما بر بلاک چین بنیادینِ اتریوم به‌عنوان زیربنای امنیت خودش استفاده می‌کند. ازآنجایی‌که این زنجیره‌ها می‌توانند خودشان زنجیره‌های فرزند داشته باشند، یک درخت از بلاک چین‌ها به شکل زیر ایجاد می‌شود:



هر زنجیره مستقل است و بنابراین هر یک تا زمانی که به زنجیره مادر گزارش می‌دهند، می‌توانند قانون مدیریتی خودشان را داشته باشند. تا زمانی که زنجیره اصلی یا ریشه (root chain) ایمن است، هر زنجیره فرزند حتی می‌تواند یک قدرت متمرکز داشته باشد و به لحاظ نظری کاملاً ایمن باشد.

پلاسما چگونه کار می‌کند؟

برای ایجاد یک زنجیره فرزند روی زنجیره اصلی اتریوم، باید مجموعه‌ای از قراردادهای هوشمند ایجاد کنید. این قراردادها حاوی قوانین اساسی زنجیره فرزند و هش‌های ثبت‌شده آن هستند و مانند یک پل عمل می‌کنند که کاربران می‌توانند از طریق آن دارایی‌هایشان را از زنجیره مادر به زنجیره فرزند و بالعکس انتقال دهند. این زنجیره فرزند الگوریتم اجماع خودش را دارد و به شکل مستقل از زنجیره اصلی اتریوم کار می‌کند. (می‌تواند اثبات سهام، اثبات اعتبار یا هر چیز دیگری باشد). هنگامی‌که زنجیره فرزند در حال اجراست، سازنده (های) بلاک به شکل دوره‌ای اعتبارسنجی را به زنجیره اصلی می‌سپارند و اساساً اثبات می‌کنند که وضعیت فعلی زنجیره فرزند بر اساس قوانین اجماع معتبر است. این تعهدات روی زنجیره اصلی در پلاسما به‌عنوان یک اثبات از اتفاقی که در زنجیره فرزند رخداده است ثبت می‌شود. کاربر فقط با زنجیره‌های فرزند تعامل برقرار می‌کند و به‌طور مستقیم با زنجیره اصلی کاری ندارد

برای اطمینان از اینکه این عمل ایمن است و اینکه همه عملیاتی که روی زنجیره فرزند رخ می‌دهد می‌تواند نهایی شود، پلاسما تضمین می‌کند که هر طرف قرارداد می‌تواند پول و دارایی‌اش را هر زمان که بخواهد به زنجیره اصلی بازگرداند. بنابراین حتی اگر یک مهاجم سعی کند که کنترل شبکه را به‌دست بگیرد، بدترین حالت این است که شمارا مجبور کند زنجیره فرزند را ترک کنید و به زنجیره اصلی برگردید. هنگامی‌که یک کاربر در حال انجام معامله در یک زنجیره پلاسما است و می‌خواهد پولش را به زنجیره اصلی انتقال دهد، یک (تراکنش انصراف) برای خروج ارسال می‌کند و یک مبلغ کوچک به آن پیوست می‌کند (یک اثبات مرکل از تاریخچه تراکنش او که ثابت می‌کند مقدار مشخصی پول دارد). در آن لحظه، یک (دوره چالش) وجود دارد. طرف دوم قرارداد می‌تواند با ارائه مدرکی دال بر اینکه ادعای بازگشت شما نامعتبر است یا تاریخ آن گذشته است ادعایتان را به چالش بکشد. (این امر در پلاسما همان اثبات مرکلِ تاریخچه تراکنش است. در کانال‌های شبکه لایتنینگ،

پیام امضاشده از طرف دوم قرارداد همین کار را انجام می‌دهد). اگر ادعای شما واقعاً در طی این دوره چالش نامعتبر باشد حق انصراف به شما تعلق نمی‌گیرد و طرف می‌تواند مبلغ را به‌دست آورد.

اگر در زنجیره فرزند یک گره جعلی باشد، قبل از اینکه پولتان خارج شود می‌توانید یک اثبات تقلب در قرارداد اصلی (ریشه) منتشر کنید که نشان دهد او تقلب کرده است. این اثباتِ تقلب حاوی اطلاعاتی درباره بلاک قبلی است. بر این اساس و طبق قوانین انتقال از زنجیره فرزند موجود در زنجیره اصلی، می‌توانید نشان دهید که این بلاک به‌درستی از بلاک قبلی پیروی نکرده است و تقلب شده است. اگر این تقلب اثبات شود، زنجیره فرزند به‌عقب بازمی‌گردد. همچنین می‌توانید مطمئن باشید که هر سازنده بلاک که بلاک نادرست را در هر زنجیره جانبی تأیید نهایی کرده است جریمه خواهد شد. به زبان ساده، زنجیره‌های جانبی اعتبارشان را از زنجیره مادر می‌گیرند. زنجیره مادر مانند دادگاه عالی عمل می‌کند و او هم اعتبارش را از مراجع بالاتر می‌گیرد. اگر شما می‌خواهید تصمیم دادگاه محلی (زنجیره فرزند) را به چالش بکشید، می‌توانید درخواست تجدیدنظر کنید و قضاوت را به عهده دادگاه عالی (زنجیره اصلی) بگذارید.

مزایای مقیاس پذیری

مزایای مقیاس‌پذیری و سرعت زنجیره‌های لایه دوم به شکل مطلوبی آشکار است؛ زیرا دیگر نیازی نیست بسیاری از تراکنش‌ها توسط زنجیره اصلی پردازش شوند و زنجیره جانبی می‌تواند تحت پروتکل اجماع سریع‌تری (با امنیت کمتر) اجرا شود. ازآنجایی‌که در زنجیره جانبی فقط تعداد کمی از گره‌ها تراکنش‌ها را پردازش می‌کنند (احتمالاً یکی)، کارمزدها می‌توانند بسیار کمتر باشند و عملیات می‌توانند سریع‌تر انجام شوند. پلاسما قادر خواهد بود حجم زیادی از داده‌هایی را که درحال حاضر به شکل غیرضروری در زنجیره اصلی پردازش می‌شوند به زنجیره‌های جانبی منتقل کند و بنابراین در حجم عظیمی از قدرت پردازش و حافظه گره‌های اتریوم صرفه‌جویی خواهد شد. علاوه‌براین، برخی گره‌ها ممکن است علاقه داشته باشند که فقط زنجیره جانبی را که سبک‌تر از زنجیره کلی اتریوم است اجرا کنند. در این صورت آنها قادر خواهند بود بدون داشتن قدرت محاسباتی زیاد و فضای ذخیره‌سازی بزرگ در اکوسیستم اتریوم شرکت کنند.

پلاسما فقط مجموعه‌ای از ابزاری است که مردم بتوانند با آن قراردادهای هوشمند مقیاس‌پذیرشان را اجرا کنند. پلاسما یک پروتکل نیست، فقط یک الگوی طراحی‌شده است. باید دانست که پلاسما در حال حاضر با اختلافات زیادی درباره امنیت و سهم خود از مقیاس‌پذیری ایجاد کرده است.

شاردینگ

شاردینگ مفهومی است که از معماری پایگاه داده می‌آید. با شاردینگ که روی بلاک چین اِعمال می‌شود دیگری نیازی نیست که کل شبکه گره‌ها برای پردازش هر یک از تراکنش‌ها کار کنند. در حال حاضر در تمام پروتکل‌های بلاک چین، هر گره توضیحات همه تراکنش‌ها را ذخیره می‌کند و همه تراکنش را پردازش می‌کند. این امر امنیت زیادی را به وجود می‌آورد، اما مقیاس‌پذیری را به‌شدت محدود می‌کند. یک بلاک چین نمی‌تواند تراکنش‌های بیشتری نسبت به هر یک از گره‌هایش پردازش کند. قرار است که این محدودیت رفع شود تا سامانه بتواند تراکنش‌های زیادی را به شکل موازی پردازش کند و درعین‌حال ایمن باقی بماند.

شاردینگ اصطلاحات فنی گسترده‌ای دارد و می‌تواند عملاً به روش‌های متعددی پیاده‌سازی شود. در حال حاضر، هیچ‌کس از شاردینگ در استخراج استفاده نمی‌کند و فرایندی که اتریوم ممکن بود از آن استفاده کند کاملاً ناشناخته باقی‌مانده است.

چگونه می‌توان تراکنش‌های کراس شاردها را مدیریت کرد؟ این سامانه از نوعی رسید (receipt) استفاده می‌کند (چیزی که سبب می‌شود تراکنشی که در بخش توضیحات سامانه ذخیره نشده است اما در درخت مرکل نگهداری می‌شود، وجود آن به‌راحتی برای یک گره قابل‌تأیید باشد) تا بتواند ارتباط بین کراس شاردها را حفظ کند و مانع از گسیختگی اجزای آنها شود.

حساب کاربری A روی شارد M می‌خواهد ۱۰۰ سکه به‌حساب کاربری B در شارد N ارسال کند:

۱) ارسال یک تراکنش روی شارد M که به‌اندازه ۱۰۰ سکه از موجودی A کسر می‌شود و یک رسید ایجاد می‌کند.
۲) انتظار برای انجام اولین تراکنش.
۳) ارسال یک تراکنش روی شارد N که شامل اثبات مرکل رسید از مرحله ۱ است. این تراکنش همچنین در بخش توضیحات شارد N بررسی می‌شود تا اطمینان حاصل شود که این رسید خرج نشده است. اگر همه‌چیز درست باشد، به‌اندازه ۱۰۰ سکه به موجودی B اضافه می‌کند و در بخش توضیحات، رسید را به‌عنوان (خرج شده) ثبت می‌کند.
۴) به شکل اختیاری تراکنش در مرحله ۳ نیز رسید را ذخیره می‌کند که سپس می‌تواند برای انجام اقدامات بیشتر روی شارد M که مشروط به موفقیت عملیات اصلی است استفاده شود.

چگونه از حمله ۵۱ درصدی جلوگیری می‌شود؟

ویژگی تصادفی بودن به ما اطمینان می‌دهد تقسیم شبکه به شاردهای متعدد، کار مهاجمان را برای پیوستن به شبکه و رسیدن به‌قدرت رأی و احاطه بر شاردها بسیار دشوار باشد. (زیرا شما به N برابر قدرت محاسباتی / قدرت رأی برای انجام یک حمله موفقیت‌آمیز نیاز دارید). در این صورت اعتبارسنج‌ها قادر نخواهند بود شاردشان را انتخاب کنند زیرا اغلب ترتیبشان به شکل تصادفی در هم می‌ریزد (حالت شافل) و هرگز نمی‌توانند به یک ترتیب قرار بگیرند.

شاردینگ ابتدا به کسپر نیاز دارد تا بتواند شبکه را به‌آسانی به چند شاخه تقسیم‌بندی کند. درواقع، ازآنجایی‌که اعتبارسنج‌ها باید ثبت‌نام کنند و وثیقه بگذارند، اثبات سهام می‌تواند فهرستی از همه اعتبارسنج‌ها باقدرت رأی‌شان تهیه کند. شبکه بر اساس این فهرست به شاردهایی تقسیم می‌شود. انجام شاردینگ خودش یک چالش بزرگ است، بنابراین تا قبل از سال ۲۰۲۰ هیچ انتظاری از عملی شدن آنها نمی‌رود. همه این‌ها در حال حاضر فقط روی کاغذ است و طرح‌هایی که در اینجا نشان داده‌شده است فقط نمونه‌هایی از انجام‌شدن احتمالی این ایده قدرتمند است. شاردها و شاردهای احتمالی ساخته‌شده از شاردها (شاردینگ چهارگانه) سرعت‌بالای انجام تراکنش‌ها در آینده را نوید می‌دهد و خیلی‌ها آن را به‌عنوان بهترین راه‌حل در حال توسعه برای حل مشکل مقیاس‌پذیری می‌دانند.

این سه راه‌حل مکمل، هنوز کامل نشده‌اند و موارد مبهم زیادی درباره آنها وجود دارد. مقیاس‌پذیری موضوعی داغ است و اختلافات زیادی بر سر آن وجود دارد. ورای همه اینها، بهترین توسعه‌دهندگان و جوامع قدرتمندارز دیجیتال بر حل این مشکلات پیچیده فنی تمرکز کرده‌اند تا این فناوری را یک گام به پتانسیل کامل آن نزدیک‌تر کنند.

عصر یخبندان اتریوم

عصر یخبندان اتریوم یا (بمب سختی) مفهومی است که در سال ۲۰۱۵ توسط توسعه دهندگان اتریوم مطرح شد که طی یک نقشه عمدی با افزایش سختی استخراج شبکه اتریوم را نابود می‌کند. این برنامه بدین منظور طراحی شد که توسعه دهندگان اتریوم مجبور شوند به سمت اثبات سهام حرکت کنند.

شبکه اتریوم پس از عرضه و از همان ابتدا به مانند بسیاری از ارزهای دیجیتال دیگر نظیر بیت کوین، مونرو و زی‌کش بر روی مکانیزم اثبات کار فعال بود. در این مکانیزم استخراج‌کنندگان یا همان ماینرها با استفاده از سخت‌افزارهایی برای حل معادله‌ی بلاک‌ها با یکدیگر رقابت می‌کنند. برنده این رقابت علاوه بر پاداش شبکه، اجازه اضافه کردن بلاک بعدی به بلاک چین را نیز دریافت می‌کند. بسیاری از ارزهای دیجیتال بر پایه اثبات کار مانند اتریوم، طوری طراحی شده‌اند که سختی شبکه با اضافه یا کم شدن ماینر یا به عبارتی دیگر قدرت پردازشی به شبکه، تغییر پیدا می‌کند. این مکانیزم سبب می‌شود نرخ یافتن معادلات شبکه توسط ماینرها و به تبع آن آزاد شدن کوین‌های جدید در شبکه به صورت تقریباً ثابتی در یک بازه زمانی انجام گیرد. این امر با تعویض سخت‌افزارهای قدیمی با دستگاه‌های قدرتمندتر و جدیدتر توسط ماینرها نیز پابرجا می‌ماند.

با همه این توضیحات به بمب سختی شبکه می‌رسیم. پس از فعال شدن آن، سختی شبکه به صورت نمایی افزایش خواهد یافت و زمان بیشتری برای حل معادله یک بلاک مورد نیاز خواهد بود. قدرت بمب سختی شبکه و تغییرات آن به قدری محسوس خواهد بود که شبکه اتریوم را در حالت فعلی متوقف یا به اصطلاح فریز خواهد کرد و دیگر هیچ تراکنشی در شبکه به دلیل سختی بسیار بالای آن انجام نخواهد شد. این مفهوم با اصطلاح (عصر یخبندان اتریوم) شناخته می‌شود.

بمب سختی اتریوم زمانی فعال می‌شود که شبکه اتریوم از مکانیزم اثبات کار (PoW) به مکانیزم اثبات سهام (PoS) انتقال یابد. مکانیزم اثبات سهام در نسخه‌ای از اتریوم که با نام کسپر (Casper) شناخته می‌شود، رخ خواهد داد و این تغییرات به قدری گسترده خواهد بود که به هارد فورک جدیدی در شبکه برای پیاده‌سازی نسخه دوم اتریوم (Ethereum 2.0) نیاز است. در شبکه اتریوم پس از هارد فورک نهایی که سرنیتی (Serenity) نام دارد احتمالا دو شبکه اتریوم وجود خواهد داشت؛ بلاک چین جدید اتریوم که با مکانیزم اثبات سهام کار می‌کند و بلاک چین قدیمی که هنوز بر پایه اثبات کار است و برای زنده بودن به ماینرهایش احتیاج دارد.

توسعه‌دهندگان هر بلاک چینی این خطر را پس از هر هارد فورک احساس می‌کنند که ماینرها یا به اصطلاح کسانی که بلاک چین را زنده نگه می‌دارند، به انتقال بر روی شبکه جدید متقاعد نشوند و بر فعالیت خود روی شبکه قدیمی اصرار ورزند. این اتفاق پس از هارد فورک DAO برای شبکه اتریوم رخ داد که در نتیجه آن ارز جدیدی به نام اتریوم کلاسیک (بلاک چین قدیمی اتریوم) پدید آید. هم‌اکنون اتریوم کلاسیک به همراه شبکه اتریوم در حال فعالیت است و ماینرهای خاص خودش را دارد. برنامه‌ی اتریوم برای جلوگیری از رخداد دوباره این حادثه در شبکه این است که بمب سختی شبکه با با عرضه کسپر و انتقال به بلاک چین جدید فعال شده و عملاً شبکه قدیمی را برای کاربران و ماینرهایش با سختی بسیار بالا، فریز کند. در واقع اتریوم با این راه‌حل ماینرهای شبکه قدیمی خود را برای انتقال به بلاک چین کسپر مجاب خواهد کرد.

ریپل RIPPLE

چهارم ژانویه ۲۰۱۸، هر واحد ریپل (XRP)، به قیمتی معادل ۳.۳۱ دلار رسید. این یعنی چیزی در حدود ۵۱,۷۰۹ درصد رشد قیمت از ابتدای سال ۲۰۱۷. با رسیدن به این قیمت، حجم بازار ریپل به ۳۳۱ میلیارد دلار صعود کرد و به نزدیکی غول‌هایی نظیر گوگل، اپل، فیس‌بوک، علی‌بابا و آمازون رسید. نام‌هایی که در صدر فهرست بزرگ‌ترین شرکت‌های دنیا قرار دارند. بر اساس اعلام مجله (فوربس)، (کریس لارسن)، مدیر اجرایی ریپل، هفده درصد از سهام ریپل را در اختیار دارد و این یعنی چیزی در حدود ۵.۱۹ میلیارد واحد XRP. رقمی که در اوج قیمت ریپل معادل پنجاه میلیارد دلار تخمین زده می‌شود. با این حساب می‌توان گفت که لارسن یکی از ثروتمندترین افراد دنیاست. علیرغم ارزش بالای ریپل در بازار، به نظر می‌رسد که بسیاری از دارندگان توکن های ریپل، آشنایی چندانی با تاریخچه و فناوری پشت آن ندارند. در ادامه قصد داریم به بررسی اجمالی از تاریخچه ریپل پرداخته و برخی از بسترهای فنی آن را به زیر ذره‌بین ببریم.

تاریخچه ریپل : ریپل پی (RipplePay) از سال ۲۰۰۴ تا ۲۰۱۲

(رایان فوجر) (Ryan Fugger)، در سال ۲۰۰۴ یعنی چهار سال قبل از ظهور بیت کوین، شرکتی را بنا نهاد که ریپل‌پی نام داشت. ایده اصلی پشت ریپل پی، پروتکلی همتا به همتا از یک شبکه قابل‌اطمینان بود که با رویکردی اقتصادی می‌توانست جایگزین بانک‌ها شود.

ارکان تئوری اصلی ریپل:

۱- تمام کاری که بانک‌ها انجام می‌دهند، دریافت وام است. سرمایه‌های دریافتی بانک‌ها، قروضی است که از طرف مشتری‌ها به بانک‌ها پرداخت می‌شود.

۲- پرداختی که (باب) به (آلیس) در یک سیستم سنتی بانکداری انجام می‌شود، درواقع باعث به‌روزرسانی مانده‌حساب آنها در بانک خواهد شد. در اینجا قرض باب به بانک مقدار اندکی کاهش‌یافته و از طرف دیگر قرض آلیس به مقدار کمی بیشتر خواهد شد.

۳- ریپل پی به دنبال جایگزینی بانک‌هاست. این کار به‌وسیله ایجاد شبکه‌ای مورد اعتماد و همتا به همتا صورت می‌گیرد که در آن هر فرد می‌تواند به‌صورت مستقل به دیگران وام دهد و تغییراتی که در این قروض ایجاد می‌شوند، امکان انجام پرداخت‌ها را مهیا می‌کند.

۴- سپس پرداخت‌ها باعث به‌روزرسانی مانده قروض آنها خواهد شد. بدین ترتیب سیستم این امکان را پیدا می‌کند که رابطه‌ای میان اعطاکننده و دریافت‌کننده بیابد.

طبق این مثال، فرد سمت راست، بیست دلار به فرد سمت چپ پرداخت می‌کند. از طرف دیگر، پرداخت‌کننده و دریافت‌کننده به‌صورت مستقیم به یکدیگر اعتماد ندارند، این پرداخت طی یک زنجیره (بدهکاری) (IOU) که شامل هفت نفر دست‌به‌دست می‌شود. این هفت نفر به‌وسیله شش رابط قابل‌اعتماد به یکدیگر مرتبط‌اند.

ساختار شبکه ریپل بی‌شباهت به ایده پشت (شبکه لایتنینگ) بیت کوین نیست. بنا بر عقیده ما (بیتمکس)، مدل ریپل از ثبات خوبی برخوردار نیست و شبکه‌های مورد اطمینان را نمی‌توان قابل‌اتکا دانست. از همین رو نمی‌توان از نظر کارآمدی آن را تائید کرد. این سیستم یا در نهایت شبیه به تعداد کمی از بانک‌های بزرگ متمرکز خواهد شد و نسبت به سیستم‌های موجود تفاوت چندانی نخواهد داشت یا طبق پیش‌فرض‌های از پیش تعیین شده، قابل‌اتکا به‌حساب خواهد آمد. گرچه، سیستم فعلی ریپل با ایده اصلی آن فاصله بسیار دارد.

در ابتدای سال ۲۰۱۱، (زمانی که ریپل هنوز به هیچ موفقیتی دست نیافته بود)، بیت کوین در حال جلب توجهات بسیاری بود و این مسئله سبب شد که نظر ریپل را نیز با خود معطوف کند. این‌طور به نظر می‌رسید که ریپل، خود را با بیت کوین همسو می‌دید. بنا بر برخی از دلایل، بیت کوین در جایی که ریپل با شکست روبه‌رو شد، به موفقیت دست پیدا کرده بود. این‌طور که به نظر می‌رسید که ساخت شبکه‌ی پرداخت به‌صورت همتا به همتا توسط بیت کوین، از نمونه‌های ارائه‌شده توسط ریپل بهتر و کارآمدتر بود. در ماه می سال ۲۰۱۱، (جد مک کالب) (Jed McCaleb)، یکی از حامیان ابتدایی بیت کوین به تیم ریپل ملحق می‌شود. دلیل پیوستن مک کالب به تیم ریپل را می‌توان رفع برخی از مشکلاتی دانست که به آنها اشاره کردیم.

مک کالب در سال ۲۰۱۰، صرافی مشهور (ام تی گاکس) (Mt Gox) را پایه‌گذار کرد و در مارس ۲۰۱۱، آن را به (مارک کارپلس) فروخت. طبق بررسی‌ها و تفسیرهای (کیم نلسون) از WizSec، پلتفرم ام تی گاکس در زمان فروش در ورشکستی قرار داشت و در پرداخت مبلغی معادل هشتاد هزار بیت کوین (پنجاه هزار دلار) با مشکلاتی روبه‌رو شده بود. کمی بعد از این اتفاق بود که رایان فاجر، افسار پروژه ریپل را به‌دست مک کالب سپرد.

تغییر نام ریپل به اوپن کوین (OpenCoin) سپتامبر سال ۲۰۱۲ تا سپتامبر سال ۲۰۱۴

در سال ۲۰۱۲، مک کالب، کریس لارسن را استخدام کرد و وی تا به امروز مدیریت اجرایی این شرکت را بر عهده دارد. در وبسایت فعلی ریپل از لارسن به‌عنوان یکی از بنیان‌گذاران ریپل یاد شده است. با پیوستن لارسن به تیم، دوران جدیدی در تاریخ ریپل شروع شد که با عنوان اوپن کوین از آن نام‌برده می‌شود. اوپن کوین اولین تغییر نام از سه تغییر نامی است که شرکت تابه‌حال تجربه کرده است. لارسن که پیش‌تر مدیرعاملی E-Loan را بر عهده داشت و از بنیان‌گذاران آن در سال ۱۹۹۶ نیز به‌حساب می‌آید، E-Loan را در اوج حباب تکنولوژی و در سال ۱۹۹۹، وارد بازار بورس کرد و سپس در سال ۲۰۰۵ آن را به شرکت Banco Popular فروخت. پس‌ازآن بود که لارسن پلتفرمی همتا به همتا با عنوان Prosper Marketplace را ایجاد نمود که مخصوص اعطای وام بود. وی در سال ۲۰۱۲ به‌منظور پیوستن به ریپل، از Prosper Marketplace خارج شد.

لارسن نسبت به قیمت‌های پر افت‌وخیز و حباب‌های قیمتی آشناست. شرکتی که لارسن قبلا روی آن کار می‌کرد یعنی E-Loan طی سال‌های ۱۹۹۹ تا ۲۰۰۱، فراز و نشیبی ۹۹.۱ درصدی را تجربه کرد. سهام IPO این شرکت در ۲۸ ژوئن سال ۱۹۹۹، در قیمت ۱۴ دلار ثابت بود، این قیمت در سال ۲۰۰۵ به رقم ۴.۲۵ دلار کاهش یافت.

به‌منظور بیان ابعاد موفقیت بیت کوین، ریپل در آن زمان اجازه انجام پرداخت‌ها با بیت کوین را نیز داد و از آن به‌عنوان یک روش برای تسویه‌حساب استفاده کرد. این زمان مصادف شده بود با عرضه ساختاری با عنوان Ripple Gateway. جامعه ریپل به این نتیجه رسیده بود که ساختار همتا به همتا کارآمد نیست، چراکه کاربران عادی تمایلی نسبت به اعتماد به طرفین نشان نمی‌دهند و در صورت نبود چنین اعتمادی، پرداختی نیز در شبکه صورت نمی‌گیرد. به‌منظور حل این مشکل، ریپل تصمیم گرفت که درگاه‌هایی ایجاد نماید. این درگاه‌ها را کسب‌وکارهای بزرگی شکل می‌دادند که بسیاری از کاربران بتوانند به آنها اعتماد کنند. به عقیده برخی این مسئله نوعی رخنه به‌حساب می‌آید و آن را سیستمی هیبریدی از بانکداری سنتی و شبکه همتا به همتا می‌دانستند.

نحوه عملکرد درگاه‌های ریپل

اواخر سال ۲۰۱۲، اوپن کوین، پیشنهاد شرکت ریپل کامینیوکیشنز (Ripple Communications) مبنی بر استفاده از نام (ریپل کارت) (Ripple Card) را رد کرد. شرکت ریپل کامینیوکیشنز مدت‌ها بود که روی شبکه ریپل کار می‌کرد. این مسئله را می‌توان توضیحی بر آغاز تغییر رویکردهای شرکت به‌حساب آورد. تمایل به بکار گیری قوانین، به‌منظور حمایت و حفاظت از شرکت و همچنین تغییر در استراتژی برای تمرکز هر چه بیشتر بر روی برند ریپل، از جمله این تغییرات بود.

Ripple Communications شرکتی است که در زمینه ارتباطات فعالیت می‌کند و مقر آن در نوادا قرار دارد. این شرکت همچنین حق امتیاز دامنه ریپل (Ripple.com) را داراست و پیش از عرضه شبکه پرداخت ریپل، از نام ریپل استفاده می‌کرد.

در اکتبر سال ۲۰۱۲، (جسی پاول)، بنیان‌گذار و مدیرعامل صرافی (کراکن) (Kraken)، و یکی از دوستان صمیمی مک کالب نیز بود، از اولین سرمایه‌گذاران ریپل بود. به عقیده برخی این سرمایه‌گذاری ارزشی معادل دویست هزار دلار داشت. (راجر ور) (Roger Ver) نیز به‌عنوان یکی از اولین سرمایه‌گذاران ریپل شناخته می‌شود. بر طبق اظهارات برخی، ور حتی پیش از اینکه خالقان ریپل بدانند طرحشان چه هدفی را دنبال می‌کند، بر روی آن سرمایه‌گذاری کرده بود.

عرضه توکن XRP – ژانویه سال ۲۰۱۳

ریپل توکن های خود را با عنوان XRP در ژانویه سال ۲۰۱۳ عرضه نمود. به‌مانند بیت کوین، XRP نیز بر پایه یک زنجیره عمومی و امضاهای رمزنگاری‌شده ایجاد شده است. از همین رو به یک شبکه اولیه که بر پایه اعتمادسازی بنا شده یا هرگونه درگاهی نیاز ندارد. XRP می‌تواند به‌صورت مستقیم از یک کاربر به کاربر دیگر منتقل شود و انتقال آنها نیازی به درگاه نداشته و بدون خطراتی که طرفین معامله را تهدید می‌کند، انجام می‌شود. این روش، همان روشی است که برای تمام ارزها ازجمله دلار آمریکا بر روی شبکه ریپل استفاده می‌شده. شاید قصد

ریپل از ایجاد XRP، برقراری ارتباط میان ساختار شبکه اعتمادسازی برای پرداخت‌هایی باشد که بر پایه دلار آمریکا صورت می‌گیرند. پرداخت کارمزد تراکنش‌ها را می‌توان یکی از این اهداف احتمالی دانست. طبق برنامه‌های این شرکت، چیزی در حدود صد میلیارد XRP میان کاربران توزیع خواهند شد. به عقیده برخی این کار، نوعی پیشگیری از افزایش قیمت‌های ناگهانی و غیرمنطقی در XRP بوده. منتقدین ریپل نیز بر این عقیده‌اند که وجود توکن های XRP در شبکه ضرورت چندانی ندارد.

در آوریل سال ۲۰۱۳، اوپن کوین توانست از شرکت‌ها و افرادی نظیر: (گوگل ونچرز)، (اندرسن هورویتز)، IDG Capital Partners، FF Angels، (لایت اسپید)، (بیت کوین اپرتونیتی فاند) و (وست ونچرز)، بودجه‌ای یک و نیم میلیون دلاری دریافت کند. این تأمین سرمایه اولین بخش از چندین بخش تأمین سرمایه‌ای بود که موجب جلب‌توجه بسیاری از شرکت‌های بزرگ در زمینه سرمایه‌گذاری شد.

بین ژوئن سال ۲۰۱۳ تا می سال ۲۰۱۴ بحث جدایی جد مک کالب از ریپل مطرح شد. این مسئله در ماه می سال ۲۰۱۴ موجب بالا گرفتن بحث‌ها در جامعه ریپل شد. بعدها و طی بیانیه‌ای که توسط شرکت ریپل منتشر شد، اعلام شد که وی با روی کار آمدن (استفان توماس) به‌جای او در مقام مسئول بخش تکنولوژی شرکت، از این تیم جدا شد. توماس در مارس سال ۲۰۱۱ وب‌سایت We Use Coins را بنا نهاد و در همان سال نیز ویدیو (بیت کوین چیست؟) را در وب‌سایت یوتیوب منتشر نمود.

بنا بر شواهد مک کالب در ارتباط با رویکردهای اتخاذ شده توسط لارسن، اختلاف‌نظر داشت و از همین رو فشارها بر وی نسبت به خروج از تیم بیشتر شده بود. بعدها و در سال ۲۰۱۴، ازآن‌جهت که حمایت بسیاری از شرکت‌های سرمایه‌گذاری را پشت خود می‌دید، به سمت سرمایه‌گذاری در پروژه (استلار) رفت.

تغییر نام به (ریپل لبز) (Ripple Labs)- سپتامبر سال ۲۰۱۳ تا اکتبر سال ۲۰۱۵

در سپتامبر سال ۲۰۱۳، اوپن کوین به ریپل لبز تغییر نام داد. فوریه سال ۲۰۱۴، ریپل از قابلیتی پرده‌برداری کرد که (مسدود کردن مانده‌حساب) نام داشت. این قابلیت در آگوست همان سال به بهره‌برداری رسید. بر اساس این قابلیت، درگاه‌های ریپل قادر بودند تا سکه‌های موجود در درگاه‌ها را بدون در نظر گرفتن امضاهای معتبر برای تراکنش‌ها، مسدود یا حتی آنها را ضبط کند. هدف از این کار همگام شدن هر چه بیشتر با ملزومات قانونی ارائه‌شده توسط مراجع قضایی بود. به‌عنوان‌مثال درصورتی‌که دادگاه دستور ضبط دارایی‌ها را بدهد، این درگاه‌ها قادرند تا دستور مراجع قضایی را اجرایی کنند. تنظیمات پیش‌فرض درگاه‌ها قابلیت مسدودسازی را به آنها می‌داد، اما این قابلیت نیز وجود داشت که درگاه توسط گزینه‌ای با عنوان (بدون مسدودسازی)، امکان مسدود کردن سکه‌ها را نداشته باشد. بزرگ‌ترین درگاه در آن زمان با عنوان Bitstamp، چنین قابلیتی را اجرایی نکرد.

در ماه می سال ۲۰۱۵، مقامات قانون‌گذار در ایالات‌متحده آمریکا، شکایتی هفتصد هزار دلاری را بر ضد ریپل لبز انجام داد. نقض قانون محرمانه بودن اطلاعات بانکی توسط فروش بدون مجوز XRP، محور این شکایت بود. پس از این شکایت، ریپل موافقت کرد که اقداماتی را به‌منظور بهبود وضعیت خود انجام دهد. اصلی‌ترین این اقدامات به شرح زیر بودند:

۱- ریپل لبز موظف شد تا در FinCEN ثبت شود.

۲- در صورتی‌که ریپل هرگونه XRP را به فروش می‌رساند، دریافت‌کنندگان آنها موظف بودند تا اطلاعات حقیقی خود را در ریپل به ثبت برسانند.

۳- ریپل ملزم به پیروی از قوانین ضد پول‌شویی و ایجاد واحدی مخصوص رسیدگی به شکایات شد.

۴- ریپل موظف شد تا اطلاعات خود را جهت حسابرسی به مراجع ذی‌ربط تسلیم کند.

۵- ریپل موظف شد تا اطلاعات یا ابزارهای لازم را جهت اعمال قانون‌گذاری و بررسی‌های قانونی در ارتباط با تراکنش‌ها و ورود و خروج سرمایه‌ها در اختیار مراجع قضایی قرار دهد.

تغییر نام به ریپل (Ripple) – اکتبر سال ۲۰۱۵ تابه‌حال

ماه اکتبر سال ۲۰۱۵ بود که ریپل از کلمه (ریپل) به‌عنوان نام اصلی خود استفاده نمود. در سپتامبر سال ۲۰۱۶،ریپل توانست بودجه‌ای ۵۵ میلیون دلاری را در یک دوره، توسط شرکتی ژاپنی با عنوان SBI Holdings، به‌دست آورد. SBI، توانست ۱۰.۵ درصد از سهام ریپل را از آن خود کند. این سرمایه‌گذاری از جمله چندین سرمایه‌گذاری بزرگ شرکت SBI در حوزه ارزهای دیجیتال بود. SBI و ریپل با همکاری و مشارکت در پروژه‌ای مشترک بخش آسیایی (ریپل – اس بی آی) را ایجاد کردند. سهم ریپل از این بخش چهل درصد و شصت درصد باقی‌مانده نیز سهم اس بی آی بود. هدف از این شرکت، ارائه پلتفرمی با استفاده از فناوری اقتصاد توزیع‌شده ریپل، برای انجام معاملات بود.

در سپتامبر سال ۲۰۱۷، R3، شرکتی دیگر در حوزه بلاک چین از ریپل شکایت کرد. بر پایه ادعای R3، ریپل در سپتامبر سال ۲۰۱۶، موافقت کرده بود که گزینه خرید پنج میلیارد XRP را در ازای قیمت هر واحد ۰.۰۰۰۸۵ دلار، پیش از سپتامبر سال ۲۰۱۹، پیش روی آنها قرار دهد. در بالاترین قیمت (بیش از ۳ دلار)، ارزش این قرارداد، چیزی حدود ۱۶.۵ میلیارد دلار برآورد می‌شد. یعنی R3 می‌توانست چندین میلیارد دلار سودآوری داشته باشد. اما ریپل قرارداد را فسخ کرد. R3 ادعا کرد که در ژوئن سال ۲۰۱۷، ریپل، علیرغم نداشتن حق فسخ یک طرفه قرارداد، اقدام به این کارکرده. ریپل نیز طی اقدامی تلافی‌جویانه، از R3 برای متعهد نبودن به قرارداد اصلی در سال ۲۰۱۶ شکایت می‌کند. طبق ادعای ریپل، R3 موظف بود که این شرکت را به تعداد بالایی از مشتری‌های بانکی خود معرفی نماید تا آنها از XRP در سیستم‌های بانکی خود استفاده نمایند. این پرونده تا مارس سال ۲۰۱۸ همچنان حل نشده باقی ماند.

عرضه ریپل و ذخایر شرکت

در زمان بنا نهادن ریپل، ۱۰۰ میلیارد توکن XRP عرضه شد. از این صد میلیارد ۸۰ میلیارد در حساب کمپانی ذخیره و ۲۰ میلیارد دیگر، میان سه بنیان‌گذار آن تقسیم شد. تقسیم‌بندی دقیق‌تر توکن ها به شرح زیر است:

- شرکت ریپل ۸۰ میلیارد توکن دریافت کرد.
- کریس لارسن، ۹.۴ میلیارد توکن دریافت کرد. (از این میزان، لارسن چیزی در حدود هفت میلیارد آن را در مؤسسات خیریه صرف نمود.)
- جد مک کالب، ۹ میلیارد توکن دریافت کرد که:

۱. پس از ترک ریپل، ۶ میلیارد XRP را به ریپل بازگرداند. این شش میلیارد تحت توافق‌نامه عدم فروش به غیر قرار گرفتند.
۲. دو میلیارد از توکن هایی که توافق‌نامه شامل آنها می‌شد، به فرزندان مک کالب تعلق گرفتند.
۳. یک و نیم میلیارد توکن به امور خیریه و اعضای دیگر خانواده مک کالب تعلق گرفت. این میزان شامل توافق نمی‌شدند.

- (آرتور بریتو)، ۱ میلیارد توکن دریافت کرد. این میزان تحت توافق عدم فروش به غیر قرار دارد.

وقتی‌که مک کالب از ریپل جدا شد، این نگرانی وجود داشت که وی تمایل، توانایی یا قصد عرضه XRP های خود به بازار را داشته باشد. در این صورت قیمت توکن ها به‌شدت کاهش می‌یافت. مک کالب و ریپل برای جلوگیری از چنین اقدامی توافقی را انجام دادند. این توافق‌نامه در سال ۲۰۱۶ و پس از ادعای ریپل مبنی بر نقض مفاد آن توسط مک کالب، بازنگری شد.

مفاد این توافق‌نامه سال ۲۰۱۴ به شرح زیر بود:

- فروش توکن های مک کالب در سال اول در رقم ده هزار دلار در هفته محدود شود.
- فروش توکن های مک کالب در سال‌های دوم، سوم و چهارم در رقم بیست هزار دلار در هفته محدود شود.
- فروش توکن های مک کالب در سال‌های پنجم و ششم در رقم ۷۵۰ میلیون XRP در سال محدود شود.
- فروش توکن های مک کالب در سال هفتم در رقم یک میلیارد XRP در سال محدود شود.
- فروش توکن های مک کالب پس از سال هفتم در رقم دو میلیارد XRP در سال محدود شود.

در مورد ۸۰ میلیارد توکنی که شرکت ریپل در اختیار داشت، مقرر شد که این میزان برای سرمایه‌گذاری در امور شرکت و پایه‌گذاری درگاه‌های انتقال پول صرف شوند. صفحه ریپل در وب‌سایت (ویکی) می‌نویسد:

اعتبار XRP را نمی‌توان زیر سوال برد. وقتی‌که شبکه ریپل ایجاد شد، صد میلیارد XRP ساخته شد. بنیان‌گذاران شرکت هشتاد میلیون XRP را به ریپل لبز اختصاص دادند و ریپل لبز وظیفه توسعه نرم‌افزار ریپل، تبلیغ سیستم پرداخت ریپل، تخصیص XRP و فروش XRP را بر عهده دارد.

از دسامبر سال ۲۰۱۴ تا جولای سال ۲۰۱۵، شرکت بر روی وب‌سایت خود میزان XRP هایی که در اختیار دارد و حجم XRP های در گردش را نشان می‌داد. این وب‌سایت همچنین به‌صورت غیرمستقیم، مقدار ریپل هایی که توسط عملیات‌های شرکت مصرف شده‌اند را نیز برای عموم به نمایش در می‌آورد. از طرفی این وب‌سایت تمایزی میان XRP های به فروش رفته و آن دسته از توکن هایی که به‌صورت رایگان در اختیار افراد قرار داده، اعمال نمی‌کرد و تمام آنها را تحت یک رقم نمایش می‌داد. این نمایشگر ۳۰ ژوئن سال ۲۰۱۵، ارقام زیر را نمایش داد:

کمی بعد از جولای ۲۰۱۵، نمایشگر بازنگری شد. پس از این اتفاق میزان مانده‌حساب ذخایر شرکت نمایش داده نمی‌شد. حداقل تا سال ۲۰۱۷ این نمایشگر سه گزینه را به کاربران وب‌سایت نشان می‌داد: (XRP هایی که در اختیار ریپل بودند)، (XRP های توزیع‌شده) و (XRP هایی که به امانت نزد اشخاص و شرکت‌های ثالث نگهداری می‌شوند). این ارقام تا تاریخ سی ژانویه ۲۰۱۸ به شرح زیر بودند:

- هفت میلیارد XRP که در اختیار ریپل بودند.
- سی‌ونه میلیارد XRP توزیع‌شده.
- پنجاه‌وپنج میلیون XRP امانی، نزد شرکت‌های ثالث.

ما (بیتمکس) قادر به تطبیق و برقراری ارتباط میان نمودارهای ذخایر گذشته و نمودارهای XRP فعلی ریپل نبودیم، از همین رو نمی‌توان با اطمینان گفت که شرکت تابه‌حال چه میزان از توکن های خود را صرف امور جاری خود نموده است. بااین‌حال، با بررسی اطلاعات به نمایش درآمده تا جولای ۲۰۱۵، ۱۲ نقطه داده و پست‌هایی که در انجمن ریپل توسط (دیوید شوارتز) (David Schwartz) به جمع‌بندی‌هایی مفیدی دست‌یافتیم. دیوید شواترز به‌عنوان یکی از اصلی‌ترین معماران فناوری ریپل شناخته می‌شود. وی بانام مستعار JoelKatz در انجمن ریپل مطالبی را قرار می‌دهد. به گفته شوارتز جمع دارایی‌های ریپل وی، به رقمی نزدیک به یک میلیارد XRP می‌رسد.

توزیع XRP و XRP هایی که در امور جاری شرکت صرف شده‌اند. ارقام در این نمودار به میلیارد نوشته‌شده‌اند. علائم ضربدر نشان‌دهنده تاریخ‌هایی هستند که اطلاعاتی از آنها در دست نیست. از دلیل کاهش میزان خرج کرده شرکت که به سال ۲۰۱۵ منتهی می‌شود، اطلاعاتی در دست نیست.

XRP در گردش. ارقام در این نمودار به میلیارد دلار نوشته‌شده‌اند. داده‌ها نشان می‌دهند که ریپل از ژانویه سال ۲۰۱۳ تا جولای سال ۲۰۱۵، ۱۲.۵ میلیارد XRP را توزیع یا به فروش رسانده است. از میزان XRP های فروخته‌شده و قیمت آنها یا XRP هایی که به‌صورت مجانی در اختیار افراد مختلف قرارگرفته‌اند، اطلاعاتی در دست نیست. شرکت حداقل چهار ملیارد توکن را بین تاریخ‌های مارس ۲۰۱۴ و جولای ۲۰۱۵ خرج کرده است. بااین‌حال از جزئیات این خرج کرد ها اطلاعاتی در دست نیست.

دعاوی میان بنیان‌گذاران شرکت

همان‌طور که پیش‌تر اعلام شد، مک کالب در ارتباط با شرایط ذکرشده با شرکت همکاری کافی را نداشت. در می سال ۲۰۱۴، جسی پاول از اولین سرمایه‌گذاران ریپل، وضعیت را چنین توصیف کرد: ازآنجایی‌که جد شرکت را ترک کرده است، مدیریت شرکت جهت‌گیری متفاوتی را اتخاذ نموده. متأسفانه دورنمایی که من و جد در روزهای اول از پروژه در ذهن داشتیم، دیگر وجود ندارد. من دیگر نه به مدیریت اعتماد دارم و نه بر این عقیده هستم که شرکت توانایی بازیابی مقرری بنیان‌گذاران شرکت که بالغبر بیست درصد XRP می‌شود را ندارد. امیدوار بودم که این مقدار برگشت داده می‌شد. تا قبل از ترک شرکت توسط جد، از بنیان‌گذاران شرکت خواستم که XRP های خود را به شرکت بازگردانند. جد با این خواسته موافقت کرد اما کریس آن را رد کرد و مذاکرات به بن‌بست خورد. امروز عصر بار دیگر با هر دوی آنها صحبت کردم، اما این بار نیز کریس برخلاف جد، مخالفت کرد.

ریپل در جواب بیانیه پاول، ادعا کرد که او اطلاعات اشتباه و افتراآمیزی را اعلام نموده که باعث تخطی از وظایفش به‌عنوان اعضای هیئت‌مدیره ریپل شده. در این نامه آمده بود: درواقع، همان‌طور که کریس پیش‌تر طول بحث‌ها با شما [پاول] و جد اعلام کرده بود، تمایل داشته و دارد که بیشتر XRP هایی که در اختیاردارند را به ریپل لبز بازگردانند.

پاول در جواب این نامه اعلام کرد که لارسن تنها به بازگشت قرضی بخشی از XRP هایش به شرکت راضی شد و تمایلی به پس دادن کامل آنها نداشت. پاول نامه خود را با بیان دیدگاه خود نسبت به وضعیت بیست میلیارد XRP که به بنیان‌گذاران شرکت تعلق‌گرفته به‌پایان رساند: من و جد ریپل را در سپتامبر سال ۲۰۱۱ بنیان گذاشتیم. فکر می‌کنم کریس حدود آگوست ۲۰۱۲ به ما ملحق شد. پیش از ورود کریس، شرکت دو سرمایه‌گذار داشت. مطمئن نیستم که جد و کریس چه زمانی XRP ها را به خود تخصیص دادند، اما طبق گفته‌های آنها، این کار پیش از ایجاد شخصیت حقوقی شرکت و در سپتامبر سال ۲۰۱۲ صورت گرفته بود. ازنقطه‌نظر من، این دو نفر وقتی بدون تائید سرمایه‌گذاران اولیه XRP ها را برای خود برداشتند و آنها را میان سهام‌داران تقسیم نکردند، از اموال شرکت دزدی کردند. هر میزان سکه که پیش از شکل‌گیری شرکت اوپن کوین به آنها تخصیص‌یافته، مشکل‌دار است. بین سپتامبر سال ۲۰۱۲ و دسامبر همان سال، چندین بار دفتر کل راه‌اندازی مجدد شد و نسخه جدیدی از ریپل که توسط که اوپن کوین ساخته‌شده بود به وجود آمد و مشخصاً این کارها همه با منابع مالی شرکت صورت گرفتند. اگر جد و کریس از همان نسخه قدیمی نرم‌افزار برای نگه‌داشتن (بتاکوین) (Betacoin) های خود استفاده می‌کردند، مشکلی نداشتم. متأسفانه جد و کریس دوباره و در تاریخ دسامبر سال ۲۰۱۷، توکن هایی را به خود تخصیص دادند. این XRP ها بعداً نیز به شرکت بازگردانده نشد و پیش از تولد شرکت نیز وجود نداشتند و با منابع مالی شرکت ایجاد شدند. این توکن ها همیشه متعلق به شرکت بودند، اما توسط جد و کریس از چنگ شرکت درآورده شدند. من از آنها می‌خواهم چیزهایی که دزدیده‌اند را بازگردانند.

پاول همچنین جوابیه‌ای را در انجمن ریپل منتشر نمود. متن این جوابیه به شرح زیر بود: هیئت مدیره و سرمایه‌گذاران این مسئله را از مدت‌ها قبل می‌دانستند. به‌محض فهمیدن این مسئله مدام از آنها می‌خواستم که توکن ها را به شرکت بازگردانند. جد همیشه با این خواسته موفق بود اما کریس نظر مخالفی داشت. جد همیشه سهم خود را برای مواقعی که مجبور شود از آنها به‌عنوان یک اهرم فشار برای بازگشت سهم کریس، نگه می‌داشت. این مسئله یک موضوع معمولی نبود که روی آن بحث کنیم. بلکه فقط چیزی بود که فکر می‌کردم با آگاهی کریس از آسیب‌هایی که می‌تواند به شرکت بزند، حل می‌شد. احتمالاً اگر می‌خواستم سهمم از این مسئله بردارم، تنها اقدامات پیشگیرانه بیشتری انجام می‌دادم، اما این‌طور فرض کردم که تمام توکن ها سرانجام به شرکت بازخواهد گشت. می‌توانستم بر سر مقدار کمتری از XRP و پرداخت به‌صورت نقدی توافق کنم، اما این کار را نکردم. ما همه باید XRP های خود را مانند بقیه، با نرخ بازار خریداری می‌کردیم.

شرکت کمی بعد و توسط معاون بازاریابی خود، (مونیکا لانگ)، به این اظهارات واکنش نشان داد. این پاسخ به‌منظور تحت‌فشار گذاشتن پاول از جانب افکار عمومی صورت گرفت. در این بیانیه آمده بود:

به‌علاوه، کریس لارسن، از بنیان‌گذاران و مدیرعامل شرکت، مجوز ایجاد یک موسسه را به‌منظور توزیع کمک هفت میلیون XRP خود به افرادی که از سرویس‌های مالی مناسب برخوردار نیستند و تمایلی به استفاده از بانک‌ها ندارند، صادر کرد. این اقدام پیش‌تر برنامه‌ریزی و توسعه‌یافته

بود ما حالا به آن سرعت بخشیده شده و مستقل از توافق‌نامه رسمی میان بنیان‌گذاران اصلی، در حال نهایی شدن است. وی بر این عقیده است که هردوی این اقدامات درست‌اند و بهترین راه برای تحقق اهداف شرکت و از میان برداشتن موانع‌اند. در آینده، جزئیات بیشتری از این موسسه، مدیران مستقل و میزان کمک‌ها اعلام خواهد شد.

کریس لارسن از بنیانگذاران ریپل

این واکنش برای منحرف کردن فشارهای جامعه ریپل، از لارسن و شرکت، صورت گرفت. موسسه نامبرده با عنوان (ریپل وورکس) (Ripple Works)، کار خود را آغاز کرد. با بررسی ورودی‌های سال مالی ۲۰۱۶-۲۰۱۵ ایالات‌متحده بر مسئله مالیات بر کارهای خیریه ایالات‌متحده آمریکا، میزان کمک‌هایی که به‌صورت XRP صورت گرفته بود، به شرح زیر است:

نوامبر	۲۰۱۴	–	کریس	لارسن	–	۲۰۰	میلیون	واحد
آوریل	۲۰۱۵	–	کریس	لارسن	–	۵۰۰	میلیون	واحد
جولای	۲۰۱۵	–	کریس	لارسن	–	۵۰۰	میلیون	واحد

نوامبر ۲۰۱۶ – شرکت ریپل – یک میلیارد

تا تاریخ آوریل ۲۰۱۶، یعنی دو سال پس از اعلام تعهد، لارسن حداقل یک میلیارد و دویست میلیون XRP را از هفت میلیارد وعده داده شده به موسسه پرداخت کرده بود. متأسفانه امکان مشاهده ارقام سال مالی منتهی به آوریل ۲۰۱۷ وجود نداشت؛ دلیل این مسئله می‌تواند عدم ورود اطلاعات سال نامبرده دانست.

دعاوی مربوط به مسدودسازی سرمایه‌ها در (بیت استامپ)

در سال ۲۰۱۵، ریپل شروع به استفاده از قابلیتی که به آنها اجازه می‌داد تا سرمایه‌ها را مسدود نمایند. سرمایه‌های مسدود شده بیت استامپ متعلق به اعضای خانواده جد مک کالب بودند. برخی این مسئله را کنایه می‌خوانند: ریپل در ابتدا اعلام کرده بود که قابلیت مسدودسازی به‌منظور همگام‌سازی شرکت و درگاه‌ها با الزامات قانونی صورت می‌گیرند. اما این‌طور که به نظر می‌رسید این قابلیت تنها برای اجرای دستوراتی که مستقیماً از شرکت می‌آمد ایجادشده بود تا به این وسیله دارایی‌های یکی از بنیان‌گذاران ریپل را مسدود نماید.

این‌طور که به نظر می‌رسد، یکی از اعضای خانواده مک کالب، ۹۶ میلیون XRP را به قیمتی نزدیک به یک‌میلیون دلار به شرکت ریپل می‌فروشد. این میزان از XRP جزو آن دسته‌ای بودند که تحت توافق عدم فروش به غیر جای نمی‌گرفتند. پس از خریداری XRP ها توسط ریپل، این شرکت از بیت استامپ می‌خواهد که با استفاده از قابلیت مسدودسازی، یک میلیون دلار ریپلی که به‌تازگی صرف خرید توکن شده است را ضبط کند. در سال ۲۰۱۵، بیت استامپ شکایتی از مک کالب و ریپل را به دادگاه می‌برد تا بهترین تصمیم را در ارتباط با آنها اتخاذ کند. طبق شواهد و دادخواست‌های دادگاه، شرایط به شرح زیر بود:

۱- مک کالب پنج و نیم میلیارد XRP در اختیار داشت.

۲- دو فرزند مک کالب، دو میلیون XRP در اختیار داشتند.

۳- یک و نیم میلیون توکن دیگر در اختیار بقیه اعضای خانواده و مؤسسات خیریه بود.

۴- در ماه مارس سال ۲۰۱۵، (جیکوب استفانسون)، یکی از اقوام مک کالب، پیشنهاد فروش ۹۶ میلیون XRP را به ریپل می‌دهد.

ریپل موافقت می‌کند که طی یک تراکنش پیچیده که منجر به دست‌کاری بازار به‌منظور گمراه کردن خریداران دیگر نسبت به قیمت هر ریپل در این تراکنش می‌شد، نزدیک به یک میلیون دلار پرداخت کند. از همین رو، ریپل مبلغ بیشتری را پرداخت و از استفانسون خواست تا مبلغ اضافی را به آنها بازگرداند که چیزی در حدود هفتادوپنج هزار دلار می‌شد.

مسئول بخش حقوقی بیت استامپ به‌عنوان مشاور در ریپل نیز کار می‌کرد و این مسئله سبب تضاد منافع می‌شد. دعوی حقوقی میان مک کالب و ریپل تا فوریه سال ۲۰۱۶ ادامه داشت. در این تاریخ شرکت اذعان کرد که مک کالب قرارداد عدم فروش XRP ها را که در سال ۲۰۱۴ به امضا رسیده بود، نقض کرده. این شرکت پس از آن بیانیه نهایی خود را منتشر نمود:

جد، در ژوئن سال ۲۰۱۳ و هنگامی‌که شرکت اوپن کوین نام داشت، از آن جدا شد. وی ازآن‌پس هیچ نقشی در اتخاذ رویکردها و امور جاری ریپل نداشته. بااین‌حال او سهم بزرگی از XRP ها و سهام‌های شرکت را داراست. در آگوست سال ۲۰۱۴، ما یک توافق فروشی را به امضا رساندیم که طی آن بازه‌های زمانی و محدودیت فروش XRP ها توسط جد مشخص‌شده بود. هدف از امضای چنین توافقی، اطمینان از این مسئله بود که توزیع XRP ها به‌درستی صورت گیرد تا اکوسیستم ریپل با آسیب روبه‌رو نشود. از آوریل سال ۲۰۱۵، جد هدف اقدامات قانونی ما قرار گرفت. این اقدامات بر پایه نقض توافق‌نامه سال ۲۰۱۴ صورت پذیرفته بودند.

مک کالب نیز با بیان نقطه‌نظر خود در ارتباط با این مسئله، به بیانیه واکنش نشان داد. وی همچنین اعلام کرد که از توافق نهایی حاصل‌شده خوشحال است:

این هفته یک مشکل قدیمی را حل نمودیم. من و استلار بالاخره بر سر دعوی جاری خود با ریپل به توافق رسیدیم. توافق نشان می‌دهد که ادعاهای ریپل کاملاً بی‌اساس بودند. ریپل نیز این مسئله را قبول و من نیز توافق را پذیرفتم.

طی توافق‌نامه نهایی، مسدودسازی یک میلیون دلار دارایی خانواده مک کالب برداشته و ریپل قبول کرد که تمامی هزینه‌های دادرسی را بپردازد و دو میلیارد XRP نیز برای اهدا به مراکز خیریه آزاد شدند. مک کالب نیز اجازه یافت تا XRP های باقی‌مانده خود را به فروش برساند دیگر مفاد توافق‌نامه و تغییرات آن به شرح زیر است:

- مک کالب باید دو میلیارد XRP را به سازمان‌های خیریه اهدا کند.
- مک کالب به‌عنوان دارنده ۵.۳ میلیارد XRP ابقا شد. بااین‌حال کنترل این میزان از سرمایه بر عهده ریپل خواهد بود.
- مک کالب و موسسه خیریه قادرند تا به میزان ذکرشده از حجم متوسط روزانه به فروش برسانند. این حجم به شرح زیر است:
- ۰.۵ درصد در سال اول
- ۰.۷۵ درصد در سال‌های دوم و سوم
- ۱ درصد در سال چهارم
- ۱.۵ درصد در سال پنجم و بیشتر از آن

سیستم اجماع (Consensus)

این‌طور که به نظر می‌رسد فناوری ریپل از چندین تکرار تشکیل‌شده، اما محور اصلی در بازاریابی‌های ریپل حور سیستم اجماع آن می‌چرخد. در سال ۲۰۱۴، ریپل از تصویر زیر برای شرح سیستم اجماع خود پرده برداشت. بنا بر شواهد یک روند تکرارشونده با سرورهایی که درخواست‌ها را در سیستم ثبت می‌کنند، این پروسه را تشکیل می‌دهند. نودها در سیستم تنها درصورتی‌که حدنصاب ملزومات برآورده شده باشند، این درخواست‌ها را قبول می‌کنند. یک آستانه هشتاد درصدی از سرورها به‌عنوان سطح اصلی در نظر گرفته می‌شوند و به‌محض اینکه این آستانه محقق شود، نود درخواست را نهایی خواهد کرد. تصویر با پیچیدگی‌هایی همراه است و از همین رو نمی‌توان به قطع از نحوه کارکرد سیستم اجماع ریپل مطلع شد. به‌علاوه به دلیل این پیچیدگی فهم جزئیات نیز مشکل است.

در ژانویه سال ۲۰۱۸، تیم تحقیقاتی BitMEX، به‌منظور تحقق اهداف و اطلاعات موردنیاز برای این مطلب، نسخه‌ای از Rippled را اجرا نمود. همان‌طور که در اسکرین شات زیر دیده می‌شود، نود به‌وسیله دانلود فهرستی از پنج کلید عمومی از آدرس v1.ripple.com، عمل می‌کرده. نرم‌افزار نشان می‌دهد که چهار کلید از پنج کلید نامبرده برای پشتیبانی از یک درخواست و قبول آن ضروری است. ازآن‌جهت که کلیدها، همگی از سرور ریپل دانلود می‌شوند، ریپل کنترل کاملی بر بقای دفتر کل خود دارد، از همین رو می‌توان گفت که این سیستم متمرکز است. علائم نودها به ما میگویند که کلیدها در تاریخ اول فوریه سال ۲۰۱۸ (تنها چند روز پس از تاریخ اسکرین شات) منقضی خواهند شد، این یعنی نرم‌افزار ملزم است تا بار دیگر در این تاریخ به سرور ریپل متصل شده تا مجموعه کلیدهای جدیدی را دانلود نماید.

صد البته، نمی‌توان گفت که سیستم‌های متمرکز مشکل دارند. بخش گسترده‌ای از سیستم‌های الکترونیکی متمرکزند. متمرکز بودن امکان ساخت راحت را به سیستم‌ها می‌دهد و آن‌ها را کارآمدتر و سریع‌تر کرده، هزینه‌های اجرای آنها را پایین‌تر آورده و جلوی صرف دوباره یک سرمایه (Double Spending) را به شیوه کارآمدتری می‌گیرد. بااین‌حال، برخی از بازاریابی‌های ریپل اعلام می‌کنند که سیستم ریپل توزیع‌شده است. این مسئله به عقیده برخی گمراه‌کننده است.

علاوه بر گمراه‌کننده بودن بالقوه تبلیغات ریپل، ما بر این عقیده هستیم که پروسه حدنصاب و آستانه هشتاد درصدی ضروری نیست و صرفاً باعث گمراهی بیشتر خواهد شد. مدافعان و حامیان ریپل بر این موضوع مانور می‌دهند که فهرست پنج کلید عمومی قابلیت شخصی‌سازی دارند چراکه هر فردی می‌تواند فایل‌های پیکربندی را دست‌کاری نموده و آنها را به شکل موردنظر خود دربیاورد. در وب‌سایت ریپل فهرستی از این قبیل اعتبارسنج‌ها وجود دارد. بااین‌وجود هیچ مدرکی مبنی بر اینکه عده گسترده‌ای از کاربران ریپل به‌صورت دستی این فایل‌های پیکربندی را دست‌کاری کرده‌اند وجود ندارد.

حتی اگر کاربران اقدام به دست‌کاری نیز می‌کردند، کمک چندانی به تغییر وضعیت نمی‌کرد. در چنین شرایطی هیچ‌گونه دلیل خاصی وجود ندارد که بتوان متصور شد که سیستم بر روی یک دفتر کل تمرکز دارد. به‌عنوان‌مثال، یک کاربر می‌تواند با رسیدن هر نود به آستانه هشتاد درصدی به پنج اعتبارسنج متصل شود، بااین‌حال پای دو دفتر کل متضاد در میان است. حدنصاب آستانه هشتاد درصدی هیچ‌گونه ویژگی همگرایی یا اجماع را در خود جای نداده. از همین می‌توان گفت که این‌چنین پروسه اجماع غیرضروری است.

اعتبار سنجی دفتر کل

باوجود متمرکز بودن پروسه اجماع، یک فرد می‌تواند بر سر این مسئله بحث نماید که نودهای ریپل همچنان می‌توانند داده‌های تراکنش‌ها را از تمام افراد مشترک در شبکه تائید اعتبار نمایند. علیرغم کارایی در بحث‌های پردازشی، می‌توان گفت که این مدت می‌تواند از نقطه‌نظر کارایی نویدبخش باشد. بااینکه دفتر کل توسط پروسه‌ای متمرکز به جلو پیش می‌رود، اگر سرورهای ریپل، تراکنشی غیرمجاز را پردازش کنند، نود ممکن است آن بلاک‌ها را رد نموده و آنگاه شبکه قفل خواهد شد. این تهدید می‌تواند باعث عملکرد شفاف سرورهای ریپل شود. بااین‌حال، این تهدید نمی‌تواند تفاوت چندانی با ساختارهای قانونی و اهرم‌های فشاری باشد که از جانب کاربران و مشتری‌های بانک‌ها، بر آنها اعمال و باعث شفافیت در عملکردشان می‌شوند.

این‌طور که به نظر می‌رسد، ریپل از همان زمان شروع به‌کار دفتر کل ۳۲۵۷۰ بلاک ازدست‌رفته دارد و نودها قادر به دریافت این اطلاعات نیستند. این یعنی هیچ‌کس نمی‌تواند تمام زنجیره ریپل را موردحسابرسی قرار داده و مسیر دقیق صد میلیارد ریپلی که از ابتدا وجود داشته‌اند را ره‌گیری کند. همین مسئله می‌تواند برای عده‌ای نگران‌کننده باشد. به‌علاوه که پاول نیز در اعلام نظری، گفته بود که دفتر کل تابه‌حال چندین بار راه‌اندازی مجدد شده. دیوید شوارتز ابعاد گسترده بلاک‌های ازدست‌رفته را این‌طور بازگو می‌کند:

این مسئله چندان برای کاربران عادی ریپل مهم نیست. در ژانویه سال ۲۰۱۳، یک باگ در سرورهای ریپل باعث شد تا بلاک‌های اولیه دفتر کل نابود شوند. تمام داده از تمام سرورهای فعال ریپل جمع‌آوری شد، اما برای ساخت دفتر کل کافی نبود. تراکنش‌های خام همچنان در سرور وجود داشتند، این تراکنش‌ها با بقیه تراکنش‌ها مخلوط شده هیچ اطلاعاتی از اینکه کدام تراکنش، وارد کدام دفتر کل شده وجود ندارد. بدون

بلاک‌های اولیه دفتر کل، بازسازی دفتر کل میسر نیست. باید هش دفتر کل N-1 را بدانید تا بتوانید دفتر کل N را بسازید. همین خود پیچیدگی‌های مخصوص به خود را دارد.

جمع بندی

بخش عمده‌ای از این گزارش را دعاوی مربوط به ریپل تشکیل می‌داد و تمرکز اصلی آن حول محور کنترل XRP می‌چرخید و در این میان به برخی از اتهامات دزدی اموال نیز اشاره شد. شاید با بیان این مسئله که ارزش اکوسیستم به‌صورت غیرمنتظره و سریعی با رشد مواجه شد، بتوان گفت که چنین دعاوی‌ای چندان هم دور از ذهن به نظر نمی‌رسید. درواقع این دعاوی بی‌شباهت به نزاع‌های قانونی که در برخی از غول‌های تکنولوژی جهان که در ابتدا به آنها اشاره کردیم نیستند.

اما نکته قابل تأمل تر این مطلب، شاید متمرکز بودن ریپل باشد. این مسئله می‌تواند اهدافی نظیر سانسور ستیزی که ارزهایی نظیر بیت کوین از آنها برخوردارند را تحت شجاع قرار دهد. اما نباید این موضوع را این‌طور برداشت که ریپل یا XRP به دلیل نداشتن چنین ویژگی‌ای محکوم به فنا هستند. شرکت ریپل از سرمایه‌های بزرگی برخوردار است و با توجه به شیوه‌های بازاریابی و شراکت با شرکت‌های مختلف، بتواند راه موفقیت خود را پیداکرده و پای توکن هایش را به کسب‌وکارهای مختلف باز کند. اگر این مسئله محقق شود، شاید انتقادات‌هایی که به بیت کوین وارد باشد، در ارتباط با XRP مصداق بهتری پیدا کنند. نکاتی مانند:

۱- نبود تورم یک سیاست خام اقتصادی است.

۲- قیمت توکن ها بسیار بی‌ثبات است و می‌تواند هدف سفته‌بازی باشد.

۳- اگر سیستم با موفقیت هم روبه‌رو شود، مراجع قانونی می‌توانند آن را نابود کنند.

۴- شاید مهم‌ترین سؤال این باشد که چرا از دلار استفاده نکنیم؟ بانک‌ها نیز به سمت سیستم‌های دیجیتال که مبتنی بر ارزهای سنتی است روی خواهند آورد (اگر تا به اینجا این کار را نکرده باشند).

معمای اصلی در مورد ریپل اینجاست که با وجود بازاری با این ارزش هنگفت، چرا منتقدین بیت کوین ساکت‌اند؟ شاید جواب این سؤال برای منتقدین بیت کوین نیز به همین اندازه کاربرد داشته باشد. بیشتر مردم به‌جای توجه به اصول فنی، از روی مشاهدات خود نسبت به فرهنگ و شخصیت افرادی که با آن کسب‌وکار یا سیستم درگیرند، قضاوت می‌کنند.

افراد تاثیر گذار در ارزهای دیجیتال

ساتوشی ناکاموتو

بیت کوین به‌عنوان یک پروژه همگانی شکل گرفت. این ارز دیجیتال به‌عنوان یک نرم‌افزار متن‌باز واضح طراحی‌شده و در سال ۲۰۰۹ ارائه شد. بیت کوین یک پروژه متن‌باز عمومی است که روی دفتر کل باز که برای عموم قابل‌دسترس است، کار می‌کند. ولی با تمام شفافیت و واضح بودنش هنوز یک راز بزرگ دارد: چه کسی بیت کوین را ساخته و ساتوشی ناکاموتو کیست؟

اولین گام در سال ۲۰۰۷ برداشته شد، زمانی که ناکاموتو کد بیت کوین را نوشت. در نوامبر سال ۲۰۰۸ ساتوشی ناکاموتو گزارش عملکرد یا همان وایت‌پیپر (White paper) اختراع خودش را که امروزه معروف شده منتشر کرد. در سوم ژانویه سال ۲۰۰۹ اولین بلاک بیت کوین ماین شد و این پیام را در خود داشت: روزنامه تایم سوم ژانویه ۲۰۰۹: صدر اعظم در آستانه دومین کمک مالی به بانک‌ها

ساتوشی به‌منظور اصلاح کردن اصول اولیه پروتکل بیت کوین، به‌شدت درگیر جامعه بیت کوین و همکاری با آن بود. بعد از دو سال مشارکت، ساتوشی ناکاموتو از توسعه بیت کوین کنار رفت و در دسامبر ۲۰۱۰ مسئولیت‌ها را گوین اندرسون به صورت داوطلبانه برعهده گرفت. سپس در بهار سال ۲۰۱۱ ناکاموتو برای رساندن پیام نهایی بازگشت. او در پستی نوشت که در حال حاضر مشغول موضوع دیگری است و مسئولیت بیت کوین در اختیار فرد مناسبی (گوین اندرسون) قرار دارد. این آخرین حرفی بود که جهان از خالق ناشناس بیت کوین به یاد می‌آورد. راز هویت ناکاموتو فقط به خاطر گمانه‌زنی کنجکاوانه‌ی جامعه بیت کوین به‌منظور شناخت وی مهم شد. گفته می‌شود که ساتوشی ناکاموتو یک فرد ژاپنی، متود پنجم آپریل سال ۱۹۷۵ است. کسی در مورد جنسیت ناکاموتو چیزی نمی‌داند و حتی کسی نمی‌داند که ناکاموتو یک نفر است یا چند نفر.

آیا ساتوشی ناکاموتو بریتانیایی است؟

در حالی که هویت ساتوشی ناکاموتو نامشخص است همچنان تحقیقات و نتیجه‌گیری‌ها درباره‌ی گذشته وی ادامه دارد. استفاده بی‌عیب و نقص ناکاموتو از زبان انگلیسی و پست‌ها و وایت پیپر وی باعث به وجود آمدن شک و تردید در هویت ژاپنی او شده است. همچنین گاها استفاده او از زبان انگلیسی بریتانیایی (بریتیش) در کد و کامنت ها باعث به وجود آمدن این حدث و گمان شده که او یک فرد اصیل انگلیسی است. علاوه بر این استفان توماس یک برنامه‌نویس سوییسی و عضو فعال جامعه بیت کوین نمودار زمانی بیش از ۵۰۰ پست ناکاموتو را به نمایش گذاشت و این نمودار بیانگر غیاب او در ساعات نیمه‌شب تا ۶ صبح به‌وقت گرینویچ بود و همچنین اطلاعاتی را منتشر کرد که محل زندگی احتمالی او را نشان می‌داد.

نیک سابو (Nick Szabo)

تا به امروز افراد متعددی وجود دارند که گمان می‌رود یکی از آنها خالق سری بیت کوین یعنی ناکاموتو باشد. یکی از اولین گزینه‌های ما نیک سابو است، او یکی از هواداران واحد پولی غیرمتمرکز بود. او قبل از بیت کوین در سال ۱۹۹۸ به دنبال راه‌اندازی یک ارز دیجیتال به نام بیت‌گلد (BitGold) بود که به دلیل وجود مشکل (دوبار خرج کردن)، شکست خورد. یکی از محققان مطرح اینترنت، اسکای گری(Skye Grey) با بررسی سبک نوشته‌های سابو مدعی شد که سبک نوشتار او مشابه با سبک نوشتار وایت‌پیپر ساتوشی ناکاموتو است. البته این فقط یک احتمال بوده که بارها توسط سابو رد شده است.

دوریان پرینتیس ساتوشی ناکاموتو (Dorian Prentice Satoshi Nakamoto)

یکی دیگر از گزینه‌های احتمالی یک فرد ژاپنی آمریکایی ساکن کالیفرنیا به نام دوریان پرنتیس ساتوشی ناکاموتو است. این موضوع اولین بار در یک هفته نامه خبری در مارس ۲۰۱۴ مطرح شد. در آن مقاله، نویسنده به تدریس ناکاموتو به‌عنوان فیزیکدان در دانشگاه کال پولی پاناما و سابقه آزادی‌خواهانه او در گذشته به‌عنوان یک مدرک برای هویت او اشاره کرد. بزرگ‌ترین مدرک او پاسخ ناکاموتو درباره سؤالی در رابطه با

بیت کوین بود که این فرد در جواب گفته بود: من دیگر با این موضوع کاری ندارم به همین خاطر دیگر نمی‌توانم درباره‌ی آن نظری بدهم، حالا دیگر این موضوع در دست افراد دیگری است و آنها مسئولش هستند و من دیگر هیچ ارتباطی با این ماجرا ندارم. این موضوع سبب شور و حال در رسانه ها و حتی تعقیب خودرو وی شد. هرچند بعدها در یک مصاحبه گفته خودش را انکار کرد و اذعان داشت که سؤال خبرنگار را اشتباه متوجه شده است و فکر می‌کرده که سؤال خبرنگار در مورد شغل سری سابق او به‌عنوان پیمانکار نظامی بوده است.

هال فینی

هال فینی یکی دیگر از احتمالات مخترع نامعلوم بیت کوین یعنی ساتوشی ناکاموتو است. فینی یک پیشرو در زمینه رمزنگاری حتی قبل از بیت کوین بوده و شخص دوم بعد از ناکاموتو محسوب می‌شده که از نرم‌افزار استفاده بیت کوین می‌کرده، باگ‌های فایل‌ها را گزارش کرده و برای بهبود شبکه نظرات خود را ارائه داد. همچنین او اولین کسی بوده که از طریق تراکنش بیت کوین دریافت کرده است. خود او در یک مصاحبه‌ای گفته بود که وقتی برای اولین بار ساتوشی قصد آزمایش تراکنش را داشته برای او ۱۰ بیت کوین فرستاده است. روزنامه‌نگار فوربز، اندی گرینبرگ نوشت این موضوع که فینی در ساخت بیت کوین مشارکت داشته و با نیک سابو در ارتباط بوده و خانه او فقط چند ساختمان با دوریان پرینتیس ساتوشی ناکاموتو فاصله داشته شک او را بیشتر کرد. در زمان مرگ وی در ۲۸ آگوست سال ۲۰۱۴ همه بر این گمان بودند که هال فینی ساتوشی ناکاموتو واقعی است.

کریگ رایت

ولی همچنان یک کاندید احتمالی قابل‌قبول نیز وجود دارد این فرد کریگ رایت اهل استرالیا متخصص آکادمیک مهندسی کامپیوتر است. در اوایل نوامبر سال ۲۰۱۵، موسسه گیزمودو یک ایمیل ناشناس دریافت کرد، که در آن فردی نوشته بود نه تنها مطمئن است که کریگ رایت ناکاموتو واقعیست بلکه برای او کار نیز کرده است. در نهم دسامبر ساعاتی بعد از آن گزارش عجیب‌وغریبی که ادعا کرد کریگ رایت همان ناکاموتو است، پلیس فدرال استرالیا به خانه وی یورش برد و سپس اعلام کرد که این مسئله (ورود به خانه) ربطی به موضوع گزارش اخیر در رسانه‌ها در رابطه با ارز دیجیتالی بیت کوین نداشته است. بعد از آن رایت تا سال ۲۰۱۶ در فضای اینترنتی حضور پیدا نکرد و بعد در سال ۲۰۱۶ او در توییتر، خودش را سازنده‌ی ارز دیجیتالیبیت کوین معرفی کرد و ادعا کرد که برای حرف‌هایش مدرک دارد. سپس در میان سیلی از شک و تردید رایت ادعاهای خودش را رد کرد و مدارک شگفت‌آوری که وعده داده بود را ارائه نداد و گفت که جرات فاش کردن هویتش را ندارد.

اهمیت هویت واقعی ساتوشی ناکاموتو

در عصری که اطلاعات به‌سرعت منتشر می‌شود ساتوشی ناکاموتو موفق شده که هویت خودش را کاملاً پنهان نگاه دارد. ولی چرا فاش کردن هویت ساتوشی ناکاموتو این‌قدر اهمیت دارد؟ اگر ناکاموتو یک فرد باشد او مالک حدود ٪۵ از بیت کوین‌های جهان است که او را در تاریخ ۱۲ سپتامبر در رتبه پنجاه و دومین فرد ثروتمند کره زمین قرار می‌دهد. این میزان از ثروت پیامدهای زیادی در پی دارد، پیامدهایی فراتر از تصور. اگر ساتوشی ناکاموتو قرار بود بیت کوین‌هایش را به فروش بگذارد (طبق شایعات ۹۸۰.۰۰۰ بیت کوین) بازار به شدت تکان خواهد خورد و این موضوع در آینده، در صورت رشد قیمت بیت کوین خطرناک و خطرناک‌تر می‌شود.

بحث بر سر مقیاس پذیری

گذشته از موضوع هویت واقعی ساتوشی ناکاموتو، مخترع بیت کوین با آینده آن هم در ارتباط است. این بحث‌های داغ باعث به وجود آمدن مسائل نگران‌کننده‌ای برای بیت کوین شده است، بخصوص بحث چگونگی برخورد با معضل زیاد شدن تراکنش‌ها در شبکه بیت کوین. هرچه میزان بلاک‌ها زیادتر شود ریسک سنگین شدن شبکه بالا می‌رود. یک طرف بحث خواستار تغییر اساسی نود بیت کوین از طریق افزایش اندازه بلاک است تا به سیستم این اجازه را بدهد که تراکنش‌ها سریع‌تر شود. طرف دیگر ماجرا این بحث را خیانتی به مفهوم اصلی می‌داند و اعتقاد

دارد که این مسئله موجب متمرکز شدن می‌شود. تشخیص هویت فرد سازنده ی بیت کوین اطمینان ما را بیشتر خواهد کرد و می‌تواند قدمی برای رشد بیت کوین باشد.

نتیجه گیری

درنهایت، تشخیص هویت سازنده‌ی بیت کوین یک تلاش آرمان‌گرایانه است. و سکوت او از بهار سال ۲۰۱۱ می‌تواند به این معنی باشد که احتمالاً از این پس نیز خبری از او نخواهد بود. با این اوصاف، بیت کوین این ارز دیجیتالی متن‌باز که حدود یک دهه پیش ساخته شده با وجود این راز همچنان ادامه خواهد داد. جامعه بیت کوین به هر حال مجبور خواهد بود تا با معمای ساتوشی ناکاموتو کنار بیاید.

ویتالیک بوترین

ویتالیک بوترین برنامه‌نویس و نویسنده روسی‌کانادایی است که از سال ۲۰۱۱ در جامعه بیت کوین حضور دارد. وی بنیان‌گذار مجله بیت کوین (Bitcoin magazine)بوده و مقاله‌هایی برای آن می‌نویسد. اما بیشتر شهرت وی از شخصیت پسربچه نابغه‌ای نشأت می‌گیرد که زیربنای اتریوم که در حال حاضر سومین ارز دیجیتال ارزشمند و پلتفرم شناخته شده ارزهای دیجیتال پس از بیت کوین و ریپل است را پایه‌گذاری کرد. در زمان نگارش این مقاله، حجم بازار اتریوم ۱۴ میلیارد دلار است و پلتفرم آن به رشد خود ادامه می‌دهد. در همین حال ویتالیک نیز تنها ۲۳ سال سن داشته و نقشه‌های دور و درازی برای ساخته خویش دارد.

ویتالیک در ۳۱ ژانویه سال ۱۹۹۴ در شهر کولومنا از استان مسکو روسیه به دنیا آمد. او تا ۶ سالگی و تا زمانی که والیدینش تصمیم گرفتند برای فرصت‌های شغلی بهتر به کانادا مهاجرت کنند، در روسیه زندگی کرد. زمانیکه او در کلاس سوم یک مدرسه ابتدایی در کانادا درس می‌خواند، در جمع کودکان با استعداد برای بورسیه جای گرفت. در حالیکه قرار گرفتن نام ویتالیک در این برنامه به معنی فرصت‌های آموزشی بیشتر بود، اما اساساً او را از هم‌کلاسی‌ها و دوستانش جدا کرد. ویتالیک در این برنامه تحصیلی به سرعت دریافت که مجموعه استعدادها و مهارت‌های خاص او برای همتایان و حتی معلمانش عجیب‌وغریب است.

او اساساً آماده یادگیری هرگونه مطالب مرتبط با ریاضی و برنامه‌نویسی بود و از ابتدا علاقه شدیدی به اقتصاد نشان می‌داد بطوریکه اعداد سه‌رقمی را دوبرابر سریعتر از هم‌سن‌وسالان خود می‌توانست به صورت ذهنی با هم جمع کند. اما بوترین با گردهمایی‌های اجتماعی و فعالیت‌های فوق برنامه غریبه بود. همانطور که خودش نیز به یاد می‌آورد بسیاری از مردم درباره اینکه او به یک نابغه ریاضی بسیار شبیه است، صحبت می‌کردند. آن زمان این فکر در سر ویتالیک شکل گرفت که چرا نمی‌تواند یک شخص عادی با میانگین نمراتی مثل هر کس دیگر باشد.

شاید برخی بگویند ویتالیک با ذهن غیرطبیعی و استعدادهای شگفت‌انگیزش که او را از همتایانش جدا ساخته بود، اوقات سختی برای وفق یافتن با کشور و فرهنگ جدید سپری کرد. در نتیجه او عمیقاً در فرایند یادگیری و همچنین اینترنت فرو رفت؛ محلی که بسیاری از روابط شخصی و حرفه‌ای ویتالیک را شکل داد. بوترین دوران دبیرستان خود را به مدت ۴ سال در یک مدرسه خصوصی به نام آبلارد در تورنتو گذراند. ویتالیک از سال‌هایی که در دبیرستان سپری کرده بود به عنوان جذاب و پربازده‌ترین سال‌های زندگی‌اش یاد کرد.. این مدرسه درک وی را از آموزش تغییر داد، بطوریکه اخلاق و نتایج تحصیلی‌اش بلافاصله پس از تحصیل در این مدرسه به طور قابل توجهی تغییر پیدا کرد. در آبلارد بود که ویتالیک عطش و اشتیاق به یادگیری‌اش را گسترش داد؛ به خصوص اینکه در این مرحله یادگیری را برترین هدف زندگی خود قرار داد.

ویتالیک همواره نمرات قابل قبولی داشت، اما در دوره‌ای از زندگی اولویت او به جای زمان گذاشتن بر روی تکالیف درسی، بیشتر بر روی بازی ورلد آف وارکرفت (World of Warcraft) و دست یافتن به سطوح بالاتر در این بازی بود. ویتالیک از وقتی ۱۳ سال داشت به بازی WoW

مشغول بود تا اینکه یک روز در سال ۲۰۱۰، شخصیت ویتالیک به دلیل بروزرسانی بلیزارد که شرکت سازنده بازی بود، اندکی تغییر یافت. او طول شب را با گریه سر کرد تا متعاقباً به چشم خود ببیند که سرویس‌های غیرمتمرکز و کنار گذاشتن ورلد آف وارکرفت روی هم رفته چقدر می‌تواند وحشتناک باشد.

احتمالاً گشتن به دنبال یک علاقه‌مندی دیگر، در زندگی بود که ویتالیک را به سوی دنیای ارزهای دیجیتال رهنمون کرد. او اولین بار درباره بیت کوین از پدرش که استارت‌آپ نرم‌افزاری در سال ۲۰۱۳ به راه انداخته بود، شنید. زرق و برق ارزهای دیجیتال در نگاه اول نظر او را معطوف خود نکرد. اولین فکری که به ذهنش خطور کرد این بود که شکست ارزهای دیجیتال به دلیل فقدان ارزش ذاتی برای آن‌ها اجتناب‌ناپذیر خواهد بود. هرچند بعدها این موضوع بیشتر و بیشتر به گوشش خورد و باعث ایجاد علاقه ویتالیک به ارزهای دیجیتال شد. همانطور که خود او نیز اشاره کرده، اگر شما چیزی را دوبار بشنوید، ایده خوبی است که کمی از زمان خود را صرف آن کرده و اطلاعات بیشتری درباره آن کسب کنید.

در آن دوران به دید ویتالیک هر چیزی که با قانون‌گذاری دولت‌ها سروکار داشت یا تحت کنترل شرکت‌ها بود، شرورانه به نظر می‌رسید. طبیعتاً، ماهیت غیرمتمرکز و غیرقابل کنترل بیت کوین علاقه او را جلب کرد. حتی با وجود اینکه خط مشی او درباره خوب و بد از آن زمان به‌طور قابل توجهی به‌روزتر شده است، اما عقیده قلبی ویتالیک هنوز هم این است که قدرتمندان قدرت بی‌حدوحصری در اختیار دارند.

بوترین بیشتر زمان خود را بر روی در انجمن‌های گوناگون مرتبط با بیت کوین سپری می‌کرد و به تحقیق درباره این شبکه مشغول بود. در ابتدا، عنصر ارز دیجیتال در این شبکه بود که توجه ویتالیک را به خود جلب کرد. اما هرچه بیشتر درگیر جامعه ارزهای دیجیتال می‌شد، بیشتر درباره فناوری زیرین و بی‌نهایت پتانسیل‌دار مجازی بیت کوین فکر می‌کرد. او رسماً می‌خواست که وارد این اقتصاد جدید و تجربی شود و چند سکه به دست آورد، اما نه قدرت پردازشی لازم برای استخراج و نه پول لازم برای خرید بیت کوین در اختیار داشت. پس در انجمن‌های مختلف به دنبال کارهایی رفت که در ازای آن می‌توانست بیت کوین بگیرد. نهایتاً شروع به نوشتن مقاله‌هایی برای یک وبلاگ کرد که حاصل آن ۵ بیت کوین برای هر مقاله بود. ویتالیک از طریق کار در انجمن و مقاله‌هایی که می‌نوشت، تلاش می‌کرد آموخته‌ها و تجربیاتش درباره بیت کوین را افزایش دهد و در عین حال در انجمن خود را مطرح سازد. در زمان مشابه، در حال زیر و رو کردن تمامی جنبه‌های مختلف اقتصادی، تکنولوژیکی و سیاسی ارزهای دیجیتال بود. مقاله‌های او توجه میهای آلیسی (Mihai Alisie) که از دوست‌داران بیت کوین در رومانی بود را به خود جلب کرد که به مکاتبات فعالانه این دو و در نهایت پیدایش مجله بیت کوین (Bitcoin Magazine) منجر شد. بوترین فعالیت خود را به عنوان سردبیر مجله بیت کوین و کار پاره وقت دیگری برای رمزنویس معروف، ایان گلدبرگ، به عنوان دستیار محقق ادامه داد. افزون بر این آن زمان ویتالیک ۵ دوره درسی پیشرفته را در دانشگاه واترلو نیز می‌گذراند. در ماه می سال ۲۰۱۳ به شهر سن خوزه کالیفرنیا سفر کرد تا در کنفرانس مرتبط با بیت کوین به عنوان نماینده مجله بیت کوین حضور پیدا کند. این اولین بار بود که بوترین به عینه شاهد سرزنده و پرجنب‌وجوش بودن جامعه شکل گرفته پیرامون ارزهای دیجیتال بود. وی قانع شده بود که این پروژه‌ای است که قطعاً ارزش وقت گذاشتن و وارد شدن به آن را دارد. اواخر همان سال ویتالیک تحصیل در دانشگاه را کنار گذاشت و تصمیم گرفت با بیت کوین‌هایی که بدست آورده، دور دنیا سفر کند و افرادی که به گسترش قابلیت‌های شبکه بیت کوین کمک می‌کنند تا آن را در نوع خود به چیزی بزرگتر و قدرتمندتر از آنچه هست تبدیل کنند را ملاقات کند.

ویتالیک طی سفرهایش با پروژه‌های مرتبط با بیت کوین مختلفی از مغازه‌های کوچک در نیوهمپشایر و رستوران‌هایی در برلین که بیت کوین در آن‌ها پذیرفته شده بود گرفته تا خودپردازهای بیت کوین و جوامع کوچک سرتاسر جهان، آشنا شد. هر چند تمامی آن‌ها بیشتر بر روی نحوه بهبود عملکرد و مطرح ساختن بیت کوین به عنوان یک پول تمرکز کرده بودند. در اکتبر ۲۰۱۳، او از اسرائیل دیدن و افرادی که پروژه‌های کاورت‌کوینز و مسترکوین را هدایت می‌کردند، ملاقات کرد. پروژه‌های ذکر شده کاربردهای بلاک چین برای مقاصد مختلف مانند ایجاد توکن بر روی شبکه بیت کوین، امکان ایجاد قراردادهای مالی و غیره را مورد پژوهش قرار داده بودند. با اینکه آن‌ها همچنان از بلاک چین بیت کوین استفاده می‌کردند اما با این حال خصوصیات جدیدی به تراکنش‌های بیت کوین اختصاص می‌دادند.

پس از مشاهده پروتکل‌هایی که پروژه‌های مختلف از آن استفاده می‌کردند، ویتالیک دریافت که تعمیم گسترده کاری که پروتکل‌ها انجام می‌دهند با جایگزین کردن کارکرد آن‌ها با زبان برنامه‌نویسی کامل تورینگ امری امکان‌پذیر است. در علوم کامپیوتر زبان برنامه‌نویسی کامل تورینگ چیزی است که کامپیوتر را قادر می‌سازد هر مسئله‌ای را با دادن الگوریتم مناسب و حافظه و زمان کافی حل کند. ویتالیک در ابتدا ایده‌ای که داشت را به پروژه‌های آن دوران معرفی کرد اما همه آن‌ها به او گوشزد کردند که زمان مناسبی برای اجرای چنین چیز بزرگی نیست. پس او تصمیم گرفت که به تنهایی دنبال ایده‌ای که داشت برود.

اواخر سال ۲۰۱۳، ویتالیک ایده‌هایش را در قالب گزارش عملکردی (Whitepaper) که به چندنفر از دوستانش ارسال شده و توسط آن‌ها گسترش پیدا کرده بود، خلاصه کرد. در نتیجه نزدیک به ۳۰ نفر برای بحث و گفتگو پیرامون این موضوع با ویتالیک گرد هم آمدند. بوترین منتظر انتقادات بود و بقیه نیز به اشتباهات اساسی که در مفهوم آن وجود داشت، اشاره می‌کردند. حتی در آن دوران مفهوم اتریوم محوریت بیشتری درباره یک ارز داشت. طی دیدار و مباحثه با افرادی که این ایده را داشتند، گذشت زمان آن را تغییر داد و شکل جدیدی به آن بخشید. پس از اینکه به زبان برنامه‌نویسی مدنظر دست یافتند، هرهفته روش‌های جدیدی برای استفاده از آن به کار می‌بردند. در اواخر ژانویه ۲۰۱۴، تیم پروژه دریافت که ایجاد فضای ذخیره‌سازی فایل در بستری غیرمتمرکز نسبتاً آسان است و مفاهیمی مانند رجیستری نام (Name Registery) را تنها با چندخط کد می‌توان به وجود آورد. با روی هم انباشته‌شدن موارد استفاده‌های جدید، ایده ویتالیک آرام‌آرام تغییر شکل داد و به اتریومی که امروز می‌بینیم، تبدیل شد.

اتریوم در ژانویه ۲۰۱۴ اعلان عمومی شد. هسته تیم پروژه شامل ویتالیک بوترین (Vitalik Buterin)، میهای آلیسی (Mihai Alisie)، آنتونی دی‌لوریو (Anthony Di Iorio)، چارلز هاسکینسون (Charles Hoskinson)، جوزف لوبین (Joe Lubin) و گاوین وود (Gavin Wood) بود. همچنین بوترین اتریوم را در کنفرانس بیت کوین در شهر میامی روی صحنه معرفی کرد. چندماه بعد تیم پروژه تصمیم گرفت برای اتر که ارز دیجیتال شبکه محسوب می‌شد، فروش جمعی انجام دهد. در همان دوران خود ویتالیک وام بلاعوض تیل فلوشیپ با مبلغ ۱۰۰ هزار دلار دریافت کرده بود.

در طول فروش جمعی که اتر در ازای بیت کوین فروخته شد، تیم اتریوم بیش از ۳۱،۰۰۰ بیت کوین از جامعه ارزهای دیجیتال جمع‌آوری کرد که ارزشش در آن زمان چیزی نزدیک به ۱۸ میلیون دلار بود. هرچند در زمان فروش جمعی بیت کوین در محدوده ۶۵۰ دلار معامله می‌شد، اما پس از گذشت زمان قیمت بیت کوین سقوط شدیدی تجربه کرد و تیم پروژه باید با زیان از دست دادن میلیون‌ها دلار روبرو می‌شد. با این وجود، سرمایه جمع‌آوری شده برای تاسیس بنیاد اتریوم که یک سازمان غیرانتفاعی واقع در سوییس بود، کافی به نظر می‌رسید. این بنیاد با هدف نظارت بر توسعه نرم‌افزار منبع‌باز اتریوم ایجاد شده بود.

علی‌رغم برخی مشکلات، سرمایه‌پذیری جمعی اتریوم سومین کمپین برتر در این زمینه بود که همین نیز موجب پوشش رسانه‌ای پلتفرم در نشریات مالی بزرگ و معتبری از جمله وال‌استریت جورنال شد. پس از اینکه شبکه به طور رسمی کار خود را آغاز کرد، بنیاد اتریوم چندین نمونه آزمایشی از پلتفرم اتریوم را مورد آزمایش قرار داد. آخرین نسخه نمونه‌های آزمایشی المپیک (Olympic) نام داشت که به همراه نسخه عمومی بتا پس از آن منتشر شد. در اوایل چندین کاربر باگ‌ها و خطاهای سیستم را پیدا کردند و تیم اتریوم نیز برای کسی که بر روی شبکه اتریوم تست استرس انجام دهد، پاداش ۲۵ هزار اتریومی تعیین کرد.

در ۳۰ام ماه جولای سال ۲۰۱۵، اولین نسخه عمومی در دسترس اتریوم تحت عنوان (فرانتیر) (Frontier) منتشر شد. این نسخه که بیشتر شبیه به یک راه‌اندازی آزمایشی بود، تنها ضروری‌ترین ویژگی‌هایش را داشت که با ظاهر خط فرمان منتشر شده بود و به توسعه‌دهندگان امکان آزمایش زنده پلتفرم را با ایجادبرنامه‌های غیرمتمرکز می‌داد. پس از اینکه پلتفرم از سوی توسعه‌دهندگان و استفاده‌کنندگان پایدار ارزیابی شد، به نسخه (هومستد) (Homestead) ارتقا یافت. ارتقا به این نسخه ۱۴ام مارس ۲۰۱۶ انجام شد و شبکه اتریوم اولین نسخه رسمی منتشر شده محصول خود را آن روز مشاهده کرد. ورود اتریوم با معرفی نسل بعدی فناوری بلاک چین برابر بود که به توسعه‌دهندگان آزادی بیشتری می‌داد و به طور قابل توجهی استفاده از آن آسان‌تر بود. علاوه بر آن چندین بهبود تکنولوژیکی نیز در زیرساخت‌های آن اتفاق افتاده بود.

در این زمان اتریوم با قدرت خود را در بازار ارزهای دیجیتال معرفی کرده بود. تعداد نودهای اتریوم در آن دوران به ۵,۱۰۰ عدد می‌رسید که در مقایسه با بیت کوین در زمان مشابه با ۶,۰۰۰ نود، رقم قابل توجهی بود. علاوه بر آن، تعداد صرافی‌هایی که اتر معامله می‌کردند به صورت فزاینده‌ای رشد می‌کرد که خود این بر سرعت افزایش ارزش آن می‌افزود. با وجود اینکه نسخه اولیه اتریوم منتشر شده بود، غول‌های فناوری مانند مایکروسافت و آی‌بی‌ام با همکاری مستقیم تیم پروژه و ویتالیک بوترین در حال انجام پروژه‌هایی بر بستر اتریوم بودند.

بروزرسانی بزرگ بعدی (متروپلیس) (Metropolis) نام داشت که مقرر شده بود در دو بخش انجام شود. انتشار بخش اول آن تحت عنوان (بیزانس) که قرار بود در اکتبر ۲۰۱۷ انجام شود، چندین بار به تأخیر افتاد. این بروزرسانی بر روی کاربرپسندتر کردن شبکه به همراه سریعتر، سبک‌تر و امن‌تر کردن پلتفرم نسبت به نسخه‌های قبلی تمرکز یافته بود. نهایتاً آخرین مرحله اتریوم با نام (سرنیتی) (Serenity) معرفی خواهد شد، اما هنوز هیچ تاریخ قطعی برای اجرای آن تعیین شده است.

جدا از ساخت برنامه‌های غیرمتمرکز و دیگر موارد استفاده‌ای که فراهم می‌کند، پلتفرم اتریوم این قابلیت را به کاربران می‌دهد تا سازمان خودگردان غیرمتمرکز (DAO) ایجاد کنند. بطور اساسی این‌ها نهادهایی هستند که دارایی‌های دیجیتال را نگه داشته و آن‌ها را با توجه به قوانین از پیش تعیین شده به روش‌های مختلفی خرج می‌کنند. این قوانین در قراردادهای هوشمند که توسط شخصی یا گروهی از افراد نوشته شده، گنجانده شده است. بازه سرمایه‌پذیری اولیه‌ای وجود دارد که کاربران با خرید توکن و ادعای مالکیت بر روی آن‌ها می‌توانند سرمایه DAO را افزایش دهند. پس از اینکه بازه زمانی سرمایه‌پذیری تمام شد، دائو شروع به کار می‌کند. کاربران برای نحوه صرف سرمایه جمع‌آوری شده می‌توانند طرح‌های پیشنهادی خود را ارائه دهند و اعضایی که توکن‌ها را خریداری کرده‌اند می‌توانند به طرح‌های پیشنهادی رای مثبت یا منفی دهند. لازم به ذکر است که با تمام این اوصاف، توکن‌های خریداری شده واقعاً به معنی حق مالکیت نیست. در عوض، آن‌ها درباره مسائل مختلف به مردم حق رأی‌دهی می‌دهند. از آنجا که اجماع بیت کوین توسط تیم اصلی توسعه و شبکه استخراج آن حاصل می‌شود، بیت کوین اساساً اولین DAOای بود که به وجود آمد. دیگر سازمان‌های خودگردان غیرمتمرکز بر روی بستر اتریوم ایجاد شدند.

نام یکی از این پروژه‌های به خصوص (The DAO) بود که توسط یک تیم استارت‌آپ آلمانی به نام Slock.it هدایت می‌شد. پروژه DAO این قابلیت را به کاربران می‌داد که با استفاده از قراردادهای هوشمند وسایل خود نظیر ماشین، آپارتمان و این قبیل چیزها را همانند نسخه‌ی غیرمتمرکزی از اِیربی‌ان‌بی به اشتراک بگذارند. به طریقی DAO موفق شد تا به بزرگترین پروژه سرمایه‌پذیری جمعی تاریخ تبدیل شود و بیش از ۱۵۰ میلیون دلار سرمایه از ۱۱ هزار عضو جمع‌آوری کند. هیچ نیازی به توضیح اضافه نیست که این مقدار پول بسیار بیشتر از آن چیزی بود که سازندگانش برای به دست آوردن آن امید داشته یا حتی آمادگی مدیریت آن را داشتند.

ماجرا را کمی جلوتر ببریم و به جایی برسیم که DAO هک شد. مهم است بدانیم که باگ کار گذاشته توسط هکر، در شبکه اتریوم یافت نشده بود و این پلتفرم به خوبی به فعالیت خود ادامه می‌داد. تمامی سیستم‌های شبکه شده در مقابل حملات هکری آسیب‌پذیر هستند. حتی خود هکر هم بعداً اظهار داشت که به سادگی از خطای فنی که در کد DAO وجود داشته، سواستفاده کرده است.

هرچند در ۱۷ ژوئن سال ۲۰۱۶ شخصی شروع به انتقال پول‌های DAO به دائوی کوچک (Child DAO) کرد که ساختار DAO را کپی کرده بود. در انتها این هکر موفق شد ۵۰ میلیون دلار اتر از پروژه سازمان خودگردان غیرمتمرکز بیرون بکشد. قیمت اتر پس از این اتفاق از ۲۰ دلار به ۱۳ دلار سقوط کرد. این در حالی بود که اتریوم هیچ نقشی در این قضیه نداشت و پروژه The DAO با هکی که اتفاق افتاده بود، باید به تنهایی با این فاجعه روبرو می‌شد.

آن‌ها تنها موفق به جلوگیری از ته کشیدن سرمایه شدند و آن‌ها را به سوی قرارداد هوشمند دیگری هدایت کردند. اما این فقط یک راهکار موقت بود. به دلیل ساختار کدنوشته شده توسط The DAO، این امکان وجود داشت که هکر همچنان بر روی این سرمایه ادعای مالکیت داشته باشد. مداخله از سوی تیم اتریوم امری لازم به نظر می‌رسید. در دنیای ارزهای دیجیتال این مداخلات (فورک) نام دارند. در ابتدا سافت فورکی پیشنهاد شد که اساساً مانند دکمه ریست شبکه غیرمتمرکز بود. در واقع براساس این فورک شبکه اتریوم به عقب بازمی‌گشت و پروژه

The DAO و تمامی پول‌هایی که جمع‌آوری کرده بود را به قرارداد هوشمندی انتقال می‌داد که مبلغ جمع‌آوری شده را تنها به سرمایه‌گذاران واقعی می‌توانست بازپرداخت کند.

هرچند طرح پیشنهادی ارائه شده سوال مهمی درباره ماهیت شبکه به وجود آورد که به جدایش جامعه اتریوم منجر شد. یکی از ابتدایی‌ترین و مهم‌ترین خصوصیات شبکه، ماهیت غیرمتمرکز آن با این مضمون بود که تمام قدرت تصمیم‌گیری درون جامعه پخش شده است. قدم برداشتن در جهت رفع مشکل پیش‌آمده به معنی زیرپا گذاشتن کامل این قاعده بود. علاوه برآن، قبول طرح پیشنهادی نیازمند این بود که بیشتر ماینرهای اتریوم به بازگشت شبکه رای دهند، اما نقص امنیتی که طی فرایند رأی‌گیری به‌وجود آمد، اختیار انتخاب آن را به کل حذف کرد.

تنها گزینه‌ای که باقی‌مانده بود، اجرای یک هاردفورک بود. این اساساً به این معنی بود که نسخه جدیدی از شبکه اتریوم با اندکی تغییر در قوانین به وجود آید. پس از آن بود که ماینرها، صرافی‌ها، کاربران عادی و دیگر برنامه‌های بزرگ باید تصمیم می‌گرفتند که بخشی از نسخه جدید اتریوم باشند یا بر روی نسخه اصلی به فعالیت خود ادامه دهند. طرح پیشنهادی هاردفورک میان دارندگان اتر به رأی گذاشته شد و اکثریت آن‌ها که نزدیک به ۸۹ درصد رای‌دهندگان را تشکیل می‌دادند، به اجرای هاردفورک رای دادند و نهایتاً در تاریخ ۲۰ جولای ۲۰۱۶ هاردفورک اتریوم اتفاق افتاد.

اتریوم کلاسیک پس ازاتفاق افتادن هاردفورک متولد شد. اساساً از آنجایی که این ارز دیجیتال بلاک چین خودش را داشت و مستقل از اتریوم بود، باید به عنوان ارز دیجیتال جدید با آن برخورد می‌شد. خصوصیات دو بلاک چین پیش از بلاک ۱۹۲۰۰۰۰ که برای هاردفورک تعیین شده بود تا پول سرمایه‌گذاران پروژه The DAO را به صاحبانشان برگرداند، کاملاً یکسان بود. در حال حاضر اتریوم کلاسیک ویژگی‌هایی که اتریوم ارائه می‌دهد را نیز شامل می‌شود.

هرچند، شرایط پس از آن گیج‌کننده شده است. اول از همه، وجود دو بلاک چین در بین سرمایه‌گذاران و کاربران عادی سردرگمی ایجاد می‌کند. به علاوه این می‌تواند به حملات بازپخش (replay attack) بر روی هر دو زنجیره بلاک ختم شود. زیرا از آنجا که امضای رمزنگاری برای یک تراکنش انجام شده بر روی یک زنجیره ثبت می‌شود، تراکنش مشابهی می‌توان بدون رضایت کاربر یا اطلاع او، بر روی زنجیره دیگر تکرار کرد.

بوترین موسس و سردبیر مجله بیت کوین بود. این پروژه به صورت آنلاین و با همراهی ویتالیک و دیگر موسس آن یعنی میهای آلیسی آغاز شد. در ابتدا که وضعیت مالی مجله و دو موسس آن خوب نبود، این دو در ازای دریافت بیت کوین در انجمن‌های مختلف، مقالاتی با محوریت بیت کوین می‌نوشتند. هر چند در سال ۲۰۱۲ اولین نسخه پرینت‌شده که از آن به عنوان اولین مجموعه کاملاً اختصاص یافته به ارزهای دیجیتال یاد می‌شود، منتشر شد. این نسخه به تمامی مشترکان مجله در سراسر دنیا ایمیل شد، و برخی کتاب‌فروشی‌ها از جمله بارنز اند نوبل نیز آن را به فروش رساندند. ویتالیک هر هفته نزدیک به ۱۰ الی ۲۰ ساعت بر روی نشریه وقت می‌گذاشت. ویتالیک بوترین تا سال ۲۰۱۴ در این پروژه شرکت داشت. مجله بیت کوین در حال حاضر توسط BTC Media خریداری شده و اداره می‌شود.

ویتالیک همچنین در لجر که یک ژورنال علمی برای انتشار تحقیقات انجام شده بر روی فناوری ارزهای دیجیتال و بلاک چین بوده و دانشگاه پیتسبرگ حامی آن است، به عنوان داور همتا فعالیت داشته است.

در ماه مارس ۲۰۱۷، چندین استارت‌آپ بلاک چینی، برخی شرکت‌های فورچون ۵۰۰، مراجع آکادمیک و عرضه‌کنندگان فناوری ساخت پیمان تشکیلاتی اتریوم (EEA) را اعلام کردند که آن زمان نزدیک به ۳۰ نفر عضو اصلی داشت. در زمان نگارش این مقاله بیش از ۱۵۰ عضو در این پیمان حضور دارند که شامل شرکت‌های بزرگ بین‌المللی نظیر مسترکارت، سیسکو، سامسونگ اس‌دی‌اس، مایکروسافت، اینتل و بسیاری دیگر می‌شوند.

هدف از این پیمان ایجاد پل ارتباطی بین اعضای آن و متخصصین موارد مرتبط با اتریوم است تا امر آموزش انجام شده و سپس از عهده توسعه برنامه‌های پرتقاضا و پیچیده سازمانی بر بستر اتریوم برآیند. بسیاری از شرکت‌هایی که در زمینه بانکی، مدیریت، مشاوره، فناوری، سرگرمی و صنایع دیگر فعال هستند، با متخصصین اتریوم برای پیگیری امکان پیاده‌سازی فناوری‌های بلاک چین در عملیاتشان در ارتباط هستند.

علی‌رغم موضع سردرگم و سفت و سخت دولت چین در برابر بیت کوین و سایر ارزهای دیجیتال، فناوری بلاک چین و پلتفرم اتریوم شدیداً در حال پذیرش توسط کسب‌وکارهای بزرگ و کوچک در سراسر این کشور است. شخصیت ویتالیک نیز نقش اساسی در توسعه این امر داشته است؛ مخصوصاً اگر این را در نظر داشته باشیم که ویتالیک تنها با استفاده برنامه‌ای در گوشی‌اش طی چندماه زبان چینی را یاد گرفت.

در کشور چین، اتریوم در سطوح سازمانی مورد تحقیق و استفاده قرار می‌گیرد. برای نمونه، دانشگاه پکینگ که برترین دانشگاه این کشور از نظر رتبه‌بندی است، آزمایشگاه اتریوم ایجاد کرده است و بر روی بهبود پروتکل و کاربردهای آن در زنجیره تأمین چین و بازار انرژی در حال تحقیق است. نهاد سلطنتی چاپ پول چین که از واحدهای وابسته به چاپ و عرضه اسکناس چین است، در حال پژوهش بر روی استاندارد ERC20 اتریوم و قراردادهای هوشمند برای دیجیتالی کردن یوان چین است. همچنین چندین شرکت و استارت‌آپ در این کشور که از اعضای پیمان تشکیلاتی اتریوم نیز هستند، با صرف منابع و نیروی انسانی فراوان بر روی پیاده‌سازی جنبه‌های مختلفی از پلتفرم اتریوم تمرکز کرده‌اند.

در ماه می ۲۰۱۶، یازده بنگاه معاملاتی کالای منطقه‌ای، بورس سهام و بازار خرید و فروش دارایی‌های مالی اتحاد چاینالجر(ChinaLedger) را به وجود آوردند. هدف از این اتحاد، ایجاد پروتکل بلاک چین متن‌بازی بود با چارچوب قوانین چین در این حوزه مطابقت داشته باشد و به توسعه‌دهندگان اجازه دهد که در آینده قادر به ایجاد برنامه‌های کاربردی بر بستر آن باشند.

کارگروه اینترنت از سازمان امنیت چین نیز در قالب مشاوره از برخی اعضای برجسته جامعه بلاک چین مانند ویتالیک بوترین استفاده می‌کند.

ماهیت پایه و اساسی ارزهای دیجیتال که غیرمتمرکز بودن و ذات غیرقابل کنترل آن‌هاست، به طریقی یاغی‌گرانه و ضدسازمانی تلقی می‌شود؛ موردی که هیچ‌وقت به کام روسی‌ها خوش نیامده است. علاوه بر این، روسیه خانه بسیاری از دانشمندان کامپیوتر است که ویتالیک نیز علی‌رغم مهاجرتش در سن ۶ سالگی یکی از نمونه‌های بارز این افراد به شمار می‌آید. تمامی این فاکتورها او را مثال برجسته، مورداحترام و تحسین‌شده‌ای در روسیه کرده است.

در آگوست ۲۰۱۷، بیش از ۵۰۰۰ نفر برای سخنرانی بوترین در مرکز نوآوری اسکولکوو گرد هم آمدند. ویتالیک بین گفته‌هایش اشاره کرد که روسیه به همراه انگلیس و سنگاپور بین سه کشور برتر در زمینه تحقیق و آزمایش بر روی فناوری‌های بلاک چین است. نکته دیگر تعداد بالای نودهای شبکه اتریوم در شهر مسکو روسیه است که یکی از بزرگترین خوشه‌های نود را در سراسر جهان رقم زده است.

ویتالیک بوترین همچنین با اشاره به اینکه رئیس‌جمهور روسیه، ولادیمیر پوتین، از پتانسیل فناوری بلاک چین آگاه است، اظهار داشت که این به معنی قرارداشتن این فناوری در کانون توجهات است. بوترین با پوتین طی این ملاقات دیدار کرد بطوریکه برخی رسانه‌ها ادعا کردند این دیدار از دلایل سفر ویتالیک محسوب می‌شد. طی این ملاقات بوترین از فرصت‌های موجود در روسیه برای استفاده از فناوری‌هایی که توسعه داده سخن گفت و به نظر می‌رسد که رئیس جمهور نیز از این ایده حمایت کرد. طبق گزارش‌های قبلی پوتین علاقه فراوانی به ایده اقتصاد دیجیتال دارد و به همین دلیل روسیه در حال حاضر فرصت‌های مرتبط با بلاک چین را در زمینه‌های رهگیری کالا، احراز هویت اشخاص و محافظت از حق مالکیت دیجیتال بررسی می‌کند.

در اکتبر ۲۰۱۷ اسبربانک، بزرگترین بانک روسیه، اعلام کرد که عضو پیمان تشکیلاتی اتریوم شده است. پیش از آن تنها عضو روسی این پیمان، شرکت روسی QIWI که یک شرکت ارائه‌دهنده خدمات پرداخت الکترونیک است، بود. قبل از این اسبربانک گزارش داده بود که با قانون‌گذاران، وزارت اقتصاد، دیگر بانک‌های روسی و اتاق بازرگانی بین‌المللی روسیه در حال همکاری است و آزمایش بر روی اعتبارنامه و ضمانت‌نامه‌های هوشمند را به پایان رسانده است.

ویتالیک طی سفرش به روسیه در آگوست ۲۰۱۷، با ولادیسلاو مارتینوف مدیرعامل یوتا سرویس که یک شرکت ارتباطات و مخابراتی گوشی در روسیه است، به تفاهم رسید. این تفاهم‌نامه شامل ساخت نهادی جدید تحت عنوان اتریوم روسیه بود که آموزش، برگزاری رویداد و مروری بر معماری بانک دولتی وی‌تی‌بی بانک را فراهم می‌کرد. همچنین، این بانک تأمین مالی توسعه یک مرکز جدید برای پژوهش در زمینه بلاک چین را در دانشگاه ملی مطالعات فناوری روسیه به همراه اتریوم روسیه به عهده خواهد گرفت. این مرکز جدید راه‌حل‌های جدیدی در خدمات دولتی که با بدنه قانونی و سازمانی سازگار است، ارائه خواهد داد.

در ۲۵ ژوئن سال ۲۰۱۷، اخبار جعلی منتشر شد که ادعا داشت ویتالیک بوترین طی سانحه رانندگی کشته شده است. این خبر منجر به کاهش ۴ میلیارد دلار از حجم بازار اتریوم شد. این خبر از وبسایتی نشأت گرفت که بهشت ترول‌ها (افرادی که از عمد پیام‌های آزاردهنده می‌فرستند) است. هرچند اتریوم ارزش از دست رفته خود را بازیافت اما این شوخی باعث شد تا نقش اساسی ویتالیک در پلتفرم اتریوم و کل جامعه ارزهای دیجیتال و بلاک چین مشخص شود. از این رو شاید ناشناس ماندن خالق (یا خالقین) بیت کوین روش بسیار هوشمندانه‌ای به حساب آید.

هم‌اکنون

این روزها ویتالیک در سنگاپور زندگی می‌کند و بر روی چیزی که چندسال پیش خلق کرد، به شدت در حال کار کردن است. در اولین روزها، تنها سه نفر بر روی پروتکل‌های اتریوم کار می‌کردند اما او امیدوار است که تیم پروژه یک روز به نقطه‌ای برسد که کمتر و کمتر به وجود او نیاز باشد. او درمورد آینده پلتفرم خوش‌بین است و در این باره عقیده دارد تنها چیزی که می‌تواند اتریوم را نابود کند، خود اتریوم است. بوترین و تیم او آماده عرضه نسخه‌های جدید، پایدارتر، امن‌تر و بهینه‌تری از اتریوم هستند و بزرگترین چالش‌های پیش رو را مقیاس‌پذیری، بهینه‌سازی، به صرفه بودن از نظر اقتصادی و امنیت می‌دانند.

جایزه ها

- جایزه تیل فلوشیپ (۲۰۱۴)
- جایزه WTA در بخش نرم‌افزار آی‌تی (۲۰۱۴)
- قرارگرفتن در لیست فورچون ۴۰
- قرارگرفتن در لیست فوربز ۳۰

واژه نامه

HODL

یک میم اینترنتی و اصطلاح عامیانه است که در جامعه بیت کوین و ارزهای دیجیتال برای تاکید بر نگهداری و عدم فروش آن ها، استفاده می شود.

سال ۲۰۱۳ هنگام سقوط نسبتا بزرگ بیت کوین، در انجمن جهانی (بیت کوین تاک) در حالی که سرمایه گذاران نا امید مشغول بحث درباره نگه داری یا فروش بیت کوین هایشان بودند، کاربری با نام مستعار GameKyuubi، پستی با عنوان I AM HODLING (من نگه می‌دارم) درج می‌کند. او به جای I AM HODLING ،I AM HOLDING را اشتباها نوشته بود. این کاربر که به نظردر زمان نگارش پست مست بوده است، قصد اعلام نگهداری بیت کوین ها و عدم فروش آن ها را داشته است. همین موضوع باعث شد تا اصطلاح HODL در فضای ارزهای دیجیتال و بیت کوین بسیار محبوب شود و برای توصیه به نگهداری ارزهای دیجیتال و عدم فروش آن ها استفاده شود. در حال حاضر یک ارز دیجیتال هم به نام HODL وجود دارد.

FOMO

مخففFear of missing out))، که به معنای ترسِ از دست دادن است. از این اصطلاح در فضای ارزهای دیجیتال، زمانی استفاده می‌شود که فردی نگران از دست رفتن سود سرمایه گذاری یا تصمیمش باشد.

ATH: بالاترین قیمت تاریخ

مخفف (All time high) به معنای بالاترین قیمت تاریخ. از این اصطلاح زمانی استفاده می‌شود که قیمت یک ارز، سهام یا چیزهایی شبیه این، به رکورد جدیدی برسد.

BEAR

این اصطلاح از اشخاص فعال در وال استریت گرفته شده است. از واژه خرس در حوزه اقتصاد برای بیان موارد نزولی و کاهشی یک دارایی استفاده می‌شود. مثلا بازار خرسی به معنای بازار نزولی و رو به پایین است.

BULL

این اصطلاح از اشخاص فعال در وال استریت گرفته شده است. از واژه گاو در حوزه اقتصاد برای بیان موارد صعودی و افزایشی یک دارایی استفاده می‌شود. مثلا بازار گاوی به معنای بازار صعودی و رو به بالا است.

WHALE

این واژه در میان قماربازان کاربرد داشته است. نهنگ ها معامله گران سرمایه داری هستند که مقدار زیادی از آن سکه را در اختیار دارند و هر زمان که شروع به خرید و یا فروش دارند با توجه به حجم معاملات و یا اعتبار آنها می توانند روی روند بازار تاثیر بگذارند

BEARWHALE

نهنگ های خرسی معامله گران سرمایه داری هستند که مقدار زیادی از دارایی خود را می‌فروشند و باعث یک کاهش قیمت در بازار می‌شوند.

BAGHODLER

به سرمایه گذار و مخصوصا معامله گری که در نگهداری غیرمنطقی یک دارایی پافشاری می‌کند، اصطلاحا bag-holder یا از دیدگاه طنز BAGHODLER می‌گویند.

REKT

کلمه (REKT)، یک نگارش عمدا اشتباه از کلمه (wrecked) است که به معنای (نابود شده) است. از این اصطلاح برای اشاره به ورشکستی و یا نابودی افراد در بازارهای اقتصادی استفاده می‌شود.

TO THE MOON

این اصطلاح در بیان اخبار صعود بسیار بزرگ یک دارایی استفاده می‌شود.

ADDY

این اصطلاح به آدرس کیف پول یک ارزهای دیجیتال اختصاص دارد.

FUD

مخفف کلمات متوالی (Fear, uncertainty, and doubt)، به معنای ترس، عدم قطعیت و شک است. از این اصطلاح معمولا برای اشاره به عدم اطمینان از یک موقعیت استفاده می‌شود.

shitcoin

ارز بی ارزش

CHOYNA

یک اصلاح رایج برای اشاره به چین. کشور چین علی رغم مخالفت دولت، در فضای بیت کوین بسیار فعال است. عمده استخراج و معاملات ارزهای دیجیتال در دست افراد چینی است.

Satoshi

یک ساتوشی کوچکترین واحد بیت کوین است. این نام از ساتوشی ناکاموتو، خالق بیت کوین نامگذاری شده است. یک واحد ساتوشی برابر با ۰.۰۰۰۰۰۰۰۱ بیت کوین است.

Confirmation

زمان انجام یک تراکنش، بلاک چین معتبر بودن آن را تایید می کند. تأیید توسط ماینرها انجام می شود.

Recovery phrase

کلمات تصادی ۱۲، ۱۸و یا ۲۴ کلمه ای که در زمان گرفتن بک آپ به شما داده می شود. با این کلمات خواهید توانست که در کیف پول دیگری، کیف پول خود را بازیابی کنید.

Transaction ID

رشته ای حروف و ارقام مختلف است که از طریق آن شما می توانید جزئیات کلی یک تراکنش را روی بلاک چین مشاهده کنید.

Transaction Fees

هزینه ای که کاربران برای تایید تراکنش پرداخت می کنند. حداقل این هزینه در زمان های مختلف و نسبت به شلوغی شبکه متفاوت است. هر چه کارمزد بیشتر باشد تراکنش ما زودتر تایید خواهد شد.

P2P

همتا به همتا به معنای ارتباط مستقیم و بدون واسطه ی دو شخص حقیقی یا حقوقی است.

Faucet

سایت هایی که در قبال کارهایی مانند بخت آزمایی یا بازی کردن، به کاربران ارز دیجیتال می دهند که اغلب برداشت از این سایت ها بسیار سخت است.

Fiat

پول کاغذی تنظیم شده و متمرکز (و البته بدون پشتوانه) هر کشوری را فیات می گویند.

Block Reward

در پروتکل های اثبات کار مثل بیت کوین یا اتریوم، با استخراج هر بلاک، مقداری از ارز بومی آن شبکه به استخراج کننده می رسد. در حال حاضر پاداش استخراج هر بلاک ۱۲.۵ بیت کوین است که به مرور زمان کمتر می شود.

Block Hight

بعد از اولین بلاک هر ارز دیجیتال، به آخرین بلاک استخراج شده آن ارتفاع بلاک می گویند.

Halving

پس از هر ۲۱۰,۰۰۰ بلاک در بیت کوین، پاداش بلاک نصف می شود.

DYOR

مخفف عبارت "Do Your Own Research" یعنی خودت تحقیق کن. وقتی یک نفر پاسخ سوال یا پیشنهادی را می‌دهد، گاهی از این اصطلاح استفاده می‌کند تا شخص خواننده صرفا به خاطر گفته‌های شخص دست به اقدامی نزند و خود نیز تحقیق کند و به این ترتیب شخص پاسخ دهنده، مسئولیت را از دوش خود برمی‌دارد. این اصطلاح غیر از حوزه ارزهای دیجیتال، در سایر زمینه‌ها نیز به کار برده می‌شود.

BTFD

بخرش تا دیر نشده

Bitcoin Maximalists

به افرادی متعصبی گفته می‌شود که فقط به بیت‌کوین باور دارند و برای سایر آلتکوین‌ها ارزشی قائل نیستند. این اصطلاح توسط افرادی که به آلتکوین‌ها اعتقاد بیشتری دارند به افراد طرفدار بیت‌کوین نسبت داده شده است. اصطلاح دیگر برای این افراد، Bitcoinerاست.

BTFD

مخفف جمله "Buy the F*cking Dip" است که در بین معامله‌گران رایج است. مفهوم این است که کوین مورد نظر را در کف قیمت خریداری کنید. کف قیمت جایی است که انتظار می‌رود قیمت از آن پایین‌تر نیاید.

Exit Scam

به ارزهایی گفته می‌شود که پس از بدست آوردن شهرت کافی، بیت کوین‌هایی که از سرمایه‌گذاران بدست آورده‌اند را برمی‌دارند و ناپدید می‌شوند. این اصطلاح در ICO ها زیاد بکار برده می‌شود.

FUD

مخفف "Fear, Uncertainty, and Doubt" به معنای ترس، بلاتکلیفی و تردید است. این شرایط احساسی ممکن است در سرمایه‌گذاران و معامله‌گران به دلایل مختلف روی دهد. گاهی اوقات افرادی با انتشار اخبار منفی و شایعاتی مانند کلاهبردار بودن یا هک شدن آن ارز، در تلاش هستند FUD را در ذهن افراد ایجاد کنند . گاهی اوقات هدف از اینکار این است که افراد زیادی شروع به فروش ارز کنند و قیمت ارز پایین بیاید و خودشان خرید کنند.

KYC

به طور کلی KYC کوتاه شده‌ی عبارت Know Your customer، به معنی (مشتری‌ات را بشناس) است. در این روش یک نهاد دارای تراکنش‌های مالی با دریافت یک سری اطلاعات از مشتری، خود را نسبت به مشکلات قانونی کاربر و پیگیری‌های احتمالی بیمه می‌کند. این قانون دو طرفه بوده و از هر دو طرف معامله محافظت می‌کند. با داشتن این اطلاعات، مشاوران سرمایه‌گذار یا صرافی‌ها با توجه به وضعیت مشتری خدمات بهتری به مشتری می‌دهند و همچنین طرف مقابل از ریسک ارائه‌ی خدمات غیرقانونی مانند پول‌شویی محافظت می‌شود.

KYC

قانون KYC یک الزام اخلاقی برای همه‌ی افرادی است که در صنعت اوراق بهادار چه هنگام باز کردن حساب و چه نگهداری از آن هستند. در این خصوص دو قانون در جولای ۲۰۱۲ تصویب گردید. این قوانین برای حفاظت از کارگزار/فروشنده و مشتری به طوری که روابط بین این دو منصفانه باشد، به وجود آمده‌اند.

از مواردی که توسط قانون KYC کنترل می‌شود می‌توان به موارد زیر اشاره کرد:

- جمع‌آوری و تجزیه و تحلیل اطلاعات اساسی مانند اسناد هویت (که در قوانین و مقررات ایالات‌متحده به عنوان (برنامه شناسایی مشتری) یا CIP خوانده می‌شود)
- تطبیق هویت فرد با احزاب سیاسی (شخص مقام سیاسی خاصی داشته باشد که این عنوان هم PEP نامیده می‌شود)
- تعیین میزان ریسک مشتری برای اعمال تروریسی، پول‌شویی یا سرقت اطلاعات افراد
- ایجاد یک چهارچوب برای رفتارهای مالی مشتری
- زیر نظر گرفتن تراکنش‌های مشتری در برابر رفتارهای ناهنجار و همچنین ذخیره‌ی اطلاعات افرادی که مشتری با آن تراکنش ایجاد می‌کند.

AML (Anti Mony Laundry)

قانون ضد پولشویی

Stable coin

ارزهای با پشتوانه یک ارز فیات مانند دلار و یا کالای ارزشمند مانند طلا که همیشه دارای ارزشی ثابت با مقداری تعیین شده با آن ارز یا کالا را دارند. یک True USD همیشه یک دلار است.

PUMP and DUMP

کسانی که روی کالا و سهام سرمایه گذاری هنگفتی می کنند و سپس به شدت تبلیغات انجام می دهند، اغلب از اظهارات دروغین و گمراه کننده استفاده می کنند. مثلا با تبلیغات ادعا می کنند که اکنون بهترین موقع برای خرید ارز است و یا با ایجاد تراکنش های سوری حجم معاملات را بصورت غیر واقعی بالا می برند این باعث افزایش تقاضا و بالا رفتن قیمت می شود که PUMP نامیده می شود. هنگامی که دامپ رخ دهد، افراد مورد نظر سهام خود را با بالاترین قیمت می فروشند. این کار معمولا برای آنها سود به همراه دارد اما باعث می شود که ارزش همان کالا بعد از مدتی پایین بیاید. این بخش از اصطلاح "دامپ" نامیده می شود.

بازارهای ارزدیجیتال به اندازه بازارهای دیگر مستعد پذیرش استراتژی های پامپ و دامپ هستند. برای در امان ماندن از آن، باید از سرمایه گذاری زیاد و تهاجمی اجتناب کرد و سرمایه گذاران باید به سرعت منشا اطلاعات نادرست را دریابند.

منابع

https://arzdigital.com

https://mihanblockchain.com

https://fa.wikipedia.org

https://coiniran.com

https://arznegar.com

http://blockchainlabs.ir

https://irancryptomarket.com

https://pishro-asak.com

https://pishro-asak.com

https://www.coinit.ir

https://finmag.ir

https://way2pay.ir

https://manapal.ir

https://blog.dericoin.com

https://coinextend.com

https://virgool.io

https://arzjoo.com

https://www.bourseiness.com

http://hrahmani.ir

https://donya-e-eqtesad.com