مبانی و مقایسهٔ روش‌های اجماعِ اثباتِ کار و اثباتِ سهم

ویراست دوم – نسخهٔ موبایل

بهار ۱۴۰۲

اجماع[1] روی تراکنش‌های معتبر در پروتکلِ بیت‌کوین بر اساس روش اثباتِ کار[2] حاصل می‌شود. یکی از هشت ارجاع موجود در وایت‌پیپرِ[3] بیت‌کوین مربوط به فعالیت‌های آدام بک[4] در توسعهٔ اثباتِ کار است.

از زمان معرفی روش اثباتِ کار توسط ساتوشی ناکاموتو[5] افرادی مدعی بوده‌اند که روش‌های جایگزینِ دیگری مانند روش اثباتِ سهم[6]، وجود دارند که از روش اثباتِ کار بهینه‌ترند. مزیت‌های این روش‌ها اغلب با نادیده گرفته‌شدنِ عواقب به‌کارگیری آن‌ها در مقایسه با روش اثباتِ کار مورد بررسی قرار می‌گیرند. در این مقاله به واکاوی این موضوع می‌پردازیم.

مبانی اثباتِ کار

شبکهٔ بیت‌کوین طوری برنامه‌ریزی شده است که به‌طور متوسط هر ده دقیقه یک بلوک[7] ایجاد، و آن را به زنجیرهٔ بیت‌کوین اضافه کند. این زنجیره در سال ۲۰۰۹

---

1 Consensus
2 Proof of Work
3 Bitcoin Whitepaper
4 Adam Back
5 Satoshi Nakamoto
6 Proof of Stake
7 Block

آغاز به کار کرده و در حال حاضر شامل صدها هزار بلوک است.

هر بلوک جدید توسط یک ماینر[1] بیت‌کوین ساخته می‌شود. ماینرها با تأمین برق برای دستگاه‌های استخراج، قدرت پردازشی خود را برای حل کردن یک مسألهٔ رمزنگاری که توسط بلوک قبلی طرح شده به‌کار می‌گیرند. ماینرها از این روش تراکنش‌های در صف انتظار را دسته‌بندی، و در یک بلوک قرار می‌دهند. تراکنش‌ها در شبکهٔ بیت‌کوین این‌گونه تسویه می‌شوند. شبکه طوری برنامه‌ریزی شده است که متوسط زمان ایجاد بلوک‌ها در آن ده دقیقه باشد. یعنی به‌طور میانگین هر ده دقیقه یک بلوک شامل هزاران تراکنش به زنجیره‌ی بلوک[2] بیت‌کوین اضافه می‌شود.

پردازنده‌های دستگاه‌های استخراج بیت‌کوین برای حل کردن مسأله‌ای که توسط بلوک قبلی طرح شده حدس‌های تصادفی می‌زنند اما، قانون اعداد بزرگ به نحوی است که هر چه تجهیزات استخراج بیت‌کوین بیشتری داشته باشید، در یک بازه زمانی نسبتاً طولانی بلاک‌های بیشتری نیز پیدا خواهید کرد.

---

1 Bitcoin Miner
2 Blockchain

اگر بخشی از ماینرها شبکه را ترک کنند و ایجاد بلوک‌های جدید به‌طور متوسط بیشتر از ده دقیقه طول بکشد، شبکه به‌صورت خودکار، حل مسأله، یا به عبارت دیگر ایجاد یک بلوک را به مقدار مشخصی آسان‌تر می‌کند تا میانگین زمان مورد نیاز برای ساخت بلوک‌ها در شبکه به ده دقیقه بازگردد. برعکس، اگر تعداد زیادی ماینر به شبکه بپیوندند و میانگین زمان تولید هر بلوک کمتر از ده دقیقه شود، شبکه مسأله را سخت‌تر می‌کند. این، به «تنظیم سختی[1]» معروف است که به‌طور خودکار و تقریباً هر دو هفته یک بار اتفاق می‌افتد. این موضوع یکی از چالش‌های کلیدی برنامه‌ریزی شبکه بود و ساتوشی ناکاموتو موفق به حل کردن آن شد.

بنابراین در هر لحظه، میلیون‌ها دستگاه استخراج بیت‌کوین در سراسر جهان به دنبال حل مسأله و ایجاد بلوک بعدی هستند و یک مکانیزم نیز وجود دارد تا شبکه اطمینان حاصل کند بلوک‌ها،- فارغ از اینکه ماینرهای شبکه چقدر کم یا زیاد باشند،- بطور متوسط هر ده دقیقه ایجاد می‌شوند.

در نیمهٔ اول ۲۰۲۱، چین که در آن زمان بیشترین تمرکز ماینرها را در اختیار داشت، صنعت استخراج

1 Difficulty adjustment

رمزارز[1]ها را ممنوع کرد و این مسأله موجب خاموش شدن تقریباً نیمی از شبکهٔ استخراجِ جهانی بیت‌کوین، و مهاجرت آن‌ها به سایر نقاط جهان شد. سرعت شبکهٔ پرداخت بیت‌کوین اندکی کاهش پیدا کرد اما هیچ‌گونه اختلالی در کار آن رخ نداد. سپس تنظیم سختی شبکه به‌صورت خودکار اتفاق افتاد و سرعت تولید بلوک را به مقدار برنامه‌ریزی‌شده بازگرداند. تصور کنید به شرکت آمازون یا مایکروسافت یک هفته زودتر اطلاع داده می‌شد که باید نیمی از سرورهایشان را در سطح بین‌المللی جابجا کنند. احتمالاً خدمات ارائه شده این شرکت‌ها در حین جابه‌جایی و بازسازیِ نیمی از زیرساخت‌هایشان، ماه‌ها یا حتی زمان طولانی‌تری دستخوش مشکلات جدی می‌شد. اما این موضوع هیچ‌گونه اختلالی در کار شبکهٔ بیت‌کوین به‌وجود نیاورد.

اگر ماینری یک بلوک نامعتبر، یعنی بلوکی که از قوانین مشترک نودهای[2] موجود در شبکه پیروی نمی‌کند را بسازد، این مورد پذیرش شبکه قرار نخواهد گرفت و مردود خواهد شد.

---

1 Cryptocurrency

2 Node

اگر دو ماینر یک بلوک معتبر را تقریباً همزمان بسازند، بلوک برنده، بلوکی است که زودتر توسط بقیهٔ نودهای شبکه دریافت، بلوک معتبر بعدی به آن اضافه، و بخشی از بلندترین زنجیره[1] شود. اگر بلوک‌های بعدی هم در یک محدودهٔ زمانی ایجاد شوند، برنده با ساخت سومین یا چهارمین بلوک معتبر مشخص خواهد شد. بر اساس قوانینِ اجماع، بلوک برنده، بلوکی است که جزئی از بلندترین زنجیرهٔ بلوک‌های معتبر باشد.

این فرایند با عنوان «اثباتِ کار» شناخته می‌شود. میلیون‌ها دستگاه قدرت پردازشی خود را با صرف برق وقفِ حدس‌زدنِ پاسخ معمای رمزنگاری که توسط بلوک قبل طرح شده می‌کنند. این ممکن است هدر دادن انرژی به نظر برسد، اما همان چیزی است که موجب غیرمتمرکز ماندن شبکهٔ بیت‌کوین می‌شود.

اینجا کار، معیار واقعیت است. در این شبکه هیچ نهاد متمرکزی برای تعیین بلوک یا تراکنش‌های معتبر وجود ندارد. طولانی‌ترین زنجیرهٔ بلوک همواره قابل راستی‌آزمایی است و توسط بقیهٔ شبکه و بر اساس کُدهای نرم‌افزاری قابل شناسایی است.

---

1 Best Chain

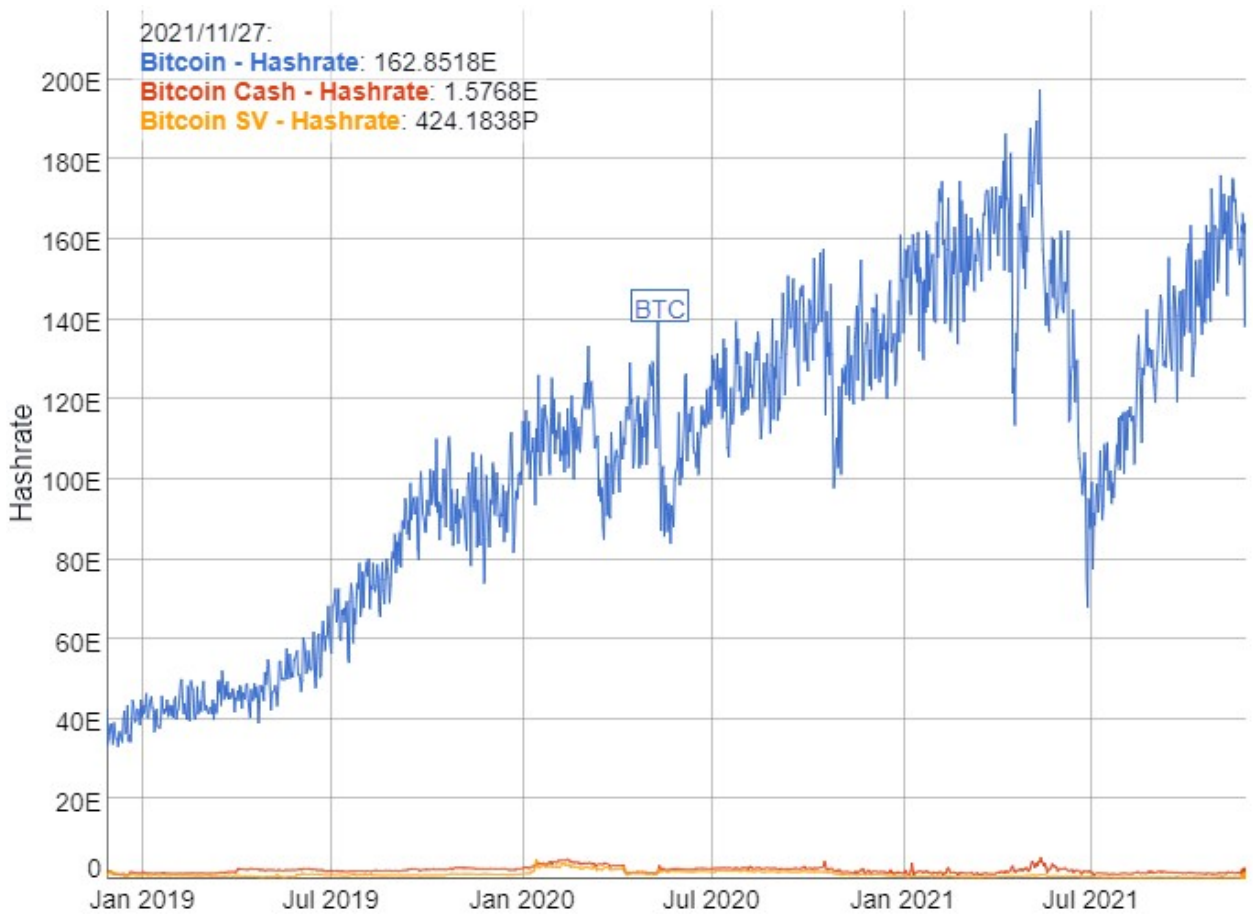
بلندترین زنجیرهٔ بلوک، زنجیره‌ای‌ست که بیشترین کار بر روی آن انجام گرفته است. این همان معیاری است که توسط شبکه تصدیق، و به یک اجماع سراسری تبدیل می‌شود.

هر چه شبکهٔ بیت‌کوین انرژی بیشتری مصرف کند، بازگشت‌ناپذیریِ تراکنش‌های آن در مقابل حمله‌های مختلف نیز افزایش خواهد یافت. زنجیرهٔ بلوک بسیاری از پروژه‌های کوچکی که روش اجماع آنها مانند بیت‌کوین روش اثباتِ کار است، قربانی حمله‌ی ۵۱ درصدی[1] شده‌اند. در یک حملهٔ ۵۱ درصدی، یک موجودیتِ واحد، کنترل بیش از ۵۱ درصد از قدرت پردازشی شبکه را به‌طور موقت یا دائم به‌دست می‌آورد، و از آن برای بازترتیب بلوک‌ها[2] و ایجاد تراکنش‌های

1 51 Percent Attack
2 Reorganization (reorg)

خرج کردنِ دوباره[3] (که اساساً دزدی است) استفاده می‌کند.

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



منبع نمودار: BitInfoCharts.com

زنجیرهٔ بلوک هر دوی آن‌ها تنها ۱ درصد یا کمتر از کل قدرت پردازش بیت‌کوین را در اختیار دارد، و هر دو تحت حملهٔ بازترتیب بلوک‌ها قرار گرفته‌اند. در واقع، اگر تنها ۱ درصد از ماینرهای بیت‌کوین تصمیم بگیرند، قادرند یک حملهٔ ۵۱ درصدی به هر یک از این دو هاردفورک انجام دهند. اما برعکس آن ممکن

3 Double Spend

نیست، زیرا شبکهٔ بیتکوین تقریبا تمامی ماینرها را در اختیار خود دارد و میزان توان پردازشی آن حدود ۱۰۰ برابر هریک از آن‌ها است.

این نشان دهنده‌ی اهمیت اثر شبکه‌ای[1] [2] در صنعت بلاک‌چین است و نشان می‌دهد چگونه مصرف بالای برق شبکهٔ بیت‌کوین موجب تأمین امنیت زنجیرهٔ بلوک آن شده است.

برای همین در جواب کسی که می‌پرسد «مگر نمی‌شود به‌راحتی بیت‌کوین را کپی کرد؟» می‌گوییم «خیر، نمی‌شود». شما می‌توانید کد متن‌باز پروژهٔ بیت‌کوین را کپی کنید، اما این حقیقت را که میلیون‌ها دستگاه ماینر با مدار مجتمع و کاربرد خاص در حال تأمین امنیت شبکهٔ بیت‌کوین و نه شبکهٔ کپی شدهٔ شما هستند نمی‌توانید کپی کنید. شما نمی‌توانید این حقیقت را که ده‌ها هزار نود (گره) شبکه در حال اعمال قوانین اجماع هستند کپی کنید. همچنین نمی‌توانید این حقیقت را که هزاران برنامه‌نویس هر روز در حال کار روی بهبود شبکهٔ بیت‌کوین و نه شبکهٔ کپی‌شدهٔ شما هستند کپی کنید. همچنین لایهٔ دوم بیتکوین، لایتنینگ، کانال‌های

---

1 Network Effect

2 https://www.lynalden.com/bitcoins-network-effect

پرداختِ موجود و نقدینگی فراوانی که به آسانی قابل کپی کَردن نیست. ساخت آن‌ها سال‌ها زمان برده است.

تلاش برای کپی کردن بیت‌کوین مانند آن است که محتوای ویکی‌پدیا را کپی کرده و بر روی وبسایت خود قرار دهیم. این کار از نظر فنی امکان‌پذیر است، اما فایدهٔ چندانی ندارد. این امر باعث بدست آوردن ترافیک واقعی ویکی‌پدیا نمی‌شود، چون صدها میلیون لینکی که از سایر وبسایت‌ها به آن ارجاع داده‌شده را شامل نمی‌شود. و مانند ویکی‌پدیای واقعی به‌روزرسانی نمی‌شود، چون امکان ندارد من بتوانم اکثریت ویراستارهای داوطلب را راضی کنم که بیایند روی نسخهٔ ویکی‌پدیای من مشغول شوند. پس در صورتی که نتوانم از عهده‌ی وظیفه‌ی دشوار قانع نمودن اکثریت شبکه جهت فعالیت بر روی نسخهٔ خودم برآیم، این کپی تنها سایه‌ای از نسخهٔ 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.

مبانی اثبات سهم

همان‌طور که قبلاً گفتیم، اثباتِ کار سیستمی است که در آن ماینرها با صرف برق و قدرت پردازشی خود بر سر ساخت طولانی‌ترین زنجیرهٔ بلوک رقابت می‌کنند؛ زنجیره‌ای که طبق قوانین اجماع مورد پذیرش نودهای شبکه است. به عبارت دیگر اثباتِ کار نقطهٔ اتصال زنجیرهٔ بلوکِ دیجیتال با دنیای واقعی (فیزیکی) است.

شبکهٔ بیت‌کوین از زمان آغاز به کار خود در سال ۲۰۰۹ بر اساس روش اثبات کار عملیاتی شده و تا به امروز هم هیچ برنامه‌ای برای تغییر آن وجود ندارد.

شبکهٔ اتریوم هم از زمان پدید آمدن در سال ۲۰۱۵ بر اساس روش اثبات کار فعالیت کرده است. اما چندین سال است گردانندگان این پروژه در حال برنامه‌ریزی برای تغییر روش اجماع به سیستم اثبات سهم هستند.

بسیاری از پروژه‌های جدیدی که بعد از اتریوم معرفی شدند و روی بستر زنجیرهٔ بلوکِ خود قراردادهای هوشمند[1] ارائه می‌کنند، کار خود را از ابتدا بر اساس روش اثبات سهم آغاز نمودند. این پروژه‌ها از این نظر

1 Smart Contract

نسبت به اتریوم پیشگام‌اند اما، اثر شبکه‌ای قابل‌توجه اتریوم را در اختیار ندارند.

حال وقت آن فرا رسیده در مورد نحوهٔ کار روش اثبات سهم صحبت کنیم.

اثبات سهم سیستمی است که دارندگان یک رمزارز با گروگذاری[1] سکه‌های[2] خود، از آن‌ها به‌عنوان پشتوانه‌ای برای رأی‌دهی روی زنجیرهٔ بلوک استفاده، و سکه‌های جدیدی بابت ایجاد موفقیت‌آمیز بلوک‌های جدید به‌عنوان پاداش دریافت می‌کنند. به عبارت دیگر آن‌ها به جای صرف برق و تأمین قدرت پردازشی برای ایجاد بلوک‌های جدید در زنجیرهٔ بلوک، سکه‌هایشان را گروگذاری می‌کنند.

طرز کار روش اثباتِ کار ساده است، زیرا در این روش نیازی به مجازات ماینرهای متقلبی که بلاک‌های نامعتبر می‌سازند، یا زنجیرهٔ نادرستی را تأیید می‌کنند، نیست. جریمهٔ آن‌ها از بین رفتن هزینهٔ برقی است که برای تولید بلاک‌هایی صرف شده که از نظر نودهای حاضر در شبکه معتبر نیستند و به انتهای زنجیرهٔ بلوک معتبرِ شبکه اضافه نخواهند شد. این کار خودزنی است و به‌ندرت رخ می‌دهد. در روش اثباتِ کار یک ارتباط

1 Stake
2 Coins

ملموس بین زنجیرهٔ بلوک و منابع دنیای واقعی وجود دارد.

روش اثبات سهم پیچیده‌تر از اثباتِ کار است. در این روش هیچ ارتباط ملموسی میان زنجیرهٔ بلوکِ دیجیتال با منابع دنیای واقعی وجود ندارد و سیستم باید راهی برای مجازات گروگذارانِ متقلبی که به زنجیرهٔ «اشتباه» رأی می‌دهند پیدا کند.

بعلاوه، گردانندگان سیستم باید از طریقی مطمئن شوند که گروگذارانِ به همهٔ زنجیره‌های ممکن رأی نمی‌دهند. (کاری که در روش اثباتِ کار به دلیل نیاز به منابع جداگانه در دنیای واقعی، امکان‌پذیر نیست). بنابراین، اثبات سهم روش بسیار پیچیده‌تری است که سکه‌های گروگذاشته شده در صورت تقلب به‌عنوان جریمه درنظر گرفته می‌شوند، و برای جلوگیری از رأی‌دادن به‌صورت همزمان روی زنجیره‌های مختلف، به راه‌حل‌هایی نیاز دارد.

بن ادگینگتون[1]، برنامه‌نویس اتریوم و کسی که موافق تغییر روش اجماعِ اتریوم به اثبات سهم است، در پادکست کامپَس ماینینگ[2] به شرح دقیق چالش‌های

1 Ben Edgington
2 https://compassmining.io/education/heres-how-ethereum-developers-are-thinking-about-mev-and-

بلندمدتی که اتریوم در مسیر چندین ساله (و به تأخیر افتاده) تغییر از اثبات کار به اثبات سهم با آنها روبه‌رو شده است پرداخت:

«اینکه اجرای این تغییر این اندازه زمان برد و ما در اتریوم بیش از ۵ سال به اثبات کار تکیه کردیم این است که اثبات سهم روش پیچیده‌ای است. اثبات کار اساساً بسیار ساده است، تحلیل آن آسان است، راه‌اندازی و به‌کارگیری آن ساده است، اما در مقابل اثبات سهم اجزای زیادی دارد و پیچیده است. شما می‌توانید یک الگوریتم اثبات کار را با حدود چندصد خط کُد پیاده‌سازی کنید اما، بخش مربوط به اثباتِ سهم در نرم‌افزار کلاینت[1]های ما در حال حاضر به حدود صدها هزار خط کُد هم می‌رسد.

و من فکر می‌کنم مبانی نظری روش اثبات سهم برای بلوغ به زمان نیاز داشته‌اند. راه‌های قابل‌اعتمادکردنِ آن مشخص نیست. ما باید برای مقابله با حمله‌هایی چون حمله‌های با دامنهٔ طولانی[2] و مسائلی که در اثبات کار وجود ندارد ولی اینجا موضوعیت پیدا می‌کنند، راه‌حل‌هایی پیدا

---

eth2

1 Client

2 Long range attacks

می‌کردیم و این کار از ما زمان می‌بُرد. بنابراین به الگوریتم اثباتِ کار که امتحان خود را پس داده تکیه کردیم و این به نفع اتریوم بود.»

سپس میزبان این پادکست در مورد علاقهٔ طرفداران اولیهٔ شبکهٔ بیت‌کوین به روش اثبات سهم، قبل از مشخص شدن روش‌های مختلف حمله به آن اشاره کرد و از بِن پرسید برنامه اتریوم و مدلِ اثباتِ سهم آن برای مقابله با این حمله‌ها چیست. بن پاسخ داد که این ایده از نظر او قابل‌اعتماد است و راه‌حل‌های روش اثباتِ سهم را به شرح زیر توصیف کرد:

«اولین مشکل اصلی که باید حل می‌شد مسأله‌ای به نام «ایجاد ابهام[1]» بود. به این معنی که ایجاد بلاک‌ها اساساً هزینه‌ای ندارد. پس اگر من یک پیشنهاددهندهٔ بلوک باشم، می‌توانم دو یا سه یا صد بلوک رقیب ایجاد، و آنها را به شبکه ارسال کنم و هیچ راهی برای تمایز دادن این بلوک‌ها از یکدیگر وجود ندارد.

موضوعی که می‌تواند به شدت مخرب باشد و زنجیره را مورد حمله قرار دهد و مطمئناً موجب فورک شدن زنجیره خواهد شد. بنابراین ما از

1 Equivocation

طریق یک مکانیسم به نام «مجازات[1]» با آن مقابله می‌کنیم. یعنی اگر یک پیشنهاددهنده بلوک‌های متناقضی را پیشنهاد دهد، اقدامی مجرمانه مرتکب شده و مجازات خواهد شد. شبکه قادر به شناسایی این نوع حمله است، زیرا یک پیشنهاد دهندهٔ دیگر می‌تواند مدعی وجود داشتن دو بلوک شود که توسط یک تأییدکننده در یک زمان پیشنهاد و امضا شده‌اند. بنابراین این مسأله چیزی نیست که بتوان آن را جعل کرد و امضای موجود روی بلوک‌ها تقلب آن‌ها را اثبات می‌کند. در این صورت پیشنهادکنندهٔ بلوک از شبکه اخراج، و بخشی از دارایی خود را به‌عنوان جریمه از دست می‌دهد. این روش برخلاف روش اثباتِ کار به کسی فرصت دوباره نخواهد داد.

اگر حمله‌ی ۵۱ درصدی شما در روش اثباتِ کار شکست بخورد، شما می‌توانید بارها و بارها دوباره با قدرت بیشتری برای حمله به شبکه تلاش کنید اما در اثبات سهم، تنها یک شانس دارید و در صورت شکست مجازات خواهید شد، از شبکه اخراج می‌شوید و داراییِ اتِر شما تا

1 Slashing

مدتی بلوکه خواهد بود. این روش تا حدودی به‌صورت خودترمیم‌شونده عمل می‌کند. این یکی از پیشرفت‌هایی بود که باعث شد افراد اطمینان پیدا کنند و فکر کنند «واقعاً می‌توان راه‌هایی برای حملات مرسوم پیدا کرد.»

یکی دیگر از این نوع حملات «حمله با دامنهٔ طولانی[1]» نام دارد که یک حملهٔ زیرکانه است. این حمله به این شکل اجرا می‌شود که وقتی شما به عنوان یک تأییدکننده از شبکه خارج شدید، می‌توانید بعد از گذشت یک زمان مشخص دوباره به شبکه برگردید. پس من از شبکه خارج می‌شوم و در زمان به عقب می‌روم و (اگر کلیدهای تأییدکنندهٔ کافی در اختیار داشته باشم) می‌توانم هر تعداد بلوک که بخواهم بسازم و تاریخ‌های متفاوتی که با زنجیره در تضاد هستند برای آن‌ها تعیین کنم. و چون از شبکه خارج شده‌ام امکان مجازات کردن من نیز وجود ندارد.

ما این حمله را بخوبی درک می‌کنیم و آن را مورد بررسی قرار داده‌ایم. راه مقابله با آن مفهومی است که ویتالیک بوترین[2] آن را

1 Long-range attack
2 Vitalik Buterin

«شهودی‌گراییِ خفیف[1]» نامگذاری کرده است و بیت‌کوینرها از آن بیزارند.

ببینید، هرکس به‌طور مداوم در شبکه حضور داشته باشد از این حمله مصون است زیرا زنجیره را زیر نظر دارد و می‌داند زنجیرهٔ معتبر کدام است. اما اگر شما قصد راه‌اندازی یک نود اتریوم از بلوک اول را داشته باشید، اینجا این خطر وجود دارد که یک زنجیرهٔ نامعتبر را به‌عنوان زنجیرهٔ اصلی دنبال کرده باشید. در این صورت به نقطهٔ راهنما[2] نیاز پیدا خواهید کرد که تضمین می‌کند از زنجیرهٔ معتبر و درستی پیروی می‌کنید. این نقطهٔ راهنما باید از کسی دریافت شود که یا در طول زمان حیات زنجیره همواره آنلاین بوده، یا کسی باشد که دانش او نسبت به زنجیرهٔ درست تضمین‌شده باشد. مفهوم شهودی‌گراییِ خفیف در تعیین زنجیرهٔ اصلی در مدل اثباتِ سهم[3]، در مقابل روش اثباتِ کار قرار می‌گیرد که در آن تعیین زنجیرهٔ موردِ قبول

---

1 Weak Subjectivity
2 Checkpoint
3 https://academy.binance.com/en/glossary/weak-subjectivity

نودهای شبکه یک امر «عینی[۴]» است، نه شهودی.

قوانینی برای تعیین تعداد دفعات ساخته‌شدنِ، و همچنین اعتمادپذیر کردنِ این نقاطِ راهنماَ تدوین شده است، و در حالِ پیاده‌سازی سازوکاری «تا حدودی بی‌نیاز از اعتماد[۱]» برای مدیریت آن‌ها هستیم. من متوجهم که این با ایدئولوژی بیت‌کوین که معتقد است هرکس باید بتواند زنجیرهٔ بلوک را از ابتدا بدون اعتماد به هیچ شخص، یا نهادی شخصاً بازسازی کند کاملاً در تضاد است. اما روش کار ما این نیست. انجام این کار در مدل اثباتِ سهم بسیار دشوار است و این بهایی است که ما مجبور به پرداخت آن شده‌ایم. اما اعتقاد داریم این روش کاملاً قابل اجرا است و در عمل مورد هیچ‌گونه حمله‌ای قرار نخواهد گرفت.»

من معتقدم مشکل اصلی روش اثباتِ سهم فارغ از این همه پیچیدگی، نیاز به اعتماد، و امکان وقوع حمله‌های متنوع، این است که مستعد متمرکزشدن است.

---

4 Objective

1 Somehow Trust-less

در یک سیستم اثبات سهم قدرت رأی‌دهی رابطه مستقیم با تعداد کوین‌هایی دارد که گروگذاری شده و سکه‌های جدید نصیب کسانی می‌شود که سکه‌های خود را گروگذاری کرده‌اند. از آنجا که گروگذاریِ سکه‌ها نیازی به صرف منابع در دنیای واقعی ندارد، گروگذاران قادر خواهند بود به مرور نفوذ خود در شبکه را صرفاً با گروگذاری و به‌دست آوردن پاداشی که از شبکه دریافت می‌کنند، افزایش دهند. به عبارت دیگر تسلط روی شبکه، خود منجر به افزایش کنترل روی شبکه می‌شود.

یک سیستم سیاسیِ فرضی را در نظر بگیرید که شهروندانِ آن در ازای پرداخت هر ۱۰۰ هزارتومان یک حق رأی به‌دست می‌آورند و با هر بار رأی‌دادن ۱ هزارتومان از دولت دریافت می‌کنند. آقای تهرانی، معلم علوم مدرسه راهنمایی با پس‌انداز ۲۰۰ میلیون تومانی خود ۲ هزار حق‌رأی به‌دست می‌آورد و ۲ میلیون تومان بابت رای‌دادن دریافت می‌کند. از طرف دیگر آقای شیرازی از خواص حکومتی، قادر است با دارایی ۸۰۰ میلیارد تومانی خود ۸ میلیون حق‌رای به‌دست آورد و ۸ میلیارد تومان بابت رأی‌دادن از دولت دریافت کند. قدرت رأی او ۸,۰۰۰ برابر آقای تهرانی است و پول

بیشتری هم از دولت دریافت، و به ثروت قبلی خود اضافه می‌کند.

چنین سیستمی مطلوب بسیاری از افراد نیست. این سیستم در نهایت منجر به انحصار[1] خواص خواهد شد. آن‌ها قادر خواهند بود زمام امور را با کنترل آراء به دست بگیرند. تلاش برای رسیدن به اهداف یک زنجیرهٔ غیرمتمرکز برای شبکه‌ای تا بدین حد متمرکز، تلاشی بیهوده خواهد بود.

مدل اثباتِ سهم اتفاقاً در دارایی‌های شخصی، مانند شرکت‌هاَ خیلی خوب عمل می‌کند. هر سهم در انتخاب برنامه‌های آینده و تعیین کرسی هیئت‌مدیرهٔ یک شرکت، یک رأی دارد. زیرا این سهامداران هستند که قادرند به نسبت سهمی که در اختیار دارند، برای آینده آن تصمیم‌گیری کنند. پیوستن به سیستم اثباتِ سهام شرکت‌ها امری داوطلبانه است و درصورتی‌که کارمندان، مشتریان، و سهام‌داران از قوانین این شرکت رضایت نداشته باشند، می‌توانند شرکت دیگری را برای کار یا سرمایه‌گذاری انتخاب کنند. این مسأله در موضوع انتخابات ملی و پول قانونی صدق نمی‌کند.

---

1 Oligapoly

بنابراین، از نظر من مدل اثباتِ سهم می‌تواند در رمزارزهایی که شبیه به یک شَرکت هستند به‌صورت آزمایشی به‌کارگرفته شود. در واقع، اثبات سهم می‌تواند هزینهٔ حمله به پروتکل را افزایش دهد زیرا حمله‌کنندگان برای اجرای حمله نیاز به دارایی زیادی دارند. (مگر اینکه توانسته باشند با سوءاستفاده از یک حفره امنیتی ناشی از پیچیده‌بودنِ این روش، کوین‌های زیادی دزدیده باشند.).

به عنوان مثال پروژه‌ها یا پلتفرم‌های تأمین مالی غیرمتمرکز[1] مشخصی وجود دارند که می‌توانند مانند یک شرکت عمل کنند و اگر همه چیز خوب پیش رود برای بهینه‌تر شدن و همچنین مقاوم‌تر شدن در برابر حمله‌ها، از مدل اثباتِ سهم استفاده کنند.

آن‌ها همواره در خطر متمرکزشدن قرار خواهند داشت، اما اگر استفاده از خدمات آن‌ها داوطلبانه، و در رقابت با دیگر شرکت‌هایی باشد که خدمات‌شان را بر پایهٔ مدل اثباتِ سهام ارائه می‌کنند، مشکلی پیش نخواهد آمد. اگر خدمات آن‌ها خوب نباشد، کاربران از خدمات پروژه‌های دیگر استفاده می‌کنند. در مجموع با توجه به ماهیت شرکت‌ها، نقدی بر متمرکزبودنِ آن‌ها مطرح نمی‌شود.

1 DeFi

اما، به‌کارگیری از روش اثباتِ سهام برای یک دارایی پولیِ غیرمتمرکز و مقاوم در برابر سانسورِ جهانی مناسب نیست. در مقایسه با اثباتِ کار، اثباتِ سهام بیشتر شبیه به سهام است تا پول.

آدام بک قبلاً این موضوع را به اختصار شرح[1] داده است:

«شما این مسألهٔ [اهمیت هزینه‌بَر بودنِ تولید پول] را در طلا و دیگر کالاهایی که به‌عنوان پول مورد استفاده قرار گرفته‌اند نیز مشاهده می‌کنید. من فکر می‌کنم پولی که خلق آن هزینه نداشته باشد در نهایت ماهیت سیاسی پیدا خواهد کرد. این بدان معناست که طبق پدیده‌ای که به اثر کانتیلان[2] معروف است نزدیکی به نهاد خلق پول امتیازهای ویژه‌ای برای افراد به‌وجود می‌آورد.»

رمز ماندگاری بیت‌کوین استفاده نکردن از مدل اثباتِ سهم است

قدرت در یک سیستم اثباتِ کار مثل شبکهٔ بیت‌کوین که امکان اجرای یک نود با هزینهٔ پایین و برای همه

1 https://www.thebword.org/c/track-4-securing-the-bitcoin-network
2 Cantillon Effect

فراهم است، بین ماینرها، توسعه‌دهندگان، و نودهای شخصی تقسیم می‌شود.

در روش اثباتِ کار هرکس می‌تواند با فراهم‌آوردن سرمایهٔ کافی و تهیهٔ برق ارزان به استخراج مشغول شود. ماینرهای تازه‌وارد در مدل اثباتِ کار برخلاف روش اثباتِ سهم که قدیمی بودنِ ماینرها در آن یک امتیاز محسوب می‌شود و با گذشتِ زمان افزایش می‌یابد، نسبت به قدیمی‌ترها از مزیت‌های پیشرفت فن‌آوری برخوردار می‌شوند. آن‌ها قادرند به لطف قانون مور[1] دستگاه‌های بهینه‌تری که توان پردازشی بالاتری نسبت به مصرف برق‌شان ارائه می‌کنند، خریداری کنند.

صنعت استخراج، چه قدیمی‌ترها و چه تازه‌واردان مدام در حال سرمایه‌گذاری و به‌روزرسانی روش‌های خود هستند تا بتوانند از منابع انرژی ارزان و سرگردان استفاده کنند. امری که کیفیت مدیریت و استفاده از تجربه در آن بسیار اهمیت دارد و مزیت مقیاس[2] – برخلاف مدل اثباتِ سهام – فقط بخشی از ماجرا است.

بعلاوه، طراحان شبکهٔ بیت‌کوین تمام تلاش خود را کرده‌اند تا امکان اجرای یک نود در شبکهٔ بیت‌کوین – برخلاف تقریباً همهٔ ارزهای دیجیتالِ دیگر – برای همه

1 Moore’s Law
2 Economies of scale

فراهم باشد. این به کاربران این اجازه را می‌دهد که کل زنجیرهٔ بلوک را مورد بازبینی و بررسی قرار دهند و بلوک‌هایی که با قوانین شبکه مطابقت ندارند را رد کنند. در مدل اثباتِ کار قدرت واقعی بر خلاف روش اثباتِ سهم در دستِ کاربران است، نه ماینرها. اگر ماینرها با یکدیگر تبانی و بلاک‌های نامعتبری تولید کنند، شبکهٔ نودهای کاربران این بلاک‌ها را مورد پذیرش قرار نمی‌دهند و آن‌ها را رد می‌کنند.

شبکهٔ بیت‌کوین از نودها، ماینرها، و توسعه‌دهندگان تشکیل شده است. نودهای کاربران در این شبکه نقش تعیین‌کنندهٔ نهایی را دارند اما برای دسته‌بندی تراکنش‌ها و تولید بلوک‌ها به ماینرها، و برای بهینه‌سازی کد نرم‌افزار به توسعه‌دهندگان وابسته هستند. شبکهٔ بیت‌کوین در برابر تغییر، خصوصا تغییرات بنیادی در طراحی سیستم، مقاومت زیادی از خود نشان می‌دهد. پیش‌نیاز اعمال تغییر در پروتکل بیت‌کوین توافق همه‌جانبه میان همهٔ کاربران است. این تغییرات به‌صورت سافت فورک[1] اجرا می‌شوند و خصوصیت پساسازگاری[2] دارند. استفاده‌کردن یا نکردن از قوانین جدیدی که به روش سافت فورک به شبکه اضافه

1 Soft fork
2 Backwards compatible

می‌شوند برای کاربران اختیاری است اما در هر دو صورت با قوانین اجماع شبکه سازگار باقی خواهند ماند.

بسیاری از رمزارزهای دیگری که بعد از بیت‌کوین به‌وجود آمدند به‌صورتی طراحی شده‌اند که اجرای یک نود در شبکهٔ آن‌ها به قدرت پردازش، پهنای باند، و فضای ذخیره‌سازی بسیار زیادی نیاز دارد تا جایی که این کار تنها برای نهادهایی در مقیاس صنعتی امکان‌پذیر است. این موضوع سیستم را به سمت تمرکز سوق می‌دهد، چون فقط تعداد معدودی از نهادها یا شرکت‌ها قادر به تأمین منابع لازم برای راه‌اندازی یک فول نود، ممیزی زنجیرهٔ بلوک، و اطمینان از رعایت‌شدن قوانین اجماع در شبکه خواهند بود.

روش اثباتِ کار و همچنین بلوک‌های کوچک شبکهٔ بیت‌کوین قدرت بسیار زیادی به کاربران این شبکه می‌دهد. هرکس می‌تواند با راه‌انداختن یک نود کل زنجیرهٔ بلوک را شخصاً مورد بررسی قرار دهد، تراکنش‌های شخصی خود را مورد بازبینی قرار دهد، و به تقویت اثر شبکه‌ای که حول اعتبارسنجی و حفاظت از قوانین اجماع شکل گرفته کمک کند.

من به دوستانی که به بیت‌کوین و به‌طور کلی مقولهٔ رمزارزها علاقه‌مند هستند پیشنهاد می‌کنم کتاب The

Blocksize War[1] که در سال ۲۰۲۱ منتشر شده است را بخوانند. (این کتاب با عنوان مناقشهٔ سایز بلوک[2] به فارسی ترجمه شده است. - م) این کتاب به شرح تاریخچهٔ شبکهٔ بیت‌کوین در دوره‌ای که جناح‌های مختلف برای شکل‌دهی به اصول پایه‌ای شبکهٔ بیت‌کوین با یکدیگر مبارزه می‌کردند می‌پردازد تا مشخص کند قدرت تعیین‌کننده در شبکهٔ بیت‌کوین دست چه گروهی است؟

توسعه‌دهندگان، یا شرکت‌های قانونی پشت صنعت استخراج بیت‌کوین و صرافی‌ها، یا کاربران/نودهای شبکه. این رویداد یک آزمایش واقعی برای سنجیدن سطح غیرمتمرکزبودنِ بیت‌کوین بود. به عبارت دیگر بحرانی برای قانون اساسی شبکهٔ بیت‌کوین بود، آزمونی که در نهایت با موفقیت پشت سر گذاشته شد.

از زمان پیدایش بیت‌کوین شکاف فزاینده‌ای میان گروهی که مایل به افزایش اندازهٔ بلوک بودند و گروه دیگری که می‌خواستند اندازهٔ آن را کوچک نگه دارند، وجود داشت. بدون درنظر گرفتن راه‌حل‌های به‌کارگرفته‌شده روی لایهٔ دوم[3] و زنجیره‌های جانبی[4]

1 https://www.amazon.com/dp/B08YQMC2WM
2 https://bitcoind.me/blobs/books/monagheshe-size-block-bitmex-bitcoind_me.pdf
3 Second Layer
4 Sidechain

مانند لایتنینگ[1] و لیکوئید[2] که در آن زمان وجود نداشتند می‌توان گفت افزایش سایز بلوک شبکه را قادر به پردازش تعداد بیشتری تراکنش در واحد زمان می‌کند. اگرچه، افزایش سایز بلوک موجب افزایش پهنای باند و فضای ذخیره‌سازی موردنیاز برای راه‌اندازی یک نود نیز می‌شود. در این صورت افراد عادی قادر به راه‌اندازی نود شخصی خود روی لپ‌تاپ یا یک کامپیوتر تک بُرد[3] مثل رزبری پای[4] نخواهند بود.

حتی خود ساتوشی ناکاموتو قبل از ترک پروژه[5] و در ابتدای این مناقشه یک نقش دوگانه بازی کرد. او شخصاً محدودیت سایز بلوک را پس از راه‌اندازی شبکه اعمال کرد، اما در مورد چگونگی افزایش بالقوهٔ آن به مرور و با بهبود پهنای باند اینترنت در اثر پیشرفت تکنولوژی نیز صحبت می‌کرد.

اگر کاربران قادر به استخراج نباشند و امکان راه‌اندازی نودهای شخصی نیز برای آن‌ها فراهم نباشد مجبورند به خدمات‌دهندگانی که امکان راه‌اندازی نودهای بیت‌کوین در مقیاس بزرگ را دارند، اعتماد کنند. در این صورت کارکردِ اعمال قوانین اجماع از جانب نودهای کاربران

---

1 Lightning
2 Liquid
3 Single-Board Computer
4 Raspberry Pi
5 مقاله آخرین روزهای ساتوشی

به مرور تضعیف می‌شود و بیت‌کوین دیگر یک سیستم غیرمتمرکز و بی‌نیاز از اعتماد نخواهد بود.

مناقشهٔ سایز بلوک که بذر اختلاف آن از ابتدای شروع به‌کار شبکهٔ بیت‌کوین کاشته شده بود، طی سال‌های ۲۰۱۵ تا ۲۰۱۷ و پس از غیبت طولانی ساتوشی ناکاموتو به یک جنگ تمام‌عیار تبدیل شد.

در مقطعی از سال ۲۰۱۷، بیش از ۸۰ درصد قدرت پردازش کُل ماینرها، بزرگترین سازندهٔ تجهیزات استخراج بیت‌کوین، توسعه‌دهندگان اصلیِ و پیشگامِ پیشینِ بیت‌کوین، و تعداد زیادی از متولیان[1] و صرافی‌های اصلی شامل کوین‌بیس و گری‌اسکیل طرفدار افزایش سایز بلوک از طریق اجرای یک به‌روزرسانی به نام SegWit2x بودند (روشی که با به‌روزرسانی عادی SegWit متفاوت بود). این یک حمایت چشم‌گیر از جانب بازیگران سازمانی این صنعت بود. گروهی که در توافق‌نامهٔ نیویورک[2] از خود به عنوان «وزنهٔ سنگینِ اکوسیستم بیت‌کوین» یاد کرده بودند.

و با وجود این، شکست خوردند.

---

1 Custodians
2 New York Agreement

گروهی از توسعه‌دهندگان و مهم‌تر از آن اکثریت نودهای شخصی با این طرح موافق نبودند، و لذا اجرای این تصمیم در کنار دلایل دیگر، منتفی شد.

در صفحه SegWit2x در ویکی[1] بیت‌کوین می‌خوانیم:

SegWit2x، (که مخفف آن به‌صورت B2X یا S2X نوشته می‌شود و در اصل SegWit2Mb نام داشت) طرحی است که در توافق‌نامهٔ نیویورک برنامه‌ریزی شد و حامیان آن قصد داشتند محدودیت سایز بلوک روی شبکهٔ بیت‌کوین را با اجرای یک هارد فورک[2] دو برابر کنند اما اجرای آن در نهایت به شکست انجامید. این هارد فورک به‌عنوان تلاش مدیران عامل و صاحبان مشاغل بزرگ بیت‌کوین برای ایجاد تغییراتی در قوانین پروتکل و چرخهٔ توسعهٔ آن با انگیزه‌های ناشناخته، همواره محکوم شده است.

این طرح با وجودی که بیش از ۸۰ درصد از توان پردازشی شبکهٔ بیت‌کوین برای اجرای آن اعلام آمادگی کرده بودند، در به‌دست آوردن رأی موافق

---

1 https://en.bitcoin.it/wiki/SegWit2x
2 Hard fork

کاربران و توسعه‌دهندگان پروتکل شبکه موفق نبود و در نهایت شکست خورد.

اگر روش اجماع در شبکهٔ بیت‌کوین بر اساس مدل اثباتِ سهم بود و کاربرانی که نودهای شخصی خود را اجرا می‌کنند نقش تعیین‌کننده‌ای نداشتند، اگر نرم‌افزار نودها و قوانین پروتکل به‌صورتی طراحی نشده بودند که امکان راه‌اندازی نودهای شخصی برای همه کاربران فراهم باشد، ممکن بود شرکت‌های بزرگِ امضاکنندهٔ توافق نیویورک قادر به تغییر قوانین اساسی شبکهٔ بیت‌کوین شوند. این امر می‌توانست راه‌اندازی یک نود شخصی برای افراد عادی را دشوار و موجب متمرکزتر شدن شبکهٔ بیت‌کوین شود. البته افزایش دوبرابری سایز بلوک آنقدر هم اثرگذار نبود اما می‌توانست زمینه‌ساز افزایش‌های بسیار بزرگترِ بعدی باشد.

اگر روش اجماع در شبکهٔ بیت‌کوین بر اساس مدل اثباتِ سهم بود و حق‌رأی در مورد تعیین عمل‌کرد شبکه براساس تعداد سکه‌های دراختیار تعیین می‌شد، صرافی‌ها و متولیان بزرگ می‌توانستند از میلیون‌ها سکهٔ مشتریانی که دارایی خود را نزد آن‌ها به امانت گذاشته‌اند به نفع خود استفاده کنند. چیزی شبیه به شرایطی که امروزه در

شرکت‌های ونگارد[1] و بلک‌راک[2] مشاهده می‌کنیم. این شرکت‌ها ده‌ها تریلیون دلار از دارایی سهام و حق رأی مشتریان خود را در اختیار دارند.

برخی از اعضای کمپ طرفدار بلاک‌های بزرگ در طول این مناقشه زنجیرهٔ بلوک بیت‌کوین را فورک و نسخه‌هایی با سایز بلوک بزرگ‌تر از بیت‌کوین ایجاد کردند که از آن‌ها می‌توان به بیت‌کوین اکس‌تی[3]، بیت‌کوین کلاسیک[4]، بیت‌کوین آنلیمیتد[5]، بیت‌کوین کَش[6]، و بیت‌کوین اس‌وی[7] اشاره کرد. هیچیک از این فورک‌ها مورد پذیرش بازار قرار نگرفتند و همهٔ آن‌ها از نظر ارزش بازار[8] و میزان هَش[9] در مقایسه با بیت‌کوین به میزان قابل‌توجهی سقوط کرده‌اند. برخی از آن‌ها کاملاً از بین رفته‌اند و بقیه در معرض حمله‌های ۵۱ درصدی جدی قرار گرفته‌اند.

در حال حاضر تنها راه شناخته‌شده برای غیرمتمرکز نگاه‌داشتن یک زنجیرهٔ بلوک در لایهٔ اول و رسیدن به بالاترین سطح امنیت، استفاده از روش اثباتِ کار و

---

1 Vanguard
2 BlackRock
3 Bitcoin XT
4 Bitcoin Classic
5 Bitcoin Unlimited
6 Bitcoin Cash
7 Bitcoin SV
8 Market capitalization
9 Hash rate

فراهم‌آوردن امکان راه‌اندازی نود برای همهٔ کاربران است.

چالش‌های فنی روش اثباتِ سهم

اتریوم نسبت به بیت‌کوین با مشکلات مقیاس‌پذیری حادتری مواجه بوده و این مسأله فضا را برای ظهور رقبایی که امکان اجرای قراردادهای هوشمند بر روی زنجیرهٔ بلوک خود فراهم می‌کنند، فراهم کرده است. رقیبانی که نسبت به اتریوم متمرکزترند، در نتیجه از جهاتی از راندمان بالاتری برخوردارند.

نمونه‌های متعددی از بروز مشکلات فنی در سیستم‌های رقبای جدیدی که از روش اثبات سهم استفاده می‌کنند، وجود دارد.

وقوع یک اشکال خبرساز در زنجیرهٔ بلوک سولانا این شبکه را به مدت ۱۷ ساعت از دسترس خارج کرد[۱]. رفع این اشکال مستلزم هماهنگی و راه‌اندازی مجدد[۲] نودهای تأییدکنندگان[۳] شبکه به‌صورت دستی بود.

---

1 https://decrypt.co/81375/solana-blames-denial-of-service-attack-for-last-weeks-downtime

2 Restart

3 Validators

سولانا یک زنجیرهٔ بلوک با قابلیت اجرای قرارداد هوشمند، و مورد حمایت سرمایه‌گذاران ریسک‌پذیر[۴] است. این پروژه سعی دارد مقیاس‌پذیری خود را با اجرای طرحی ترکیبی از روش‌های اثبات سهم و اثبات تاریخ[۵] در مقایسه با اتریوم به مقدار قابل‌توجهی افزایش دهد.

بازدهی بالای شبکهٔ سولانا در مقایسه با اتریوم مستلزم پرداخت بها و پذیرش عواقبی است که در ادامه به آن‌ها اشاره می‌کنیم.

اول از همه، برای اجرای نرم‌افزارِ تأییدکنندهٔ زنجیرهٔ بلوک سولانا به یک کامپیوتر با پردازندهٔ ۱۲ هسته‌ای، ۱۲۸ گیگابایت رم، و سرعت آپلود ۳۰۰ مگابیت بر ثانیه دارید. البته توصیه می‌شود سرعت‌تان ۱ گیگابیت بر ثانیه باشد. این تنظیمات مخصوصاً بخش سرعت آپلود، اساساً یعنی شما باید برای راه‌اندازی یک تأییدکننده‌ی سولانا اپراتور یک مرکز داده[۳] باشید. برخلاف شبکهٔ بیت‌کوین شما نمی‌توانید برای اعتبارسنجی کُل زنجیرهٔ بلوکِ سولانا از یک لپ‌تاپ خانگی استفاده کنید. به عبارتِ دیگر، کاربران عادی امکان بازبینی زنجیرهٔ بلوک سولانا را ندارند.

---

4 VC-backed smart contract blockchain
5 Proof of History
3 Data-center

دوم اینکه حتی تأییدکنندگانی که فعالیت آن‌ها در سطح مراکز داده است نیز باید برای به‌دست آوردن کُل تاریخچهٔ زنجیرهٔ بلوک به نودهای بایگانی‌کننده[1] تکیه کنند. زیرا حجم اطلاعات ذخیره‌شده در گذر زمان بسیار زیاد می‌شود.

بیت‌کوین این مشکل را ندارد و می‌توان اطلاعات مربوط به کُل زنجیرهٔ بلوک آن را پس از گذشت ۱۳ سال روی هارد دیسکِ یک کامپیوتر خانگی ذخیره کرد. فضای موردنیاز برای ذخیرهٔ بایگانی زنجیرهٔ بلوک سولانا پس از گذشت یک یا دو دهه به مقادیر حیرت‌آوری خواهد رسید، درحالی‌که ذخیرهٔ زنجیرهٔ بلوک بیت‌کوین تا ۱۳ سال آینده نیز بر روی هارد دیسکی که امروزه در دسترس همگان است امکان‌پذیر خواهد بود.

سوماً، مکانیزم اعمال مجازات در سولانا خودکار نیست. به عبارت دیگر، سولانا زنجیرهٔ بلوکی است که برای رسیدن به اجماع در زمان وقوع حملات قابل‌توجه، به تصمیمات انسانی نیاز دارد.

اتریوم نیز گهگاه دچار فورک‌شدنِ زنجیره و توقف شبکه می‌شود. این پروژه احتمالاً پس از تغییر مدل

1 Archivers

اجماع به مدل اثباتِ با مشکلات شدیدتری مشابه با آنچه سولانا با آن مواجه است روبرو خواهد شد. برعکس، شبکهٔ بیت‌کوین پس از رفع مشکلی که در بهار سال ۲۰۱۳ که ارزش بازار آن کمتر از ۱ میلیارد دلار بود و می‌توان گفت در مرحلهٔ آزمایشی قرار داشته پدید آمد، به معنای واقعی کلمه همواره در حالِ کار و عملیاتی بوده است.

در اکتبر سال ۲۰۲۱ مقاله‌ای با عنوان «سه حمله به اثباتِ سهمِ اتریوم[1]» از دانشگاه استنفورد و با حمایت مالی بنیاد اتریوم[2] منتشر شد که به بررسی راه‌های حمله به اتریوم پس از تغییر روش اجماع به اثباتِ سهم پرداخته است. بهتر است متخصصان و کارشناسان علوم کامپیوتر در مورد روش‌های حمله به روش اثباتِ سهم به بحث و تبادل‌نظر بپردازند و اینجا وارد این مقوله نمی‌شوم. اما پیشنهاد می‌کنم این مقاله را مطالعه کنید.

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[3]» به راه‌هایی برای حمله به سیستم اثبات سهم اتریوم اشاره می‌کند. من به آن نمی‌پردازم و بهتر است متخصصان علوم کامپیوتر مشخص کنند کدام

1 Three Attacks on Proof-of-Stake Ethereum
2 Ethereum Foundation
3 https://arxiv.org/abs/2110.10086

راه‌های حمله معتبر و کدام‌ها در صورت شناسایی، با یک به‌روزرسانی قابل پیشگیری هستند. پیشنهاد می‌کنم این مقاله را مطالعه نمایید.

هوگو نگوین[1] مجموعه مقالاتی دارد که در آن‌ها به نقد روش اثباتِ سهم از منظر اصول اولیه[2] می‌پردازد. این مقالات اینجا[3]، اینجا[4]، و اینجا[5] در دسترس علاقه‌مندان هستند. مضمون کلی انتقاد او این است که سیستم اثباتِ سهم ذاتاً یک سیستم بسته[6] است و همواره برای کارکردن به درجاتی از اعتماد نیاز دارد و بدون مداخلهٔ انسانی قادر به مدیریت فورک‌های ناخواسته[7] در زنجیرهٔ بلوک خود نیست و توانایی محدودی برای تأمین امنیت تاریخچهٔ زنجیرهٔ بلوک دارد. زیرا، هزینهٔ تقلب در این سیستم به‌اندازهٔ کافی بالا نیست (این مفهوم توسط نیک زابو[8] به جعل‌ناپذیری از راه بالابردنِ هزینه تقلب[9] نام‌گذاری شده است.) گزیده‌ای از یکی از مقالات این‌گونه شرح می‌دهد:

---

1 Hugo Nguyen
2 First principles
3 https://hugonguyen.medium.com/work-is-timeless-stake-is-not-554c4450ce18
4 https://hugonguyen.medium.com/proof-of-stake-private-keys-attacks-and-unforgeable-costliness-the-unsung-hero-5caca70b01cb
5 https://hugonguyen.medium.com/proof-of-stake-the-wrong-engineering-mindset-15e641ab65a2
6 Circular
7 Chain split
8 Nick Szabo
9 Unforgeable costliness

”دوماً و بسیار مهم‌تر اینکه، صاحب یک نود (گره) در روش اثباتِ کار می‌تواند پس از دریافت نرم‌افزار اصلی و دریافت تاریخچهٔ زنجیرهٔ بلوک، هر زمان بخواهد از شبکه جدا شود و نود خود را برای مدت زمان دلخواه خاموش نگه دارد. این کار هیچ‌گونه خطر امنیتی برای او در پی نخواهد داشت. شبکه‌ای که از روش اثباتِ کار استفاده می‌کند بعد از پشت‌سرگذاشتن مرحلهٔ تثبیت[1] دیگر نیازی به کسب تکلیف از هیچ موجودیتی ندارد و نود (گره‌ها) هر زمان بخواهند می‌توانند به شبکه وصل شوند یا آن را ترک کنند. تنها استثناء، زمان وقوع هاردفورک‌ها است. این یکی دیگر از دلایلی است که باید تا حد امکان از اجرای هارد فورک‌ها اجتناب شود.

اما شرایط در یک سیستم اثباتِ سهم این‌گونه نیست. اپراتور نود (گره) باید حتی پس از دریافت نرم‌افزار اصلیِ نود برای اطمینان از دنبال‌کردنِ زنجیرهٔ متعارف در شبکه، با یک شخص ثالث همواره در ارتباط باشد و به اطلاعات دریافت‌شده اعتماد کند. ترسِ از دست

1 Bootstrapping stage

دادن ارتباط با شبکهٔ اصلی، و گمراه‌شدن و دنبال‌کردنِ زنجیرهٔ اشتباه، تا ابد، حتی پس از از بین‌رفتنِ اینَ اشخاصِ ثالثِ معتمد، ماندگار است. این موضوع امنیت شَبکه رَا تا حد بسیار زیادی پایین می‌آورد.

بسیاری از افرادْ بدون تحقیق و مطالعه، اثباتِ سهم را فناوری برتری نسبت به اثباتِ کار معرفی می‌کنند و بدون داشتن درکی صحیح از مسائل فنی مطرح شده صرفاً به تعریف و تمجید از سیستم‌هایی که ظرفیت پردازش تراکنش آن‌ها بالا است می‌پردازند. بسیاری از مسائلی که از نظر آن‌ها از اشکالات سیستم اثباتِ کار است، درواقع ویژگی‌هایی هستند که موجب ایمن‌ترشدن هرچه بیشتر آن می‌شوند. از این موارد می‌توان به هزینهٔ تأمین برق در سیستم اثباتِ کار اشاره کرد.

هواداران پروژه‌های اثباتِ سهام و سیستم‌های متمرکز با توان عملیاتی بالا وقتی متوجه می‌شوند بسیاری از مردم امنیت توکن‌های این پروژه‌ها را در حد و اندازه‌ای نمی‌بینند که مانند بیت‌کوین به‌عنوان «پول جهانی[1]» و «وثیقهٔ ناب[2]» در نظر گرفته شود، تعجب می‌کنند. این پروژه‌ها، پلتفرم‌های متمرکزی برای آزمایش

1 Global money
2 Pristine collateral

قراردادهای هوشمند هستند که می‌توانند در حالت ایده‌آل مورد توجه سرمایه‌گذارانی قرار گیرند که کاملاً به خطرات آن‌ها آگاه هستند.

این مقاله با عنوان انگلیسی Proof-of-Stake and Stablecoins: A Blockchain Centralization Dilemma نوشتهٔ Lyn Alden در نوامبر ۲۰۲۱ در سایت شخصی وی منتشر شده است. ویراست اول ترجمه و بازبینی این مقاله توسط «مجید گتمیری» و «ضیاء صدر» در اسفند سال ۱۴۰۰ خورشیدی صورت پذیرفته و از کانال تلگرام «ترجمهٔ مقالات بیت‌کوین» قابل دریافت است.

ویراست دوم بخش مرتبط با مقایسهٔ روش‌های اجماع اثباتِ کار و سهم توسط سایت منابع فارسی بیت‌کوین در بهار سال ۱۴۰۲ به انجام رسید و منتشر شد.

این ترجمه با مجوز «مالکیت عمومی» منتشر می‌شود و نشر آن به هر شکل آزاد است.

منابع فارسی بیت‌کوین