اثبات سهم و استیبل‌کوین‌ها: معضل تمرکز

نویسنده: Lyn Alden

ترجمه: مجید گتمیری

ویرایش: ضیا صدر

چاپ اولیه: نوامبر ۲۰۲۱

پس از مقاله‌ی من در ژانویه‌ی ۲۰۲۱ درباره‌ی اتریوم، که بیش از یک‌چهارم میلیون بار خوانده شد، چند باری از من درخواست شده نظراتم را درباره‌ی اتریوم به‌روز کنم.

در آن مقاله‌ی قبلی، من اتریوم را شرح دادم، محدوده‌هایی که دیدگاهم صعودی بود را شرح دادم، اما همچنین نگرانی‌های اساسی خودم را درباره‌ی آن اظهار کردم. محتوای کلی مقاله مسئله‌ای بحرانی در اتریوم بود، که به همین دلیل هم آن میزان توجه را به خود جلب نمود. در آن مقاله من همچنین درباره‌ی ازدیاد استیبل‌کوین‌ها در سال‌های پیش‌رو کاملاً دیدگاه صعودی داشتم.

من قصد ندارم در اینجا محتوای دیدگاه‌های قبلی‌ام را بشکافم، اما برای یک پیش‌زمینه، اعضای سرویس پریمیوم من از نقطه نظرات به‌روزشده‌ی من درباره‌ی اتریوم اطلاع دارند. چون پس از آن مقاله‌ی اولیه، من تقریباً هر ماه دیدگاه‌هایم را درباره‌ی اتریوم به‌روز می‌کردم.

خلاصه‌ی آن تعداد گزارش این بود که من مشکلات زنجیره‌ی‌بلاک اتریوم که شامل هک شدن DeFiها، مشکلات تمرکز، گسست‌زنجیره‌ی ناخواسته، سفته‌بازی در NFTها و ... بود را بطور مکرر شرح دادم، اما از وقتی از ماه ژانویه شروع به پوشش مرتب این مورد نمودم، از نظر تاکتیکی راجع به قیمت در میان‌مدت دیدگاه صعودی داشتم.

در زیر به گزیده‌ای از آنها اشاره می‌کنم:

> "برای کسانی که می‌بینند، شکست پرقدرت قیمت ۱۴۰۰ دلار توسط اتریوم باید برای این پروتوکل در میان‌مدت بسیار صعودی باشد، چون مقاومتی بالاسر خود نمی‌بیند."

-۳۱ ژانویه ۲۰۲۱

بر اساس آمار، اتریوم و سایر آلتکوین‌ها در دوره‌ی بازار صعودی می‌توانند کاملاً بازده‌ی بیشتری از بیتکوین داشته باشند. همانطور که در اکثر مواقع این‌طور بوده است. اما من نگران بسیاری از دارایی‌های دیجیتال، خصوصاً دارایی‌هایی غیر از بیتکوین، در دوره‌ی نزولی بازار شاید در سال ۲۰۲۲ و ۲۰۲۳ هستم.

-۱۴ فوریه ۲۰۲۱

مقدار اتر در صرافی‌ها از آگست ۲۰۲۰ روندی نزولی داشته، مشابه اتفاقی که برای بیتکوین در حال وقوع است. در صورت برابری سایر شرایط، دیدگاه من صعودی است.

-۱۴ آوریل ۲۰۲۱

در حالی که من نگرانی‌هایی درباره‌ی طراحی بلندمدت اتریوم و انتقال به اتریوم۲ دارم (قابلیت تغییر سیاست پولی آن نشان می‌دهد چقدر این سیاست پولی بی‌ثبات است)، اما سخت است درباره‌ی قیمت در میان‌مدت دیدگاه نزولی داشت. EIP1559، که در ژانویه در مقاله‌ی عمومی نقادانه‌ام درباره‌ی اتریوم درباره‌اش با دید مثبت نوشتم، وقتی اجرا شود باید اثر بسیار صعودی روی قیمت بگذارد. و با اتریوم۲ که از دسامبر ۲۰۲۰ قابل اجراست، توکن‌های اتر از صرافی‌ها خارج شده و قفل می‌شوند. آغاز به کار EIP1559 همزمان با انتقال به اتریوم۲ (که در حال حاضر اساساً برنامه ریزی بر این اساس انجام شده) در واقع یک طوفان کامل در جهت مثبت برای قیمت در سال پیش رو است. بنابراین، با اینکه در یک افق ۵ ساله من در مقایسه با اتریوم اعتقاد بیشتری به بیتکوین دارم، تحرکات مخصوصی که قیمت‌های اتر را بالا نگه داشته‌اند برای باقیمانده‌ی امسال قدرت بیشتری دارند. هرچند، اتر نیاز دارد قیمت ۲۹۰۰ دلار را بشکند تا دوباره جذاب شود. در حال حاضر در حال تثبیت قیمت است.

-۶ ژوئن ۲۰۲۱

در مجموع، اتریوم در حال حاضر همچنان زیر یک میزان ثابت عرضه باقی می‌ماند (انتشار سهام یک‌طرفه تا شروع به کار اتریوم۲، با حدود ۷/۴ میلیون اتریوم قفل‌شده در حال حاضر)، پس من علیرغم اینکه در بلند مدت در مورد برخی زیرساخت‌های فنی، موارد کاربردی، رقبا و غیره محتاط هستم، اما از نظر تاکتیکی راجع به قیمت دیدگاه صعودی خودم را تا حدودی حفظ خواهم کرد.

-۵ سپتامبر ۲۰۲۱

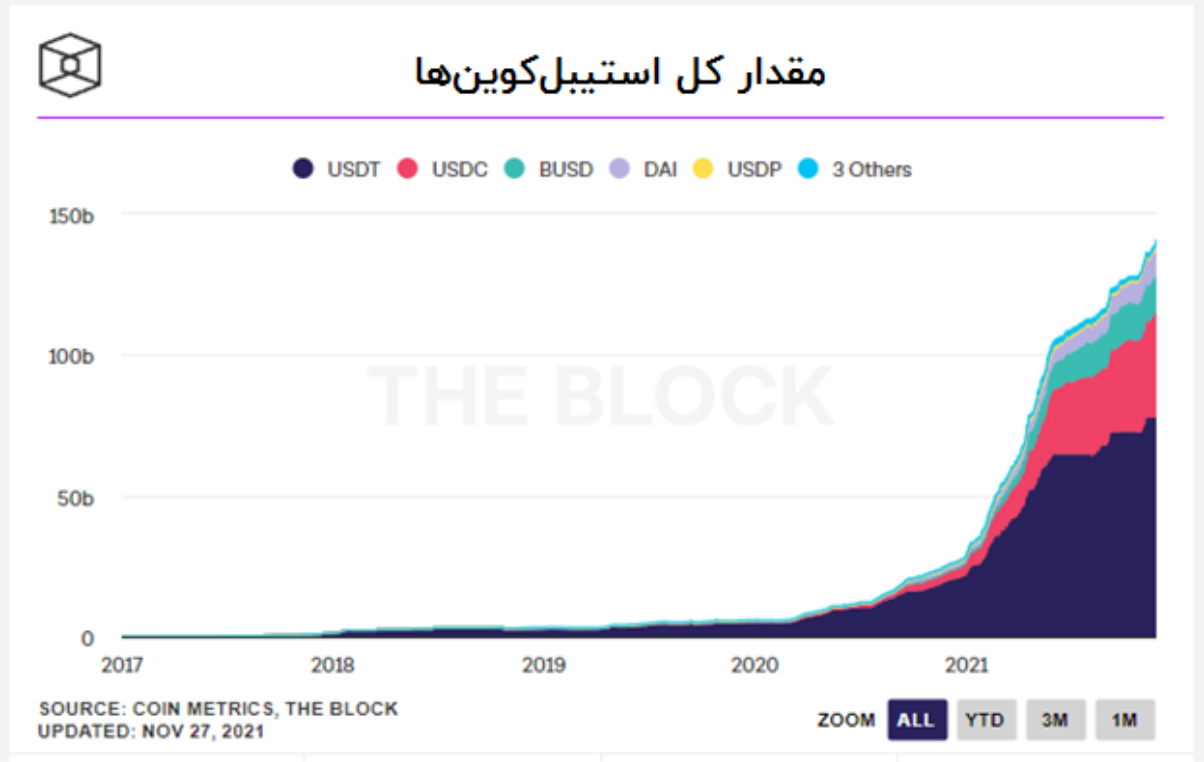
من در مورد رفتار قیمت اتر، علیرغم برخی شبهات درباره‌ی ریسک‌ها و کاربردهای بلندمدت آن، از نظر تاکتیکی دیدگاه صعودی دارم. بخشی از دیدگاه صعودی من بر مبنای قرارداد قفل‌شدن اتریوم۲ است که مقادیر زیادی اتر را درگیر خواهد کرد (بیش از ۸ میلیون تاکنون، که قادر به خارج‌شدن نیست)، و در نتیجه، اتر به سرعتی حتی بیشتر از سرعت خروج بیتکوین، از صرافی‌ها خارج خواهد شد. این فشار عرضه به نحو خوبی مهندسی شده است.

-۳۱ اکتبر ۲۰۲۱

و به نظر می‌رسد دیدگاه من در مورد استیبل‌کوین‌ها هم از زمان انتشار مقاله‌ی ژانویه‌ی ۲۰۲۱ دقیق بوده است، چون مقدار آنها ظرف کمتر از یک سال از ۳۳ میلیارد دلار در زمان نگارش مقاله به ۱۴۰ میلیارد دلار افزایش یافت:

"استیبل‌کوین‌ها از نظر من مشخصاً اهمیت دارند. من در مورد مقدار پولی که در استیبل‌کوین‌ها قفل شده دیدگاه صعودی دارم. این فضایی است که باید مورد توجه قرار گیرد، هم از نظر توسعه‌ی مطلوب و هم توسعه‌ی نامطلوب. دفتر کنترل ارز ایالات متحده در حال حاضر رسماً به بانک‌های ایالات متحده اجازه می‌دهد از استیبل‌کوین‌ها استفاده کنند. آنها از ارزهای فیات شناوری بسیار بالاتری دارند، و می‌توانند پیامدهای مختلفی برای ارزهای دیجیتال بانک‌های مرکزی و سیستم پولی فعلی جهان داشته باشند.

-۱۷ ژانویه ۲۰۲۱



منبع نمودار: The Block

از ژانویه تاکنون در مؤسسات تمایل کمی بیش از انتظار من به اتریوم مشاهده شده، همان‌طور که این تمایل در زنجیره‌های بعدی مثل سولانا هم دیده شده، بنابراین من این مورد را پیوسته زیر نظر قرار داده‌ام. هنوز ریسک‌های قانون‌گذاری فراوانی در مورد این قبیل توکن‌ها وجود دارد؛ بر خلاف بیتکوین این توکن ها عموماً به نظر می‌رسد در چارچوب تعریف اوراق بهادار مالی می‌گنجند.

در ادامه برای این مقاله‌ی عمومی، من به این نتیجه رسیدم که وقت کندوکاو در سه مفهوم مرتبط است که از اتریوم گسترده‌تر اند. اولی درباره‌ی صرفه‌های[1] اثبات سهم به عنوان یک سازوکار کلی اجماع است، دومی درباره‌ی مشکل تمرکز در استیبل‌کوین‌ها است و سومی طیف تمرکزگرایی است که زنجیره‌های قراردادهای هوشمند مختلف بکار می‌گیرند تا با یکدیگر در -کاهش هزینه‌ی- تراکنش‌ها رقابت کنند.

هر سه مورد به یکدیگر ارتباط دارند زیرا بر این مسئله که یک زنجیره‌ی‌بلاک قرارداد هوشمند تا چه میزان واقعاً می‌تواند در قیاس با شبکه‌ی بیتکوین غیرمتمرکز باشد و چگونه نسبت به هم در شرایط قانون‌گذاری خصمانه یا غیرخصمانه عمل می‌کنند تأثیر می‌گذارد.

بنابراین این مقاله می‌تواند به درک برخی نگرانی‌های بلند مدت من در مورد زنجیره‌های بلاک مختلف، حتی در زمان‌هایی که من در مورد قیمت از نظر تاکتیکی دیدگاه صعودی دارم، و در شرایطی که عموماً به مفهوم قراردادهای هوشمند علاقه دارم کمک کند.

من قصد دارم مجدداً اعلام کنم که هنگام تحلیل زنجیره‌های بلاک تا حد امکان سعی می‌کنم جانب انصاف و بی طرفی را رعایت کنم. در حال حاضر بر کسی پوشیده نیست که من کاملاً به پروتکل بیتکوین علاقه‌مندم، اما این مسئله به این دلیل است که من کمترین ایرادات را بر اساس تعدیل ریسک در این پروتکل پیدا کردم. من چندین کلاس دارایی را از سهام گرفته تا اوراق

[1] trade-offs

قرضه و کالا و دارایی‌های دیجیتال بررسی می‌کنم، و اغلب دارایی اشخاص را با این کلاس‌های دارایی مقایسه می‌کنم. بنابراین هنگامی که من زنجیره‌های بلاک را بررسی می‌کنم، به همین روش عمل می‌کنم.

و مهم‌تر اینکه، من مقوله‌ی رفتار تکنیکال قیمت را از ارزشمندی فاندامنتال تفکیک می‌کنم، چون این دو مقوله در بازه‌های زمانی مختلف می‌توانند بسیار متفاوت باشند. این مقاله اشاره‌ای به زنجیره‌های بلاکی مثل اتریوم و سولانا می‌کند، اما به طور گسترده‌تر درباره‌ی مشکل تمرکز زنجیره‌های بلاک اثبات سهم و استیبل‌کوین‌های حضانتی بطور کلی بحث می‌کند، که سرفصل‌های این مبحث می‌تواند به هر زنجیره‌ی‌بلاکی غیر از بیتکوین تعمیم یابد.

بخش‌های مقاله:

اثبات سهم در برابر اثبات کار

پروتکل بیتکوین ساتوشی ناکاموتو با روشی به نام اثبات کار به یک اجماع در تراکنش‌های معتبر می‌رسد. ساتوشی ناکاموتو به جهت توسعه‌ی قبلی آدام بک[۲] در زمینه‌ی اثبات کار، از او به عنوان یکی از هشت مرجع در وایت‌پیپر بیتکوین نام برده است.

از آن زمان، تعدادی از افراد پیشنهاد کرده‌اند روش‌های دیگری برای اجماع، مانند اثبات سهم، بهینه‌تر هستند. اغلب مزیت این پروپزال‌ها با اظهارات ناکافی در مورد برتری‌های این نوع اجماع در مقابل اثبات کار شرح داده می‌شود. این بخش این مفهوم را واکاوی می‌کند.

(خلاصه‌ی این بخش، برای آنها که می‌خواهند بخش‌های مهم این مقاله‌ی طولانی را نگاه بیاندازند، این است که اثبات کار ذاتاً مانند پول است در حالی که اثبات سهم ذاتاً مانند سهام است.)

اثبات کار ۱۰۱

شبکه‌ی بیتکوین برنامه‌نویسی شده تا به طور متوسط هر ده دقیقه یک بلاک ایجاد کند و آن بلاک را به زنجیره‌ای اضافه کند، که شامل صدها هزار بلاک از زمان آغاز به کارش در سال ۲۰۰۹ است.

بلاک جدید توسط ماینر بیتکوین ایجاد می‌شود (یک کامپیوتر مخصوص) که قدرت پردازشی (و در نتیجه الکتریسیته) خود را مشارکت می‌دهد تا یک مسئله‌ی رمزنگاری که بلاک قبلی طرح کرده را حل کند، و در این صورت ماینر می‌تواند هزاران تراکنش بیتکوین که در آن لحظه در صف انتظار هستند را جمع کرده و در آن بلاک قرار دهد. این گونه تراکنش‌ها تسویه می‌شوند. شبکه طوری برنامه‌نویسی شده تا به زمان ایجاد بلاک در هر ده دقیقه برسد، یعنی بطور میانگین هر ده دقیقه یک بلاک شامل هزاران تراکنش به زنجیره‌ی‌بلاک اضافه می‌شود.

پردازنده‌ها حدس‌های تصادفی می‌زنند تا مسئله‌ی طرح شده توسط بلاک قبلی را حل کنند، اما قانون اعداد بزرگ به نحوی است که هر چه تجهیزات ماینینگ بیتکوین بیشتری داشته باشید، در مدت زمانی که به اندازه‌ی کافی طولانی باشد، بلاک‌های بیشتری پیدا می‌کنید.

---

[2] Adam Back

اگر ماینرها شبکه را رها کنند و بلاک‌های جدید بطور متوسط شروع به پیدا شدن در زمان‌هایی بیشتر از ده دقیقه کنند، شبکه طوری برنامه‌نویسی شده تا بطور خودکار بر اساس زمان بدست آمده مسئله را آسان‌تر کند، تا بلاک‌ها به برنامه‌ی زمانی هر ده دقیقه یک بلاک برگردند. برعکس، اگر تعداد زیادی ماینر به شبکه بپیوندند و بلاک‌ها رودتر از هر ده دقیقه یک بلاک به زنجیره اضافه شوند، شبکه مسئله را سخت‌تر می‌کند. این مورد به "تنظیم سختی" معروف است که بطور خودکار هر دو هفته یک بار اتفاق می‌افتد، و یکی از چالش‌های کلیدی برنامه‌نویسی بود که ساتوشی ناکاموتو حل کرد تا شبکه بتواند به درستی کار کند.

بنابراین در هر لحظه، میلیون‌ها ماشین ماینینگ بیتکوین در سراسر جهان به دنبال حل مسئله و ایجاد بلاک بعدی هستند، و یک مکانیزم طبیعی انعکاس بازخورد وجود دارد اطمینان حاصل نماید بلاک‌ها، فارغ از اینکه ماینرهای شبکه چقدر کم یا زیاد باشند، بطور متوسط در هر ده دقیقه ایجاد شوند.

در نیمه‌ی اول ۲۰۲۱ چین (تاکنون بزرگترین کشور از نظر تمرکز ماینرها) ماینینگ بیتکوین را ممنوع کرد، و تقریباً نیمی از شبکه‌ی جهانی بیتکوین خاموش شد و شروع به مهاجرت به سایر مکان‌ها نمود. سرعت شبکه‌ی پرداخت بیتکوین اندکی کاهش پیدا کرد، اما فارغ از این نکته، بطور ۱۰۰ درصد به کار خود ادامه داد. سپس تنظیم سختی شبکه اتفاق افتاد، و شبکه را به سرعت مد نظر برگرداند. تصور کنید اگر به آمازون یا مایکروسافت از یک هفته قبل اطلاع داده می‌شد که باید نیمی از سرورهایشان را در سطح جهان جابجا نمایند؛ احتمالاً در حین جابجایی و بازسازی نیمی از زیرساخت‌هایشان، مشکلاتی در روشن نگه‌داشتن سرویس‌هایشان برای حداقل مابقی سال تجربه می‌کردند. شبکه‌ی بیتکوین در عوض با ۱۰۰ درصد ظرفیت به کار خود ادامه داد.

اگر ماینری یک بلاک نامعتبر ایجاد کند، به این معنا که از قوانین مشترک نودهای موجود در شبکه پیروی نکند، شبکه آن را رد می‌کند. اگر دو ماینر یک بلاک معتبر را در محدوده‌ی زمانی یکسانی ایجاد کنند، بلاک برنده بدین نحو مشخص می‌شود که هر کدام توسط باقی شبکه زودتر دریافت شد و یک بلاک معتبر دیگر به آن اضافه شد، و تبدیل به زنجیره‌ی بلندتر (پ در نتیجه زنجیره‌ی رسمی) گردید آن بلاک معتبر است. اگر بلاک دوم هم در یک محدوده‌ی زمانی ایجاد شد، برنده با ساخت سومین بلاک یا چهارمین بلاک معتبر مشخص می‌گردد.

در نهایت زنجیره‌ی بلندتر برنده می‌شود، زیرا سهم بیشتری از شبکه آن را پیدا کرده و بر روی آن بلاک‌ها را ایجاد می‌کنند.

این فرایند با عنوان "اثبات کار" شناخته می‌شود. میلیون‌ها ماشین از الکتریسیته استفاده می‌کنند تا قدرت پردازش را جهت حدس پاسخ مسئله‌ی رمزنگاری طرح شده توسط آخرین بلاک بکار گیرند. این ممکن است هدر دادن انرژی به نظر رسد، اما همان چیزی است که شبکه را غبرمتمرکز نگاه می‌دارد. کار، در این مورد معیار واقعیت است. هیچ قدرتی که تعیین کند چه چیز جایگزین بلاک معتبر یا تراکنش‌های معتبر می‌گردد وجود ندارد؛ بلندترین زنجیره‌ی‌بلاک در هر زمانی قابل صحت‌سنجی است، و توسط بقیه‌ی شبکه و بر اساس کد به عنوان زنجیره‌ی واقعی شناخته می‌شود.

بلندترین زنجیره‌ی‌بلاک همان است که بیشترین کار بر روی آن انجام گرفته است، و این همان معیار اجماعی است که توسط شبکه بررسی می‌گردد. این زنجیره‌ی‌بلاک تبدیل به اجماع جهانی می‌گردد.

هر چه شبکه‌ی بیتکوین انرژی بیشتری استفاده کند، آخرین تراکنش‌هایش برضد اکثر حمله‌ها امن‌تر خواهد شد. بسیاری از بلاکچین‌های کوچک، قربانی حمله‌ی ۵۱ درصدی شده‌اند، که یک موجودیت واحد بطور موقت یا دائمی کنترل بیش از ۵۱ درصد از قدرت پردارشی شبکه را به‌دست می‌آورد، و این اکثریت قدرت پردازش را برای سازمان‌دهی مجدد بلاک‌ها و ایجاد تراکنش‌های خرج‌کردن دوباره (که اساساً دزدی است) بکار می‌گیرند.

این نمودار، به عنوان نمونه قدرت پردازش شبکه‌ی بیتکوین را در مقایسه با قدرت پردازش برخی از هاردفورک‌های کپی شده از روی بیتکوین نشان می‌دهد.

منبع نمودار: BitInfoCharts.com

هر دو زنجیره‌ی‌بلاک دیگر تنها ۱ درصد یا کمتر از کل قدرت پردازش بیتکوین را دارند، و تحت حمله‌ی re-org[3] قرار گرفته‌اند. در واقع، اگر تنها ۱ درصد از ماینرهای بیتکوین تصمیم بگیرند یک حمله‌ی ۵۱ درصدی به هر یک از این دو هاردفورک انجام دهند، می‌توانند آن را اجرا کنند. اما برعکس آن امکان ندارد، چون شبکه‌ی بیتکوین تقریبا تمامی ماینرها را در اختیار خود دارد و میزان توان پردازشی بسیار بیشتری در حدود صد برابر آن دو شبکه‌ی دیگر دارد.

این نشان دهنده‌ی اهمیت اثر شبکه در صنعت زنجیره‌ی‌بلاک است، و اینکه چرا مصرف انرژی بیتکوین آن را بطور منحصر به فردی امن نگه می‌دارد.

وقتی کسی می‌پرسد، "نمیشه خیلی راحت بیتکوین رو کپی کرد؟"، به همین دلیل جواب "نه" است. شما می‌توانید کد متن‌باز را کپی کنید، اما این حقیقت را که میلیون‌ها دستگاه ماینر با مدار مجتمع و کاربرد خاص در حال تأمین امنیت شبکه‌ی بیتکوین و نه شبکه‌ی کپی شده‌ی شما هستند نمی‌توانید کپی کنید، شما نمی‌توانید این حقیقت را که ده‌ها هزار فول‌نود شبکه در حال تضمین اجماع هستند کپی کنید، و همچنین نمی‌توانید این حقیقت را که هزاران برنامه‌نویس هر روز در حال کار روی بهبود شبکه‌ی بیتکوین و نه شبکه‌ی کپی‌شده‌ی شما هستند کپی کنید. و همچنین لایه‌ی دوم بیتکوین، لایتنینگ، کانال‌های باز و شناوری فراوانی دارد که به آسانی قابل کپی کردن نیست. سال‌ها برای ساخت آن زمان صرف شده است.

سعی در کپی کردن بیتکوین مانند آن است که محتوای ویکی‌پدیا را کپی کرده و بر روی وبسایت خود قرار دهیم. از نظر فنی امکان‌پذیر است، اما فایده‌ی چندانی ندارد. این کار باعث بدست آوردن ترافیک واقعی ویکی‌پدیا نمی‌شود، چون صدها میلیون لینکی که از سایر وبسایت‌ها به آن ارجاع می‌شود را شامل نمی‌شود. و مانند ویکی‌پدیای واقعی به‌روزرسانی نمی‌شود، چون امکان ندارد من بتوانم اکثریت ویراستارهای داوطلب را راضی کنم که بیایند روی ورژن من فعالیت کنند. پس در صورتی که نتوانم از عهده‌ی وظیفه‌ی دشوار قانع نمودن اکثریت شبکه جهت فعالیت بر روی ورژن خودم برآیم، این کپی تنها سایه‌ای از ورژن اصلی با سهم ناچیزی از ارزش آن خواهد بود.

همین مسئله در مورد کپی کردن شبکه‌ی اجتماعی توئیتر هم صادق خواهد بود. من می‌توانم چیزی بسازم و آن را شبیه توئیتر کنم، اما در واقعیت تبدیل به توئیتر با کلی کاربر و برنامه‌نویس نخواهد شد.

اثبات سهم ۱۰۱ (توضیحات پایه‌ای):

بسیار خوب، همانطور که قبلاً گفتیم، اثبات کار سیستمی است که ماینرها با الکتریسیته و قدرت پردازشی بر سر ساخت طولانی‌ترین زنجیره‌ی‌بلاک رقابت می‌کنند، که به زنجیره‌ی مورد قبول تبدیل می‌گردد. بنابراین زنجیره‌ی‌بلاک دیجیتال، از طریق اثبات کار، به منابع طبیعی دنیای واقعی ارتباط دارد.

شبکه‌ی بیتکوین از آغاز به کارش در سال ۲۰۰۹ از طریق اثبات کار عملیاتی شده و تا به امروز هم هیچ برنامه‌ای برای تغییر آن وجود ندارد.

شبکه‌ی اتریوم هم از زمان شروعش در ۲۰۱۵ از طریق اثبات کار فعالیت می‌کند، اما چندین سال است در حال برنامه‌ریزی به تغییر به یک سیستم اثبات سهم است.

بسیاری از زنجیره‌های بلاک جدیدتر برای قراردادهای هوشمند که بعد از اتریوم شروع به کار کرده‌اند، از ابتدا بر اساس اجماع اثبات سهم کار خود را آغاز نمودند، که از این نظر آنها را نسبت به اتریوم پیشگام می‌سازد، البته بدون اثر شبکه‌ای مشخص اتریوم.

بنابراین، اجازه دهید وارد این بحث شویم که اثبات سهم چگونه کار می‌کند.

---

[3] بازنویسی مجدد بلاکچین

اثبات سهم سیستمی است که دارندگان رمزارز سکه‌های خود را قفل یا "استیک[4]" می‌کنند، و از آنها جهت رأی دادن روی زنجیره‌ی معتبر استفاده کرده و بابت ایجاد موفقیت‌آمیز بلاک‌های جدید، با سکه‌های بیشتر پاداش دریافت می‌کنند. به جای صرف الکتریسیته و قدرت پردازشی برای ایجاد بلاک‌های جدید در زنجیره‌ی‌بلاک، آنها استیک سکه‌هایشان را صرف این کار می‌نمایند.

اثبات کار ساده است، زیرا نیازی به مجازات ماینرهای بد که سعی در تأیید زنجیره‌ی اشتباه یا ایجاد بلاک‌های نامعتبر ناسازگار با قوانین شبکه‌ی نودها دارند، نمی‌باشد. مجازات آنها به سادگی این است که برای بلاک‌هایی هزینه‌ی الکتریسیته پرداخته‌اند که معتبر نبوده‌اند یا در بلندترین زنجیره‌ی نهایی جای نگرفته‌اند، بنابراین، پول از دست داده‌اند. آنها با این کار عملاً بر زخم خودشان نمک می‌پاشند، و لذا به ندرت از عمد اتفاق می‌افتد. یک ارتباط محسوس بین زنجیره‌ی‌بلاک و منابع دنیای واقعی وجود دارد.

اثبات سهم پیچیده‌تر است، زیرا هیچ ارتباطی با منابع دنیای واقعی وجود ندارد و سیستم باید راهی برای مجازات استیک‌کنندگانی که به ناحق به نفع زنجیره‌ی "اشتباه" رأی می‌دهند پیدا کند. بعلاوه، آنها راهی نیاز دارند تا مطمئن شوند استیکرها به همه‌ی زنجیره‌های ممکن رأی نمی‌دهند (که در اثبات کار نمی‌توان انجام داد، زیرا نیاز به منابع دنیای واقعی برای انجام هر یک از آنها وجود دارد). بنابراین، اثبات سهم سیستم بسیار پیچیده‌تری است که سعی خواهد کرد در صورت رأی دادن نامناسب، سکه‌های استیک‌کنندگان ا را از آنها بگیرد، و راه‌هایی برای سنجش اینکه آنها به نفع چند زنجیره همزمان رأی ندهند دارد

بن ادگینگتون، یک برنامه‌نویس اتریوم و کسی که موافق تغییر اتریوم به اثبات سهم است، به پادکست کامپس ماینینگ رفت و به زیبایی چالش‌های بلندمدتی که اتریوم در مسیر چندین ساله (و به تأخیر افتاده) ی تغییر از اثبات کار به اثبات سهم با آنها روبه‌رو بوده را شرح داد:

> "دلیلی که این همه طول کشید، شما می‌دانید ما در اتریوم برای بیش از ۵ سال به اثبات کار تکیه کرده بودیم، این است که اثبات سهم پیچیده است. اثبات کار اساساً بسیار ساده است، تحلیل آن آسان است، راه‌اندازی و بکارگیری آن ساده است، و اثبات سهم بخش‌های متحرک بسیاری دارد. شما می‌توانید یک الگوریتم اثبات کار را در چندصد خط (کد) یا در همین حدود بنویسید. کلاینت‌های ما در حال حاضر در حدود صدهاهزار خط کد برای اثبات سهم هستند.
>
> و من فکر می‌کنم مبانی تئوری اثبات سهم برای بلوغ نیاز به زمان داشته‌اند. واضح نیست چگونه می‌شود آن را قدرتمند ساخت، حمله‌هایی مانند حمله‌های با دامنه‌ی طولانی[5] و مسائلی که در اثبات کار وجود ندارد در اینجا وجود دارد، که مجبور بودیم به آنها و راه‌حلشان فکر کنیم، لذا زمانبر شد. بنابراین ما به الگوریتم آزموده‌شده‌ی اثبات کار تکیه کرده بودیم و این روش به خوبی به اتریوم خدمت رسانی کرده است."

میزبان پادکست راجع به اینکه چطور طرفداران اولیه‌ی شبکه‌ی بیتکوین در ابتدا طرفدار اثبات سهم بوده‌اند اما مشخص می‌شود این ایده مسیرهای حمله‌ی بسیار زیادی دارد بحث می‌کند. او سپس از بن می‌پرسد چطور اتریوم و مدل اثبات سهم در مقابل این مسیرهای حمله مقابله می‌کند. بن فکر می‌کند این ایده قدرتمند است و طرفدار آن است، و راه‌حل‌های اثبات سهم را بدین طریق شرح می‌دهد:

> "اولین مشکل اصلی برای حل کردن چیزی بود که ما آن را "ایجاد ابهام[6]" می‌نامیم و به این معناست که اساساً ایجاد بلاک‌ها بدون هزینه است، پس اگر من یک پیشنهاد دهنده‌ی بلاک باشم، می‌توانم دو یا سه یا صد بلاک رقیب ایجاد کنم و آنها را به شبکه ارسال کنم و راه واقعی برای تمایز دادن این بلاک‌ها وجود ندارد. این می‌تواند به شدت مخرب بوده و زنجیره را مورد حمله قرار دهد، مطمئناً زنجیره را دوشاخه کند، و لذا ما از طریق یک مکانیسم به نام "مجازات[7]" برای دفع آن استفاده می‌کنیم. پس اگر یک پیشنهاد دهنده بلاک‌های متناقضی را پیشنهاد دهد، این

---

[4] stake
[5] long range attacks
[6] equivocation
[7] slashing

یک اقدام تهاجمی و مخرب است. شبکه می‌تواند آن را رهگیری کند. یک پیشنهاد دهنده‌ی دیگر می‌تواند بیاید جلو و بگوید اینجا دو بلاک وجود دارد که توسط یک تأییدکننده در یک زمان پیشنهاد شده است، امضای آنها روی آن است، بنابراین نمی‌تواند جعل شود، پس این اثباتی بر این مسئله است که آنها اشتباه بازی کرده‌اند. و سپس بخشی از استیک آنها از ایشان گرفته می‌شود و در این نقطه آنها از شبکه رانده می‌شوند. پس شما تنها یک شانس دارید. در اثبات کار، اگر حمله‌ی ۵۱درصدی شما شکست بخورد، شما می‌توانید شدت را بیشتر کنید و بارها و بارها حمله کنید. در اثبات سهم، تنها یک شانس دارید، شما مجازات[8] می‌شوید، از شبکه خارج می‌شوید، و اتر شما تا مدتی قفل خواهد شد، پس از این نظر تا حدودی خود ترمیم شونده است. بنابراین، این یکی از پیشرفت‌هایی بود که باعث شد مردم فکر کنند "واقعاً یه جورایی می‌توانیم انجامش بدهیم، راه‌حل‌هایی برای حملات مرسوم وجود دارد."

یکی دیگر از این نوع حملات "حمله با دامنه‌ی طولانی" است که به نوعی ظرافت دارد، اما ایده‌ی آن این است که وقتی شما به عنوان یک تأییدکننده از شبکه خارج شدید، بطور مؤثر می‌توانید بعد از گذشت زمانی مشخص برگردید. پس من از شبکه خارج می‌شوم و یک ماه بعد می‌توانم به شبکه برگردم، و (اگر کلیدهای تأییدکننده‌ی کافی داشته باشم) می‌توانم هر تعداد بلاک تاریخی که دلم خواست تولید کنم ، می توانم بطور مؤثر تاریخ متفاوتی را برای زنجیره تولید کنم، و چون از شبکه خارج شده‌ام دیگر نمی توانم مجازات شوم. پس این یک حمله‌ی با دامنه‌ی طولانی است. ما یک تحلیل و درک از این حمله داریم، که بیتکوینرها از آن بدشان می‌آید و ما به آن "خودآگاهی ضعیف[9]" می‌گوییم. ایده‌ی آن اینگونه است که هر کس که بطور مکرر آنلاین باشد امن است، چون شبکه را تحت نظر دارند و همیشه می‌دانند کدام زنجیره صحیح است. اگر با یک نود مخدوش هماهنگ شوید، با اینکه می‌دانید از ابتدا هماهنگ شده‌اید، این خطر وجود دارد که یک زنجیره‌ی مورد حمله را دنبال کنید، پس نیاز به یک نقطه‌ی بررسی دارید، که تضمین کند بر روی زنجیره‌ی درست هستید، و این نقطه را باید از کسی که در کل دوره آنلاین بوده یا کسی که تضمین شده بر روی زنجیره‌ی درست بوده دریافت کنید. این را وابستگی ضعیف به شخص می‌گوییم. قوانینی درباره‌ی اینکه هر چند وقت یکبار این نقاط باید تولید شوند و چگونه می‌توانیم به آنها اتکا کنیم، وجود دارد و ما یک مکانیسم "تقریباً بدون نیاز به اعتماد[10]" برای دستیابی به این نقاط بررسی می‌سازیم. من متوجهم که این یک تضاد شدید با ایدئولوژی بیتکوین است از این نظر که هر کسی در هر نقطه از جهان باید قادر باشد از نقطه‌ی شروع با زنجیره هماهنگ گردد و بدون اعتماد به هیچ کس به هیچ طریق، شکل یا فرمی بداند که بر روی زنجیره‌ی درست قرار دارد. ما این کار را نمی‌کنیم. این کار با اثبات سهم بسیار مشکل به نظر می‌رسد. این مصالحه‌ای است که ما انجام دادیم، اما اعتقاد داریم در عمل این کار کاملاً قابل انجام است و منجر به هیچ حمله‌ای از هیچ نوعی نمی‌گردد."

فارغ از این همه پیچیدگی، اعتماد و سطوح حمله، من اعتقاد دارم که مشکل اصلی اثبات سهم این است که می‌تواند منجر به تمرکز گردد.

با یک سیستم اثبات سهم، هر چه سکه‌ی بیشتری داشته باشید، قدرت رأی‌دهی بیشتری دارید، و کسانی که سکه دارند همان‌هایی هستند که سکه‌ای جدیدی از طریق استیک کردن بدست می‌آورند. از آنجا که نیاز به توسعه‌ی منابعشان برای استیک کردن ندارند، به سادگی می‌توانند مقدار استیک کلی‌شان را افزایش دهند همان طور که در حال بدست آوردن سکه از پاداش استیک کردن هستند، و اثرگذاریشان را در طول زمان و تا ابد در شبکه بصورت نمایی افزایش دهند. به عبارت دیگر حاکمیت شبکه تمایل دارد منجر به حاکمیت بیشتر شبکه گردد.

این مسئله مانند یک سیستم سیاسی است که در آن شما بابت هر صد دلار دارایی یک حق رأی دریافت می‌کنید، و سپس همچنین بابت هر بار رأی دادن یک دلار از دولت دریافت می‌کنید. ماری که یک معلم علوم دبیرستان با ۲۰۰۰۰ دلار دارایی است، صاحب ۲۰۰ حق رأی است و بابت هر بار رأی دادن ۲۰۰ دلار از دولت دریافت می‌کند. جف بزوس با ۲۰۰ میلیارد دارایی ۲

[8] slash
[9] Weak Subjectivity
[10] Somehow Trustless

میلیارد حق رأی از دولت دریافت می‌کند و برای رأی دادن ۲ میلیارد دلار از دولت دریافت می‌کند. او ده میلیون برابر شهروند ارزشمندتری از ماری است و همچنین به خاطر ثروتمند بودن پول بیشتری هم ار دولت دریافت می‌کند.

این سیستمی نیست که خیلی از رفقا دوست داشته باشند در آن زندگی کنند. در نهایت هم به یک انحصار[11] با تعدادی میلیاردر به تعداد انگشتان دست که بیشتر رأی ها را کنترل می‌کنند و بر همه چیز حکمرانی می‌کنند ختم خواهد شد (اگر تاکنون به این نوع سیستم منجر نشده باشد). اگر سیستم بیش از حد متمرکز گردد، به نوعی در برابر اهداف یک زنجیره‌ی‌بلاک غیرمتمرکز قرار می‌گیرد.

در عوض، سیستم اثبات سهم اساساً به نفع سهم‌ها در یک دارایی شخصی متمرکز مانند شرکت‌ها خوب کار می‌کند. در یک شرکت، هر سهم ارزشی معادل یک رأی برای پیشنهادات و جایگاه‌های هیئت مدیره را دارد، زیرا مالکین به نسبت مالکیتشان تصمیم می‌گیرند کمپانی چه کاری انجام دهد. این‌ها شرکت‌های اختیاری هستند؛ سهامداران، مشتری‌ها و کارمندان می توانند در صورتی که قوانین را دوست ندارند به شرکتی دیگر بروند. این مسئله با انتخابات یک کشور تفاوت دارد، چرا که قرار است پلتفرمی غیرمتمرکز باشد. و همچنین با پول یا ارز رایج هم متفارت است.

بنابراین، من مدل اثبات سهم را برای سایر رمزارزهایی که شبیه به یک شرکت هستند جهت استفاده‌ی آزمایشی بد نمی‌دانم. در واقع، اثبات سهم می‌تواند هزینه‌ی حمله به پروتکل را افزایش دهد، چون یک حمله یا گروهی از حمله کنندگان نیاز دارند تعداد زیادی سکه بدست آورند (مگر اینکه یک اشکال ناشی از سطح بزرگتری از حمله را کشف و از آن استفاده کنند، یا به نحوی سکه‌ها را بدزدند). به عنوان مثال پروژه‌ها یا پلتفرم‌های تأمین مالی غیرمتمرکز[12] مشخصی وجود دارند، که می‌توانند مانند یک کمپانی عمل کنند و از اثبات سهم استفاده کنند تا اگر همه چیز خوب پیش رود بهینه‌تر گردند و هزینه‌های حمله را علیه خود بالا ببرند. آنها به سمت تمرکز متمایل می‌شوند، اما اگر خدمتی اختیاری را ارائه می‌دهند که در رقابت با سایر سرویس‌های اثبات سهم است، مشکلی ندارد. اگر خدمات آنها خوب نباشد، مردم می‌توانند جای دیگری بروند. بطور کلی، ما با متمرکز شدن کمپانی‌ها مشکلی نداریم چون آنها کمپانی هستند.

در عوض، به نظر می‌رسد اثبات سهم اساساً کمتر برای یک دارایی پولی جهانی ضدسانسور و غیرمتمرکز مناسب باشد، مخصوصاً وقتی آن را هم‌راستا با مشکلاتی که در بخش دوم این مقاله در مورد استیبل‌کوین‌ها شرح خواهم داد در نظر بگیریم. در مقایسه با اثبات کار، اثبات سهم ذاتاً بیشتر شبیه سهام است تا پول.

آدام بک این را به اختصار خیلی وقت پیش شرح داده:

> " شما این مسئله را با وجود سایر پول‌کالاها مانند طلای فیزیکی می‌بینید. این سیستمی است که کار می‌کند چون پول هزینه دارد. من فکر می‌کنم پولی که هزینه نداشته باشد در نهایت ماهیتش سیاسی می‌شود. پس مردمی که به پول نزدیکتر باشند، به اصطلاح اثر کانتیلون[13]، منتفع خواهند گردید.

چگونه بیتکوین با تبدیل نشدن به اثبات سهم نجات یافت

در یک سیستم اثبات سهم و مشخصاً شبکه‌ی بیتکوین با نودهای هدفمند-کوچکش، قدرت بین ماینرها، توسعه‌دهندگان، و نودهای شخصی توزیع شده است.

توانایی شما در تبدیل شدن به یک ماینر بر اساس توانایی شما در گذاشتن سرمایه و یافتن الکتریسیته‌ی ارزان قیمت است، تا ماینرهای جاافتاده‌ای که نوعی برتری دارند و این برتری در طول زمان نیز افزایش می‌یابد (موردی که ذاتاً در در سیستم‌های اثبات سهم وجود دارد)، ماینرهای جدید در واقع نوعی برتری فنی نسبت به ماینرهای موجود دارند چون آنها به لطف قانون مور[14]، ماشین‌های جدیدتری با قدرت پردازش بیشتر در واحد توان می‌خرند بدون هزینه‌های ازدست‌رفته. تجارت ماینینگ،

---

[11] Oligopoly
[12] DeFi
[13] Cantillon Effect
[14] Moore's Law

قدیمی و جدید، همگی مکرراً در حال به‌روز رسانی خود توسط صرف سرمایه هستند، تا از منابع انرژی جدید ارزان و سرگردان بهره ببرند. کیفیت مدیریت و تجربه حیاتی است و مزیت مقیاس[۱۵] شما را تا اینجا می‌رسانند.

بعلاوه، طراحان شبکه‌ی بیتکوین، مسیرهای طولانی را طی کردند تا راه‌اندازی یک فول نود آسان و ارزان باشد (برعکس تقریباً هر رمزارز دیگری)، که به هر کاربری اجازه می‌دهد تا کل زنجیره‌ی‌بلاک را بازرسی کند و بلاک‌هایی که با قوانین شبکه‌ی نودها تطابق ندارند را رد کند. در شبکه‌ی بیتکوین، قدرت اصلی بیشتر در اختیار نودهاست تا ماینرها. اگر ماینرها سعی کنند تبانی کنند و بلاک‌هایی را ماین کنند که نامعتبرند، شبکه‌ی نودها به سادگی آن بلاک‌ها را رد می‌کنند.

ما می‌توانیم این را مشابه قانون اساسی ایالات متحده در نظر بگیریم که سه شاخه از دولت را ایجاد کرده تا یکدیگر را محدود کنند. شاخه‌ی اجرایی، شاخه‌ی قانون‌گذاری، و شاخه‌ی قضاوت راه‌های مختلفی برای حکمرانی بر یکدیگر در شرایط خاصی دارند، و محدودیت‌های پلکانی دارند، که طراحی شده تا سیستم سیاسی را در مقابل تغییرات ناگهانی و در نتیجه انتقال قدرت به اقتدارگرایی از یک سو و حکومت اوباش از سوی دیگر مقاوم نماید.

بطور مشابه، شبکه‌ی بیتکوین شبکه‌ی نودها، ماینرها و توسعه‌دهندگان را دارد، که شبکه‌ی نودها داوران نهایی اجماع هستند اما برای درخواست انجام تراکنش به ماینرها وابسته هستند و برای ایجاد بروزرسانی‌هایی که از نظر شبکه‌ی نودها و ماینرها به عنوان بهبود پذیرفته شود به توسعه‌دهندگان وابسته هستند. حالت طبیعی شبکه مقاومت در برابر تغییر است، مخصوصاً تغییرات در طراحی زیرساختی سیستم، بنابراین برای تغییز چیزی اجماع قاطع نیاز داریم، و این تغییرات سافت‌فورک‌هایی با قابلیت بازگشت به عقب[۱۶] هستند که نودها می‌توانند انتخاب کنند با این تغییرات هماهنگ شوند یا نه در حالی که در هر حال با پروتکل سازگارند.

بسیاری از زنجیره‌های بلاک دیگر که از زمان شبکه‌ی بیتکوین به وجود آمده‌اند چندین مصالحه انجام داده اند از جمله اینکه باعث شدند نودها نیاز به قدرت پردازش، پهنای باند و حجم ذخیره‌سازی عظیمی داشته باشند، تا فقط نهادهای با مقیاس صنعتی بتوانند آنهارا راه‌اندازی کنند، که این امر شبکه را به سوی چند نود اصلی به تعداد انگشتان دست که می‌توانند زنجیره را بازرسی کرده و اجماع را شکل دهند متمرکز می‌کند.

اثبات کار بیتکوین و طراحی بلاک‌های کوچک قدرت بسیاری را در دست کاربران شخصی حفظ می‌کند. هر کس که یک نود کامل راه‌اندازی کند می‌تواند کل زنجیره را بررسی کند، تراکنش‌های شخصی خود را صحت‌سنجی کند، و در اثر شبکه‌ای که اجماع را شکل می‌دهد شرکت کند.

من پیشنهاد می‌کنم دوستانی که به بیتکوین و فضای گسترده‌تر رمزارز علاقه‌مند هستند کتاب مناقشه‌ی سایز بلاک (ترجمه) را مطالعه کنند، که کتابی چاپ سال ۲۰۲۱ است و تاریخچه‌ی شبکه‌ی بیتکوین را در زمانی که بخش‌های مختلف اکوسیستم با یکدیگر درگیر شدند تا طرح پروتکل را شکل دهند شرح می‌دهد، تا ببینند قدرت در اختیار چه گروهی است (توسعه‌دهندگان/ماینرهای سازمانی/صرافی‌ها یا کاربرها/نودهای شخصی). این مسئله یک آزمایش دنیای واقعی راجع به سطح عدم تمرکز برای بیتکوین بود. به عبارت دیگر یک بحران قانون اساسی شبکه‌ی بیتکوین بود و بیتکوین این آزمایش را با موفقیت پشت سر گذاشت.

از زمان آغاز تاریخ بیتکوین، شکاف فزاینده‌ای بین مردمی که تمایل داشتند سایز بلاک را افزایش دهند و مردمی که می‌خواستند آن را کوچک نگه دارند وجود داشت. افزایش سایز بلاک به شبکه اجازه می‌داد تراکنش‌های بیشتری را در واحد زمان پردازش کنند (راه‌حل‌های لایه‌ی دوم و راه‌حل‌های زنجیره‌های جانبی مانند لایتنینگ و لیکوئید به حساب نیامده‌اند چون در آن زمان وجود نداشتند). هرچند، افزایش سایز بلاک همچنین پهنای باند و ظرفیت ذخیره‌سازی مورد نیاز برای راه‌اندازی یک فول‌نود را نیز افزایش می‌داد، و لذا آن را از دسترس کاربر روزمره با یک لپتاپ یا رزبری پای[۱۷] خارج می‌کرد.

---

[۱۵] economies of scale

[16] backwards-compatible

[17] Raspberry Pi

حتی خود ساتوشی ناکاموتو در این مناقشه یک نقش دوگانه بازی کرد؛ خود او بود که شخصاً محدودیت سایز بلاک را پس از راه‌اندازی شبکه اعمال کرد، اما همچنین بحث کرد که چطور می‌شود بطور بالقوه و در طول زمان با بهبود پهنای باند در سطح جهان آن را افزایش داد.

اگر کاربران نه قادر به ماین کردن باشند و نه بتوانند خودشان فول‌نود شخصی‌شان را راه‌اندازی نمایند، مجبورند به خدمات‌دهندگانی دیگر که در مقیاس بزرگی امکان راه‌اندازی نودهای بیتکوین داشته باشند، در شبکه اعتماد کنند، و بیتکوین از یک سیستم بی‌نیاز از اعتماد و غیرمتمرکز خارج می‌گردد. به عبارت دیگر، این امر بطور پیوسته کاربرد اجماع توسط شبکه‌ی نودها را تضعیف می‌کند

پس از اینکه بذر این تفرقه از آغاز به کار پروتکل کاشته شد، و همزمان با طولانی شدن ترک پروژه توسط ساتوشی ناکاموتو، بین سال‌های ۲۰۱۵ تا ۲۰۱۷ مناقشه‌ی سایز بلاک تبدیل به یک مبارزه‌ی کامل شد.

از طرفی در سال ۲۰۱۷، بیش از ۸۰ درصد قدرت پردازشی ماینرها، بزرگترین سازنده‌ی تجهیزات ماینینگ بیتکوین، توسعه‌دهندگان اصلی و پیشگام بیتکوین، و تعداد زیادی از متولیان و صرافی‌ها شامل کوین‌بیس و گری‌اسکیل موافق افزایش سایز بلاک توسط یک به‌روزرسانی به نام SegWit2x (با به‌روزرسانی عادی SegWit اشتباه گرفته نشود) بودند. این یک میزان چشمگیر حمایت در بین بازیگران سازمانی در این صنعت بود، یا همان‌طور که خودشان در در توافق نیویورک توصیف می‌کنند، آنها "وزنه‌ای قطعی در اکوسیستم بیتکوین" بودند.

با این وجود، آنها شکست خوردند.

توسعه‌دهندگان موجود و مهم‌تر از آن اکثریت متصدیان نودهای شخصی با این طرح موافق نبودند، و لذا در کنار چندین دلیل دیگر، این تصمیم منتفی شد.

> "**SegWit2x** ، (بصورت مخفف **B2X** یا **S2X** که در اصل **SegWit2Mb** نامیده می‌شود) کوششی شکست‌خورده و مناقشه‌برانگیز برای هاردفورک بود که در توافق نیویورک طرح شد و قصد داشت محدودیت سایز بلاک را دوبرابر کند. از این هاردفورک به عنوان تلاشی شکست خوده توسط مدیران عامل و مالکان تجارت‌های بزرگ بیتکوین برای معرفی تغییراتی در پروتکل ارز و چرخه‌ی توسعه با انگیزه‌های پنهانی یاد می‌شود. "
>
> هرچند بیش از ۸۰ درصد از ماینرها آمادگی خود را برای SegWit2x و توافق نیویورک اعلام کردند، در بدست آوردن اجماع عموم و توسعه‌دهندگان اصلی موفق نبود.
>
> - Bitcoin Wiki

اگر بیتکوین بر اساس مدل اثبات سهم ساخته شده بود، که در آنجا هر چقدر بیشتر سکه داشته باشید رأی بیشتری راجع به اینکه شبکه چطور عمل کند خواهید داشت، صرافی‌های بزرگ و متولیان می‌توانستند میلیون‌ها سکه‌ای که از جانب مشتریانشان در اختیار داشتند را برای دادن رأی به نفع خودشان استفاده می‌کردند. این مشابه اتفاقی است که الان ون‌گارد[۱۸] و بلک‌راک[۱۹] با در اختیار داشتن تریلیون‌ها دلار دارایی از نوع سهام‌های شاخص کاربرانشان رقم می‌زنند و از این امکان برای حق رأی روی آن دارایی‌ها استفاده می‌کنند. (نکته‌ی قابل ملاحظه اینست که عمده‌ی شبکه‌های فعلی اثبات سهم و اثبات کار غیر از بیتکوین، روش اجماع روی شبکه مثل بیتکوین ندارند و با رهبری تیم یا توسعه‌دهندگان تغییراتی برای شبکه‌ی خودشان طراحی می‌کنند و اعضای شبکه از آن‌ها فرمانبرداری می‌کنند. -م)

بعضی رفقا در سمت سایز بلاک بزرگتر نیز در این مناقشه زنجیره‌ی‌بلاک خودشان را از بیتکوین فورک[۲۰] کردند و نسخه‌ای با سایز بلاک بزرگتر از بیتکوین ایجاد کردند، مانند Bitcoin XT، Bitcoin Classic، Bitcoin Unlimited، Bitcoin Cash و Bitcoin

[18] Vanguard
[19] BlackRock
[20] منشعب

Satoshi Vision. همه‌ی اینها در برابر بیتکوین از نظر سرمایه‌ی بازار و هشریت به شدت سقوط کردند، چون توسط بازار پس زده شدند. برخی از ان نسخه‌ها در حال حاضر از بین رفته‌اند، و سایر آنها در معرض حمله‌های ۵۱ درصدی جدی قرار دارند.

اثبات کار و فول‌نودهای کوچک به همراه هم مسیر اصلی هستند که در حال حاضر میشناسیم برای اینکه یک زنجیره‌ی‌بلاک را در لایه‌ی اصلی به اندازه‌ی کافی غیرمتمرکز و با بیشترین سطح از امنیت شامل سخت‌ترین سطح حمله نگاه داریم. اگر بیتکوین زمانی به یک سیستم دیگر به‌روزرسانی گردد، تنها با یک اجماع قاطع در بین کاربران خواهد بود.

چالش‌های فنی اثبات سهم

اتریوم درگیر مشکلات مقیاس‌پذیری حادتری نسبت به بیتکوین بوده است، که در را به سوی تعدادی از بلاکچین‌های قرارداد هوشمند رقیب گشوده است که متمرکزتر (و نتیجتاً به نحوی بهینه‌تر) هستند.

و از میان آن رقبای جدید اثبات سهم، چندین مثال از درگیری سیستم‌هایشان با مشکلات فنی وجود دارد.

یکی از مشکلات عمده باعث شد زنجیره‌ی‌بلاک سولانا به مدت ۱۷ ساعت از دسترس خارج گردد، و نیاز شد یک راه‌اندازی مجدد بطور دستی توسط تأییدکننده‌ها انجام شود. سولانا یک زنجیره‌ی‌بلاک قرارداد هوشمند مورد حمایت سرمایه‌گذاران ریسک‌پذیر[۲۱] است که سعی در افزایش چشمگیر مقیاس‌پذیری در مقایسه با اتریوم از راه اجرای طرحی ترکیبی از اثبات سهم و اثبات تاریخ[۲۲] برای دستیابی به توان‌های عملیاتی قابل‌توجه دارد.

بده‌بستان‌های آن چه چیزهایی هستند؟ خب تعدادشان زیاد است. توان عملیاتی بالاتر سولانا در مقایسه با اتریوم مجانی بدست نمی‌آید.

اول از همه، برای اینکه یک تأییدکننده‌ی سولانا شوید، نیاز به یک کامپیوتر با پردازنده‌ی ۱۲ هسته‌ای، ۱۲۸ گیگابایت رم، و سرعت آپلود ۳۰۰ مگابیت بر ثانیه (توصیه می‌شود سرعتتان یک گیگابیت بر ثانیه باشد) دارید. این امکانات مخصوصاً بخش سرعت آپلود، اساساً یعنی شما باید یک اپراتور مرکز داده باشید تا بتوانید تأییدکننده‌ی سولانا شوید. بر خلاف بیتکوین، شما نمی‌توانید برای تأیید کل زنجیره‌ی‌بلاک از یک لپتاپ استفاده کنید. به عبارت دیگر، سولانا برای شما قابل بازرسی نیست.

دوماً، آن تأییدکننده‌های در سطح مرکز داده نیز اگر می‌خواهند به کل تاریخچه‌ی زنجیره‌ی‌بلاک برگردند مجبورند به بایگانی‌کننده‌ها اعتماد کنند، چون در طول زمان مقدار داده‌ی ذخیره شده به طرز مضحکی حجیم می‌شود.

بیتکوین این مشکل را ندارد؛ پس از ۱۳ سال بهره‌برداری، کل زنجیره‌ی‌بلاک بیتکوین می‌تواند بر روی یک درایو کامپیوتر معمولی ذخیره گردد. در ۱۳ سال آتی، بیتکوین هنوز هم خواهد توانست بر روی یک درایو کامپیوتر معمولی ذخیره گردد.

تاریخچه‌ی بایگانی سولانا پس از یک یا دو دهه به اندازه ای زیاد خواهد شد که آن را برای شما هرچه بیشتر و بیشتر غیرقابل بررسی خواهد کرد.

سوماً، سولانا از مجازات بصورت دستی استفاده می‌کند. به عبارت دیگر، زنجیره‌ی‌بلاکی است که در صورت حملات مشخص به شبکه، نیازمند تصمیمات انسانی برای تعیین اجماع است.

> "مجازات یک مشکل دشوار است، و وقتی هدف شبکه کمترین تأخیر ممکن در انتقال اطلاعات باشد آنگاه دشوارتر هم می‌شود. مصالحه‌ها[۲۳] مخصوصاً هنگام بهینه‌سازی زمان انتقال اطلاعات[۲۴] واضح می‌شوند. به عنوان مثال، بطور ایده‌آل تأییدکننده‌ها باید رأی‌های خود را پیش از اینکه حافظه روی دیسک همگام شود اعلام و منتشر کنند، که به معنای افزایش چشمگیر ریسک و احتمال خرابی اطلاعات سیستم فرد تاییدکننده، می‌شود.

---

[21] VC-backed smart contract blockchain
[22] proof-of-history
[23] trade-offs
[24] latency

اساساً، هدف ما برای مجازات آن است که هر زمانی که یک گره بخواهد به شکل هدفمند قوانین امنیتی شبکه را زیر پا بگذارد به شکل صد در صدی آن را مجازات کنیم و از جهت دیگر گره‌هایی که عملیات تایید کردن را طبق روال عادی انجام می‌دهند صفر درصد از اوقات درگیر مجازات شوند. روشی که برای دستیابی به این هدف بکار می‌گیریم این است که ابتدا اثبات مجازات را اجرایی می‌کنیم بدون اینکه هیچ مجازات خودکاری را تابه‌حال انجام داده باشیم

در حال حاضر، برای اجماع عادی، پس از یک تخطی از موارد امنیتی، شبکه متوقف خواهد شد. ما می‌توانیم داده‌ها را تحلیل کنیم و بفهمیم چه کسی مسئول بوده و پیشنهاد کنیم استیک او پس از راه‌اندازی مجدد باید مجازات شود. راهکار مشابهی هم توسط یک تصدیق خوش‌بینانه[۲۵] اتفاق می‌افتد. تخطی از یک تصدیق خوش‌بینانه به سادگی قابل مشاهده است، اما در شرایط عادی، تخطی از تصدیق خوش‌بینانه منجر به توقف شبکه نمی‌شود. وقتی تخطی مشاهده شد، تأییدکننده‌ها استیک آسیب‌دیده را در دوره‌ی بعدی فریز کرده و در صورتی که تخطی نیاز به مجازات داشته باشد، در به‌روزرسانی بعدی راجع به آن تصمیم‌گیری خواهد شد.

در بلند مدت، تراکنش‌ها باید قادر باشند در صورتی که تخطی خوشبینانه از موارد امنیتی اثبات شد بخشی از وثیقه‌ی مجازات‌شده را بازیابی کنند. در این سناریو، هر بلاک بطور مؤثر توسط شبکه بیمه می‌شود.

- "تصدیق خوش‌بینانه و مجازات"، Solana Docs

پس، سولانا در واقع حتی یک زنجیره‌ی‌بلاک خودکار نیست. این یک قدم به عقب از هم اثبات کار بیتکوین و هم اثبات سهم اتریوم از نظر عملکرد خودکار است در مقابل توان عملیاتی بیشتر و هزینه‌های کمتر. مکانیسم اجماع به میزان بیشتری دستی، انسانی و سیاسی است.

و پیش از اینکه طرفداران سولانا از دست من عصبانی شوند، اشاره می‌کنم که من علیه سولانا غرض‌ورزی نمی‌کنم. پلتفرم‌های قراردادهای هوشمند تمایل دارند هر چه بیشتر و بیشتر به سمت تمرکز حرکت کنند، زیرا هرچه متمرکزتر شوند، بهینه‌تر می‌شوند، و کاربران بهینه شدن می‌خواهند (از جمله هزینه‌های کمتر تراکنش و تأییدیه‌های سریع‌تر). اوایل سپتامبر گذشته وقتی سرمایه‌ی بازار سولانا ۴۰ میلیارد دلار و کاردانو ۹۰ میلیارد دلار بود، من در سرویس تحقیقاتی‌ام پیشبینی کردم جای این دو عوض خواهد شد، که دو ماه قبل از وقوع آن در نوامبر ۲۰۲۱ بود:

"من فکر می‌کنم سولانا (در حال حاضر ۷ امین رمزارز بزرگ دنیا از نظر سرمایه‌ی بازار است) شانس خوبی برای گرفتن جای کاردانو (در حال حاضر سومین بزرگترین از نظر سرمایه‌ی بازار) را دارد، هرچند من روی هیچ کدامشان سرمایه‌گذاری نمی‌کنم. افق اصلی برای سولانا در حال حاضر این است که در حال ساخت صرافی‌هایی شبه‌غیرمتمرکز و ابزارهای دیگری هستند و هزینه‌های تراکنششان از اتریوم بسیار کمتر است.

- ۵ سپتامبر ۲۰۲۱

اساساً تز من درباره‌ی سولانا این بود که بیشتر کاربران پلتفرم‌های قرارداد هوشمند، حداقل در یک محیط قانون‌گذاری غیر تهاجمی، بیشتر به هزینه‌های تراکنش پایین اهمیت می‌دهند تا سطح بالای عدم تمرکز. من قبلاً این مسئله را در مورد استیبل‌کوین‌های تتر و مهاجرتشان از اتریوم به ترون با افزایش هزینه‌های تراکنش اتریوم مشاهده کردم.

در نتیجه پلتفرم‌های قرارداد هوشمندی که توان عملیاتی بالاتر و میزان مهمی از حمایت را دارا باشند، هر کدام شانس خوبی برای کسب سهمی از بازار را خواهند داشت. زمین بازی در این مواقع به تضعیف خود با شبکه‌های ارزان‌تر و متمرکز تر ادامه می‌دهد.

با این وجود، هر چند وقت یک بار بخشی از اتریوم نیز با دوشاخه شدن‌های زنجیره‌ی ناخواسته از دسترس خارج می‌شود، و امکان دارد اگر به اثبات سهم تغییر یابد با مشکلات مشابه و شدیدتری از آنچه برای سولانا اتفاق افتاد روبرو گردد. (در مقابل،

[25] Optimistic conf.

بیتکوین از بهار ۲۰۱۳ به معنای واقعی ۱۰۰ درصد کار کرده است، و هنگامی که در آن تاریخ به مشکلی برخورده بود، سرمایه‌ی بازار آن کمتر از یک میلیارد دلار بوده و لذا حقیقتاً در مرحله‌ی آزمایش بوده است).

یک مقاله در اکتبر ۲۰۲۱ از استنفورد (و حمایت مالی شده توسط بنیاد اتریوم، به اعتبار آنها) به نام سه حمله به اثبات سهم اتریوم به راه‌هایی برای حمله به سیستم وقتی که اتریوم به اثبات سهم تغییر می‌کند اشاره کرد. من به جای عمیق شدن در مقاله، اجازه می‌دهم دکترهای متخصص علوم کامپیوتر مشخص کنند کدام راه‌های حمله معتبر و کدام‌ها در صورت شناسایی، با یک به‌روز رسانی قابل‌دفع اند. پیشنهاد می‌کنم این مقاله را مطالعه نمایید.

توسعه‌دهندگان اتریوم انتقال اتریوم به اثبات سهم را برای سال‌ها به تعویق انداخته‌اند (طرح اولیه‌ی آنها برای تغییر به اثبات سهم یه سال ۲۰۱۶ برمی‌گردد و الان در حال وارد شدن به سال ۲۰۲۲ هستیم)، با یادآوری این مسئله که این سیستم از اثبات کار بسیار پیچیده‌تر است. توسعه‌دهندگان سولانا، به همین ترتیب اذعان دارند که اجرای مجازات چه میزان مشکل است (یک قسمت حیاتی برای اثبات سهم)، و مجازات دستی را دارند که به شدت سیستم را متمرکز می‌کند، ضمن اینکه اغلب شرکت‌کنندگان هم امکان بررسی ندارند.

هوگو نگوین[۲۶] یک سری مقاله دارد (مانند اینجا و اینجا و اینجا) که اثبات سهم را از منظر اصول اولیه نقد می‌کند. مضمون اصلی آن است که با وارد نکردن عدم امکان جعل از طریق افزایش هزینه[۲۷] به عنوان بخشی از طراحی‌شان، سیستم‌های اثبات سهم ذاتاً ماهیت دوار بیشتری دارند و لذا بیشتر به مرتبه‌ای از اعتماد ثابت وابسته‌اند، توانایی کمتری در بازیابی از یک دوشاخه‌شدن زنجیره بدون دخالت دستی دارند، و قابلیت محدودی برای تأمین امنیت تاریخچه‌ی زنجیره‌ی‌بلاک دارند. منتخبی از مقاله:

> "دوماً و بسیار مهم‌تر، وقتی نرم‌افزار نود (گره) اثبات کار دانلود شده، برای اپراتور نود اثبات کار، بطرز معقولی امن است که نود را برای میزان دلخواهی از زمان خاموش کند. بعد از مرحله‌ی راه‌اندازی اولیه[۲۸]، اثبات کار به اندازه‌ی زیادی بی‌نیاز از مجوز است: نودها می‌توانند هر زمان که خواستند بیایند و بروند. تنها استثنا برای این مسئله هنگام وقوع هاردفورک‌ها است، که اپراتورهای نودها نیاز دارند فرایند بوت‌استرپینگ را تکرار کنند (یک دلیل دیگر که هاردفورک‌ها باید بسیار عاقلانه استفاده شده و در صورت امکان از آنها اجتناب شود).
>
> در مقابل، یک اپراتور نود اثبات سهم، حتی با دانلود نرم‌افزار صحیح، مستمراً باید به عامل سوم مورد اعتمادی دسترسی داشته باشد تا مطمئن شود بر روی زنجیره‌ی صحیح قرار دارد. ترس از دست دادن ارتباط با شبکه‌ی اصلی و گمراه شدن به سوی زنجیره‌ی اشتباه، تا بی‌نهایت ادامه دارد، احتمالاً حتی بعد از گذشت مدت زیادی پس از اینکه عامل سوم مورد اعتماد از بین برود! این مسئله به عنوان یک تنزل درجه‌ی قابل توجه شناخته می‌شود.

بسیاری افراد بی‌جهت اثبات سهم را به عنوان یک تکنولوژی پیشگام یا بهتر از اثبات کار پیشنهاد می‌دهند، و سیستم‌های با توان عملیاتی بالاتر آن را ستایش می‌کنند، بدون اینکه این مشکلات فنی را مطلقاً درک کنند. بسیاری از مواردی که آنها درباره‌ی اثبات کار فکر می‌کنند یک نقص است و باید از سیستم حذف شود، مثل این واقعیت که سیستم اثبات کار هزینه‌ی منابع دنیای واقعی دارد، در واقع قابلیت‌هایی هستند که آن را تا حد ممکن امن نگه می‌دارند.

و سپس آنها غافلگیر می‌شوند که بسیاری از مردم توکن‌های پروتکل اثبات سهم و سیستم‌های با توان عملیاتی بالا را به اندازه‌ی بیتکوین برای در نظر گرفتن به عنوان "پول جهانی" یا "وثیقه‌ی بکر" مناسب نمی‌بینند (عنوان وثیقه‌ی بکر توسط Raoul Pal برای بیتکوین به کار برده شده. -م). در عوض، این نوع پروتکل‌ها بیشتر پلتفرم‌های آزمایشی متمرکزی برای قراردادهای هوشمند هستند، که مانند سهم‌های رشد فناوری‌ها قابل دستکاری هستند، اما در حالت ایده‌آل تنها توسط کسانی که بطور کامل ریسک آن را بپذیرند.

---

[26] Hugo Nguyen
[27] Unforgeable costliness
[28] bootstrapping

مشکل تمرکز استیبل‌کوین‌ها

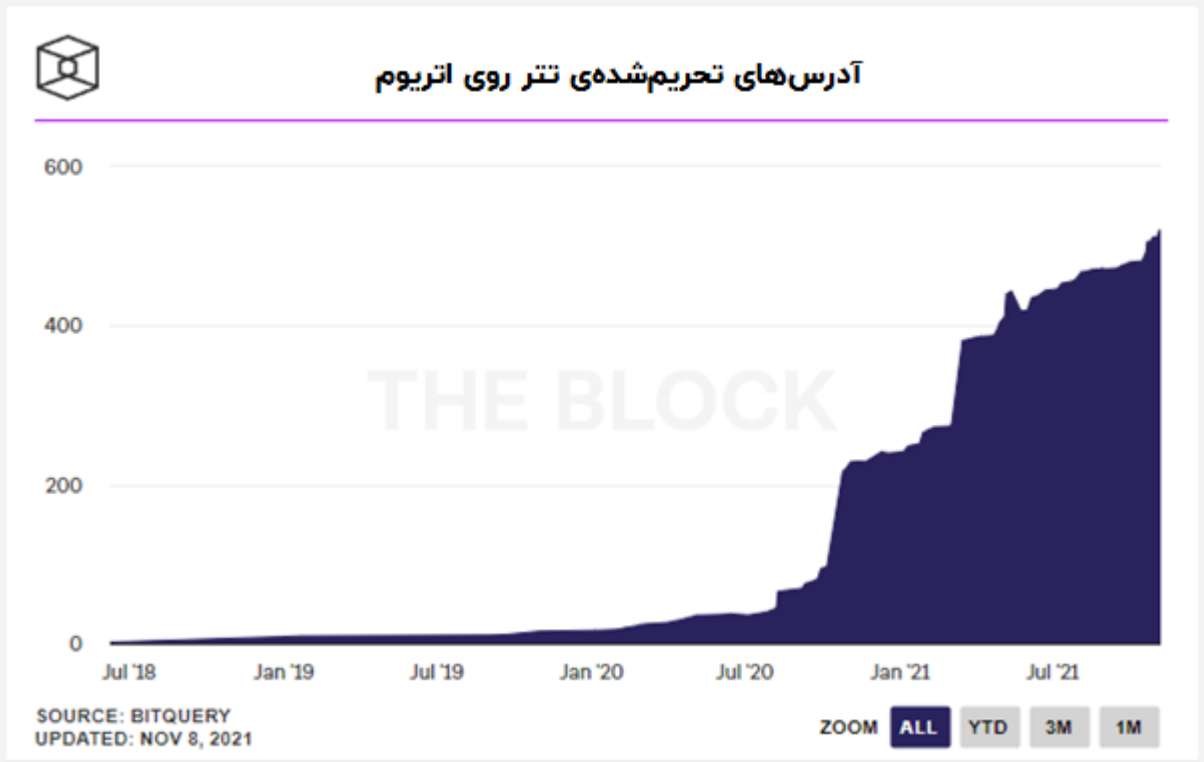
متولیان استیبل‌کوین‌ها یک مسیر حمله و مشکل تمرکز دیگر هستند علیه پلتفرم‌های قرارداد هوشمندی که DeFi را به عنوان یک بخش کلیدی اکوسیستمشان دارند، چه اثبات سهم باشند و چه اثبات کار. این مشکل بر پروتکل‌هایی نظیر اتریوم و سولانا اثرگذار است، اما بر روی بیتکوین اثر ندارد.

(خلاصه‌ی این بخش برای کسانی که می‌خواهند بخش‌های این مقاله‌ی بلند بالا را بطور سریع نگاه بیاندازند، این است که هر زنجیره‌ی‌بلاک قرارداد هوشمندی که برای کاربردهایش بطور جدی روی DeFi تکیه می‌کند، می‌تواند نتیجه‌ی هاردفورک‌هایش بطور قابل‌ملاحظه‌ای توسط متولیان استیبل‌کوین‌های متمرکز تعیین گردد. این متولیان قادرند ارزش تمام استیبل‌کوین‌هایی که در سمتی از فورک قرار گرفته‌اند که آنها به عنوان شاخه‌ی صحیح قبولش ندارند را صفر کنند، که عملاً با ورشکست شدن DeFi آن شاخه از زنجیره‌ی‌بلاک، امکان بقای آن را به شدت کاهش دهند. این می‌تواند شامل انتخاب زنجیره‌ی فورک شده در مقابل زنجیره‌ی اصلی باشد، و لذا تمام متغیرهای زنجیره‌ی‌بلاک بالقوه بی‌ثباتند حتی اگر شبکه‌ی نودها به تغییرات علاقه‌مند نباشد.)

استیبل‌کوین‌ها توکن‌هایی بر روی یک زنجیره‌ی‌بلاک هستند که نماینده‌ی واحدهای ارز فیات و عمدتاً دلار ایالات متحده هستند. حالا که زنجیره‌های بلاک قرارداد هوشمند وجود دارند، می‌توان از آنها برای اهداف مختلفی استفاده کرد. یک هدف محبوب، آن است که یک نهاد دلار ذخیره می‌کند، و سپس توکن‌هایی بر روی زنجیره‌ی‌بلاک قرارداد هوشمند منتشر می‌کند که نماینده‌ی مطالبات قابل بازخرید آن دلارها هستند، و این توکن‌ها "استیبل‌کوین" نامگذاری شده‌اند چون در برابر دلار ثابت‌اند، و ظاهراً یک‌به‌یک با دلار پشتیبانی می‌شوند و معادل یک دلاراند (گرچه قسمت آخر از نظر تاریخی کاملاً مورد بحث و اختلاف بوده است، چون همیشه این‌طور نبوده است).

هرگاه استیبل‌کوین‌ها منتشر می‌شوند، مردم پس از آن می‌توانند از زنجیره‌ی‌بلاکی که این سکه‌ها روی آن منتشر شده استفاده کنند تا مابین خود پرداخت‌ها و دریافت‌های استیبل‌کوینی را بدون عامل سوم متمرکزی تبادل کنند. از منظر یک کاربر، استیبل‌کوین‌ها یک جهش قابل توجه نسبت به سیستم‌های پرداخت موجود بانکی هستند، مخصوصاً برای پرداخت‌های بین‌المللی به هر میزانی، یا پرداخت‌های منطقه‌ای بزرگ. شما می‌توانید به شخصی در یک قاره‌ی دیگر در ساعت ۲ صبح در یک یکشنبه شب یک میلیون دلار ارسال کنید و او ظرف چند دقیقه آن را دریافت کند، و شما می‌توانید تراکنش را بر روی زنجیره‌ی‌بلاک صحت‌سنجی کنید. (و این، به هر حال، بخشی از دلیلی است که دولت‌ها مشخصاً درباره‌ی وجود این مکانیسم هیجان‌زده نیستند، و بر روی قوانینی در حال کار هستند که این مکانیسم را به شدت تحت کنترل و قابل سانسور نمایند).

این نوع استیبل‌کوین‌ها مطمئناً کاملاً متمرکز هستند. متولیان پول واقعی؛ وثیقه‌ای که تمام این توکن‌ها را پشتیبانی می‌کند را در اختیار دارند. متولیان قدرت قرار دادن برخی از توکن‌هایشان در "لیست سیاه" را دارا می‌باشند، که منجر به فریز شدن و عملاً بی‌ارزش شدنشان می‌گردد. تتر بیش از ۵۰۰ آدرس را در لیست سیاه قرار داده و همچنان هم ادامه دارد:



در نهایت، این متولیان هستند که تعیین می‌کنند کدام یک از تعهدات توکنی‌شان معیارهای لازم برای بازخرید و یا حتی قابلیت ارسال همتا به همتا را دارا می‌باشد. اگر شما کاری کنید که آنها (یا دولت‌هایشان) دوست نداشته باشند، یا توکن‌های شما در سمت اشتباهی از یک هاردفورک که منتشر کننده‌ی استیبل‌کوین به سمت دیگر آن باور دارد قرار گرفته باشد، پول شما ممکن است دیگر هیچ ارزشی نداشته باشد.

در حال حاضر بیش از ۱۴۰ میلیارد دلار در شبکه‌های قرارداد هوشمند دارایی در استیبل‌کوین‌ها وجود دارد. این رقم به آنها قدرت عظیمی بر روی شبکه می‌دهد. برای کشف علت، اجازه بدهید مفهوم یک هاردفورک را در زنجیره‌ی‌بلاک بررسی کنیم.

بررسی هاردفورک:

یک زنجیره‌ی‌بلاک می‌تواند چیزی به نام "هاردفورک" داشته باشد، که در آن توسعه دهندگان و ماینرها/تأییدکنندگان تصمیم می‌گیرند قوانین پروتکل را عوض کرده و یک مجموعه بلاک جدید ایجاد کنند که از قوانین شبکه‌ی نودهای موجود **پیروی نمی‌کند**.

اگر تعداد قابل توجهی ماینر وجود داشته باشند که با این تغییرات جدید موافق باشند، می‌توانند به‌طور نامحدود این زنجیره‌ی‌بلاک را پایدار نگاه دارند. این تغییرات می‌تواند شامل اصلاحات اصلی در مقدار پول، سایز بلاک، نرخ انتشار، و سایر قوانین زیرساختی پروتکل باشد. در عین حال، اگر سایر ماینرها همچنان به ایجاد بلاک‌هایی ادامه دهند که از شبکه‌ی فعلی نودها پیروی می‌کند، در اینجا زنجیره‌ی‌بلاک واحد به دو زنجیره تقسیم می‌شود، مانند یک دوشاخه در جاده. زنجیره‌ی‌بلاک اصلی و زنجیره‌ی‌بلاک جدید هر دو بطور موازی ادامه می‌یابند.

بیتکوین‌کش[۲۹]، مثال کاملاً شناخته‌شده‌ای است؛ آنها بطور قابل‌ملاحظه‌ای سایز بلاک را در مقایسه با پروتکل اصلی بیتکوین افزایش دادند، و راه خودشان را رفتند، و در نتیجه در برابر بیتکوین مقادیر زیادی از ارزششان را از دست دادند.

[29] Bitcoin Cash (BCH)

بیتکوین‌رؤیای‌ساتوشی[30] از بیتکوین‌کش فورک شد و در نتیجه آن نیز مقدار زیادی از ارزشش را در مقایسه با بیتکوین از دست داد.

دلیلی که بیتکوین اغلب توسط طرفدارانش "تغییرناپذیر" نامیده می‌شود آن است که بسیار در مقابل تغییر مقاوم است. وقتی یک فول‌نود داشته باشید، شما نرم‌افزاری را در اختیار دارید که بلاک‌های معتبر و نامعتبر را بر اساس قوانین اجماع پروتکل، از جمله سایز بلاک، مقدار پول و غیره شناسایی می‌کند.

اگر کسی یک هاردفورک ایجاد کند، آنها اساساً تنها زنجیره‌ی‌بلاک خود را ایجاد می‌کنند و روی زنجیره‌ی شما یا اجماع نرم‌افزاری که همان شبکه‌ی بیتکوین است اثری ندارد. تا اینجا، هر تلاشی برای هاردفورک روی بیتکوین نتوانسته است تعداد لازم کاربر برای مهاجرت به آن را بسیج کند.

اگر توسعه‌دهندگان و ماینرهای روی زنجیره‌ی‌بلاک شما تصمیم بگیرند یک سافت‌فورک ایجاد کنند (یک تغییر کوچکتر با قابلیت بازگشتی که از قوانین نودهای موجود شبکه **پیروی می‌کند** اما همچنین آنها را محدود می‌کند)، می‌توانند انجامش دهند، و شما چه شخصاً تصمیم بگیرید به آن زیردسته از قوانین جدید که سافت‌فورک را تشکیل می‌دهد به‌روزرسانی کنید یا این کار را انجام ندهید، می‌توانید با شبکه فعالیت خود را داشته باشید. در هر دو صورت شما همچنان با شبکه سازگار هستید.

به همین علت است که در مناقشه‌ی سایز بلاک سال ۲۰۱۵ تا ۲۰۱۷، نیروهای بسیار قدرتمند نتوانستند بر قدرت کاربران شخصی که نود خود را اجرا می‌کردند غلبه کنند. اکثریت ماینرها، تولیدکننده‌ی تقریباً انحصاری تجهیزات ماینینگ در آن زمان، بسیاری از بزرگترین صرافی‌ها و شرکت‌های مرتبط با بیتکوین، و بعضی از توسعه‌دهندگان ابتدایی و اثرگذار، همه و همه سعی کردند شبکه‌ی بیتکوین را بر اساس ترجیح خود تغییر دهند، ولی موفق نشدند.

شرح وسعت این حمله‌ی ترکیبی سخت است. شبیه فیلم انتقام‌جویان[31] بود: جنگ بی‌نهایت که کل تیم انتقام‌جویان شامل آیرون‌من، تور، هالک، کاپتن‌امریکا، بلک‌ویدو، بلک‌پنتر، اسپایدرمن، محافظان کهکشان، اسکارلت جادوگر، ویژن و دکتراسترنج علیه تانوس تیم‌شده بودند و ... با این حال علیه تانوس مغلوب شدند.

تانوس در آن فیلم اجتناب‌ناپذیر بود. مانند بیتکوین که، به لطف شبکه‌ی نودهای کنترل شده توسط کاربرانش غیرقابل تغییر بود. و این مسئله در زمین بازی ۲۰۱۷ به اثبات رسید. این بدان معنی نیست که در مقابل هر چالشی مقاومت خواهد کرد، اما با این اتفاق، راجع به غیرمتمرکز بودنش در زمین بازی در برابر چالشی مقاومت کرد بسیار بزرگتر از هر رمزارز دیگری.

قبل و بعد از عدم موفقیت در تغییر شبکه‌ی بیتکوین، بسیاری از افراد تعداد فراوانی هاردفورک از بیتکوین ایجاد نمودند، که معروف‌ترینشان بیتکوین‌کش بود. وقتی هاردفورک اتفاق می‌افتد، هر کاربر سکه‌های خودش را نگه می‌دارد (و آن شبکه، بدون اینکه وجود هاردفورک را به رسمیت بشناسد به فعالیت ادامه می‌دهد، چون آن بلاک‌ها از قوانین شبکه پیروی نمی‌کنند)، و همچنین سکه‌های جدید را هم دریافت می‌کند. پس وقتی بیتکوین‌کش از بیتکوین جدا شد، اگر کاربری در ابتدا ۱۰ بیتکوین داشت، پس از هاردفورک ۱۰ بیتکوین و ۱۰ بیتکوین‌کش داشت. او می‌توانست هر دو سری سکه‌ها را نگه دارد، یا آن سری از سکه‌هایی را که دلش نمی‌خواست بفروشد (با فرض اینکه ارزش داشت و خریدار واقعی برایش وجود داشت) و مقدار بیشتری از سکه‌هایی که دوست داشت بخرد.

در این مورد، کاربران اکثراً تصمیم گرفتند سکه‌های بیتکوین‌کش خود را بفروشند، و لذا بیتکوین‌کش ارزش خود را در برابر بیتکوین به میزان چشمگیری از دست داد. بعلاوه، شبکه‌ی بیتکوین‌کش ماینرهای بسیار کمتری داشت، و لذا در برابر حمله‌ی ۵۱ درصدی بسیار ناامن‌تر بود. این شکاف از آن موقع رو به افزایش است؛ اگر همین امروز تنها ۱ تا ۲ درصد از ماینرهای شبکه‌ی بیتکوین تصمیم بگیرند به شبکه‌ی بیتکوین‌کش حمله کنند و قدرت پردازشش را درهم بشکنند، قادر به انجام این کار هستند.

---

[30] Bitcoin Satoshi Vision (BSV)
[31] Avengers

چیزی که ما از بینکوین یا BTC می‌دانیم یک زنجیره‌ی‌بلاک است که تحت هیچ هاردفورک رسمی قرار نگرفته است و با نودهایی که به سال‌ها و سال‌ها پیش برمی‌گردند سازگار است. بیتکوین‌کش "BCH"، بیتکوین‌رؤیای‌ساتوشی "BSV" و سایر زنجیره‌های بلاک آنهایی هستند که هاردفورک هستند، به این معنا که آنها هستند که جدا شده‌اند و توسط شبکه‌ی موجود نودها به رسمیت شناخته نشده‌اند، اما در عوض تبدیل به موجودیتی شده اند برای خودشان.

اتریوم در این مورد متفاوت است. آنچه ما امروزه از اتریوم یا "ETH" می‌دانیم یک هاردفورک از یک هاردفورک از یک هاردفورک از یک هاردفورک است. اتریوم عمداً از طریق هاردفورک به‌روزرسانی می‌شود. در واقع زنجیره‌ی ارواح[۳۲] آلتکوین فرعی که ما به نام اتریوم کلاسیک یا "ETC"می‌شناسیم زنجیره‌ی‌بلاک اصلی اتریوم است، حداقل در بین زنجیره‌های بلاک اتریومی که هنوز وجود دارند.

در روزهای ابتدایی اتریوم، یک قرارداد هوشمند به شدت و بر اثر کد ضعیفش مورد سوء استفاده قرار گرفت، و توسعه‌دهندگانش بجای اینکه اجازه دهند با سرمایه‌گذاران که پولشان را در این پروژه‌ی شکست خورده از دست داده بودند مطابق با کد رفتار شود، کل زنجیره‌ی‌بلاک را با یک هاردفورک به عقب برگرداندند، و با توجه به حمایت گسترده توسط انجمن، هاردفورک تبدیل به زنجیره‌ی حاکم شد. زنجیره‌ی اصلی که در آن تغییرات به عقب بازگردانده نشده بود، عمدتاً رها شد و تبدیل به اتریوم کلاسیک شد.

از آن زمان، اتریوم برای اعمال به‌روزرسانی‌ها چندین مرتبه به هاردفورک کردن ادامه داده است، اما آن زنجیره‌های دیگر که اتریوم از آنها فورک شده بدون نام رها شده‌اند، چون توسط هیچ کسی که مانند زنجیره‌ی اتریوم کلاسیک منابع قابل‌توجهی در اختیار داشته باشد مورد اعتراض قرار نگرفت.

از آنجا که اتریوم از طریق هاردفورک به‌روزرسانی می‌شود، و در کدش در زنجیره‌ی موجود (قبل از فورک) "بمب‌های سختی[۳۳]" قرار می‌دهد، به توسعه‌دهندگان کنترل بسیار بیشتری نسبت به نودها در جهت‌دهی به شبکه می‌دهد. شبکه‌ی نودهای اتریوم در واقع قدرت رد کردن تغییرات مانند آنچه شبکه‌ی نودهای بیتکوین دارا می‌باشند را ندارند. چون هاردفورک به هر حال فراتر از نودهای موجود آنها حرکت خواهد کرد، و در کد اتریوم بمب‌های ساعتی سختی قرار داده شده است. این مسئله کاربران و ماینرها را سوق می‌دهد به سمتی که اغلب با جابجایی به هاردفورک جدیدی که توسعه‌دهندگان بر روی آن اجماع می‌کنند موافقت نمایند.

در واقع، اتریوم در نوامبر ۲۰۲۰ یک دوشاخه‌شدن زنجیره‌ی ناخواسته را بر اثر یک ایراد به‌روزرسانی و یک دوشاخه‌شدن ناخواسته‌ی دیگر را هم در آگست ۲۰۲۱ بر اثر یک ایراد به‌روزرسانی تجربه کرد.

طرفداران بیتکوین اغلب سطح تمرکز و سادگی ایجاد تغییر در اتریوم را نقد می‌کنند. طرفداران اتریوم اغلب با این عنوان از آن دفاع می‌کنند که برای تبدیل آن به یک چیز بهتر باید سریع‌تر به‌روزرسانی گردد. این دو فلسفه‌ی متفاوت است، اما مهم است درک کنیم چطور این دو فلسفه از منظر فنی متفاوت اند.

متولیان استیبل‌کوین‌ها: تصمیم‌گیرندگان فورک قرارداد هوشمند

فارغ از بمب‌های سختی و چیزهایی شبیه به این، قدرت‌های نیرومند متمرکزی در اتریوم وجود دارند که می‌توانند در زمان وقوع هاردفورک دیکته کنند کدام هاردفورک موفق شود. با دیدن این مسئله که هر چند وقت یک‌بار هاردفورک های خواسته یا ناخواسته در اتریوم اتفاق می‌افتند، این مورد مرتبط را هم باید مد نظر قرار داد.

بنیاد اتریوم یک قدرت توانمند در تعیین مسیر اتریوم باقی می‌ماند. کانسنسیس[۳۴]، که در توسعه مشارکت می‌کند و زیرساخت نودهای اینفورا [۳۵] را راه‌اندازی می‌کند (که اگر از کار بیفتد اساساً بخش عمده‌ای از عملکرد اتریوم را از کار می‌اندازد همانطور

[32] ghostchain
[33] Difficulty bombs
[34] Consensys
[35] Infura

که در نوامبر ۲۰۲۰ بر اثر دوشاخه شدن زنجیره اتفاق افتاد) و مالک متامسک[۳۶] است (اپلیکیشن کیف‌پول کلیدی که توسط ده‌ها میلیون کاربر اتریوم برای کاربردهای DeFi و NFT ها استفاده می‌شود) یکی دیگر از اثرگذاران قدرتمند در تعیین مسیر شبکه است.

اما جدا از این دو هاب متمرکز مشخص، منابع قدرتی که اغلب از کنار آنها گذر می‌کنیم، متولیان بزرگترین استیبل‌کوین‌ها هستند. آنها اساساً قدرت کافی در این نقطه برای دیکته کردن اینکه کدام زنجیره‌ی‌بلاک اتریوم معتبر است را در زمان وقوع هاردفورک دارا می‌باشند. دو استیبل‌کوین بزرگ، با در اختیار داشتن ۱۱۵ میلیارد دلار دارایی، تأثیر بسیار زیادی بر روی اتریوم و سایر زنجیره‌های بلاک قرارداد هوشمند دارند.

وقتی یک هاردفورک به وقوع می‌پیوندد، متولیان استیبل‌کوین‌ها نمی‌توانند هر دو گروه توکن‌ها را به ازای پولشان قابل بازخرید کنند، چون دو برابر آن مقدار در حال حاضر توکن به وجود آمده است (دو گروه کامل، یک گروه به ازای هر فورک در زنجیره‌ی‌بلاک). آنها باید انتخاب کنند کدام زنجیره‌ی‌بلاک از نظر آنها معتبر است، و بر روی آن زنجیره بازخرید توکن‌هایشان را به ازای پول قبول می‌کنند، و کدام یکی را به عنوان زنجیره‌ی نامعتبر می‌شناسند، و ارزش DeFi و استیبل‌کوین‌هایشان از بین می‌رود. اکثر ۱۰۰ میلیارد دلار سرمایه‌ی تحت مدیریت که در پروتکل‌های DeFi، این شریان حیاتی مرکزی اتریوم، قفل شده‌اند، به استیبل‌کوین‌های متمرکز و همچنین استیبل‌کوین‌هایی که توسط صرافی‌های متمرکز خارجی مورد استفاده قرار می‌گیرند و یا برای امور پرداخت استفاده می‌شوند وابسته است.

بنابراین، کاربران اتریوم در صورتی که توسعه‌دهندگان و نهادهای بزرگ بخواهند هر یک از قوانین پروتکل حاکم را (شامل مقدار پول یا هر متغیر دیگری) تغییر دهند، لزوماً قادر نیستند به شبکه‌ی نود دفاعی خودشان عقب‌گرد کنند. اگر یک هاردفورک اتفاق افتد، و برخی نهادهای بزرگ و متولیان استیبل‌کوین‌ها این هاردفورک جدید را به عنوان زنجیره‌ی‌بلاک اصلی معتبر بشناسند، در این شرایط واقعاً اهمیتی ندارد که نودهای موجود چه فکری می‌کنند. زنجیره‌ی موجود آنها ، با استیبل‌کوین‌ها و DeFiهای ورشکسته، به احتمال قریب به یقین می‌بازد و هاردفورک جدید با قوانین جدید اما استیبل‌کوین‌ها و DeFiهای در حال کار، برنده خواهد شد.

و مهم است به خاطر داشته باشیم که استیبل‌کوین‌هابه عنوان نهاد شناخته می‌شوند، و در گذشته تحت اقدامات قانونی قرار گرفته‌اند. اگر دولت‌هایی که متولیان در آنها قرار دارند (یا به آنجا تحویل داده می‌شوند، یا جایی که کشورهای بزرگ روی آنها سلطه دارند) بخواهند رمزارزها را سرکوب کنند، با وجود زنجیره‌های بلاک استیبل‌کوین‌ها کار ساده‌ای خواهند داشت. دولت‌ها می‌توانند به سرعت دارایی‌های متولیان را تصاحب کنند، تمام استیبل‌کوین‌ها را در لیست سیاه قرار دهند و باعث ورشکستگی بخش عمده‌ی DeFi در تمام پلتفرم‌های قرارداد هوشمند گردند. یا می‌توانند یک هاردفورک با همکاری شرکت‌های برتر و متولیان استیبل‌کوین‌ها اعمال کنند تا قوانین مشخصی را که دولت می‌خواهد در زنجیره‌ی‌بلاک داشته باشد، مانند درهای پشتی نظارتی مشخص، و یا تغییراتی در سایر متغیرهای پروتکل اعمال کنند.

زنجیره‌ی‌بلاکی که تا حد ممکن همه‌چیز را در خود داشته باشد، مانند شبکه‌ی بیتکوین، ذاتاً به این گونه حمله‌ها یا نیروهای متمرکز مقاوم‌تر است. هیچ ارائه‌دهنده‌ی استیبل‌کوین یا توسعه‌دهنده‌ی کیف‌پول کلیدی وجود ندارد که قادر باشد شبکه‌ی بیتکوین را به روشی قابل اعتنا هدف قرار دهد، مخصوصاً وقتی صحبت از اجرای هاردفورک‌ها باشد. برخی استیبل‌کوین‌ها وجود دارند که بر لایه‌ای فراتر از شبکه‌ی بیتکوین راه‌اندازی شده‌اند، اما بطور مستقیم در لایه‌ی اصلی پروتکل اجرا نمی‌شوند، و در اندازه‌ای هم نیستند که برای اکوسیستم حیاتی باشند.

به همین علت است من بیتکوین را به عنوان یک نوع پول طبقه‌بندی می‌کنم، در حالی‌که بیشتر رمزارزهای دیگر را به عنوان نوعی سهام سرویس‌های مالی، پلتفرمی متمرکزتر با پیش استخراج (عملیات استخراج کوین توسط سازندگان آن کوین برای تامین مالی سازندگان آن کوین قبل از اینکه امکان استخراج برای دیگر افراد ممکن باشد. -م) برای توسعه‌ی کاربردهایش طبقه‌بندی می‌کنم.

[36] Metamask

زنجیره‌های بلاک قرارداد هوشمند از درجات مختلفی شبه‌متمرکز هستند، بطرز قابل اثباتی قابل تغییر هستند، و لذا در طبیعت خود سیاسی هستند. این بدان معنا نیست که قیمتشان نمی‌تواند بالا برود، و به این معنا هم نیست که نمی‌توانند کاربردی ارائه دهند، اما این مسئله آنها را ذاتاً تبدیل به چیزهایی متفاوت با دارایی‌های پولی جهانی غیرقابل تغییر می‌کند، و بنابراین مفید است که آنها را در این دو سبد مفهومی جدا از هم تقسیم کنیم.

عدم تمرکز چقدر اهمیت دارد؟

در بازارهای گاوی، و در بازه‌های زمانی که سرکوب‌ها یا نمایش‌های ناشی از قانون‌گذاری وجود ندارد، جزئیات فنی واقعاً اهمیتی ندارد.

وال‌استریت درواقع به نحوی از منظر تاکتیکی به DeFi علاقه‌مند است، چون در مجموع آنها ایده‌ی استفاده از اهرم، مدیریت نقدینگی، مبادله و ناکارآمدی نوسان‌گیری را متوجه می‌شوند و واقعاً اهمیت زیادی به جزئیات فنی و عدم تمرکز نمی‌دهند.

اما (این موضوع) برای سایفرپانک‌ها[۳۷]، مدافعان پول سالم، کسانی که راجع به تغییر ناپذیری و تضمین حجم پول در یک افق زمانی سرمایه‌گذاری بیش از یک دهه اهمیت قائل‌اند و کسانی که درباره‌ی قوانین اوراق بهادار اهمیت قائل‌اند قابل توجه است.

[37] cypherpunks

اغلب گفته می‌شود که زنجیره‌ی‌بلاک اساساً فقط یک پایگاه داده‌ی ناکارآمد است. کاربران دوست دارند با ناکارآمدی معامله کنند تا از عدم تمرکز مطمئن باشند.

یک زنجیره‌ی‌بلاک، خصوصاً یک گونه‌ی کاملاً غیرمتمرکز، پایگاه داده‌ای است که به اندازه‌ی کافی جمع‌وجور و کوچک است که هزاران یا میلیون‌ها نهاد در سرتاسر جهان می‌توانند آن را بر روی دستگاه‌های خود در محل ذخیره کرده و مستمراً آن را بصورت همتا به همتا و با استفاده از دسته‌ای از قوانین تعیین‌شده به‌روزرسانی کنند.

یک پایگاه داده‌ی کاملاً متمرکز محدودیت‌های کمتری دارد، چون نیازی ندارد کوچک و جمع‌وجور باشد. یک ارائه‌دهنده‌ی خدمات بزرگ می‌تواند یک پایگاه داده‌ی کاملاً عظیم داشته باشد، که در یک مزرعه‌ی سرور قرار گیرد. این کار می‌تواند چیزها را بسیار بهینه اداره کند، اما بر خلاف یک زنجیره‌ی‌بلاک، نهادهای خارجی نمی‌توانند مستقیماً ان را برای محتوا و تغییراتش بازرسی کنند، و هیچ کنترلی روی آن ندارند.

اکانت شبکه‌ی اجتماعی شما یک آیتم در پایگاه داده‌ی یک شرکت است؛ می‌تواند حذف شود یا تغییر یابد و شما در این مورد حق اظهار نظر ندارید. شما راهی برای بازرسی اینکه آنها چه داده‌ای را درباره‌ی شما در پایگاه داده‌شان نگهداری می‌کنند ندارید. همین مطلب در مورد حساب بانکی شما، سوابق تخلفات شما، سوابق سلامتتان و هر سرویس ابری دیگری که استفاده می‌کنید صحیح است. نهادهای شرکتی و دولتی پایگاه داده دارند، و در زمان‌هایی ممکن است تصمیم بگیرند به شما اجازه دهند یا ندهند به آن پایگاه‌های داده با مجوزهای محدودی دسترسی پیدا کنید. آنها کاملاً متمرکز، غیرقابل بازرسی و به راحتی قابل تغییر توسط ارگانی که آن را اداره می‌کند هستند.

عالی‌ترین کاربرد یک پایگاه داده‌ی به اندازه‌ی کافی غیرمتمرکز، پول است. پول، نهایتاً یک دفتر کل است، و هرچه غیرقابل تغییرتر باشد، حداقل برای ذخیره‌ی بلندمدت بهتر است. قابلیت ذخیره‌ی ارزش در یک دفتر کل توسط حفظ و به‌خاطرسپاری ساده‌ی یک عدد، و انتقال آن مقدار به دیگران بصورت بین‌المللی و در هر زمان دلخواه، بصورتی که میلیون‌ها مشارکت‌کننده‌ی دیگر آن را بپذیرند و هیچ نهاد متمرکزی نتواند آن را تغییر داده یا مانع آن شده یا در آن نقصی ایجاد کند، کاملاً مفید است.

توسعه دهندگان لایه‌ی اول قراردادهای هوشمند پیشنهاد می‌کنند کاربردهای بالقوه‌ی بسیار بیشتری وجود دارد که در کنار فقط کاربرد پول می‌توان از فناوری زنجیره‌ی‌بلاک در آنها بهره برد. این پیشنهاد در بین معامله‌گران و سرمایه‌گذاران رمزارز یک سؤال بی‌پاسخ باقی مانده است؛ کاربردهای دیگر چه هستند؟ پرداخت‌های سریع (از جمله استیبل‌کوین‌ها) به نظر یک پاسخ به این پرسش هستند، و بالقوه چیزهایی مثل تسویه‌ی اوراق بهادار، بازی‌ها و غیره.

بزرگترین چالش این پیشنهادات آن است که هر چه قابلیت‌های بیشتری به یک زنجیره‌ی‌بلاک در لایه‌ی اولش اضافه کنید، آن زنجیره کمتر "کوچک و جمع‌وجور" خواهد بود، و در نتیجه تمایل کمتری به عدم تمرکز پیدا می‌کند.

پس سؤال این گونه مطرح می‌شود، آیا مراتبی از عدم تمرکز جزئی وجود دارد که مردم در مقابل قابلیت‌های بیشتری که پایگاه داده می‌تواند ارائه دهد آن را بپذیرند؟ و آیا آن زنجیره‌های بلاک غیرمتمرکز جزئی می‌توانند از حمله‌ها، عدم توافقات، و سایر آزمایشات در طی زمان نجات یابند؟

این هم روشی دیگر در بیان این مسئله است. از آنجا که می‌دانیم کاربردهایی برای پایگاه‌های داده‌ی کاملاً متمرکز وجود دارد (از جمله سرویس‌های وب توئیتر یا آمازون)، همچنین کاربردهایی برای پایگاه‌های داده‌ی کاملاً غیرمتمرکز وجود دارد (از جمله شبکه‌ی بیتکوین)، آیا کاربردهایی برای یک پایگاه داده‌ی قسمتی متمرکز و قسمتی غیرمتمرکز وجود دارد؟

اگر پاسخ بله است، پس اساساً این استدلال مرد فولادی[۳۸] است برای وجود زنجیره‌های بلاک قرارداد هوشمند لایه‌ی اصلی مانند اتریوم، سولانا، اوالانچ[۳۹]، الگوراند[۴۰] و سایرین.

---

[38] Steel man argument
[39] Avalanche
[40] Algorand

این پایگاه‌های داده‌ی فرضی غیرمتمرکز جزئی، از نظر مفهومی رقیب بیتکوین به عنوان یک دارایی غیرقابل تغییر غیرمتمرکز نیستند، اما آیا می‌توانند در کنار بیتکوین به صورت نامحدود و به عنوان سیستم عامل اپلیکیشن‌هایی که از قابلیت بازرسی جزئی یا کنترل غیرمتمرکز جزئی نفع می‌برند وجود داشته باشند؟

به عنوان مثال، اگر یک پایگاه داده تا حدی توسط یک ارگان متمرکز کنترل گردد، اما متن‌باز باشد و به طریقی طراحی شده باشد که محتوایش بطور مستقل قابل پشتیبان‌گیری باشد و توسط نودهای مخصوص خارجی با بازدهی بالا قابل بازرسی باشد، آیا این مفهوم بازار قابل اعتنایی دارد؟ شاید برای تسویه‌ی پرداخت‌ها و اوراق بهادار.

و راجع به یک پایگاه داده‌ی فدرالی چطور، به این معنا که یک پایگاه داده که برای تغییر، نیاز به همکاری چندین ارگان بزرگ دارد، یا نیاز به اثبات سهم توسط نهادهای بزرگ (و عموماً انحصاری) دارد، تا یک نهاد واحد؟ آیا این ارزش بلند مدت دارد؟

من پاسخ این سؤالات را ندارم، غیر از اینکه با تکنولوژی که در حال حاضر وجود دارد و یا آنچه در افق زمان نگارش این مقاله قابل دید است، اینها به وضوح برای پول جهانی غیرمتمرکز واقعی به ترتیبی که در شبکه‌ی بیتکوین وجود دارد مناسب نیست. اینها ممکن است برای بازی‌ها، سیستم‌های پرداخت دارای مجوز، مبادله، و از این قبیل موارد کار کند، اما زمان مشخص خواهد کرد آیا می‌توانند از پس فاز سفته‌بازی و فاز نوسان‌گیری (با ابزار قرار دادن) قانون‌گذاری که الان در آن قرار داریم بربیایند.

در مجموع، من به برخی از آنها به عنوان پدیده‌هایی نگاه می‌کنم که در صورتی که قانون‌گذاری بهشان اجازه دهد، می‌توانند مدت طولانی باقی بمانند، مانند فناوری اطلاعات یا سهام سرویس‌های مالی که از تست هاوی[41] عبور کردند و لذا الان اوراق بهادار هستند.

همچنین باید اشاره کنم که قراردادهای هوشمند می‌توانند به عنوان لایه‌ی فوقانی بیتکوین به عنوان راهکارهای لایه‌ی دوم وجود داشته باشند. در واقع، بصورت شکلی در حال حاضر وجود دارند، اما هنوز راهکارهای غالب نیستند. راهکارهای غالب نسخه‌هایی هستند که در حال حاضر به عنوان راهکارهای لایه‌ی اول قد علم کرده‌اند، مانند اتریوم، سولانا و رقبای مختلفشان.

کاربردهای قراردادهای هوشمند

تا اینجا، تأمین مالی غیرمتمرکز "DeFi" و توکن‌های‌تعویض‌ناپذیر "NFT"ها، دو کاربرد محبوب قراردادهای هوشمند غیر از فقط ذخیره و انتقال ارزش هستند، که ارزش بازار قابل توجهی را بر روی زنجیره‌های بلاک عمومی جذب کرده‌اند. و هر دو آنها نیاز به پیچیدگی اضافی دارند و لذا، تمایل به تجمع در زنجیره‌های بلاکی مانند اتریوم و سولانا دارند، که همانطور که در این مقاله بحث کردیم، متمرکزتر از شبکه‌ی بیتکوین هستند.

یک گروه سوم هم وجود دارد، ارگان‌های غیرمتمرکز خودمختار[42] یا "DAO"ها که پوشش مطبوعاتی زیادی طی ماه‌های اخیر جذب کرده‌اند، حتی با اینکه هنوز در مقیاس مالی DeFi و NFTها نیستند. آنها را برای یک مقاله‌ی دیگر کنار می‌گذارم.

DeFi شامل صرافی‌های غیرمتمرکزی است که کاربران می‌توانند توکن‌های مختلفی را در آنها بین خود ردوبدل کنند، و شامل پلتفرم‌هایی غیرمتمرکز برای اهرم‌سازی با توکن‌هاست، به این معنی که کاربران می‌توانند با وام دادن سود کسب کنند، یا سود پرداخت کنند تا با وثیقه وام بگیرند. بسیاری از آنها هنوز هم شرکت‌های متمرکزی دارند که آنها را می‌گردانند (از جمله یونی‌سواپ[43] و کامپاند[44] هر دو شرکت‌هایی با پشتیبانی سرمایه‌ی ریسک‌پذیر متمرکز هستند)، اما کد متن‌باز دارند که کاربران سطح بالا می‌توانند بدون دخالت شرکت و تا زمانی که زنجیره‌ی‌بلاک زیرساختی به خطر نیفتاده (همانطور که در قبل بحث کردیم، این زنجیره‌های بلاک زیرساختی، سطوح حمله‌ی متمرکزی دارند، لذا در درجات مختلفی قابل تغییر هستند) در آن به جست‌وجو بپردازند.

---

[41] Howey Test
[42] Decentralized Autonomous Organizations (DAO)
[43] Uniswap
[44] Compound

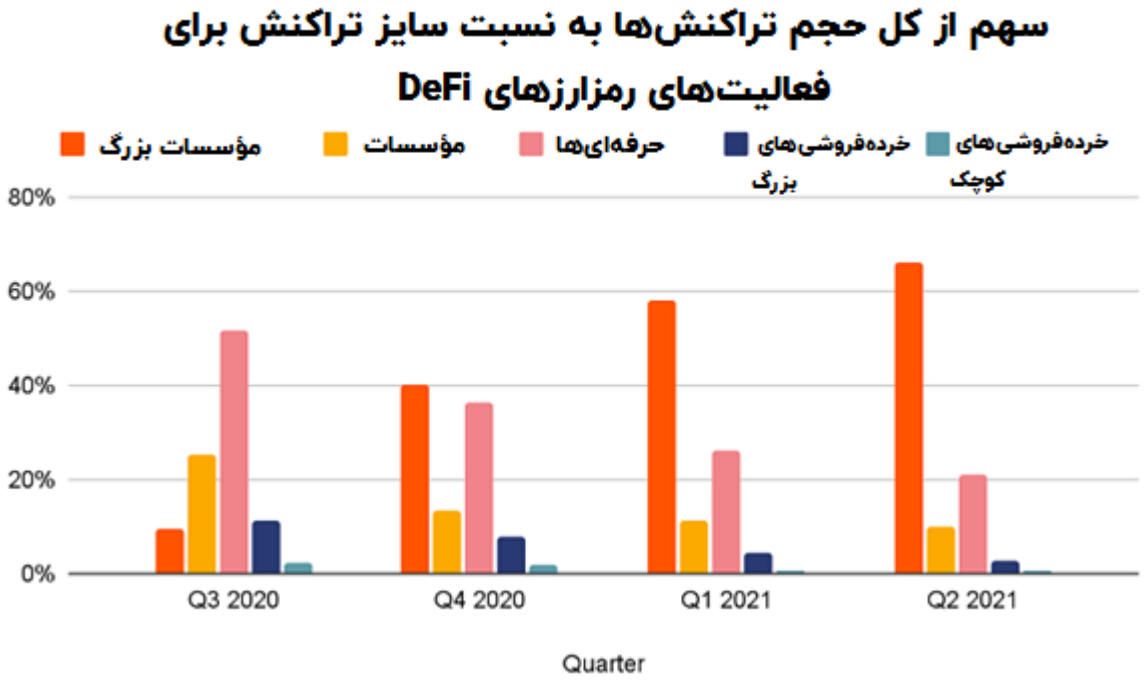
NFT ها شامل چیزهایی مثل هنرهای دیجیتال، آیتم‌های بازی منحصربه‌فرد، یا بلیط‌های فیلم دیجیتالی هستند که به عنوان آیتم‌هایی منحصربه‌فرد بر روی زنجیره‌ی‌بلاک قرار دارند. هر دسته‌بندی شامل تفاوت‌های ظریفی درباره‌ی نحوه‌ی عملکردش است. به عنوان مثال، هنرهای دیجیتال، واقعاً بر روی زنجیره‌ی‌بلاک قرار ندارد، اما نشانه‌ای روی زنجیره‌ی‌بلاک قرار دارد که به محلی مرتبط است که تصویر در آنجا ذخیره شده است. این مانند آن است که مالک یک "رسید امضا شده" از طرف هنرمند آن تصویر باشید.

آیتم‌های منحصربه‌فرد بازی‌ها می‌توانند شامل حیوانات خانگی دیجیتال، یا آیتم‌های درون بازی یا دارایی/زمین‌های درون بازی باشند، و می‌توانند به دیگر بازیکنان فروخته شده یا حتی از بازی حذف شده و بالقوه توسط یک بازی دیگر که آنها را به رسمیت می‌شناسد پذیرفته شود.

انتقادهای وارده به این کاربردها تا اینجا آن است که آنها اساساً حول و حوش سفته‌بازی می‌گردند. به عنوان مثال، در اینجا در مقاله‌ی ژانویه ۲۰۲۱ ام درباره‌ی اتریوم DeFi را به این صورت شرح داده‌ام:

> "یکی از نگرانی‌های من، وقتی بزرگترین کاربردهای اپلیکیشن‌های غیرمتمرکز را بررسی می‌کنم، این است که بسیاری از کاربردها گمراه‌کننده و سفته‌بازانه است.
>
> اتریوم بسیاری برای صرافی‌های غیرمتمرکز توکن‌های کریپتو، استیبل‌کوین‌های کریپتویی که به عنوان واحدهای شناور حساب برای معامله‌ی توکن‌های کریپتو استفاده می‌شوند، و سود وام‌دهی و درآمدزایی در توکن‌ها مورد استفاده قرار می‌گیرد که عملی است که به عنوان منبع نقدینگی/وام‌گرفتن برای معامله‌گران توکن‌های کریپتو کاربرد دارد.
>
> بنابراین، یک سیستم عامل بزرگ است که توسط توکن‌های کریپتو تأمین می‌شود به منظور چرخاندن .... توکن‌های کریپتو
>
> یک سیستم بانکی سالم در دنیای واقعی باید شامل مردمی باشد که پول سپرده‌گذاری می‌کنند، و بانک‌هایی که وام‌های مختلفی برای مسکن و تأمین مالی کسب‌وکارها می‌دهد تا کاربردی در دنیای واقعی ایجاد کند.
>
> از طرف دیگر، یک سیستم مبتنی بر سفته‌بازی، شامل تعدادی بانک است که پول سپرده را می‌گیرند و سپس آن را در بازار سهام به سفته‌بازها، وام می‌دهند، به همراه ارائه‌دهندگان فناوری که ابن کار را تسهیل می‌کنند، و سپس چیزی که این سفته‌بازان معامله می‌کنند عمدتاً شامل سهام همان بانک‌ها، سهام همان شرکت‌های فناوری، و سهام همان صرافی سهام است، که منجر به یک مهمانی سفته‌بازی دوار بزرگ می‌گردد. بزرگترین کاربرد تابه‌حال برای اتریوم یک ورژن غیرمتمرکز از آن سیستم دوار سفته‌بازی است."

و داده‌ها نشان داده‌اند که از زمانی که من این مطلب را نوشتم، حتی بیشتر شبیه به وضعیت فوق شده است. بر اساس شرکت بزرگ تحلیل زنجیره‌ی‌بلاک Chainalysis، DeFi تقریباً بطور کامل محیطی برای معامله/اهرم‌سازی/نوسان‌گیری برای معامله‌گران با مقیاس سازمانی و نهنگ‌های حرفه‌ای، و عمدتاً در غیاب معامله‌گران خرد است:



منبع نمودار: Chainalysis

عموماً همین مطلب در مورد NFTها هم صحیح است. به عنوان مثال، اطراف کریپتوپانک‌ها هم همین سفته‌بازی‌های به شدت دیوانه‌وار در جریان بوده است.

مشکل اصلی آن است که این نوع گروه‌های NFT به سادگی قابل دست‌کاری هستند چون هر کدام یک قیمت مخصوص به خود دارند، که منجر به این می‌شود که تعیین تقاضای واقعی برایش مشکل شود. دو راه ساده برای کلاهبرداری درباره‌ی این دارایی وجود دارد که بر روی دارایی‌های نقد تعویض‌پذیر قابل انجام نیست.

اولین کلاهبرداری این است که پیشنهاد قیمت‌های این دارایی‌ها را بالا ببریم و خریداران را به این اشتباه بیاندازیم که این قیمت‌ها واقعی هستند تا خرید کنند. به عبارت دیگر، این دست‌کاری بازار است. به عنوان مثال، یک کاربر می‌تواند ۵ آدرس متفاوت اتریوم بسازد، و شروع به معامله‌ی یک NFT بین آدرس‌های خودش با قیمت‌های فزاینده نماید.

ناظران بیرونی نمی‌دانند که تمام این کیف‌پول‌ها متعلق به یک شخص است و این‌که این فقط معامله بین یک شخص است. این کار تنها در مورد یک دارایی غیرتعویض‌پذیر امکان دارد؛ شما نمی‌توانید قیمت یک بیتکوین یا یک اتر را خودتان به تنهایی دستکاری کنید، شما تنهامی‌توانید اشیاء منحصربه‌فرد مانند کریپتوپانک شماره ۹۹۹۸ را دست‌کاری کنید. سپس، با قیمت‌های (به نظر) بسیار بالا، بعضی افراد می‌خواهند در این جریان وارد شوند و NFT را بخرند، در این حال کسی که بین کیف‌پول‌های خودش در حال معامله با خود بود بالاخره دارایی‌اش را در قیمت بالاتری به تازه‌وارد خوش‌خیال به فروش می‌رساند.

وقتی تازه‌وارد سعی می‌کند دارایی‌اش را بفروشد، نمی‌تواند خریدارهای دیگری پیدا کند که واقعاً حاضر باشند آن قیمت را بپردازند. آنها نمی‌دانند که در عمل، بسیاری از نقدینگی و تشدید قیمت‌ها در تراکنش‌ها فقط دست‌کاری بازار بوده است.

کلاهبرداری دوم آن است که یک ضرر بزرگ ایجاد می‌کنند تا تعهدات مالیاتی را با تقلب کاهش دهند. دوباره، شما تعداد بسیاری کیف‌پول مختلف می‌سازید. یکی از آنها به اسم واقعی شما مرتبط است و بقیه ناشناس هستند. شما با یکی از اکانت‌های ناشناسی که در اختیارتان است یک NFT به قیمت ۲۰۰ دلار می‌خرید، و آن را به یک اکانت ناشناس دیگر در اختیارتان به قیمت ۲۵۰ دلار می‌فروشید. سپس آن را به اکانت با نام واقعیتان به قیمت ۵۰۰ دلار می‌فروشید. اکانت با نام واقعیتان سپس آن را به یکی دیگر از اکانت‌های ناشناس‌تان به قیمت ۲۰۰ دلار می‌فروشد، که منجر به یک "ضرر" سنگین

۳۰۰ دلاری می‌شود. سپس اکانت ناشناس شما می‌تواند بطور بالقوه آن را تقریباً به همان قیمتی که برایش پول داده‌اید یعنی ۲۰۰ دلار در صورتی که بازار زیاد از زمانی که این حقه را شروع کردید تغییر نکرده باشد به فروش رساند. این یک "ضرر" مالیاتی مفید است (که در واقع ضرر نیست، چون شما مخفیانه به خودتان پرداختش کرده‌اید) که می‌تواند سود معامله‌ی واقعی کریپتوی شما را از سایر حوزه‌های معاملاتی جبران کند.

صراحتاً، کسانی که از وقت گذراندن با دستبند لذت نمی برند نباید این اقدامات را انجام دهند. این قبیل اقدامات در هنرهای سنتی هم اتفاق می‌افتد اما در فرم دیجیتالی می‌تواند چندین و چند برابر سریع‌تر اتفاق افتد.

و لازم نیست ذکر کنم که تمام نقدینگی و رفتار قیمت کلاهبرداری است. من نمی‌دانم چقدر است. به سادگی می‌توان گفت که با فناوری امروزه، بسیار مشکل است که بتوانیم تفکیک کنیم چند درصد کلاهبرداری و چند درصد واقعی است، و رفتار قیمت صعودی بر اساس کلاهبرداری می‌تواند موقتاً نقدینگی ناشی از تقاضای واقعی را وارد کند، که منجر به کدر شدن تفاوت این دو می‌گردد. این مسئله مشکل خاصی برای توکن‌های نقدی با سرمایه‌ی بالا ایجاد نمی‌کند، اما بالقوه مشکل بزرگی برای توکن‌های غیرقابل‌معاوضه است.

مثالی در اکتبر ۲۰۲۱ وجود داشت که در آن کریپتوپانک شماره‌ی ۹۹۹۸ به قیمت ۵۳۲ میلیون دلار فروخته شد. در نگاه اول، این باارزش‌ترین فروش هنری تمام ادوار بود. هرچند، با تحلیل بیشتر، مشخص می‌شود که خریدار از یک پروتکل DeFi استفاده کرده بود تا توسط یک وام پرسروصدا این دارایی را به خودش بفروشد. آنها سپس سعی کردند آن را برای یک میلیارد دلار لیست کنند، اما به وضوح کسی تمایلی به خرید آن در آن قیمت نداشت. این موارد قیمت‌های تقلبی هستند.

تا اینجا، محبوب‌ترین کاربرد NFT برای سرمایه‌گذاران خرد شاید اکسی اینفینیتی[45] باشد، که قطعاً مردم فیلیپین و بسیاری از کشورهای دیگر در سراسر جهان آن را بازی کردند، و ارز درون بازی آن توسط بعضی تجار خارج از محیط بازی پذیرفته می‌شود. هرچند، اقتصاد آن بازی هم ذاتاً ماهیت سفته‌بازی دارد چون اغلب مردم فقط در صورتی می‌توانند پول در بیاورند که تعداد بازیکنان جدید به رشدش ادامه دهد. یک بازی ویدیویی طبعاً به رقابت و در جایی به یک مقیاس محدود می‌انجامد، که در آنجا اکثریت شرکت‌کنندگان دیگر از بازی پول درنمی‌آورند.

حالا، استدلال مدافعان و موافقان این پلتفرم‌های اختصاصی قرارداد هوشمند این است که این‌ها در ابتدا سفته‌بازانه‌اند، اما در طی زمان کامل می‌شوند و برای کاربری‌های غیرسفته‌بازانه‌ی بیشتری مرتبط با یک اقتصاد مجازی مشترک مفید خواهند بود. و من با این نگاه هم‌ذات‌پنداری می‌کنم. به‌هرحال، سرمایه‌گذاران بیتکوین با همین نوع اتهامات روبه‌رو هستند. در روزهای اول، بیتکوین‌ها مستمراً در دارک‌وب مورد استفاده قرار می‌گرفتند، و امروزه بسیاری از مردم مقدار کمی بیتکوین به قصد سفته‌بازی می‌خرند، و پس از اینکه بیشتر در موردش یاد می‌گیرند، شروع می‌کنند و به دیدن آن به عنوان یک دارایی بلند مدت که باید آن را نگهداری کرد نه اینکه با آن سفته‌بازی کرد.

استیبل‌کوین‌ها

یکی از کاربردهای کلیدی قراردادهای هوشمند که من فکر می‌کنم به وضوح مفید است استیبل‌کوین‌ها هستند.

از منظر کاربر، آنها عموماً نسبت به انتقالات بین‌المللی از انتقال پول الکترونیکی[46] یا پرداخت‌های محلی بزرگ روش بهتری برای انجام پرداخت‌های ارزهای فیات هستند. شما می‌توانید پرداخت‌ها را ظرف چند دقیقه و در هر زمانی از هفته ارسال و شفاف کنید. آنها به‌طور طبیعی با قانون‌گذاری‌های ادامه‌دار دولت مواجه‌اند و به عنوان بخشی از سیستم بانکی در موارد فراوانی کنترل شده و تحت نظر قرار می‌گیرند، اما به نظر واضح می‌رسد که آنها برای پرداخت‌های واقعی کاربرد دارند و احتمالاً بصورت فزاینده با سیستم‌های مالی ادغام خواهند شد، یا در قالب ارزهای دیجیتال بانک‌های مرکزی یا ناشران خصوصی ولی به‌شدت قانون‌گذاری‌شده‌ی استیبل‌کوین‌ها.

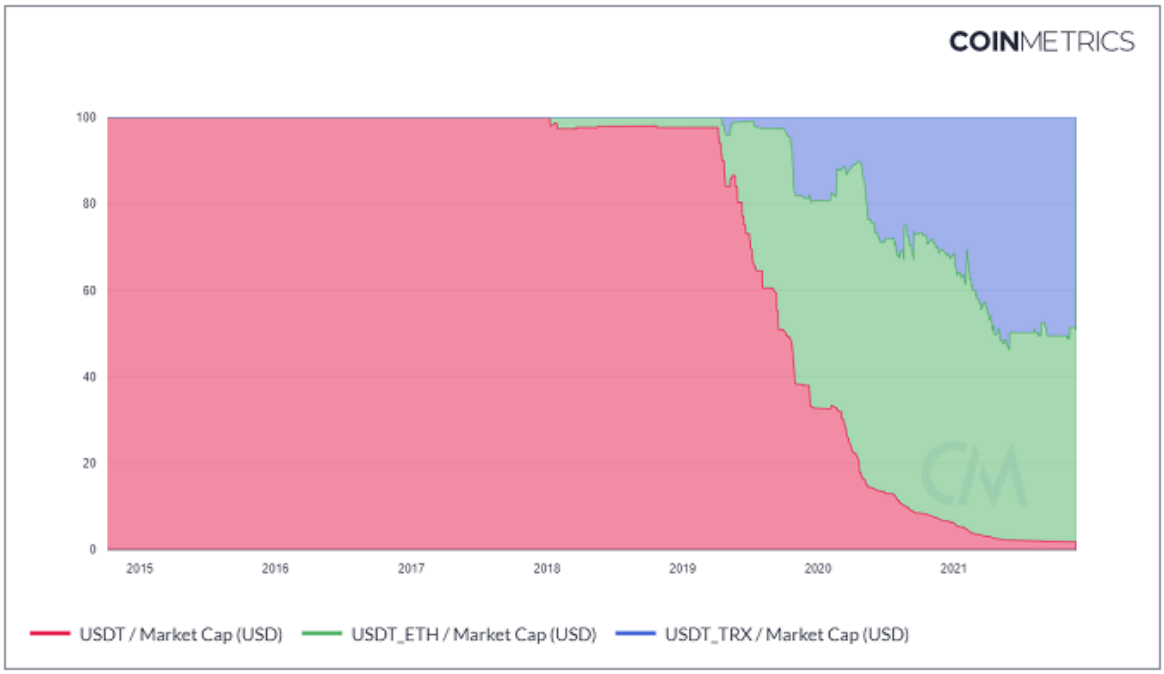
---

[45] Axie Infinity
[46] wire Transfer

این به سادگی ناشی از اتوماتیک‌کردن و فناوری پیشرو است. وقتی شما یک انتقال از طریق انتقال پول الکترونیکی انجام می‌دهید، بانک باید *فعالانه کاری انجام* دهد تا تراکنش را بررسی کند. و چنین انتقالاتی اغلب زمانی که بین بانک‌ها ارتباط ایجاد می‌کنند با تأخیر یا مسدودی مواجه‌اند یا مشکلات دیگری دارند. از منظر کاربر، اغلب مشخص نیست تراکنش در کدام بانک گیر کرده یا به چه کسی باید زنگ بزند. و لذا اغلب روزها طول می‌کشد تا مشکل حل شود. با استیبل‌کوین‌ها، برعکس است. ماهیت اتوماتیک زنجیره‌ی‌بلاک تراکنش‌های همتا به همتا که توسط نرم‌افزار انجام می‌شود در سطح بین‌المللی و مقادیر زیاد پول را ممکن می‌سازد. متولیان، در این باره موضع *انفعالی* دارند و اجازه می‌دهند فناوری برایشان کار را انجام دهد، و فقط هنگامی عمل می‌کنند که بخواهند بعضی از توکن‌هایشان را به دلایلی که کشف کرده‌اند در لیست سیاه قرار دهند.

به عبارت دیگر، استیبل‌کوین‌های قانون‌گذاری‌شده، یک سیستم همتا به همتای اتوماتیک را امکان‌پذیر می‌کنند، اما با یک پوشش نظارتی و سانسور بر اساس قوانین شناسایی مشتری و ضدپولشویی "KYC AML".

هرچند، اهمیت دارد که ببینیم استیبل‌کوین‌ها کلاً اعتقادی به یک پلتفرم ندارند. تتر، به عنوان مثال، از اجرا روی یک راهکار لایه‌ای بر بستر بیتکوین به نام Omni (قرمز) در ابتدا، به اجرا بر بستر اتریوم (سبز) و سپس به اجرای بیشتر بر روی ترون (آبی) روی آورد.



منبع نمودار: Coin Metrics

آیا ترون زنجیره‌ی‌بلاک بهتری از اتریوم است؟ نه، فقط ارزان‌تر است. هر چه کاربرد کمتر حساس باشد، مردم می‌خواهند ارزان‌تر باشد.

به عبارت دیگر، استیبل‌کوین‌ها به عنوان راهکارهای پرداخت تمایل دارند به سمت هزینه‌های انتقال کمتر بهینه شوند، و لذا تمایل دارند به سوی پلتفرم‌هایی بهینه-اما-متمرکز حرکت کنند. و تمام استیبل‌کوین‌های بزرگی که از DeFi پشتیبانی می‌کنند به هر حال به متولیان متمرکز وابسته هستند.

آیا بانک‌ها در نهایت بالاخره خودشان ریل‌گذاری پرداخت‌های استیبل‌کوین سازمانی را ایجاد می‌کنند، یا راهکارهایی مشابه به وجود می‌آورند که ارزان و کارا باشد؟ این اساساً همان کاری است که فیسبوک در تلاش برای انجام آن با Novi و Diem است؛ بهینه‌سازی استیبل‌کوین‌ها برای پرداخت‌های واقعی بجای استفاده برای مبادله‌ی دارایی‌های کریپتو.

هنوز مانده تا ببینیم کدام پلتفرم‌ها برندگان بلندمدت استیبل‌کوین هستند، اما به نظر می‌رسد که آنها به سمت شبکه‌هایی متمرکز یا فدرالی پیش می‌روند تا هزینه‌ها را پایین نگاه دارند. هدف بسیاری از کاربران در واقع عدم تمرکز نیست. در عوض هدف آنها بهینه بودن به همراه پوشش قانون‌گذاری است.

رقابت لایه‌های اصلی، یا رقابت لایه‌های دوم؟

اگر مسئله‌ی فعلی با DeFi و NFTها را کنار بگذاریم و به خاطر تحلیل بیشتر بپذیریم که قراردادهای هوشمند بازار بسیار بزرگ و قابل ذکری دارند، و فارغ از بحث سفته‌بازی و استیبل‌کوین‌ها، آنگاه این سؤال مطرح می‌شود که پلتفرم برنده کدام خواهد بود؟

یک رقابت لفظی جالب در چند ماه اخیر بین اتریوم، سولانا، آوالانچ و دیگران وجود داشته است. اتریوم زنجیره‌ی‌بلاک قرارداد هوشمندی است با اثر شبکه‌ای گسترده، اما با مشکلات مقیاس‌پذیری قابل‌توجه و هزینه‌های انتقال بسیار بالا (و در نتیجه، کاربران خرد عمدتاً غیر از سفته‌بازی بر روی توکن‌ها با خریدن‌شان در صرافی‌های متمرکز، غایب‌اند)، و در تلاش برای انتقال از اثبات کار به اثبات سهم است. سولانا یک زنجیره‌ی‌بلاک قرارداد هوشمند جوان با پشتیبانی شرکت‌های سرمایه‌گذاری ریسک‌پذیر است که مقیاس‌پذیری قابل توجهی هم به همراه دارد، اما با این هزینه که متمرکزتر است. و آوالانچ که یک راهکار پیچیده ارائه می‌دهد تا تلاش کند این مسئله را پاسخ دهد. پس از آن هم الگوراند و دیگران هستند.

DeFi و NFTها شروع به بیرون آمدن از اتریوم به سمت این زنجیره‌های بلاک قرارداد هوشمند دیگر نموده‌اند. بسیاری کاربران حاضرند کمی از امنیت را برای هزینه‌های تراکنشی که به مراتب کم‌ترند فدا کنند.

مدافعان اتریوم اغلب (به‌درستی) سولانا را نقد می‌کنند که خیلی متمرکز است، به عنوان دفاع کلیدی‌شان که چرا اتریوم از سولانا بهتر است. اما این اتریوم را در موقعیت سختی قرار می‌دهد، چون مدافعان اتریوم بعد از این باید در حالی سولانا را به خاطر تمرکز بیش از حدش نقد کنند که همزمان در حال دفاع از این واقعیت هستند که اتریوم تحت سطوحی از حمله‌های متمرکز قرار دارد و پیچیدگی بالاتری در مقابل بیتکوین دارد. به عبارت دیگر، آنها باید این را توجیه کنند که چه سطحی از تمرکز جزئی و عدم تمرکز جزئی سطح درستی است و اینکه آیا آنها به این نقطه‌ی تعادل دست‌یافته‌اند؟

در نتیجه، پلتفرم‌های قرارداد هوشمند در عین حال که برای سهمی از بازار مبارزه می‌کنند، در میان یک "جنگ لایه‌ی اول" با یکدیگر باقی می‌مانند.

در عین حال، شبکه‌ی بیتکوین لایه‌هایی دارد که قادرند قراردادهای هوشمند را به درون خود بیاورند، و مرتباً پیچیده‌تر می‌شوند. زنجیره‌ی جانبی Liquid، که یک زنجیره‌ی جانبی فدرالی است که بر روی شبکه‌ی بیتکوین راه‌اندازی شده است، NFTها از جمله آثار هنری، توکن‌های بازی، استیبل‌کوین‌ها، و توکن‌های کاربردی را میزبانی می‌کند. ال‌سالوادور برنامه‌هایش را برای انتشار یک میلیارد دلار اوراق قرضه بر روی شبکه‌ی Liquid اعلام کرد. Rootstock هم بر روی شبکه‌ی بیتکوین راه‌اندازی شده است، تا DeFi و کاربردهای مشابه را وارد اکوسیستم کند. شبکه‌ی Lightning هم همه‌ی انواع کاربردهای پروتکل را با تمرکز بر انتقال داده بصورت همتا به همتا میزبانی می‌کند.

این لایه‌های قرارداد هوشمند بنا شده بر بیتکوین در حال حاضر از اتریوم بسیار کوچک‌ترند. یکی از دلایلش فرهنگی است؛ بیتکوینرها تمایل دارند بیشتر هولدر باشند تا سفته‌باز، تمایل ندارند خیلی مکرر اقدام به معامله‌ی انواع دیگر توکن کنند و به همین ترتیب. اما همچنین ناشی از اثر شبکه و نقدینگی هم هست؛ در حال حاضر اتریوم با اینکه رفته رفته به مقصد پلتفرم‌های قرارداد هوشمند ارزان‌تر تخلیه می‌گردد، هنوز پلتفرم حاکم برای معاملات آلتکوین‌های شبه‌غیرمتمرکز، اهرم‌سازی، سفته‌بازی NFTها، و بازی‌های زنجیره‌بلاکی است.

با وجود جست‌وجوی بیش از ۵ ساله‌ام، برای من مبهم است که این نقدینگی قراردادهای هوشمند کجا تمام می‌شود. آیا بر روی اتریوم باقی خواهد ماند؟ آیا به سمت پلتفرم‌هایی حتی متمرکزتر مانند سولانا و آوالانچ و از این قبیل جذب می‌شود، به نحوی که ما دنیای قراردادهای هوشمند چندزنجیره‌ای آبکی بیشتری خواهیم داشت؟ یا سفته‌بازی فروکش خواهد کرد و

کاربردی‌ترین استفاده‌ها بر اساس درک استحکام بیشتر لایه‌ی اصلی بیتکوین، راهشان را به لایه‌هایی روی بیتکوین خواهد یافت؟

در نهایت، بخشی از این مسئله به این وابسته است که دولت‌ها چه می‌خواهند. پلتفرم‌های قرارداد هوشمند با سطوح متمرکزی از حمله تنها قادرند به دلخواه دولت‌ها وجود داشته باشند، لذا به این حد تنزل می‌یابد که چه میزان از سرکوب با قانون‌گذاری را می‌توانند تحمل کنند در برابر اینکه چه میزان تأییدیه از قانون می‌توانند اخذ کنند.

در یک شرایط نسبتاً غیر تهاجمی، پلتفرم‌های قرارداد هوشمند تمایل به تبدیل شدن به یک کالا دارند، که بیشتر بر اساس قیمت رقابت می‌کنند تا کیفیت. نقدینگی به سمت هر چیزی که ارزان، متمرکز و با حجم مورد نیاز کافی باشد حرکت می‌کند. برای نقدینگی اثر شبکه‌ای وجود دارد، اما با هزینه‌های تراکنش بالا تا حدودی جبران شده است، که به نحوی به عنوان اثرات ضد-شبکه‌ای عمل می‌کند.

در یک شرایط تهاجمی‌تر با قانون‌گذاری سرکوبگر یا سایر حمله‌ها، زنجیره‌هایی که بیش از حد متمرکز هستند احتمالاً کار کردن برایشان غیرممکن می‌شود، در حالی‌که زنجیره‌هایی که توان عملیاتی خود را برای تأمین درجاتی از عدم تمرکز فدا می‌کنند، قادراند تا حدی کار کنند. نقدینگی به‌طور طبیعی نیاز به حرکت به سمت یک زنجیره یا تعداد کمی زنجیره دارد که قادر باشند در این شرایط کار کنند.

جمع‌بندی من این است که ببینم تعدادی از پلتفرم‌های قرارداد هوشمند به کار خود در شرایطی که قانون‌گذاری در حال تشدید است ادامه دهند و بطور مستمر برای سهمی از بازار مبارزه کنند.

همتا به همتا، بدون DeFi

وقتی شبکه‌ی بیتکوین در ابتدا ایجاد شد، هیچ صرافی وجود نداشت. اگر مردم می‌خواستند بیتکوین‌ها را بخرند یا بفروشند، باید بین خودشان توافق می‌کردند. ملاقات‌های از پیش تعیین شده‌ای بود که این کار را آسان‌تر کند، و صنعت در نهایت صرافی‌های متمرکز را شکل داد.

اما در هسته‌اش، این یک فناوری همتا به همتاست. اگر من و شما شخصاً ملاقات کنیم، من می‌توانم توافق کنم بخشی از یک بیتکوین را از آدرس بیتکوینم به مال شما ارسال کنم، در مقابل پول نقد یا هر کالای دیگری که شما به من تحویل دهید، و ما می‌توانیم این کار را در یک کافی‌شاپ انجام دهیم.

برای مردمی که ترجیح می‌دهند از صرافی‌های متمرکز دوری کنند، فناوری‌های همتا به همتای مختلفی وجود دارد که این را از ملاقات‌های حضوری شبیه به این راحت‌تر می‌کند. Bisq، Hodl Hodl، LocalBitcoins، و Paxful همگی راه‌های مختلفی هستند که تبادلات بیتکوین همتا به همتا را انجام می‌دهند، و هر یک مزایا و معایبی دارند اما به توکن‌های خارجی نیازی ندارند.

یک پلتفرم سپرده‌گذاری چندامضایی، به عنوان مثال، می‌تواند به عنوان یک عامل سوم عمل کند. خریداران و فروشندگان می‌توانند به یک قرارداد آنلاین چند امضایی ۲ از ۳ وارد شوند، که در آن فروشنده بیتکوین‌هایش را در قرارداد قرار می‌دهد، و تنها وقتی آزاد می‌شود که پرداخت از سمت خریدار انجام شود. یک عامل سوم کلید سوم قرارداد را نگه‌می‌دارد، که اطمینان حاصل کند بیتکوین‌ها تنها در صورت رضایت هر دو طرف معامله آزاد شود، و اگر یکی از طرفین رضایت نداشت، پیش از نهایی نمودن تراکنش، می‌تواند به عنوان یک داور حل اختلاف مدارک را بپذیرد.

نیجریه چندی پیش معاملات کریپتو را از سیستم بانکی خود حذف کرد. آنها معامله یا نگهداری رمزارزها را غیرقانونی نکردند (که البته اعمال آن بسیار سخت است)، اما در عوض آنها مسیر آسان تر قطع کریپتو از هر نوع ارتباط رسمی با سیستم بانکی محلی‌شان را در پیش گرفتند. به عبارت دیگر، شما نمی‌توانید ارز فیات نیجریه را بگیرید و به راحتی آن را به یک صرافی رمزارز بفرستید تا بیتکوین بخرید.

برای فهم دینامیک بازی این تصمیم، باید بدانید که نیجریه تورم مستمر دورقمی دارد و نمی‌خواهد سرمایه از سیستم بانکی‌اش به سوی یک ارز دیجیتال پول سالم که شهروندانش به راحتی بتوانند با آن مبادله کنند سرازیر شود، همچنین نمی‌خواهد جرقه‌ی یک آشوب اجتماعی غیرضروری را با ممنوع کردن آن آغاز کند (چون بسیار محبوب است) و می‌خواهد شهروندانش بتوانند پرداخت‌های بیتکوینی از خارج از کشور دریافت کنند. چون نیجریه برنامه‌نویسان و طراحان گرافیک خوب بسیار زیادی دارد که خارجی‌ها دوست دارند استخدامشان کنند و با بیتکوین به آنها پرداخت کنند، با جمعیتی بالغ بر ۲۰۰ میلیون، نیجریه انگیزه‌ای برای اختصاص منابع جهت بازرسی خانه به خانه و اطمینان از عدم استفاده‌ی نیجریه‌ای‌ها از بیتکوین ندارد.

اما نکته اینجاست که اشخاص نیجریه‌ای نیاز داشتند راه‌های جایگزینی برای انجام تراکنش با بیتکوین پیدا کنند. و علیرغم آن، نیجریه یکی از بالاترین نرخ‌ها برای نگهداری بیتکوین را به ازای هر فرد با رتبه‌ی ششم جهان در اختیار دارد. آنها عمدتاً از روش معامله‌ی همتا به همتا با استفاده از Paxful و LocalBitcoins برای ارسال و دریافت همتا به همتای بیتکوین استفاده می‌کنند. و از گروه‌های تلگرامی و سایر انواع روش‌های هماهنگی برای تبادل ارزهای فیات با بیتکوین استفاده می‌کنند. آنها به طور گسترده از پلتفرم‌های زنجیره‌ی‌بلاک DeFi استفاده نمی‌کنند. DeFi با هزینه‌های بالای تراکنش، اساساً برای سفته‌بازان بزرگ سازمانی، بازیگران نوسان‌گیر، نهنگ‌ها و غیره است.

DeFi تا اینجا ابتداعاً برای سفته‌بازی است. وقتی مردمی که در کشورهایی با درآمد سرانه‌ی ۲۰۰۰ دلار ، ۳۰۰۰ دلار، یا ۴۰۰۰ دلار در سال، به بیتکوین علاقه دارند، آنها روی اتریوم هزینه‌های تراکنش صد دلاری پرداخت نمی‌کنند تا با NFT ها یا معاملات کریپتو یا سفته‌بازی سرگرم شوند. آنها گروه‌هایی را تشکیل می‌دهند تا خرید و فروش بیتکوین را هماهنگ کنند، یا به دنبال ارزان‌ترین (و اغلب متمرکزترین) پلتفرم‌های قرارداد هوشمند هستند.

استثنای قابل توجه در این مشاهده‌ی عمومی، بازی‌ها هستند. همان‌طور که از قبل به آن اشاره شد، Axie Infinity در فیلیپین بسیار محبوب است، اما بسیاری از این محبوبیت شامل مردمی می‌شود که به سختی تلاش می‌کنند تا از بازی درآمد کسب کنند و اقتصاد بازی تنها تا جایی کار می‌کند که بازی به رشد خود ادامه دهد. اگر دارایی‌های بازیکنان جدید مستمراً درآمدهای بازیکنان موجود را تأمین نکند، آنگاه بازی در معرض یک سقوط بازیکن قرار می‌گیرد، مگر اینکه ذاتاً به اندازه‌ی کافی برای اکثر کاربران جالب باشد که علیرغم عدم کسب درآمد از آن، در آن سرمایه‌گذاری سنگین انجام دهند.

پروتکل یا سیستم عامل

از زمانی که ساتوشی ناکاموتو بیتکوین را خلق کرد، تلاش‌های بیشماری برای بهبود طراحی او انجام شده است. در دسته‌بندی های اصلی زیر:

- مردم بر سر افزایش سایز بلاک در ازای مشکل‌تر شدن راه‌اندازی نودها که منجر به متمرکزتر شدن می‌شد بحث کردند، و سکه‌های جدیدی را بر این اساس ساختند.
- مردم بر سر کاهش زمان ایجاد بلاک، در ازای کاهش پایداری شبکه بحث کردند و سکه‌های جدیدی بر این اساس ساختند.
- مردم تصمیم گرفتند برخی از درجات قابلیت بازرسی را برای دستیابی به حریم خصوصی بیشتر فدا کنند، و سکه‌های جدیدی بر این اساس ساختند.

این سکه‌ها بطور مداوم حتی موفق نشدند ۵ درصد از سرمایه‌ی بازار بیتکوین را حفظ کنند. حکمت بازار پس از مدت زمانی نسبتاً طولانی تصمیم گرفته است که این قابلیت‌ها، حداقل خارج از یک شرایط خاص، مورد نظر نمی‌باشد.

در این حین، خود شبکه‌ی بیتکوین هم به‌روزرسانی آرام خود را در لایه‌ی اصلی از طریق سافت‌فورک‌ها ادامه می‌دهد، به معنی اینکه تنها به‌روزرسانی‌های سازگار با گذشته را، تنها زمانی که اجماع چشمگیری برای اعمال آن وجود داشته باشد اعمال می‌کند. و به‌روزرسانی پرسرعت خود را بر روی لایه‌ی دوم، بر روی زنجیره‌های جانبی، و با تأمین‌کنندگان سخت‌افزار و نرم‌افزار اطراف اکوسیستم پی می‌گیرد، که بر لایه‌ی اصلی تأثیر نمی‌گذارد. برخی از آن به‌روزرسانی‌ها می‌توانند استفاده از شبکه‌ی بیتکوین را سریع‌تر، با توان عملیاتی بیشتر، با قابلیت‌های بیشتر، و یا با حریم‌خصوصی بیشتر بکنند.

گرچه، سرفصل اصلی که بازار هنوز در حال تصمیم‌گیری راجع به آن است، این یکی است:

- مردم بر سر اضافه‌کردن قابلیت‌های بیشتر به زنجیره‌های بلاک در لایه‌ی اصلی در ازای تمرکز بیشتر و سطوح حمله بحث کردند و سکه‌هایی (آلتکوین‌هایی) را بر این اساس ساختند.

پس، یک موضوع بزرگ که بازار هنوز در حال ارزیابی آن است، این است که آیا این پلتفرم‌های قرارداد همشمند متمرکز جزئی، نقش بزرگی در کنار شبکه‌ی بیتکوین بازی می‌کنند، یا اینکه آنها هم در نهایت مثل سرنوشت آلتکوین‌های خیالی قبلی، راکد خواهند شد؟

من استدلالاتی در مورد اینکه حوزه‌ی رمزارزها پس از سپری شدن زمانی به اندازه‌ی کافی طولانی به چه شکل خواهد بود دیده‌ام. در نهایت، به این ختم می‌شود که آیا فضا به گونه‌ای تغییر می‌کند که بیشتر شبیه عملکرد پروتکل هاست یا بیشتر شبیه به عملکرد سیستم‌های عامل است.

پروتکل‌ها تمایل دارند دستاوردشان برنده همه چیز را می‌برد[۴۷] باشد، و لذا موقعیت خود را با حدود ۹۰ درصد یا بیشتر از سهم بازار برای زمانی بسیار طولانی حفظ می‌کنند. TCP/IP پروتکلی است که اینترنت بر روی آن در دهه‌ی ۱۹۷۰ اجرا شد. SMTP پروتکل ایمیل است و در اوایل دهه‌ی ۱۹۸۰ توسعه یافت. Ethernet پروتکل شبکه است و در اوایل دهه‌ی ۱۹۸۰ توسعه یافت. USB پروتکل ارتباطی است و در دهه‌ی ۱۹۹۰ توسعه یافت.

در طی ده یا ۲۰ سال، ما همچنان بر روی اکثر یا تمام این پروتکل‌ها اجرا خواهیم کرد، و این پروتکل‌ها هم در طول زمان به‌روزرسانی خواهند شد. همه‌ی این پروتکل‌ها در ابتدا رقبایی داشتند، اما اکثر مردم امروزه آن رقبا را نمی‌توانند نام ببرند.

سیستمهای عامل تمایل دارند دستاوردشان بازار شبه‌انحصاری باشد، نه برنده همه چیز را می‌برد. چند سیستم عامل می‌تواند هم‌زمان وجود داشته باشد، هر یک با اثر شبکه‌ای و حوزه‌های ترجیحی خودش، اما تنها به تعداد انگشتان یک دست می‌توانند بطور واقعی تقاضای گسترده‌ای به همراه جذب تعداد زیادی از توسعه‌دهندگان را داشته باشند. همین موضوع قابل تعمیم به پلتفرم‌های شبکه‌های اجتماعی و همچنین صرافی‌های مالی است.

برخی افراد پیشنهاد می‌کنند که پس از بلوغ کافی این حوزه، یک زنجیره‌ی‌بلاک بر این حوزه حاکم می‌شود، با این استدلال که این‌ها پروتکل هستند و یک پروتکل (مثل بیتکوین) برنده خواهد شد.

افراد دیگری پیشنهاد می‌کنند که دستاورد نهایی چیزی شبیه به سیستم‌های عامل خواهد بود، با تعداد کمی از بازیگران بزرگ دائمی. حتی اگر یک بازیگر شاید ۳۰، ۴۰، ۵۰ درصد یا بیشتری از بازار را در اختیار داشته باشد، بر اساس این دیدگاه نخواهد توانست بیش از ۹۰ درصد را داشته باشد. یک زیرمجموعه‌ی این استدلال پیشنهاد می‌کند که بیتکوین و پلتفرم‌های قرارداد هوشمندی مثل اتریوم حتی واقعاً برای یک بازار یکسان رقابت نمی‌کنند، و لذا می‌توانند بطور مجزا با تنها مقدار متوسطی همپوشانی گروه‌بندی شوند.

من راجع به اینکه این موضوع به کجا ختم می‌شود اعتقاد کاملی ندارم. واضح است که بیتکوین تا جایی که مربوط به پول زنجیره‌ی‌بلاکی اثبات کار غیرمتمرکز می شود برنده است. و من فکر می‌کنم مردم اندازه‌ی نهایی کل بازار این مفهوم را دست کم گرفته‌اند.

جدای از این، آیا پلتفرم قرارداد هوشمند بزرگ ماندگاری وجود خواهد داشت، یا روزی همه‌ی آنها به عنوان لایه‌هایی بر روی بیتکوین قرار می‌گیرند؟ و تا حدی که به عنوان پلتفرم‌های قرارداد هوشمند مستقل لایه‌اول باقی می‌مانند، تا چه میزان یکدیگر را تضعیف می‌کنند و به زنجیره‌های بلاکی به شدت متمرکز، ارزان و کالایی شده تبدیل می‌شوند؟ بازار هنوز در حال یافتن پاسخ این قبیل سؤالات است.

در نهایت، مسئله‌ی اصلی من بین دستاورد پروتکل و سیستم‌عامل بستگی به سطح سرکوب به وسیله‌ی قانون‌گذاری دارد.

---

[47] winner-take-all

در مورد خروجی پروتکل، من می‌توانم تصور کنم که پلتفرم‌های قرارداد هوشمند یا در سطوح حمله‌شان به شدت مورد حمله قرار می‌گیرند (به عنوان مثال سرکوب بی‌رحمانه توسط قانون‌گذاری[۴۸])، یا بر اثر سنگینی جنبه‌ی سفته‌بازانه‌ی دوار خودشان فرو می‌ریزند. در همین حین، بیتکوین یک لایه‌ی اصلی غیرمتمرکز و توانایی ساخت کاربردهای قرارداد هوشمند را بر روی لایه‌های دیگر روی خود دارد، و می‌تواند این ارزش را در طی زمانی که سایر زنجیره‌های بلاک دچار مشکلاتی شده‌اند به درون خود جذب کند.

در مورد خروجی سیستم عامل، من می‌توانم تصور کنم که بیتکوین سهم حاکم خود را از بازار پول و وثیقه‌ی جهانی در فضای دارایی دیجیتال، با لایه‌های اضافی پیچیده‌ی ساخته شده بر روی خود حفظ می‌کند، اما آن پلتفرم‌های مجزای بزرگ قرارداد هوشمند به عنوان پلتفرم‌هایی قانون‌گذاری شده برای پردازش ارزان استیبل‌کوین‌ها، بازی‌های کریپتویی، معاملات آلتکوین‌ها، سفته‌بازی NFTها، تسویه‌ی اوراق بهادار، و سایر کاربردها وجود دارند. این‌ها اساساً باید اوراق بهادار سهام باشند.

تفکرات نهایی: همیشه بده‌بستان‌ها را در نظر بگیرید

مطابق لیست CoinMarketCap، در زمان نگارش این مقاله، حدود ۱۵۰۰۰ رمزارز وجود دارد.

سهم بیتکوین از کل بازار رمزارز در طول زمان تغییر می‌کند، اما به عنوان مثال در حال حاضر همان سهمی را از بازار (درحدود ۴۰ درصد) در مقابل این ۱۵۰۰۰ سکه دارد که چهار سال پیش در مقابل فقط ۱۵۰۰ سکه داشت. پس آلتکوین‌ها عمدتاً یکدیگر را تضعیف کرده‌اند.

راهی که آلتکوین‌ها با آن برای خود بازار دست‌وپا می‌کنند، عمدتاً بدین صورت است که کاستی‌های بیتکوین را برجسته می‌کنند به‌طوری که انگار تکنولوژی آن قدیمی و سکه‌ی نسل قدیمی است، و سپس توضیح می‌دهند که چگونه خودشان بهتر از بیتکوین هستند.

وقتی درباره‌ی آنها دقیق بررسی می‌کنید، معلوم می‌شود بده‌بستان‌های عظیمی در یک بخش انجام داده‌اند تا در جای دیگری قابلیت دیگری به‌دست آورند. آنها درجاتی از امنیت، عدم تمرکز، قابل بازرسی بودن، و امثال این را فدا می‌کنند تا چیزهایی مثل قابلیت‌های بیشتر، سرعت بیشتر، یا توان عملیاتی بیشتر به‌دست بیاورند. و حالا همین اتفاق دارد برای اتریوم می‌افتد؛ زنجیره‌های قرارداد هوشمند جدیدتر، بهره‌وری بیشتر را در عوض تمرکز بیشتر ارائه می‌دهند، و اتریوم را برای بیشتر قربانی نکردن عدم تمرکز برای مقیاس‌پذیری سریع‌تر نقد می‌کنند.

ساتوشی ناکاموتو متغیرهایش را بسیار بادقت انتخاب کرد. هر یک مورد مناقشه قرار گرفت و آزمایش شد.

> "دولت‌ها قطع کردن سر شبکه‌های کنترل شونده‌ی مرکزی (متمرکز) مثل Napster را خوب بلدند، اما شبکه‌های تماما همتا به همتایی مثل Guntella و Tor به نظر می‌رسد می‌توانند خود را حفظ کنند.
>
> - ساتوشی ناکاموتو، ۷ نوامبر ۲۰۰۸

وقتی یک ایده‌ی کاملا بهتر برای یک بخش کوچک از پروتکل بعد از سال‌ها اثبات مورد موافقت قرار می‌گیرد، توسعه‌دهندگان بیتکوین، به پشتیبانی کاربران، در نهایت مایل‌اند آن را در بیتکوین به وسیله‌ی یک اجماع سافت‌فورک بگنجانند، مانند به‌روزرسانی‌های SegWit و Taproot.

مردم اغلب راجع به رمزارزها مثل یک کلاس دارایی بزرگ مشابه فکر می‌کنند اما در بیشتر موارد، پرسروصداترین منتقدین شبکه‌ی بیتکوین، طرفداران سایر زنجیره‌های بلاکی هستند که هم‌زمان سعی دارند برای سکه‌ی خودشان به‌جای بیتکوین بازاریابی کنند. در همین حین، علاقه‌مندان بیتکوین هم جزو بزرگترین منتقدان اکوسیستم کریپتو هستند، و تمایل دارند کلاهبرداری‌ها، هک‌ها، معاملات صوری[۴۹]، و مشکلات تمرکزی را که در فضای رمزارزی آلتکوین‌ها شایع است برجسته کنند.

---

[48] draconian regulatory crackdown
[49] wash sales

صرافی‌های کریپتو با بیشمار انواع سکه، انگیزه دارند تا شما را درباره‌ی سکه‌های جدید هیجان‌زده کنند، چون آنها از حجم معاملات پول درمی‌آورند. حتی اگر سکه‌های مسخره‌ای[50] مثل Doge یا Shiba Inu باشند، آنها می‌خواهند شما را مجبور به اقدام نمایند، مخصوصا نزدیک قله وقتی تمایل شما زیاد است. انگیزه‌ی مالی آنها آن است که کاربرانشان تعداد زیادی سکه نگهداری نمایند، و مرتبا آن سکه‌ها را معامله کنند، و خیلی خوشحال می‌شوند تا هر سکه‌ای که در هر لحظه محبوبیتی کسب کرد را برجسته کنند. در این شرایط، این صاحبخانه (یعنی همان صرافی) است که در هر حالت برنده است.

در مواردی که یک سرمایه‌گذار تصمیم می‌گیرد که در دارایی‌های دیجیتالی غیر از بیتکوین یه سفته‌بازی بپردازد، باید همیشه قادر باشد به این پرسش پاسخ دهد "بده‌وبستان ها چه چیزهایی هستند؟" پیش از آن‌که تصمیم بگیرد یک پروتکل را در مقایسه با دیگری بخرد. در مجموع، من مفهوم بیتکوین را به عنوان دارایی پولی، و مفهوم توکن‌های پلتفرم قرارداد هوشمند را به عنوان اوراق بهادار سهام در نظر می‌گیرم.

هر کس استدلال‌های خودش را دارد و تمایل دارد سفته‌بازی کند یا سرمایه‌گذاری بلندمدت انجام دهد، اما وقتی مبادرت به ورود در زنجیره‌های بلاکی غیر از شبکه‌ی بیتکوین می‌کنید، قبل از آن مطمئن شوید که تحت تأثیر بازاریابی آن کوین‌ها نباشید و بدون صحت‌سنجی هر ادعایی خریدی انجام ندهید، بدانید در چه راهی قدم می‌گذارید.

[50] Meme-coins