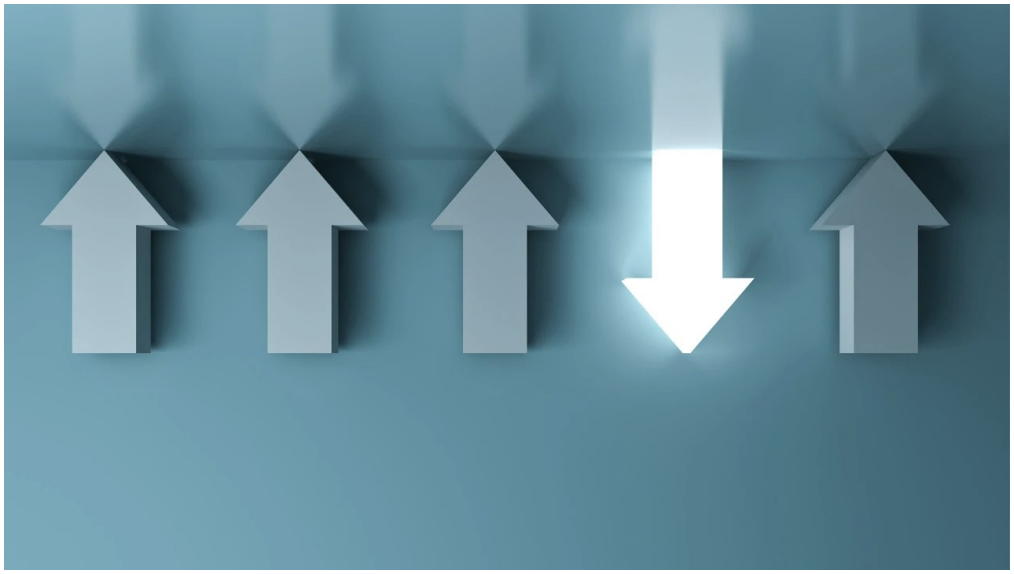

مناقشه سایز بلاک

۲۰۱۷ - ۲۰۱۵

“There was truth and there was untruth, and if you clung to the truth even against the whole world, you were not mad.”

— George Orwell

تقدیم به کاوه مشتاق

سخنی با خوانندگان

اولین سؤالی که ممکن است بعد از آشنایی با پروتکل بیت‌کوین به ذهن یک فرد کنجکاو برسد این است:

> بیت‌کوین مجموعه‌ای از قوانین شفاف است و در قالب یک پروتکل و نرم‌افزار اپن سورس[1] ارائه می‌شود، اما تغییر یا ارتقاء این قوانین چگونه انجام می‌پذیرد؟ استخرهای ماین بیت‌کوین با توان هش بالا بلاک‌های زنجیره بیت‌کوین را می‌سازند، توسعه‌دهندگان بیت‌کوین پیشنهادهای فنی ارائه می‌کنند و مسئول نگهداری و ارتقاء نرم‌افزار بیت‌کوین هستند، و در نهایت کاربران بیت‌کوین با اجرای فول‌نود از قوانین شبکه حفاظت می‌کنند. هرکدام از این بازیگران تا کجا برای تغییر قوانین شبکه بیت‌کوین آزادی عمل و اختیار دارند؟

یک پاسخ کلی به این سؤال این است که سه‌گانه استخرهای ماین، توسعه‌دهندگان، و کاربران بیت‌کوین بر اساس قوانین طراحی شده بر پایه نظریه بازی[2] و در یک بستر غیرمتمرکز به توافق می‌رسند و تغییرات را بر روی شبکه اعمال می‌کنند. اما اگر نظرات و

1 Open source
2 Game theory

اهداف این بازیگران به‌قدری متفاوت باشد که رسیدن به توافق غیرممکن شود، در نهایت تغییر و ارتقاء قوانین شبکه از چه راهی امکان‌پذیر می‌شود؟

بهترین روش برای بررسی دقیق این موضوع بررسی تاریخ درگیری‌های پیش آمده بین سال‌های ۲۰۱۷ – ۲۰۱۵ برای افزایش سایز بلاک است.

قبلاً مطلبی تحت عنوان «مروری بر مناقشه افزایش سایز بلاک (UASF)» در سایت منابع فارسی بیت‌کوین منتشر شده است که به بررسی تاریخچه مختصر این درگیری‌ها می‌پردازد ولی اخیراً کتابی با عنوان "The Blocksize War" توسط بخش تحقیق و پژوهش شرکت BitMEX منتشر شده است و فصل‌های این کتاب به‌صورت هفته‌ای و رایگان روی وبلاگ این مؤسسه قرار می‌گیرند که اتفاقات در این قائله را به تفصیل بررسی می‌کند. ما در سایت منابع فارسی بیت‌کوین تلاش می‌کنیم فصول این کتاب را به مرور ترجمه و در اختیار علاقه‌مندان به بیت‌کوین قرار دهیم.

اگر برای ترجمه این کتاب مایل به همکاری هستید از طریق ایمیل سایت با ما در ارتباط باشید.

سایت منابع فارسی بیت‌کوین
بهار ۱۴۰۰

فصل ۱

جرقه اول

در روز شنبه ۱۵ آگوست سال ۲۰۱۵ میلادی واقعه‌ای رخ داد که بسیاری از فعالان فضای بیت‌کوین را غافلگیر کرد. دو نفر از برجسته‌ترین و معتبرترین توسعه‌دهندگان بیت‌کوین در آن زمان یعنی «مایک هرن[۱]» و «گوین اندریسن[۲]» یک نسخه جدید از نرم‌افزار بیت‌کوین (که با قوانین شبکه ناسازگار بود) را منتشر، و از آن حمایت کردند. این نسخه از نرم‌افزار، Bitcoin XT نام داشت. افراد زیادی چشم امید به بیت‌کوین دوخته بودند ولی به نظر می‌رسید ظهور این نرم‌افزار جدید سیستم را به نابه‌سامانی و احتمالاً وقوع یک فاجعه سوق دهد. همان‌طور که روزنامه گاردین[۳] روز دوشنبه بعد تیتر زد:

جنگ‌های بیت‌کوین شروع شد[۴]

1 Mike Hearn
2 Gavin Andresen
3 Guardian
4 https://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist

در ظاهر به‌نظر می‌رسید این جنگ، محدود به یک مسأله مشخص و جزئی؛ یعنی حداکثر سایز مجاز بلاک در بلاک‌چین بیت‌کوین باشد. نرم‌افزار Bitcoin XT پیشنهادی برای افزایش فضای موجود در بلاک‌ها ارائه می‌داد. در سال ۲۰۱۵ محدودیت سایز بلاک ۱ مگابایت بود و Bitcoin XT قصد داشت آن را در قدم اول به ۸ مگابایت افزایش دهد و تا سال ۲۰۳۶ که در نهایت سایز بلاک به ۸,۰۰۰ مگابایت می‌رسید، هر دوسال آن را دوبرابر کند. هدف این بود که همگام با افزایش محبوبیت بیت‌کوین، بلاک‌ها هم بزرگ‌تر شوند و از طرف دیگر با توجه به محدودیت ۱ مگابایتی، بلاک‌ها اغلب پر می‌شدند. طرفداران افزایش سایز بلاک معتقد بودند که بیت‌کوین برای تبدیل شدن به یک سیستم پرداخت جهانی ارزان‌قیمت، به ظرفیت بالاتری نیاز دارد.

آن‌ها نگران بودند که این محدودیت، استفاده از شبکه را دشوار و گران می‌کند و رشد سیستم را در درازمدت به مخاطره می‌اندازد. از نظر گوین و مایک یک بحران جدی در پیش بود و ممکن بود کاربران بیت‌کوین را دلسرد کند و برای همین باید اقدام‌هایی برای جلوگیری از وقوع این بحران انجام شود. مخالفان گوین و مایک از انتشار این نرم‌افزار ناسازگار با قوانین فعلی شبکه نگران بودند. از نظر آنان ممکن بود شبکه به دو زنجیره مستقل منشعب، و باعث هرج و مرج و سردرگمی کاربران شود. این جنگ بر سر سایز بلاک می‌توانست اکوسیستم بیت‌کوین را در طول دو سال آینده متلاشی کند و باعث دو دستگی آن شود.

با ادامه پیدا کردن این درگیری مشخص شد که این اختلافات، عمیق‌تر از محدودیت سایز بلاک است و ارتباط مستقیم با ذات و تعریف بیت‌کوین دارد و اساساً به چهار موضوع زیر مرتبط است:

۱. **مقدار فضای موجود در هر بلاک بیت‌کوین** – آیا فضای بلاک در نهایت باید به اندازه‌ای باشد که همیشه یک مقدار ظرفیت خالی در هر بلاک باقی بماند، یا می‌توان به‌طور مداوم از همه ظرفیت بلاک استفاده کرد و شاهد بلاک‌های پر بود.
۲. **قوانین پروتکل بیت‌کوین از چه روشی تغییر کنند** – آیا تغییر قوانین مربوط به بخش اعتبارسنجی بلاک‌های بیت‌کوین باید نسبتاً راحت باشد، یا این قوانین باید محکم و تغییرناپذیر باشند و فقط در شرایط استثنایی و با حمایت گسترده از همه طرف‌های ذینفع تغییر کنند.
۳. **اهمیت نودهای[1] راه‌اندازی شده توسط کاربران عادی** – تأثیر نودهای راه‌اندازی شده توسط کاربران عادی بیت‌کوین بر اعمال قوانین پروتکل بیت‌کوین تا چه اندازه است.
۴. **ترجیحات زمانی[2]** – آیا بیت‌کوین به‌مانند یک شرکت نوپا[3] است و باید اولویت کوتاه‌مدت خود را روی به‌دست آوردن سهم هرچه بیشتر بازار قرار دهد؛ یا یک پروژه بلندمدت است، یک پول جهانی است و در هنگام تصمیم‌گیری در مورد آن باید دهه‌های آینده را هم در نظر گرفت.

در این مرحله بیشتر تمرکز مشخصاً بر روی موضوع محدودیت سایز بلاک بود. تقریباً همگان توافق داشتند که سایز ۱ مگابایتی بلاک بسیار کوچک است. اما هیچگونه اتفاق نظری بر روی تعیین سایز بلاک و نحوه تغییر آن وجود نداشت. همچنین به نظر می‌رسید اکثریت کاربران معتقدند که افزایش سایز بلاک پیشنهاد شده از طرف Bitcoin XT افراطی است و به یک روش متعادل‌تری نیاز داریم.

حرکت اول این جنگ را مایک و گوین انجام دادند که بخشی از اردوگاه ملقب به «طرفداران بلاک‌های بزرگ[4]» در این منازعه بودند. اولین حرکت باید از جانب آن‌ها

1 Bitcoin nodes
2 Time preference
3 Startup
4 Large blocker

انجام می‌شد، چون مخالفان آن‌ها از وضع موجود رضایت داشتند. مایک و گوین این پیشنهاد را چند ماه قبل ارائه کرده بودند، با این حال نرم‌افزار آن‌ها در ماه آگوست سال ۲۰۱۵ منتشر شد و کاربران را به اجرای آن تشویق کردند. بنابراین از نظر ما شروع رسمی منازعات از اینجا است. این بدان معنا نیست که مایک و گوین کارشان را اقدامی خصمانه یا عملی ناشایست تلقی می‌کردند.

Bitcoin XT پیاده‌سازی نرم‌افزاری BIP-101[1] و یکی از ده‌ها پیشنهاد افزایش سایز بلاک بود. این پیشنهاد اولین بار به‌طور رسمی توسط گوین اندریسن و چند ماه زودتر در ۲۲ ژوئن ۲۰۱۵ منتشر شد. یک نرم‌افزار نمی‌تواند به سادگی محدودیت بلاک را افزایش دهد بلکه به یک روش فعال‌سازی، یا سیستمی برای اطمینان از اعمال قوانین بر روی شبکه بیت‌کوین نیاز دارد. روش فعال‌سازی انتخاب شده در این مورد تشکیل شده بود از روش تعیین «روز موعود[2]» و «علامت‌دهی ماینرها[3]». اولین روز تعیین شده برای فعال‌سازی قوانین جدید، روز ۱۱ ژانویه ۲۰۱۶، حدوداً ۵ ماه بعد بود. علاوه بر این، فعال‌سازی نیاز به دریافت علامت از ماینرهای بیت‌کوین داشت. ماینرهای بیت‌کوین می‌بایست در داخل بلاک‌هایی که تولید می‌کردند یک علامت مشخص قرار می‌دادند که نشان می‌داد نرم‌افزارشان را به‌روز کرده‌اند و آماده اعمال قوانین جدید هستند. اگر از ۱۰۰۰ بلاک آخر، ۷۵۰ بلاک حاوی علامت مشخص ارسال شده توسط ماینرها باشد، قوانین جدید فعال می‌شوند و در نهایت و بعد از گذشت یک دوره دوهفته‌ای که به «دوره تنفس[4]» معروف است، قوانین جدید بر روی شبکه اعمال و سرانجام سایز بلاک افزایش می‌یابد. اگر علامت‌دهی ماینرها به آستانه ۷۵ درصد نرسد، فعال‌سازی با شکست مواجه خواهد شد.

نرم‌افزار Bitcoin XT در اردوگاه موسوم به «طرفداران بلاک‌های کوچک[5]» بسیار بحث‌برانگیز بود. دلیل اصلی آن این بود که این ارتقاء، با قوانین موجود در شبکه ناسازگار

1 Bitcoin Improvement Proposal
2 Flag day
3 Miner signaling
4 Grace period
5 Small block

بود. اساساً به این معنی که هرکس که یک نود بیت‌کوین اجرا و قوانین شبکه را تأیید می‌کرد، می‌بایست نرم‌افزار خود را به‌روزرسانی می‌کرد. به اعتقاد افرادی که در اردوگاه بلاک‌های کوچک بودند، اگر همه روی قوانین جدید به توافق نمی‌رسیدند و نرم‌افزار خود را به‌روز نمی‌کردند، بیت‌کوین به دو زنجیره متفاوت منشعب می‌شد. این روش ارتقاء، یک «هارد فورک[5]» نام دارد و افراطی‌ترین روش ممکن برای ارتقاء قوانین در شبکه است. اساساً می‌توان با استفاده از یک هارد فورک، هر تغییر دلخواهی روی قوانین بیت‌کوین اعمال کرد. از افزایش سقف عرضه بیت‌کوین از ۲۱ میلیون، تا مصادره کوین اشخاص. پیش‌فرض بسیاری از بیت‌کوینرها این بود که هیچکس نباید قبل از حصول اطمینان از وجود اتفاق نظر بین همه کاربران بیت‌کوین، اقدام به ارتقاء قوانین شبکه از روش هارد فورک نماید. از نظر آن‌ها، این ویژگی‌ها یعنی عرضه ۲۱ میلیون و غیرقابل مصادره بودن کوین‌ها دقیقاً نقطه قوت بیت‌کوین هستند و بیت‌کوین با آن‌ها تعریف می‌شود. تلاش برای اعمال هارد فورک بدون اجماع همگانی، از نظر برخی فعالان مصداق حمله به شبکه بود. اما افراد دیگری هم بودند که با این دیدگاه موافق نبودند؛ آن‌ها معتقد بودند که بیت‌کوین برای رشد و موفقیت نیاز به انعطاف‌پذیری دارد و این مورد مشخص، یعنی موضوع سایز بلاک، تغییر عمده‌ای نیست. آن‌ها فکر می‌کردند که مطرح کردن موضوع افزایش سقف عرضه بیت‌کوین از ۲۱ میلیون صرفاً یک مغالطه در بحث، و رد گم کنی است.

تنش بر روی این مسأله، در طول سال‌های گذشته میان جامعه فعالان بیت‌کوین ایجاد شده بود ولی علنی نبود. اما در این مرحله، این تفاوت اساسیِ ایدئولوژیک، عیان شد و همگان از آن مطلع شدند. بیت‌کوین یک شبکه عمومی بود و امکان پنهان کردن این اختلاف نظر از عموم مردم دیگر ممکن نبود.

5 Hard fork

در ۲۴ اوت سال ۲۰۱۵ و تنها ۹ روز پس از انتشار نرم‌افزار Bitcoin XT، نامه‌ای توسط بزرگترین و مهم‌ترین شرکت‌های فعال در زمینه بیت‌کوین منتشر شد و از آن حمایت کرد.

جامعه ما بر سر یک دو راهی قرار گرفته است. بحث بر روی انتخاب مسیر به‌طور کلی بحث مفیدی بوده است و ما تاکنون اعلام موضع نکرده و در بحث دخالت نکرده‌ایم. تا امروز مشارکت ما صرفاً شنیدن نظرات، تحقیق، و آزمایش [روش‌های پیشنهاد شده] بوده است.

ما معتقدیم دیگر وقت آن رسیده است که دیدگاه خود را به روشی شفاف و روشن بیان کنیم. بعد از صحبت‌های طولانی با توسعه‌دهندگان اصلی، استخراج‌کنندگان، تیم‌های فنی خودمان، و دیگر شرکت‌های فعال، به این نتیجه رسیده‌ایم که افزایش محدودیت سایز بلاک برای موفقیت بیت‌کوین ضروری است.

ما از نرم‌افزاری که BIP-101 پیاده‌سازی کرده است حمایت می‌کنیم. استدلال‌های گوین اندریسن مبنی بر لزوم بلاک‌های بزرگ‌تر و کارآمد بودن نرم‌افزاری که تهیه شده است، در حالی که از نامتمرکز بودن شبکه بیت‌کوین محافظت شود – ما را قانع کرده است. اکثر ماینرها همین امروز از بلاک‌های ۸ مگابایتی مطرح شده در BIP-101 پشتیبانی می‌کنند و ما احساس می‌کنیم زمان آن فرا رسیده است که همه فعالان پشت این پیشنهاد با یکدیگر متحد شوند.

شرکت‌های ما تا ماه دسامبر ۲۰۱۵ برای بلاک‌های بزرگ‌تر آماده خواهند شد و ما نرم‌افزاری که برای این منظور تهیه شده است را اجرا خواهیم کرد. با رشد جامعه کاربران بیت‌کوین، ضروری است برای تضمین ثبات شبکه به دنبال اجماع محکمی باشیم و اکنون بیش از هر زمان دیگری به آن نیاز داریم. ما

متعهد می‌شویم که تا ماه دسامبر ۲۰۱۵ در سیستم‌ها و نرم‌افزارهای خود از BIP-101 استفاده کنیم و دیگران را هم تشویق می‌کنیم به ما بپیوندند.[1]

این نامه توسط مدیران عامل شرکت‌های Circle، Blockchain.info، BitPay، Xapo، Bitnet، itBit، Kncminer و BitGo امضاء شده بود. این‌ها نه‌تنها از بزرگترین شرکت‌های موجود در این فضا بودند، بلکه بسیاری از آن‌ها بودجه‌های زیادی داشتند و سرمایه‌گذاری‌های بزرگی بر روی آن‌ها انجام شده بود. شرکت BitPay بزرگترین پذیرنده فروشگاهی و کیف پول Blockchain.info بزرگترین ارائه دهنده کیف پول بیت‌کوین بود. این نامه شرایط را ملتهب‌تر کرد. از یک طرف برای صنعت بسیار مهم بود که با مسائل موجود در توسعه بیت‌کوین درگیر شود و به پیشرفت امور کمک کند، در حالی برخی از افراد در اردوگاه مخالف با این روش مخالف بودند و این رویکرد را غلط می‌دانستند. قرار بود بیت‌کوین به‌صورت مردمی، از پایین به بالا، و توسط کاربران هدایت شود. لابی کردن از بالا به پایین توسط شرکت‌های بزرگ این هدف اصلی را تضعیف می‌کرد. گروهی که به طرفداران بلاک‌های کوچک[1] معروف بود، معتقد بودند گوین باید بیشتر تلاش خود را معطوف به لابی کردن با کاربران بیت‌کوین می‌کرد و قبل از درگیر کردن شرکت‌های بزرگ و فعال در صنعت برای اجرای یک نرم‌افزار ناسازگار با سیستم فعلی، ابتدا کاربران را برای پذیرش بلاک‌های بزرگ‌تر مجاب می‌کرد. از نظر آن‌ها این روش احتمالاً اخلاقی‌تر و از آن مهم‌تر مؤثرتر بود.

احتمالاً گوین مغرور شده بود و پس از سال‌ها بحث و استدلال خسته‌کننده، او می‌خواست قدرت و نفوذ خود را به رخ توسعه‌دهندگان دیگر بکشد. او برای به دست آوردن حمایت شرکت‌های بزرگ و سرمایه‌دار لابی کرده بود. این فرصتی برای گوین بود تا به توسعه‌دهندگانی که با او مخالفت می‌کردند نشان دهد که اصلاً مهم نیستند و شرکت‌های

1 https://blog.bitmex.com/wp-content/uploads/2017/09/industry-letter.pdf
1 Small blockers

بزرگ فعال در این صنعت حتی آن‌ها را نمی‌شناسند. بدون شک مخالفان او از این موضوع بیشتر عصبانی شدند و ادعا می‌کردند که تصمیمات این شرکت‌ها اهمیتی نخواهد داشت.

اکنون زمان مناسبی است تا کمی درباره گوین اندریسن صحبت کنیم. خالق بیت‌کوین «ساتوشی ناکاموتو[1]» است. به‌طور دقیق‌تر، ساتوشی سیستم را طراحی کرد، نرم‌افزار پیاده‌سازی آن را که پر از اشکالات نرم‌افزاری بود نوشت، و مقاله معرفی[2] آن را هم تألیف کرد. ساتوشی کمتر از ۲ سال بعد از راه‌اندازی شبکه و در ماه دسامبر سال ۲۰۱۰ میلادی پروژه را ترک کرد. بعد از این مرحله او دیگر مشارکتی در کُد بیت‌کوین نداشت و فعالیت او در انجمن‌های گفتگوی آنلاین هم متوقف شد. گوین توضیح می‌دهد که از نظر او چگونه هدایت پروژه به او سپرده شد:

> با گذشت زمان ساتوشی به روش کُدنویسی من اعتماد کرد و سرانجام کار عجیبی از او سر زد. او از من پرسید آیا با قرارگرفتن آدرس ایمیل‌ام بر روی صفحه اصلی سایت بیت‌کوین موافق هستم یا نه. و من هم موافقت کردم ولی نمی‌دانستم او بعد از اضافه کردن آدرس ایمیل من، آدرس ایمیل خود را حذف می‌کند. هرکس می‌خواست درمورد بیت‌کوین اطلاعاتی به‌دست بیاورد به من ایمیل ارسال می‌کرد. ساتوشی آرام آرام از رهبری پروژه کناره‌گیری کرد و من را در جایگاه رهبری پروژه قرار داد.[3]

از قرار معلوم زمانی که ساتوشی پروژه را به گوین اندریسن تحویل داده است، سورس کد[4] پروژه بر روی سایت «سورس‌فورج[5]» قرار گرفته و در ژانویه سال ۲۰۱۱ نام دو نفر یعنی خود ساتوشی و گوین به‌عنوان نگهدارنده[6] ذکر شده است. البته روایت گوین از وقایع مورد مناقشه است و مخالفان وی ادعا می‌کنند که هیچ سندی از جانب ساتوشی مبنی بر

1 Satoshi Nakamoto
2 Whitepaper
3 https://www.huffingtonpost.co.uk/entry/gavin-andresen-bitcoin_n_3093316
4 Source code
5 Sourceforge
6 Maintainer

ادعای تحویل پروژه به او وجود ندارد. به‌ویژه ادعای «رهبر پروژه[1]» بودن او بعید و غیرمستند به‌نظر می‌رسد. بیت‌کوین رهبر ندارد. گوین مخزن[2] نرم‌افزار بیت‌کوین در سورس‌فورج و بعداً «گیت‌هاب[3]» را کنترل می‌کرد تا اینکه چندین سال بعد یعنی در آوریل سال ۲۰۱۴ آن را به «ولادیمیر ون در لان[4]» تحویل داد. کنترل مخزن نرم‌افزار البته به معنی کنترل بیت‌کوین نیست زیرا کاربران می‌توانند هر نرم‌افزاری که دوست دارند، از هر مخزنی که دوست دارند، اجرا کنند. این باور غلط سال‌ها است که همچنان باقی مانده است. به احتمال زیاد ادعای گوین مبنی بر تحویل گرفتن پروژه از ساتوشی درست باشد ولی ادعای رهبری پروژه کمی اغراق‌آمیز به نظر می‌رسد.

با این حال تمرکز بر روایت بحث‌برانگیز تحویل پروژه از ساتوشی به گوین، یا نقش فنی او در رابطه با مخزن نرم‌افزار بیت‌کوین باعث می‌شود از موضوع اصلی منحرف شویم. افراد در هر دو طرف این منازعه مدام این نکات را بیان می‌کردند، اما این مسائل واقعاً اهمیتی ندارد. تأثیر زیادی که گوین در این فضا داشت درواقع به‌دلیل ویژگی‌های شخصیتی و توانایی رهبری او بود. چون بیان این مسأله دشوار بود افراد درباره موارد فرعی مثل تحویل پروژه به او تمرکز کردند. چیزی که برای درک نقش گوین در کامیونیتی آن زمان مهم است، شخصیت وی است. او در پست‌هایی که در تالارهای گفتگو می‌نوشت، یا حضورش در رویدادها، صبور، متفکر، آرام، و عمل‌گرا بود. همین ویژگی‌های شخصیتی و ویژگی‌های رهبری بود که او را از سایر توسعه‌دهندگان پروژه متمایز می‌کرد. مردم به حرف‌های او گوش می‌دادند. به نظر آدم منطقی می‌رسید و برای توضیح دادن مسائل وقت می‌گذاشت. برعکس برخی دیگر از توسعه‌دهندگان بیت‌کوین که نسبت به کسانی که دانش فنی پایین‌تری داشتند کم‌تحمل‌تر بودند، یا ترجیح می‌دادند پشت صحنه بمانند. نفوذ او بر کامیونیتی فنی بیت‌کوین به‌دلیل شخصیت او بود، نه اینکه ساتوشی پروژه را به او تحویل داده است.

1 Leader of the project
2 Repository
3 Github
4 Wladimir Van Der Laan

گوین همچنین در چند سال اول پروژه به‌طور قابل‌توجهی به آن کمک کرد. در سال ۲۰۱۰ او ۲۰,۰۰۰ بیت‌کوین به ارزش ۵۰ دلار خریداری و آن‌ها را از طریق یک وب‌سایت بین مردم تقسیم کرد. فقط کافی بود آن‌ها یک پازل Captcha را حل کنند تا ۵ بیت‌کوین به‌صورت رایگان به آدرس آن‌ها ارسال شود. این توزیع سکه‌ها به تعداد زیادی از افراد به موفقیت شبکه در اوایل راه‌اندازی کمک زیادی کرد. مردم در آن زمان واقعاً بیت‌کوین را درک نمی‌کردند و بعید بود برای خرید آن پولی خرج کنند، چون هنوز اعتمادی به آن نداشتند ولی می‌توانستند از این راه به‌راحتی بیت‌کوین به‌دست بیاورند.
گوین در سال ۲۰۱۲ یکی از بنیانگذاران بنیاد بیت‌کوین[1] و یکی از اعضای هیات مدیره آن شد. یکی از مسئولیت‌های اصلی این بنیاد علاوه بر فعالیت‌های مختلفی که داشت، پرداخت پول به گوین برای کار در زمینه توسعه بیت‌کوین بود. بنابراین گوین اولین توسعه‌دهنده بیت‌کوین بود که برای این کار پول دریافت می‌کرد. او تا اواسط سال ۲۰۱۷ و با سمت «محقق ارشد[2]» در بنیاد باقی ماند.

احترامی که اعضای جامعه بیت‌کوین برای گوین قائل بودند بر کسی پوشیده نیست. بسیاری او را «فرد اصلی» پروژه می‌دانستند. البته اختلافات فزاینده‌ای در سطح جامعه فنی بیت‌کوین وجود داشت که غالباً از چشم یک ناظر عادی دور می‌ماند. افراد زیادی اعتقاد داشتند گوین در این فضا یک نقش کلیدی دارد. پس باید تصمیم او برای پشتیبانی از نرم‌افزار Bitcoin XT و تشویق کاربران برای اجرای آن را با توجه به موقعیتی که در جامعه بیت‌کوین داشت مورد قضاوت قرار دهیم. این موضوع بخاطر حمایت شخص گوین مثل بمب صدا کرد وگرنه اگر هر شخص دیگری این کار را کرده بود، تأثیری تا این اندازه عمیق نمی‌داشت و وقایع بعدی هم رخ نمی‌داد.

مایک هرن هم یکی از توسعه‌دهندگان اولیه بیت‌کوین بود که وقت آزاد خود را در شرکت گوگل (پروژه ۲۰ درصد[3]) به بیت‌کوین اختصاص داده بود. با این حال، مایک به

1 Bitcoin foundation
2 Chief scientist
3 20 percent free time project at Google

اندازه گوین درگیر توسعه نرم‌افزار اصلی[1] بیت‌کوین نبود. او برخلاف گوین که محافظه‌کار، میانه‌رو و به دنبال برقراری اجماع میان کاربران بود، فردی بود که در تصمیماتش خطر می‌کرد و محافظه‌کار نبود. مایک کارهای زیادی در نرم‌افزار Bitconij انجام داد که یک کتابخانه با زبان جاوا[2] برای کار کردن با پروتکل بیت‌کوین بود. همین کار او باعث شد امکان تولید کیف پول‌های قابل نصب بر روی موبایل فراهم شود که مسلماً در آن زمان کمک بزرگ و چشمگیری به فضای بیت‌کوین محسوب می‌شد.

با شدت گرفتن قائله در ماه آگوست سال ۲۰۱۵، جنگی شدید و خشن در شبکه‌های اجتماعی در جریان بود. دو بستر اصلی برای بحث در مورد بیت‌کوین در آن زمان انجمن‌های گفتگوی سایت BitcoinTalk و ساب‌ردیت[3] /r/bitcoin بود. بحث و مناظره مدتی بود که در این دو بستر درگرفته بود ولی انتشار Bitcoin XT آن‌ها را تند و آتشین‌تر کرد. در کل بیشتر مطالبی که منتشر می‌شد در حمایت از بلاک‌های بزرگ‌تر بود. پیام هواداران بلاک‌های بزرگ روشن و ساده بود: بیت‌کوین به ظرفیت بیشتری نیاز داشت. از نظر یک ناظر عادی استدلال‌هایی که با این دیدگاه غالب مخالف بودند، معمولاً بسیار پیچیده و تا حدی گیج‌کننده بودند. علاوه بر این به نظر می‌رسید ۱ مگابایت با توجه به تاریخچه علوم کامپیوتر و رشد تصاعدی ظرفیت، مقدار کمی باشد. در تابستان سال ۲۰۱۵ در حالی که بسیاری از افراد دیگر از بحث‌های طولانی خسته شده بودند، انجمن‌های گفتگوی آنلاین پر شده بودند از مطالبی که از بلاک‌های بزرگ و نرم‌افزارهای ناسازگار با سیستم فعلی شبکه حمایت می‌کردند. آنقدر پست‌های تکراری وجود داشت که یافتن سایر اخبار در حوزه بیت‌کوین کار دشواری شده بود و کار مدیران این انجمن‌ها و مدیریت مطالب چند برابر شده بود. مدیریت مطالب در این انجمن‌ها باعث می‌شد طرفداران بلاک‌های بزرگ عصبانی شوند و از نظر آن‌ها سیاست مدیریت یا به زعم آن‌ها سانسور مطالب، از پیشرفت بیت‌کوین جلوگیری می‌کرد.

1 Reference implementation
2 Java library
3 subreddit

انجمن‌های BitcoinTalk و ساب‌ردیت r/bitcoin/ هر دو توسط یک شخص با نام کاربری «تی‌مُس[1]» کنترل می‌شدند. نام واقعی او «مایکل مارکوارت[2]» و یکی از پیش‌کسوتان فضای بیت‌کوین است و علاوه بر انجمن‌هایی که معرفی شدند سایت bitcoin.it (Bitcoin Wiki) را هم مدیریت می‌کرد. او همچین اولین وب‌سایت بلاک اکسپلورر بیت‌کوین[3] را ایجاد کرده است. یک صفحه اینترنتی که کاربران می‌توانستند در آن اطلاعات تراکنش‌هایشان[4] را مشاهده کنند. این امر در اوایل برای توسعه فضا و آموزش مردم در مورد نحوه کار بیت‌کوین بسیار مهم بود. ولی در نهایت بلاک اکسپلورر blockchain.info در حدود سال ۲۰۱۱ از سایت او (blockexplorer.com) به دلیل فراهم کردن چارت‌های کاربردی و ابتکاری برای کاربران، پیشی گرفت. به نظر می‌رسید تی‌مُس حداقل از این نظر که کاربران باید قبل از اجرای یک نرم‌افزار ناسازگار با شبکه فعلی بیت‌کوین با هم به توافق برسند، با گروه طرفدار بلاک‌های کوچک هم نظر بود.

در روز ۱۷ اوت سال ۲۰۱۵، یعنی دو روز بعد از منتشر شدن نرم‌افزار Bitcoin XT او سیاست جدید مدیریت مطالب ساب‌ردیت r/bitcoin/ را اعلام کرد. سیاست‌های جدید بسیار بحث‌برانگیز و تفرقه‌برانگیز بود. انتشار نرم‌افزار Bitcoin XT موجب افزایش تعداد مطالب در انجمن‌های گفتگو و درنتیجه اعمال محدودیت و اداره سختگیرانه‌تر انجمن‌های گفتگو شده بود. بنابراین تی‌مُس توضیحی درباره قوانین جدید منتشر کرد.

> ساب‌ردیت r/bitcoin/ برای کمک به بیت‌کوین ایجاد شده است. اگر فورک XT فعال شود، از بیت‌کوین جدا خواهد شد و شبکه / ارز جداگانه‌ای ایجاد خواهد کرد. بنابراین تبلیغ خودش و شرکت‌هایی که از آن پشتیبانی می‌کنند در r/bitcoin/ مجاز نیست. اگر به فرض محال اکثریت قریب به اتفاق کاربران بیت‌کوین از XT استفاده کنند و تصور غالب این باشد که

1 Theymos
2 Michael Marquardt
3 Block explorer
4 Bitcoin transaction

بیت‌کوین واقعی است، در این صورت اوضاع تغییر خواهد کرد و فقط مطالب مربوط به XT مجاز خواهند بود. در این صورت تعریف «بیت‌کوین» تغییر خواهد کرد. منطقی نیست که در این ساب‌ردیت از دو شبکه / ارز ناسازگار با یکدیگر حمایت شود چون فقط یک بیت‌کوین وجود دارد و /r/bitcoin فقط در خدمت بیت‌کوین خواهد بود.

اگر همه کارشناسان فعال در بیت‌کوین روی یک هارد فورک به یک اجماع همگانی برسند و اکثریت قریب به اتفاق کاربران و شرکت‌های بیت‌کوین نیز از آن پشتیبانی کنند، در این صورت می‌توانیم بگوییم به احتمال خیلی زیاد این شبکه / ارز جدید به تعریف جدید بیت‌کوین تبدیل و مورد استفاده همه کاربران قرار خواهد گرفت. (نظر ماینرها در این موضوع اهمیتی ندارد) به محض اینکه مشخص شود این هارد فورک با روح بیت‌کوین سازگار است و به‌طور مثال عرضه کوین خارج از برنامه ندارد، می‌تواند به سرعت در این ساب‌ردیت مطرح شود. در حال حاضر بحث و جدل زیادی حول هر هارد فورکی که اندازه بلاک را افزایش می‌دهد وجود دارد ولی این شرایط احتمالاً با بحث و بررسی بیشتر و پر شدن بلاک‌ها در آینده تغییر خواهد کرد. من فکر می‌کنم تا ۶ ماه آینده به یک توافق عمومی برای افزایش فضای بلاک برسیم ولی این افزایش باید کمتر از مقداری باشد که در سیستم XT پیشنهاد شده است.

تفاوت قابل توجهی بین گفتگو درباره یک پیشنهاد هارد فورک (که هرچند من با آن مخالف هستم، قبلاً در این ساب‌ردیت مجاز بوده است) و تبلیغ نرم‌افزاری که برای فورک زنجیره بیت‌کوین و ایجاد یک شبکه / ارز رقیب برای بیت‌کوین تهیه شده است وجود دارد. مورد دوم علناً در تضاد با قوانین تعیین شده برای ساب‌ردیت /r/bitcoin است. هرچند فناوری بیت‌کوین بدون توجه به این اتفاقات به کار خود ادامه می‌دهد، این تلاش‌ها برای فورک بیت‌کوین به اکوسیستم و اقتصاد بیت‌کوین آسیب می‌رساند.

> اگر این سیاست‌ها برای ۹۰ درصد از کاربران /r/bitcoin غیر قابل تحمل است، من از این ۹۰ درصد درخواست می‌کنم اینجا را ترک کنند. این اتفاق به نفع این ساب‌ردیت و آن کاربران است. این افراد هم از این به بعد مطالب خلاف قوانین جدید ننویسند و برای تغییر این سیاست‌ها درخواست ندهند و به دنبال به‌دست آوردن رأی و گرفتن تأیید کاربران دیگر نباشند و حمله‌های شخصی به مدیران این ساب‌ردیت نکنند. هیچ آدم عاقلی با یک استدلال غیرمنطقی مجاب نخواهد شد و شما فقط وقت خود و ما را تلف می‌کنید. این قوانین جدید درواقع این افراد را به ترک این ساب‌ردیت تشویق می‌کند تا بتوانیم در مورد اخبار بیت‌کوین در آرامش به گفتگو بپردازیم.[1]

قوانین جدید برای ساب‌ردیت بیت‌کوین کاملاً شفاف بود: از آنجا که کاربران روی Bitcoin XT توافق نداشتند و این نرم‌افزار با قوانین فعلی شبکه بیت‌کوین سازگار نبود و منجر به ایجاد یک زنجیره و کوین جدید می‌شد، تبلیغ آن هم ممنوع است. این مسأله بسیاری از به اصطلاح «طرفداران بلاک‌های بزرگ» را خشمگین‌تر کرد. از نظر آن‌ها این ساب‌ردیت اصلی‌ترین انجمن برای بحث و گفتگو بود و آن‌ها در نظر داشتند برای اعمال تغییر موردنظرشان لابی کنند. بحث‌های ضدسانسور با قدرت بیشتری پیش می‌رفت و افراد زیادی به آن معتقد بودند. اگر صرفاً به‌خاطر توافق نداشتن روی موضوعی نتوانیم روی آن بحث و گفتگو کنیم، پس اصلاً چطور می‌توانیم به یک توافق برسیم؟ این دو با هم در تناقض هستند. اصلاً تی‌مُس چه‌کاره است که درباره به‌توافق رسیدن یا نرسیدن ما تصمیم بگیرد؟ بیت‌کوین به همان اندازه که به او تعلق دارد مال من هم هست! اگر استدلال خوبی دارند پس چرا به سانسور متوسل می‌شوند؟ اگر بیت‌کوین به این اندازه شکننده است که به این سانسورها نیاز دارد، پس خیلی ضعیف و بی‌فایده است. اگر بحث درباره Bitcoin XT ممنوع است، پس حتماً چیز خوبی است ... و از این قبیل صحبت‌ها.

1 https://www.reddit.com/r/Bitcoin/comments/3h9cq4/its_time_for_a_break_about_the_recent_mess/

برای درک میزان خشمی که نسبت به تِی‌مُس وجود داشت، باید ببینیم افرادی که به اندازه کافی درگیر این بحث بودند، چه کسانی هستند. آن‌ها عموما «آنارکو-کاپیتالیست[1]» یا آزادیخواهانی[2] بودند که به شدت از آزادی بیان حمایت می‌کردند. به راحتی می‌توان فهمید که چرا یک پیام ضد سانسور خوشایند این گروه است. اصلاً بسیاری از این افراد به‌خاطر احساس محرومیت از سیستم مالی سنتی به بیت‌کوین پیوسته بودند. بانک‌های مرکزی درگیر سیاست‌هایی شده‌اند که بسیاری از بیت‌کوینرها به شدت با آن‌ها مخالف هستند، مثل برنامه‌های «تسهیل مقداری[3]» یا سیاست‌های پولیِ انبساطی. بیت‌کوینرها معمولاً هنگام ابراز مخالفت با این سیاست‌ها احساس می‌کردند صدای آن‌ها شنیده نمی‌شود و به نظرات‌شان اهمیتی داده نمی‌شود. به همین دلیل است که بیشتر این افراد بیت‌کوینر شدند. آن‌ها احساس کردند که این بار واقعاً این پول برای خودشان است و اختیار آن دست دیگری نیست و صدایشان شنیده می‌شود. بنابراین خشم و عصبانیت آن‌ها از خاموش شدن صدایشان در فضای بیت‌کوین بسیار زیاد بود.

اعمال این سیاست‌های کنترلی بر مطالب کاربران جامعه بیت‌کوین را دچار دودستگی کرد. گروه طرفدار بلاک‌های بزرگ‌تر به تدریج به یک ساب‌ردیت جدید به آدرس `/r/btc` کوچ کردند. آن‌ها همچنین به‌تدریج سایت `BitcoinTalk` را ترک و به انجمن‌های دیگری مانند `Bitco.in` منتقل شدند. سطح تعامل طرفین درگیر به تدریج کاهش یافت و افراد بیشتر وقتشان را صرف گفتگو با کسانی می‌کردند که عقاید مشابهی داشتند. سلامت کامیونیتی به خطر افتاد و «سوگیریِ تأییدی[4]» به یک خطر جدی تبدیل شد.

به راحتی می‌توان تِی‌مُس را مسئول این انشقاق در جامعه بیت‌کوین دانست. هرچند با بررسی توسعه دیگرِ جوامع در فضای مجازی شاید بتوان گفت که این امر تا حدودی اجتناب‌ناپذیر بوده است. مردم به خواندن چیزهایی که با آن‌ها موافق هستند و دنبال کردن

1 anarcho-capitalist
2 libertarian
3 Quantitative Easing (QE)
4 Confirmation bias

افرادی که با آن‌ها هم‌نظر هستند گرایش دارند. سوگیری تأییدی به شدت در بسترهای فضای مجازی وجود دارد و باعث دو قطبی شدن جوامع می‌شود. دنیای سیاست از مشهورترین نمونه‌ها است، که در آن راست‌گرایان و چپ‌گرایان به روایت داستان‌های واقعی بر روی بسترهای انتخابی خود می‌پردازند که منطبق با فرضیات و ایدئولوژی اولیه آن‌ها است. ایمان مردم نسبت به عقایدشان هر روز عمیق‌تر می‌شود و کمتر در معرض استدلال‌های مخالف قرار می‌گیرند. در این مرحله و با قرار گرفتن در معرض انبوهی از اطلاعاتی که در راستای اعتقادات ایشان است، هر دو طرف درگیری به سختی باور می‌کنند ممکن باشد کسی یک عقیده مخالف جدی و منطقی با آن‌ها داشته باشد. بنابراین تصور می‌شود کسانی که دیدگاه متضادی با آن‌ها دارند، یا احمق‌اند، یا فاسدند، یا بدخواه. موضوعاتی که مطرح کردیم به سرعت در جامعه فعالان بیت‌کوین پیش آمد. با توجه به این واقعیت که این اتفاق برای همه شبکه‌های اجتماعی رخ می‌دهد، ساده‌لوحانه است که تِی‌مُس را مقصر این قضایا بدانیم، گرچه او مانند دیگران در هر دو گروه، در ایجاد دودستگی به‌وجود آمده بین جامعه فعالان بیت‌کوین نقش داشت.

با مرور دوباره مطلبی که در آن تِی‌مُس به تبیین سیاست‌های جدید کنترل مطالب انجمن‌های گفتگو پرداخته بود متوجه ظرایفی می‌شویم که در آن زمان چندان مورد استقبال قرار نگرفت. از بسیاری جهات او حق داشت و جلوتر از زمان خود فکر می‌کرد. ممکن بود `Bitcoin XT` به دلیل نبود اجماع عمومی میان کاربران بیت‌کوین، باعث بوجود آمدن یک کوین جدید شود. شاید کار درست همین بود که فرآیند تغییر قوانین شبکه به دو مرحله تقسیم شود: اول برای رسیدن به اتفاق نظر میان کاربران تلاش، و بعد از رسیدن به توافق همگانی برای اجرای نرم‌افزاری که با قوانین فعلی شبکه سازگار نیست تبلیغ شود. امروزه روند تغییر و به‌روزرسانی قوانین شبکه شفاف‌تر به نظر می‌رسد: اگر کسی بخواهد یک نرم‌افزار ناسازگار با قوانین فعلی شبکه منتشر کند، دو انتخاب پیش رو خواهد داشت:

۱. بدون نیاز به توافق همگانی بین کاربران شبکه، یک کوین جدید و متفاوت با بیت‌کوین به‌وجود بیاورد؛ یا
۲. قبل از تشویق کاربران برای اجرای این نرم‌افزار ناسازگار به قوانین فعلی شبکه برای رسیدن به توافق همگانی لابی کند. اگر همه کاربران با این تغییرات موافق بودند و به اجماع همگانی رسیدند، آنوقت این نرم‌افزار جدید را اجرا خواهند کرد و کوین جدیدی که به‌وجود آمده را به نام «بیت‌کوین» می‌شناسند.

این موضوع در حال حاضر تقریباً برای همه جا افتاده است که تلاش برای هارد فورک در شرایطی جز ۲ مورد ذکر شده، می‌تواند باعث یک انشعاب بسیار دردسرساز در زنجیره بیت‌کوین شود. متأسفانه در آن زمان، همگان از این ظرافت‌ها اطلاع نداشتند، بنابراین طرفداران بلاک‌های بزرگ نمی‌دانستند دقیقاً باید چه‌کار کنند. آن‌ها مطمئن نبودند آیا به یک اجماع عمومی میان همه کاربران نیاز دارند یا نه.

در مراحل اولیه درگیری به نظر می‌رسید که طرفداران بلاک‌های بزرگ در حال پیشرفت هستند و در جنگ پیروز خواهند شد. به نظر می‌رسید که آن‌ها یک پیام ساده و روشن دارند و اکثریت کاربران با آن‌ها موافق هستند. در همین حین شعارهای مبارزه با سانسور انجمن‌های گفتگوی آنلاین هم رفته‌رفته بیشتر مورد استقبال افکار عمومی قرار می‌گرفت.

اما از سوی دیگر، همچنین برای همگان روشن بود که پیشنهاد افزایش سایز بلاک مطرح شده در Bitcoin XT مبنی بر افزایش‌های ۸ مگابایتی سایز بلاک بر اساس یک برنامه مشخص و تا ۲۰ سال آینده خیلی افراطی است. اصلاً مایک هرن که بود که همچین تصمیمی بگیرد؟ و او از کجا می‌دانست که قرار است در آینده دور چه اتفاقی برای فضای بیت‌کوین بیفتد؟ فضایی که بسیار سریع و غیرقابل پیش‌بینی تغییر می‌کرد. بسیاری از افراد معتقد بودند که بهتر است سایز بلاک به روش ساده‌تر و متعادل‌تری افزایش یابد. در حالی که تقریباً همه خواهان افزایش محدودیت سایز بلاک بودند ولی به نظر می‌رسید

اغلب افراد فکر می‌کردند Bitcoin XT شکست خواهد خورد و سرانجام یک پیشنهاد متعادل‌تر موفق خواهد شد. اما از نظر طرفداران بلاک‌های بزرگ‌تر، Bitcoin XT یک گام ضروری برای ادامه یافتن گفتگوها و مناظره‌ها بود و برای مطرح شدن پیشنهادهای مخالف مثل یک کاتالیزور عمل می‌کرد. شاید اولین اشتباه مهم طرفداران بلاک‌های بزرگ هم همین بود [که از یک روش افراطی افزایش سایز بلاک با وجود اقبال کمی که بین عموم کاربران بیت‌کوین داشت، حمایت کردند]. آخر چطور می‌توان بعد از باخت در اولین نبرد در یک جنگ پیروز شد؟

فصل دوم

صف‌آرایی مخالفین

در روزهای ابتدایی بیت‌کوین یعنی از سال ۲۰۰۹ تا اوایل ۲۰۱۱، کل اکوسیستم بیت‌کوین فقط از نرم‌افزار بیت‌کوین[1] تشکیل شده بود. این نرم‌افزار در ابتدا فقط روی سیستم عامل ویندوز قابل اجرا بود و از بخش‌های کیف پول، فول نود[2]، و ماینر تشکیل شده بود. خبری از کیف پول‌های موبایلی، پذیرش بیت‌کوین در فروشگاه‌ها، وب‌سایت‌های شرط‌بندی، بازارهای دارک‌وب[3]، تهاتر کالا، صرافی‌ها، و سرمایه‌گذاری شرکت‌ها نبود؛ فقط همین یک نرم‌افزار خیلی ابتدایی وجود داشت. تنها کاری که یک نفر می‌توانست در آن زمان انجام دهد این بود که چندتا کوین استخراج کند و آن‌ها را برای دیگران بفرستد یا دریافت کند. در آن زمان بیت‌کوین تقریباً بی‌فایده بود و به نظر نمی‌رسید که ارزشی یا آینده‌ای داشته باشد. در آن زمان فقط کسانی به فضای بیت‌کوین علاقه‌مند می‌شدند که قوه تخیل بالایی داشتند. آن‌ها باید آینده دور و مراحل تحول و توسعه این سیستم را در ذهن خود تصور می‌کردند و پیش‌فرض‌های مختلفی را در رابطه با چگونگی تکامل بیت‌کوین روی هم می‌گذاشتند.

1 Bitcoin client
2 Full node
3 Darknet markets

بسیاری از این فرضیات هرگز مورد آزمایش و بررسی دقیق قرار نگرفته بودند و امری بدیهی تلقی می‌شدند و پذیرفته شده بودند. در سال ۲۰۱۵ حدود ۶ سال از عمر بیت‌کوین می‌گذشت و پذیرش این فرضیات برای کسانی که تمام وقت‌شان را به این فضا اختصاص داده بودند، زمان طولانی‌ای بود. بسیاری از افراد فعال در جامعه بیت‌کوین در رابطه با نحوه کار بیت‌کوین، فرضیات کاملاً متفاوت و متناقضی داشتند ولی دامنه این اختلافات هرگز تا آن روز آشکار نشده بود. حالا این اختلاف‌نظرها داشت عیان می‌شد و با توجه به اهمیتی که بیت‌کوین برای این افراد داشت، ممکن بود نتیجه وحشتناک و پیش‌بینی نشده باشد.

قیمت بیت‌کوین هم به مقدار قابل توجهی افزایش یافته بود و از چند سنت[1] در سال ۲۰۱۰ به حدود ۲۲۰ دلار در تابستان سال ۲۰۱۵ رسیده بود. بنابراین بسیاری از طرفین درگیری با سرمایه‌گذاری زودهنگام در بیت‌کوین سود چشم‌گیری کرده بودند. این امر یک پیامد ناگوار دارد و باعث می‌شود افراد اعتماد به نفس بیش از حد پیدا کنند یا حتی کمی گستاخ شوند. به‌عنوان مثال فرض کنیم کسی تصمیم گرفته بود در اوایل سال ۲۰۱۱ وقتی که قیمت بیت‌کوین زیر ۱ دلار بود روی آن سرمایه‌گذاری کند. آن‌ها این سرمایه‌گذاری را بر اساس فرضیات و چشم‌انداز خاصی انجام داده بودند و با نفروختن کوین‌ها تا سال ۲۰۱۵، سرمایه آن‌ها ۲۰۰ برابر رشد کرده بود. این اتفاق احتمالاً بر رفتار آن‌ها اثر می‌گذارد و با خود فکر می‌کنند حتماً مفروضات سال ۲۰۱۱ آن‌ها درست بوده‌اند. بالاخره آن‌ها سود بالایی کرده‌اند.

این سرمایه‌گذاران احتمالاً فکر می‌کند که درک بسیار خوبی از بیت‌کوین دارند و می‌توانند مسیر درست را برای ادامه راه بیت‌کوین تشخیص دهند، چون معتقدند بیت‌کوین را به‌خوبی در سال ۲۰۱۱ فهمیده‌اند و شاهد این ادعا هم سود بزرگی است که به‌دست آمده است. متأسفانه آن‌ها در نظر نداشتند که افراد دیگری هم هستند که دیدگاه‌های متفاوت و کاملاً متناقضی با آن‌ها دارند و اتفاقاً آن‌ها هم اوایل سال ۲۰۱۱ روی بیت‌کوین سرمایه‌گذاری کرده‌اند و منطق آن‌ها مبنی بر درک درست بیت‌کوین تا حدودی نادرست

1 Cent

و مغرضانه است. اغلب به نظر می‌رسید که این افراد معتقد بودند سایر سرمایه‌گذاران اولیه با نظرات آن‌ها موافق‌اند و جبهه مخالف آن‌ها در جنگ بر سر سایز بلاک، تازه‌واردان هستند. به همین خاطر بود که این جنگ در مدت کوتاهی بالاگرفت و به سرعت جدی شد.

اکنون بهتر است کمی به تاریخچه اولیه بیت‌کوین بپردازیم. اولین نسخه از نرم‌افزار بیت‌کوین هیچگونه محدودیتی روی سایز بلاک نداشت، اگرچه احتمالاً بلاک‌های بزرگ‌تر از ۳۲ مگابایت کارکرد سیستم را مختل می‌کردند. این محدودیت را ساتوشی شخصاً در تابستان سال ۲۰۱۰ و با وارد کردن یک خط کُد به مخزن نرم‌افزار[1]، [و به قوانین شبکه] اضافه کرد.

```
static const unsigned int MAX_BLOCK_SIZE = 1000000;[2]
```

نرم‌افزار بیت‌کوین‌ای که شامل این تغییر و قانون جدید بود در روز ۱۰ جولای ۲۰۱۰ منتشر شد ولی این محدودیت ۱ مگابایتی تا روز ۷ سپتامبر سال ۲۰۱۰ و بلاک شماره ۷۹,۴۰۰ روی شبکه اعمال نشد. به این نوع ارتقاء قوانین شبکه یک «سافت فورک[3]» گفته می‌شود که در آن قوانین جدید محدودتر از قبل می‌شوند. (قوانین اعتبارسنجی بلاک اگر محدودتر شوند، ارتقاء قوانین به روش سافت فورک امکان‌پذیر خواهند شد. برای مثال در مورد سایز بلاک، وقتی سایز جدید کمتر از سایز قبلی باشد، این به‌روزرسانی از روش سافت فورک امکان‌پذیر خواهد بود. برای کسب اطلاعات بیشتر در مورد سافت فورک‌ها و هارد فورک‌ها به پیوست مراجعه کنید. - م)

1 Software repository
2 https://github.com/bitcoin/bitcoin/blob/a30b56ebe76ffff9f9cc8a6667186179413c6349/main.h#L18
3 Soft fork

افزایش سایز بلاک با توجه به اینکه قوانین را آسانتر می‌کند به نام هارد فورک[1] شناخته می‌شود. اگر در زنجیره بیت‌کوین یک هارد فورک رخ دهد، همه کاربران باید نرم‌افزار خود را به آخرین نسخه ارتقاء دهند. اگرچه این اصطلاح سافت فورک / هارد فورک در آن زمان رایج نبود و در ماه آپریل سال ۲۰۱۲ مورد استفاده قرار گرفت[2]. سافت فورک اعمال محدودیت ۱ مگابایتی اولین ارتقاء قوانین شبکه بیت‌کوین بود که از یک روش فعال‌سازی استفاده می‌کرد. این روش فعال‌سازی روش روز موعود نام دارد که قوانین جدید در یک شماره بلاک به‌خصوص فعال می‌شوند. ساتوشی هرگز دلیل واضحی برای اعمال این محدودیت بر روی سایز بلاک ارائه نداد. بسیاری از طرفداران بلاک‌های بزرگ معتقد بودند که این اقدام موقتی بوده، هرچند من هیچ‌گونه یادداشتی که این ادعا را تأیید کند پیدا نکرده‌ام.

رویداد مهم بعدی که طرفداران بلاک‌های بزرگ خیلی به آن ارجاع می‌دهند، در ۴ اکتبر سال ۲۰۱۰ رخ داد. هنوز از اعمال محدودیت ۱ مگابایتی بر روی سایز بلاک نگذشته بود که یکی از توسعه‌دهندگان بیت‌کوین به نام «جف گارزیک[3]»، پیشنهاد حذف آن و افزایش سایز بلاک را داد[4]. وی یک وصله نرم‌افزاری[5] را با حذف قانون ۱ مگابایت ارائه کرد و معتقد بود با این کار می‌توان ظرفیت پردازش تراکنش‌های شبکه بیت‌کوین را به ظرفیت شرکت Paypal رساند. اگرچه جف می‌دانست که چنین موضوعی در آن زمان امکان‌پذیر نخواهد بود ولی از نظر او این کار از منظر بازاریابی و روایت[6] بیت‌کوین اهمیت داشت. بعد از گذشت فقط ۱۵ دقیقه، تی‌مُس پاسخ داد و اظهار کرد: «این افزونه نود شما را با نودهای شبکه ناسازگار خواهد کَرد.». ساتوشی هم به گفتگوی آن‌ها پیوست و نوشت:

1 Hard fork
2 https://gist.github.com/gavinandresen/2355445
3 Jeff Garzik
4 https://bitcointalk.org/index.php?topic=1347.msg15139#msg15139
5 Software patch
6 Narrative

۱+ تِی‌مُس. از این افزونه استفاده نکنید. این به ضرر شما تمام می‌شود و باعث می‌شود [نود شما] با شبکه ناسازگار شود. بعداً هروقت لازم شد می‌توانیم برای این تغییر برنامه‌ریزی کنیم.

روز بعد ساتوشی یک مطلب جدید نوشت که طرفداران بلاک‌های بزرگ خیلی نقل قول می‌کنند:

می‌توانیم به این صورت برنامه‌ریزی کنیم:

```
if (blocknumber > 115000)
        maxblocksize = largerlimit
```

می‌توانیم قوانین جدید را از قبل در نسخه‌های بعدی قرار دهیم. بنابراین تا وقتی به شماره بلاک مورد نظر و اعمال این قوانین جدید برسیم، نسخه‌های قدیمی هم منسوخ شده‌اند.

وقتی به شماره بلاک مورد نظر نزدیک می‌شویم، من می‌توانم یک علامت هشدار بر روی نسخه‌های قدیمی نشان بدهم تا مطمئن شویم آن‌ها می‌دانند باید نرم‌افزار خود را به‌روزرسانی کنند.

لازم به ذکر است که در آن زمان شماره آخرین بلاک[1] ۸۳,۰۰۰ بود، پس تا بلاک شماره ۱۱۵,۰۰۰ به تعداد ۳۱,۵۰۰ یا حدود هفت ماه فاصله بود. هدف ساتوشی از نظر طرفداران بلاک‌های بزرگ واضح بود؛ ساتوشی این محدودیت را موقتاً در سیستم اعمال کرده و یک برنامه مشخص و روشن هم برای افزایش آن ارائه داده است.

1 Block height

با این حال، به طور کلی طرفداران بلاک‌های بزرگ همیشه همه جوانب کار را درنظر نمی‌گرفتند. می‌توان پیام ساتوشی مبنی بر استفاده نکردن از افزونه و افزایش بلافاصله سایز بلاک را به ناسازگاری با [نودهای] شبکه تفسیر کرد. سپس او موضع محتاط‌تری می‌گیرد و در ادامه راه‌حل‌هایی پیشنهاد می‌دهد که بتوان با استفاده از آن‌ها سایز بلاک را بدون دردسر افزایش داد. این روایت شباهت بیشتری به گفته‌های طرفداران بلاک‌های کوچک داشت.

نقل قول بعدی از ساتوشی که به‌طور گسترده‌ای توسط طرفداران بلاک‌های بزرگ به آن ارجاع داده می‌شود قدیمی‌تر است و به نوامبر سال ۲۰۰۸ برمی‌گردد، زمانی که بیت‌کوین هنوز راه نیفتاده بود و مربوط به بخشی است که او درباره توان شبکه برای پردازش تراکنش‌های به اندازه شبکه ویزا، یعنی حدود ۱۰۰ میلیون تراکنش در روز صحبت می‌کند. این نقل قول برای طرفداران بلاک‌های بزرگ بسیار مهم است و به وضوح با بسیاری از دیدگاه‌های آنان در مورد بیت‌کوین همسو است:

> خیلی قبل‌تر از زمانی که شبکه به این اندازه بزرگ شود، کاربران می‌توانند برای اطلاع از بروز مشکل «دو بار خرج شدن[1]» با خیال راحت از [مکانیزم] «بررسی پرداخت ساده[2]» (بخش ۸ [وایت‌پیپر]) استفاده کنند که فقط به زنجیره سربرگ بلاک‌ها[3] نیاز دارد و روزانه ۱۲ کیلوبایت است. فقط افرادی که می‌خواهند کوین‌های جدید خلق کنند (اینجا منظور ماینرها هستند. - م) باید در شبکه، نود داشته باشند. در ابتدا بیشتر کاربران در شبکه یک نود اجرا می‌کنند، اما از یک جایی به بعد که شبکه از یک حدی بزرگ‌تر شد، این کار به متخصصان مجهز به مزرعه سرورها[4] با سخت‌افزارهای خاص سپرده خواهد شد. این مزارع فقط یک نود در شبکه خود دارند و شبکه محلی[5] به آن نود متصل خواهد بود.

1 Double spend
2 Simplified Payment Verification
3 Block headers
4 Server farms
5 LAN

پهنای باند آنطور که فکر می‌کنید مانع انجام این کار نخواهد بود. یک تراکنش معمولی حدوداً ۴۰۰ بایت[1] است. (ECC بسیار فشرده است). هر تراکنش باید ۲ بار در شبکه منتشر[2] شود، پس می‌شود ۱کیلوبایت به ازای هر تراکنش. ویزا در سال مالی سال ۲۰۰۸ تعداد ۳۷ میلیون تراکنش یا به‌طور متوسط روزانه ۱۰۰ میلیون تراکنش را پردازش کرده است. این تعداد تراکنش به ۱۰۰ گیگابایت پهنای باند، به اندازه ۱۲ دی‌وی‌دی، یا ۲ فیلم HD که با قیمت‌های امروز حدود ۱۸ دلار هزینه دارد، نیاز خواهد داشت.

چندین سال طول می‌کشد که شبکه تا این اندازه بزرگ شود، و تا آن زمان ارسال ۲ فیلم HD روی شبکه اینترنت احتمالاً مشکل بزرگی به‌وجود نخواهد آورد.[3]

البته طرفداران بلاک‌های کوچک برای این [نقل قول ساتوشی] هم پاسخی دارند. آن‌ها ادعا می‌کنند که اظهارات ساتوشی را باید با فرض موجود بودن تکنولوژی بررسی پرداخت ساده یا همان SPV در نظر گرفت. به این معنی که در شرایط معمولی کیف پول‌های سبک[4] بدون نیاز به بررسی و تأیید همه تراکنش‌ها بتوانند اثباتِ دوبار خرج شدن[5] را در یک بلاک نامعتبر دریافت کنند. این تکنولوژی هنوز توسعه نیافته است و ممکن است توسعه آن اصلاً امکان‌پذیر نباشد. بنابراین برخی از طرفداران بلاک‌های کوچک استدلال می‌کنند ادعای ساتوشی مبنی بر رقابت با ظرفیت شبکه ویزا دیگر صدق نمی‌کند. این تا حدودی بحث برانگیز و تفسیر محدود معنای SPV است.

مطلبی که در زیر می‌آید پاسخ به ایمیل اصلی معرفی اولیه بیت‌کوین توسط ساتوشی و درواقع چند ماه قبل از انتشار و راه‌اندازی شبکه بیت‌کوین است. اولین پاسخ به ایمیل

1 Bytes
2 Broadcast
3 https://www.mail-archive.com/cryptography@metzdowd.com/msg09964.html
4 Light wallets
5 Proof of double spend

ساتوشی فقط یک روز بعد از مطرح شدن ایده [بیت‌کوین]، از شخصی به نام «جیمز ای دونالد[1]» و درباره ابراز نگرانی در مورد ظرفیت شبکه بیت‌کوین بود.

> برای شناسایی و مردود کردن به موقعِ یک تراکنش که [یک کوین را] دوبار خرج می‌کند، هر فرد باید [سابقه] اغلب تراکنش‌های گذشته را داشته باشد که اگر به‌صورت ساده‌لوحانه‌ای پیاده‌سازی شود، هر نود شبکه باید بیشتر تراکنش‌های گذشته یا تراکنش‌های اخیر را در اختیار داشته باشد. اگر صدها میلیون نفر بخواهند با یکدیگر تراکنش انجام دهند، به پهنای باند زیادی نیاز خواهد بود چون بیشتر افراد باید همه یا قسمتی از تاریخچه همه تراکنش‌ها را بدانند.[2]

یکی از نقل قول‌های ساتوشی که از جانب طرفداران بلاک‌های کوچک بیشترین ارجاع به آن داده می‌شود، زمانی است که ساتوشی از حضور یک رقیب برای نرم‌افزار بیت‌کوین به عنوان یک «تهدید برای شبکه» نام می‌برد و طراحی اصلی بیت‌کوین را در ماه جون سال ۲۰۱۰ طی گفتگویی با گوین اندریسن به صورت «ثابت و تغییرناپذیر[3]» معرفی می‌کند:

> ماهیت بیت‌کوین به‌گونه‌ای است که به محض انتشار نسخه `v0.1` طرح اصلی[4] تا آخر عمر [بیت‌کوین] بدون تغییر باقی خواهد ماند. به همین دلیل من می‌خواستم آن را طوری طراحی کنم که بتواند از هر نوع تراکنش ممکن پشتیبانی کند. مشکل این بود که هر موردی به کُد و فیلدهای داده‌ای مختص به خودش نیاز داشت، حالا خواه مورد استفاده قرار می‌گرفت، خواه نمی‌گرفت، و فقط همان یک مورد خاص را پوشش می‌داد. اگر این روش را پی می‌گرفتم با حجم زیادی از موارد خاص روبرو می‌شدم. راه‌حل، استفاده از یک اسکریپت بود که مسأله را طوری تعمیم دهد که طرفین معامله بتوانند تراکنش خود را به‌صورت یک «محمول[5]» (در نرم‌افزار به گزاره‌ای می‌گویند که با توجه به متغیرهایش می‌تواند درست یا نادرست باشد. – م)

1 James A Donald
2 https://www.mail-archive.com/cryptography@metzdowd.com/msg09963.html
3 Set in stone
4 Core design
5 Predicate

تعریف و ارزیابی آن را به شبکه بسپارند. اطلاعات مورد نیاز نودهای شبکه از تراکنش فقط تا حدی است که بتوانند درست بودن شرایط فرستنده را ارزیابی کنند.

این اسکریپت درواقع یک محمول است. یک معادله است که پاسخ آن یا درست است یا نادرست. محمول یک کلمه طولانی و ناشناخته است پس من اسم آن را اسکریپت می‌گذارم.

سمت گیرنده تراکنش، الگوی اسکریپت را بررسی می‌کند. در حال حاضر گیرنده فقط دو الگو را می‌پذیرد: پرداخت مستقیم و پرداخت به آدرس بیت‌کوین.
نسخه‌های بعدی نرم‌افزار می‌توانند الگوهای جدیدی را برای انواع تراکنش‌ها اضافه کنند و نودهایی که نسخه یکسان یا بالاتر از آن را اجرا می‌کنند قادر به دریافت آن‌ها هستند. همه نودهای شبکه صرف‌نظر از نسخه‌ای که اجرا می‌کنند می‌توانند هرگونه تراکنش جدیدی را تأیید [اعتبار] و پردازش کنند و به بلاک‌ها اضافه کنند، حتی اگر از آن‌ها سر درنیاورند.

این طرح از انواع گسترده‌ای از تراکنش‌هایی که من سال‌ها قبل طراحی کرده‌ام پشتیبانی می‌کند. [مثل] تراکنش‌های تضمینی[1]، قراردادهای اوراق قرضه[2]، میانجی‌گری شخص ثالث[3]، چند امضائی[4]، و غیره. این‌ها مواردی هستند که اگر بیت‌کوین همه‌گیر شود، در آینده می‌خواهیم رویشان کار کنیم ولی باید در اوایل راه طراحی شوند تا مطمئن باشیم بعداً امکان‌پذیر هستند.

من معتقدم یک نسخه دیگر که با شبکه سازگار است هرگز ایده خوبی نخواهد بود. همه نودهای شبکه باید در مرحله ارزیابی اسکریپت به نتایج یکسانی برسند و بخش زیادی از طراحی به این وابسته است. بنابراین یک نسخه جدید نرم‌افزار به عنوان

1 Escrow transactions
2 Bonded contracts
3 Third party arbitration
4 Multi-party signature

تهدیدی برای شبکه خواهد بود. مجوز MIT با سایر مجوزها و کاربردهای تجاری سازگار است، بنابراین از نظر مجوز نیازی به بازنویسی آن نیست.[1]

ساتوشی در طول دو سال اول حضور خود در فضای بیت‌کوین اظهارنظرهای زیادی کرد، و بسیاری از آن‌ها می‌توانست برای تأیید [دیدگاه‌های] هر دو طرف درگیر مورد استفاده قرار گیرد. در کل می‌توان گفت نقل قول‌های ساتوشی در مسائل محدود به محدودیت [سایز] بلاک و ظرفیت شبکه، از [دیدگاه‌های] طرفداران بلاک‌های بزرگ پشتیبانی می‌کرد، ولی از نظر انعطاف‌ناپذیری قوانین شبکه به نظر می‌رسید نقل قول‌های او به [دیدگاه‌های] طرفداران بلاک‌های کوچک نزدیک‌تر باشد. در این مرحله، درگیری بین دو طرف شبیه به مناقشات مذهبی شده بود و طرفین در میان نقل قول‌های ساتوشی به دنبال نظرات یا تفسیرهایی می‌گشتند که اهداف‌شان را تأیید کند.

اگرچه نظر ساتوشی را هم نباید خیلی ویژه و مهم تلقی کرد. بسیاری از طرفداران بلاک‌های کوچک این دیدگاه را بیان می‌کردند که [دیدگاه‌های] ساتوشی در حال حاضر موضوعیتی ندارند. حداقل نظرات پنج سال پیش او دیگر اهمیتی ندارند چون از آن زمان تا به امروز چیزهای زیادی تغییر کرده است. ما احتمالاً به‌دلیل تجربه شبکه [در دنیای واقعی و] در عمل، بیشتر از ساتوشیِ آن زمان درباره شبکه بیت‌کوین می‌دانیم. طرفداران بلاک‌های کوچک اغلب مدعی بودند بیت‌کوین یک دین نیست و ساتوشی هم یک پیامبر نیست. آن‌ها معتقد بودند تصمیمات باید فقط بر اساس شایستگی علمی گرفته شوند و نظر ساتوشی تفاوتی به‌وجود نمی‌آورد. هرچند بیت‌کوین برخی از ویژگی‌های مشابه یک دین را دارا است و به نظر می‌رسید افراد هم اینگونه احساس می‌کردند. به هر حال، ادیان بسیار موفق هستند و شاید این ویژگی‌ها در موفقیت بیت‌کوین نقشی ایفا کرده‌اند.

به نظر می‌رسد ساتوشی در بحثی که در سال ۲۰۱۵ درگرفته بود، مشارکت کرده است. همان روزی که نرم‌افزار Bitcoin XT منتشر شد، ایمیلی از یکی از آدرس‌های ایمیل

1 https://bitcointalk.org/index.php?topic=195.msg1611#msg1611

ساتوشی satoshi@vistomail.com ارسال شد که در آن بر استدلال طرفداران بلاک‌های کوچک تأکید می‌کند و مدعی می‌شود که او نظر خود را در مورد مقیاس‌پذیری تغییر داده است:

من بحث‌های اخیر در مورد سایز بلاک را از طریق گروه ایمیلی[1] دنبال می‌کردم. من امیدوار بودم که بحث به نتیجه برسد و همه بر روی پیشنهاد فورک به توافق گسترده برسند. با این حال با انتشار رسمی Bitcoin XT 0.11A احتمالاً این اتفاق نخواهد افتاد و بنابراین مجبورم که نگرانی‌هایم را در مورد این فورک بسیار خطرناک به اشتراک بگذارم.

توسعه‌دهندگان این مثلاً بیت‌کوین ادعا می‌کنند که از دیدگاه اصلی من پیروی می‌کنند ولی این کاملاً از حقیقت به دور است. هنگامی که من بیت‌کوین را طراحی کردم، آن را به گونه‌ای طراحی کردم که تغییرات آتی در قوانین اجماع بدون توافق اکثریت غریب به اتفاق [کاربران] دشوار باشد. بیت‌کوین طوری طراحی شده است که از نفوذ رهبران کاریزماتیک مصون باشد، خواه اسم آن‌ها گوین اندریسن باشد، خواه باراک اوباما، خواه ساتوشی ناکاموتو. تقریباً همه باید در مورد یک تغییر با یکدیگر به توافق برسند و نباید برای این کار تحت فشار قرار بگیرند یا مجبور شوند. روشی که این توسعه‌دهندگان برای توسعه فورک در پیش گرفته‌اند «دیدگاه اصلی»ای که مدعی پایبندی به آن هستند را درواقع نقض می‌کند.

آن‌ها از نوشته‌های قدیمی من برای تعریف چیستی بیت‌کوین استفاده می‌کنند. با این حال من تصدیق می‌کنم که از آن زمان چیزهای زیادی تغییر کرده است و معلومات جدید کسب شده است که با برخی از نظرات اولیه من مغایرت دارد. برای نمونه من پیش‌بینی استخراج مشترک[2] و تأثیرات آن بر شبکه را پیش‌بینی نکرده بودم. تبدیل بیت‌کوین به یک سیستم پولیِ رقابتی و در عین حال حفظ ویژگی‌های امنیتی آن مسأله پیش‌پا افتاده‌ای نیست و برای ارائه یک راه‌حل منسجم باید زمان

1 Mailing list
2 Pooled mining

بیشتری صرف کنیم. من گمان می‌کنم ما به انگیزه‌های بهتری نیاز داریم که بر اساس آن‌ها کاربران به‌جای صرفا اعتماد به نوع‌دوستی [دیگران]، نودهای خودشان را اجرا کنند.

اگر دو توسعه‌دهنده بتوانند بیت‌کوین را فورک کنند و در مواجهه با انتقادات فنی گسترده و با استفاده از تاکتیک‌های عوام فریبانه در بازتعریف «بیت‌کوین» موفق باشند، من چاره‌ای ندارم جز اینکه اعلام کنم پروژه بیت‌کوین شکست‌خورده است. قرار بود بیت‌کوین هم از نظر فنی و هم از نظر اجتماعی قوی باشد. وضعیت کنونی بسیار ناامید کننده است.[1]

بیشتر طرفداران بلاک‌های بزرگ این ایمیل را جعلی خواندند و به آن بی‌توجهی کردند. هرچند به نظر می‌رسید این ایمیل واقعاً از سمت Vistomail ارسال شده باشد. بنابراین یکی از این سه حالت ممکن بود: ۱. ایمیل ساتوشی هک شده بود. ۲. مسئولان Vistomail آن را ارسال کرده بودند. ۳. این ایمیل واقعاً از طرف ساتوشی بوده است. احتمال گزینه دوم بسیار پایین است، بنابراین احتمالاً یا پیام واقعی است یا حساب ایمیل او هک شده است. هک شدن حساب ایمیل کاملاً امکان‌پذیر است چون یک ایمیل دیگر ساتوشی به آدرس satoshi@gmx.com توسط شخصی و از روش بازنشانی گذرواژه[2] هک شده بود. این مسأله در هر صورت اهمیتی نداشت. اگر یک فرد مثل ساتوشی چنان نفوذی بر سیستم داشت که یک تنه می‌توانست آن را از این بحران نجات دهد، معلوم می‌شد بیت‌کوین نتوانسته از روزهای اولیه خود و وابستگی به یک فرد فاصله بگیرد. بیت‌کوین می‌بایست برای مقاومت در برابر فشارهای سهمگینی که به عنوان یک سیستم پول جنجالی در معرض آن‌ها قرار خواهد گرفت مقاوم باشد، و به یک فرد مشخص که می‌تواند به راحتی متوقف یا ناپدید شود متکی نباشد. شاید ناپدید شدن ساتوشی هم اصلاً به همین دلیل باشد. دوست داشتم بگویم این آخرین دخالت ساتوشی در این داستان است

1 https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-August/010238.html
2 Reset password

ولی متأسفانه ساتوشی، یا بهتر است بگوییم ادعاهایی در مورد ساتوشی دوباره وارد داستان خواهند شد.

در سال ۲۰۱۰ در مورد مسائل مربوط به مقیاس پذیری بحث‌هایی در می‌گرفت ولی اختلاف نظر قابل توجهی وجود نداشت؛ همه داشتند از بحث چیزهای جدید یاد می‌گرفتند. تا آپریل سال ۲۰۱۱ اوضاع اندکی تغییر کرد و اختلاف‌نظر شدیدی در مورد مسائل مربوط به مقیاس‌پذیری، کارمزد تراکنش‌ها و انگیزه‌های صنعت استخراج بیت‌کوین در درازمدت پدید آمد. همه با هم محترمانه رفتار می‌کردند ولی به نظر می‌رسید یک اختلاف‌نظر اساسی در عقاید افراد در حال شکل‌گیری است. کاربر انجمن گفتگوی BitcoinTalk با شناسه Vandroiy سؤالی را مطرح کرد: او اساساً پرسید وقتی پاداش ساختن بلاک کاهش یابد یا تمام شود، ماینرها چه انگیزه‌ای برای ادامه ماینینگ خواهند داشت. البته همه پاسخ این سؤال را می‌دانستند، همانطور که در وایت‌پیپر بیت‌کوین آمده «کارمزد تراکنش به انگیزه جدید ماینرها [برای ادامه کار] تبدیل خواهد شد[1]». البته Vandroiy در تاریخ ۲۲ آپریل سال ۲۰۱۱ پرسش چالش برانگیزی مطرح کرد:

> همه ماینرهای کوچکِ مستقل قصد دارند سودآوری خود را به حداکثر برسانند. تصمیم آن‌ها در انتخابِ تراکنش‌هایی که به بلاک اضافه می‌کنند، تغییر بزرگی در افزایش کارمزد ایجاد نخواهد کرد. بنابراین این ماینر کلیه تراکنش‌های موجود، حتی آن‌هایی که کارمزد کمی پرداخت می‌کنند را به داخل بلاک اضافه می‌کند تا حداکثر سود را ببرد. این منجر به افتِ کارمزد [در شبکه] می‌شود. این باعث می‌شود درآمد آن دسته از ماینرهایی که قبلاً سودآوری نداشتند بیشتر کاهش پیدا کند و دست بکشند. این باعث کاهش هش‌ریت[2] و درنتیجه آن کاهش سختی[3] می‌شود، و این حلقه تکرار می‌شود. با این استدلال، سختی شبکه احتمالاً تا نزدیک صفر کاهش یابد.[4]

1 https://bitcoin.org/bitcoin.pdf
2 hashrate
3 difficulty
4 http://archive.is/URni1

با تحلیل نظر Vandroiy از منظر اقتصادی، او اساساً می‌گفت که بهای اضافه کردن یک تراکنش به بلاک تقریباً صفر است و در یک فضای رقابتی، قیمت با بهای تمام‌شده رابطه دارد. در این صورت تراکنش‌ها با کارمزد پایین هم ماین خواهند شد و مشکل معروف به «مشکل مارپیچ مرگِ کارمزد[1]» رخ خواهد داد. ولی بازار کارمزد [در بیت‌کوین] یک بازار عادی نبود که تنها هدف آن رسیدن به یک قیمت تعادلی و ماین تراکنش‌ها باشد؛ برخی معتقد بودند که عوامل مثبت خارجی یا آن‌طور که در وایت‌پیپر آمده، اهداف دیگری در ایجاد انگیزه برای ماینرها اثر داشتند. اینکه آیا این مسأله واقعاً یک مشکل برای بیت‌کوین بود یا نه، بسیار بحث‌برانگیز بود. با خواندن این رشته مطالب[2] به نظر می‌رسد که تقریباً نیمی از افرادی که در آن شرکت داشتند فکر می‌کردند این یک مشکل است و نیمی دیگر معتقد بودند این موضوع مشکلی برای بیت‌کوین به‌وجود نخواهد آورد. حتی به نظر می‌رسید در ابتدا مایک هِرن هم با مشکل مارپیچ مرگِ کارمزد موافق است و اظهار داشت که به نظر او «قابل قبول به نظر می‌رسد». اگرچه او روز بعد در تاریخ ۲۳ آپریل سال ۲۰۱۱ موضع خود را تغییر داد و اعلام کرد که این موضوع مشکلی پیش نخواهد آورد:

> استدلال مارپیچ مرگ فرض را بر این می‌گذارد که من همه تراکنش‌ها را بدون درنظر گرفتن کارمزد / اولویت آن‌ها به بلاک اضافه می‌کنم، چون انجام چنین کاری برای من هزینه‌ای ندارد و چرا باید از درآمدی که از این کار حاصل می‌شود صرف‌نظر کنم؟ با این حال در دنیای واقعی شرکت‌های زیادی وجود دارند که می‌توانند این کار را انجام دهند ولی این کار را نمی‌کنند، چون آن‌ها درک می‌کنند که این امر کسب و کار خودشان را تضعیف خواهد کرد.[3]

به نظر می‌رسید اکثر افرادی که فکر می‌کردند مسأله مارپیچ مرگِ کارمزد مشکل‌ساز خواهد شد، به یک راه‌حل پیشنهادی بسنده کرده بودند: چون کاربران باید برای به‌دست

1 Fee death spiral problem
2 Thread
3 http://archive.is/URni1

آوردن فضای مورد نیاز [برای ماین شدن تراکنش‌هایشان] در بلاک‌هایی که پر هستند، با هم رقابت کنند [و کارمزد بالاتری پیشنهاد کنند]، پس محدودیت سایز بلاک از پایین آمدن کارمزد تراکنش جلوگیری خواهد کرد. بنابراین این محدودیت در سایز بلاک باعث ایجاد «مازاد تولیدکننده[1]» خواهد شد که می‌تواند برای ماینرها انگیزه ایجاد کند که بعد از تمام شدن پاداش بلاک [همچنان دستگاه‌های خود را روشن نگه دارند و] به کار خود ادامه دهند. در حالی که به نظر می‌رسید این اختلاف نظر باعث شکاف در جامعه کاربران بیت‌کوین شده است، اما این مسأله باعث نگرانی کسی نمی‌شد. به نظر می‌رسد تا چند سال مناظرات جدی بر روی این موضوع جای خود را به گفتگوهای محدود دادند. انگار طرفین این درگیری فرض را بر این گذاشته بودند که بیت‌کوین در مسیر دلخواه آن‌ها تکامل پیدا خواهد کرد. در سال ۲۰۱۳ به نظر می‌رسید مایک هِرن به اهمیت مشکل مارپیچ مرگِ کارمزد پی برده بود، ولی به‌جای محدودیت سایز بلاک، «قراردادهای تضمینی[2]» را به‌عنوان یک راه حل بالقوه پیشنهاد کرد.

اولین مورد از تبلیغات عمومی روی موضوع سایز بلاک ویدیویی بود که توسط توسعه‌دهنده بیت‌کوین و از طرفداران بلاک‌های کوچک یعنی «پیتر تاد[3]» تهیه شد. در ماه مه سال ۲۰۱۳ او یک ویدیو که به‌صورت حرفه‌ای تولید شده بود روی یوتوب[4] منتشر کرد. او در این ویدئو استدلال کرد که محدودیت سایز بلاک الزامی است، تا همه کاربران بیت‌کوین بتوانند همه تراکنش‌ها را تأیید کنند و بیت‌کوین به‌صورت غیرمتمرکز باقی بماند. در این ویدئو گفته می‌شد «به هرکس که می‌خواهد نرم‌افزاری که استفاده می‌کنید را تغییر دهد و محدودیت ۱ مگابایتی بلاک را افزایش دهد اعتنا نکنید»

1 Producer surplus
2 Assurance contracts https://bitcointalk.org/index.php?topic=157141.0;all
3 Peter Todd
4 YouTube https://www.youtube.com/watch?v=cZp7UGgBR0I

پیتر تاد همچنین به دلیل اینکه حامی اصلی قابلیتی به نام «جایگزینی تراکنش با کارمزد[1]» یا RBF بود، بسیاری از طرفداران بلاک‌های بزرگ را خشمگین کرده بود. این قابلیت به کاربران اجازه می‌دهد تراکنش بیت‌کوین خود را (قبل از ماین شدن) با تراکنش دیگری که همان ورودی[2] را خرج و کارمزد بالاتری پرداخت می‌کند، جایگزین کنند. ماینرهایی که از این قابلیت پیشتبانی می‌کنند ترجیح می‌دهند تراکنشی که کارمزد بالاتری پرداخت می‌کند را انتخاب کنند. در مقابل ماینرهایی که از این قابلیت پیشتیبانی نمی‌کردند و در عوض قابلیتی به نام «انتخاب تراکنشی که اول دیده شده[3]» را به‌کار می‌بستند، اولین تراکنشی که در شبکه مشاهده می‌کردند را انتخاب می‌کردند [و اعتنایی به تراکنش‌هایی که به دست آن‌ها می‌رسید و کارمزد بالاتری هم داشت نمی‌کردند].

در کل مایک، گوین، و طرفداران بلاک‌های بزرگ با قابلیت RBF مخالف بودند، در حالی که طرفداران بلاک‌های کوچک از آن حمایت می‌کردند. اختلاف‌نظرهایی که در مقوله RBF و سایز بلاک وجود داشت، با هم یک تفاوت اساسی داشتند؛ موضوع محدودیت سایز بلاک به پروتکل بیت‌کوین ارتباط داشت، در حالی که RBF به سیاست ماینرها [در انتخاب تراکنش‌ها] مربوط می‌شد. ماینرها در ارتباط با موضوع RBF مختارند هر سیاستی که می‌پسندند را انتخاب کنند و نیازی به توافق عمومی نیست. تمایز بین قوانین پروتکل بیت‌کوین و جنبه‌های دیگرِ آن، مثل RBF، برای طرفداران بلاک‌های کوچک بسیار مهم بود، در حالی که اکثر طرفداران بلاک‌های بزرگ یا اعتقادی به این تمایز نداشتند یا معتقد بودند به این اندازه اهمیت ندارد. برخی از آن‌ها معتقد بودند طرفداران بلاک‌های کوچک این قائله را برای رسیدن به اهداف خود ساخته‌اند. علی‌رغم این تمایز، بحث اصلی پیرامون RBF از جنبه اقتصادی تقریباً مشابه بحث درباره مشکل مارپیچ مرگِ کارمزد بود.

مخالفان RBF اظهار می‌کردند که این [قابلیت] به تجربه کاربری کاربران آسیب می‌رساند و احتمال رخ دادن مشکل دوبار خرج شدن[4] را بیشتر می‌کند، در حالی که مدافعان آن ادعا

1 Replace by Fee (RBF)
2 Transaction input
3 First seen safe (FSS)
4 Double spend

می‌کردند که ماینرها در هر صورت برای بیشتر کردن سود خود تراکنش‌هایی که کارمزد بیشتری پرداخت می‌کنند را انتخاب می‌کنند و چاره‌ای جز همسو کردن قوانین نرم‌افزار [بیت‌کوین] با این واقعیت نداریم. انتقاد طرفداران بلاک‌های بزرگ به این قابلیت این بود که از نظر آن‌ها ماینرها با توجه به وابستگی به کاربران بیت‌کوین، به تجربه کاربری آن‌ها اهمیت می‌دهند و دوست ندارند به آن آسیبی زده شود.

به نظر من کلید این معما در درجه اول به سطح رقابت در صنعت استخراج بیت‌کوین وابسته است. اگر صنعت استخراج بین چند بازیگر محدود و به‌صورت بسیار متمرکز بود، در این صورت سیاست FSS تا حدودی منطقی بود و مشکل مارپیچ مرگِ کارمزد هم موضوعیتی نداشت. زیرا در این صورت تصمیمات این ماینرها تأثیر قابلِ توجهی بر اکوسیستم، و به‌طور بالقوه بر درآمد آینده آن‌ها به عنوان ماینر می‌گذاشت. از طرف دیگر اگر سطح تمرکز در صنعت استخراج پایین باشد، تأثیر تصمیماتی که ماینرها می‌گیرند بر اکوسیستم کم‌تر است. در این صورت ممکن است ماینرها ترجیح بدهند سود کوتاه مدت خود را به حداکثر برسانند تا اینکه به تجربه کاربران خود اهمیت بدهند، و در هر صورت [با توجه به غیرمتمرکز بودن سیستم] عملکرد آن‌ها تأثیر چشمگیری بر روی شبکه نخواهد گذاشت. این مشکل غالباً به «تراژدی انبازه‌ها[2]» شناخته می‌شود. اگر اینطور باشد پس منطقی است که سیاست RBF را [بر روی شبکه] فعال و برای مشکل مارپیچ مرگِ کارمزد چاره‌ای بیاندیشیم.

درگیری‌ها بر سر RBF نقاط عطف مشابهی با مشکل سایز بلاک داشت:

- اولویت طرفداران بلاک‌های بزرگ بر روی اهداف کوتاه مدت بود، در حالی که طرفداران بلاک‌های کوچک بر اهداف بلندمدت تمرکز داشتند؛
- طرفداران بلاک‌های بزرگ تجربه کاربری را در اولویت قرار می‌دادند، در حالی که طرفداران بلاک‌های کوچک ترجیح می‌دادند شبکه مقاوم‌تر باشد؛

2 Tragedy of the commons

- طرفداران بلاک‌های بزرگ، رشد [سیستم] را اولویت می‌دانستند، در حالی که طرفداران بلاک‌های کوچک بیشتر نگران پایداری آن بودند.
- طرفداران بلاک‌های بزرگ بیشتر عمل‌گرا و بر روی کسب و کار متمرکز بودند، در حالی که طرفداران بلاک‌های کوچک که بیشترشان افراد باهوش در علوم کامپیوتر و رمزنگاری بودند، علمی و نظری به مسائل نگاه می‌کردند.

آن‌ها لزوماً روی موارد فنی با یکدیگر اختلاف نظر نداشتند، بلکه ترجیحات متفاوتی داشتند و اهمیت هریک از موضوعات مورد بحث را از زاویه متفاوتی با یکدیگر ارزیابی می‌کردند. و متأسفانه این منجر به نتیجه‌گیری‌های مختلفی می‌شد که به نظر می‌رسید هرگز با یکدیگر سازش نخواهند کرد.

روز چهارشنبه، ۱۵ آپریل سال ۲۰۱۵ یک رویداد رسمی از طرف «بنیاد بیت‌کوین[1]»، با عنوان DevCore در لندن برگزار شد. گوین هم در این رویداد شرکت داشت و آمده بود تا سخنرانی خود را با عنوان «چرا به زنجیره بزرگ‌تری [از لحاظ سایز بلاک] نیاز داریم» ارائه کند. من هم در این همایش شرکت کرده بودم. گوین خیلی خوش برخورد بود و از بحث درباره این موضوع استقبال می‌کرد. گوین به من تأکید کرد که ۱ مگابایت خیلی کم و مضحک است، و خیلی از صفحات وب بیشتر [از ۱مگابایت] هستند. از نظر او، تاریخچه فناوری اطلاعات نشان از رشد نمایی و سریع‌تر و بزرگ‌تر شدن همه چیز می‌داد. چند بار به «قانون مور[2]» به‌عنوان نمونه‌ای برای نشان دادن چگونگی بهبود سیستم‌ها در گذر زمان اشاره شد، و اینکه چطور در آینده بلاک‌های بیت‌کوین بزرگ‌تر خواهند شد و به سایز گیگابایت خواهند رسید و هیچگونه مشکل فنی در زمینه مقیاس‌پذیری پیش نخواهد آمد. گوین آهسته به من گفت که سایز مطلوب او ۲۰ مگابایت است ولی اگر [مخالفان] با او همراه شوند حاضر است کوتاه بیاید و به ۸ مگابایت راضی شود. چند روز

1 Bitcoin foundation
2 Moore’s law

بعد یعنی در ۱۸ آپریل سال ۲۰۱۵ مایک و گوین یک جلسه پرسش و پاسخ در لندن برگزار کردند. وقتی بحث سایز بلاک پیش آمد، گوین گفت:

> ممکن است از اختیاراتم استفاده کنم و بگویم به این صورت پیش خواهیم رفت، اگر آن را نمی‌پسندید این پروژه را ترک کنید. صادقانه بگویم، این همان اتفاقی است که در مورد P2SH افتاد؛ در نهایت گفتم به حرف همه شما گوش کردم و پیشنهادها را بررسی کردم، و به این صورت پیش خواهیم رفت.[۱]

در حین صحبت‌های او من یک نگاه سریع به حاضرین انداختم. اکثریت افراد از قدرتی که گوین داشت خوشحال به نظر می‌رسیدند. با این حال یک اقلیتی هم در حدود پنج درصد در میان حاضرین بود که از این موضوع تا حدودی عصبانی شدند و فکر می‌کردند این جملات گوین گستاخانه است و از این حرف‌ها خوششان نمی‌آمد. از نظر آن‌ها مسئولیت [تصمیم‌گیری برای] بیت‌کوین در اختیار گوین نبود؛ اگر قرار بود او از اختیاراتش استفاده و [سرخود] تغییراتی در بیت‌کوین ایجاد کند، پس بیت‌کوین برای چه به‌وجود آمده است؟ با ذکر P2SH او موضوع بحث‌برانگیزی که در ارتقاء قوانین بیت‌کوین به‌صورت سافت فورک در سال ۲۰۱۲ رخ داده بود را پیش کشید که در آن پیشنهادهای [فنی] مختلفی ارائه شده بود و گوین در نهایت روش اعمال قوانین جدید را انتخاب کرد[۲].

بعد از اتمام جلسه من همچنان آنجا بودم و کاملاً برای من روشن شد که مایک، گوین را تحت فشار قرار می‌دهد تا قضیه سایز بلاک موضع محکم‌تری بگیرد، در حالی که گوین کمی از این کار خودداری می‌کرد. حتی مایک از گوین می‌خواست دسترسی دیگر توسعه‌دهندگان بیت‌کوین را از مخزن کُد بیت‌کوین در گیت‌هاب[۳] مسدود کند و خودش کنترل مخزن را بر عهده بگیرد. از گفتگوی بیشتر با آن‌ها به نظر می‌رسید گوین در

1 https://www.youtube.com/watch?v=RIafZXRDH7w
2 https://bitcoinmagazine.com/articles/the-battle-for-p2sh-the-untold-story-of-the-first-bitcoin-war
3 Github

نهایت همانطور که مایک می‌خواست، موضع محکم‌تری بگیرد. هر دوی آن‌ها آشکارا فکر می‌کردند این موضوع تعیین کننده خواهد بود. ولی در آن زمان نمی‌دانستم چه زمانی گوین این کار را خواهد کرد و چه اقدام خاصی انجام خواهد داد.

در روز ۴ می سال ۲۰۱۵ گوین در وبلاگ خود مطلبی با عنوان «زمان پیاده‌سازی بلاک‌های بزرگ‌تر فرا رسیده است[1]» منتشر کرد. این قسمت اول از مجموعه مطالبی بود که او در آن‌ها سعی می‌کرد نگرانی‌هایی را که در مورد بلاک‌های بزرگ‌تر بود برطرف کند. به نظر گوین وقت آن رسیده بود که برای پیاده‌سازی بلاک‌های بزرگ‌تر [در شبکه بیت‌کوین] فشار بیاورد. در روز ۷ می سال ۲۰۱۵ «ولادمیر ون در لان[2]» نگهدارنده اصلی[3] پروژه Bitcoin Core روی گیت‌هاب، یادداشت زیر را در قالب یک ایمیل به گروه ایمیلی بیت‌کوین ارسال کرد:

> من اندکی با افزایش سایز بلاک در آینده نزدیک مخالف هستم. دلایل خودم را هم دارم. به اختصار، [از نظر من انجام این کار در کوتاه مدت] مسائل ذاتیِ عملی و سیاسی که باید برای برنامه‌ریزی یک هارد فورک در نظر گرفت را نادیده می‌گیرد.

Bitcoin Core نام پیاده‌سازی نرم‌افزار مرجع بیت‌کوین و نسل بعدی نرم‌افزاری بود که ساتوشی در ابتدا ساخته بود. این نرم‌افزار در ابتدا با نام Bitcoin یا Bitcoin-QT شناخته می‌شد، اما نام Bitcoin Core در فوریه سال ۲۰۱۳ و به پیشنهاد مایک هِرن انتخاب[4] و به‌عنوان نام جدید مورد استفاده قرار گرفت و اکنون کمی کنایه‌آمیز به نظَر می‌رسد. گوین قبلاً مالکیت مخزن پروژه بیت‌کوین روی گیت‌هاب را به ولادمیر سپرده بود تا بتواند بیشتر روی جنبه تحقیقاتی بیت‌کوین تمرکز کند. این اتفاق هم طنزآلود است، چون به نظر می‌رسد گوین کنترل پروژه را به ولادمیر داد تا بتواند بر روی موضوعاتی چون کارمزد تراکنش و فضای بلاک تحقیق کند. در آن زمان کاری که او می‌خواست انجام

1 https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg07472.html
2 Wladmir Van Der Laan
3 Lead maintainer
4 http://archive.is/kWqW0

دهد در مقایسه با کار طاقت‌فرسای نگهداری از پروژه بیت‌کوین، مهم‌تر به نظر می‌رسید و این‌طور نبود که گوین از قدرت کناره‌گیری کرده باشد. بعدها طرفداران بلاک‌های بزرگ‌تر، تصمیم گوین برای واگذاری کنترل پروژه به ولادمیر را به‌عنوان یک اشتباه مهم تلقی کردند.

با این حال طرفداران بلاک‌های کوچک معمولاً ادعا می‌کردند که ولادمیر قدرتی ندارد و در اختیار داشتن مخزن پروژه شبیه به نقش سرایدار آن است. تصمیم نهایی در مورد اضافه یا کم شدن کُد به پروژه تنها در صورت توافق گسترده بین همه توسعه‌دهندگان گرفته خواهد شد و در دست داشتن کنترل مخزن پروژه مهم نیست. علاوه بر این‌ها و از همه مهم‌تر، قوانین شبکه بیت‌کوین با تغییر دادن مخزن نرم‌افزار تعیین نمی‌شوند، بلکه توسط نرم‌افزاری که کاربران بیت‌کوین اجرا می‌کنند، تعیین می‌شوند. البته که می‌توان در مخزن پروژه یک نسخه جدید از نرم‌افزار منتشر کرد، ولی قابلیت به‌روزرسانی خودکار در سیستم وجود نداشت و از طرف دیگر نمی‌توان افراد را مجبور به ارتقاء نرم‌افزار کرد. این نمونه دیگری از تمایزهایی بود که برای طرفداران بلاک‌های کوچک بسیار با اهمیت بود ولی به چشم طرفداران بلاک‌های بزرگ نمی‌آمد و با آن موافق نبودند. از نظر طرفداران بلاک‌های بزرگ، قدرت بیش از اندازه‌ای در اختیار Bitcoin Core بود، بنابراین به سرعت به دشمن اصلی آن‌ها تبدیل شد.

صرف‌نظر از نظرات مختلف اشخاص در مورد قدرت نگهدارنده اصلی مخزن پروژه، اظهارنظر ولادمیر در باب اختلاف‌نظر «اندکی» که با افزایش سایز بلاک در آینده نزدیک داشت، از اهمیت بالایی برخوردار بود. به نظر می‌رسید با وجود لابی فوق‌العاده‌ای که از جانب گوین در جریان بود، این هارد فورک در Bitcoin Core ادغام[1] نخواهد شد و گزینه‌های گوین تا حدودی محدود است. در تاریخ ۲۹ می سال ۲۰۱۵ گوین قوی‌ترین نشانه از آنچه قصد انجام دادنش را داشت اظهار کرد: اینکه ممکن است نظر خود را عوض کند و از Bitcoin XT پشتیبانی کند و تمام توان خود را پشت یک پروتکل جایگزین

1 Merge

بیت‌کوین که با پروتکل فعلی ناسازگار است قرار دهد. با وجود ایمیل زیر که کاملاً شفاف بود، من هرگز باور نمی‌کردم که این یک تهدید باشد و فکر می‌کردم این نوعی تاکتیک [برای] مذاکره است.

> اگر به‌زودی به یک توافق نرسیم، در این صورت من برای بررسی یا تهیه افزونه‌های نرم‌افزاری[1] برای پروژه Bitcoin-Xt که مایک به‌راه انداخته است درخواست کمک خواهم کرد که در قدم اول و همچنین باگذشت زمان یک افزایش [سایز] بزرگ را اعمال می‌کند تا دیگر هرگز مجبور به تکرار این همه بحث و دشمنی [با یکدیگر] نباشیم.

> سپس برای لابی کردن با فروشندگان و پذیرندگان [بیت‌کوین] و صرافی‌ها و سرویس‌های تأمین کننده خدمات کیف‌پول آنلاین و دیگر شرکت‌هایی که بر بستر bitciond کار می‌کنند (و هرکسی که با من موافق باشد که ما هرچه سریع‌تر به بلاک‌های بزرگ‌تر نیاز داریم) درخواست کمک می‌کنم تا به‌جای Bitcoin Core نرم‌افزار Bitcoin-Xt را اجرا و به همه اعلام کنند که آن را اجرا کرده‌اند. ما می‌توانیم میزان مقبولیت [این نرم‌افزار را] از طریق نظارت بر نسخه‌هایی که کاربران در شبکه اجرا می‌کنند به‌دست آوریم.

> شاید تا زمانی که این اتفاق می‌افتد، توافق [عمومی] بر سر نیاز به بلاک‌های بزرگ‌تر حاصل شود؛ اگر چنین اتفاقی بیفتد که عالی می‌شود! نصب [و آماده‌سازی این نرم‌افزار جدید] به‌عنوان تست اولیه خواهد بود و آن‌ها برای بلاک‌های بزرگ‌تر آماده خواهند بود.

> اما اگر همچنان میان توسعه‌دهندگان اتفاق نظر وجود نداشته باشد ولی جنبش «بلاک‌های بزرگ‌تر از همین امروز[2]» [که پیشتر توضیح دادم] موفقیت‌آمیز باشد،

1 patches
2 Bigger blocks now

> من درخواست کمک می‌کنم تا ماینرهای بزرگ هم همین کار را انجام دهند و از راه مکانیزم رأی‌گیری سافت فورک به توافق اکثریت و سپس حتی بالاتر از اکثریت میان ماینرهایی که مایل به تولید بلاک‌های بزرگ‌تر هستند، برسیم. هدف از این فرآیند این است که به کسانی که [همچنان] تردید دارند ثابت کند که بهتر است از بلاک‌های بزرگ‌تر حمایت کنند وگرنه عقب می‌مانند، همچنین به آن‌ها فرصتی داده شود تا قبل از این اتفاق [یعنی اعمال قوانین جدید، نرم‌افزار خود را] به‌روزرسانی کنند.
>
> زیرا اگر نتوانیم در این مرحله به توافق برسیم، اختیار نهایی برای تعیین اجماع، کُدی است که اکثریت پذیرندگان [بیت‌کوین] و صرافی‌ها و ماینرها اجرا می‌کنند.[۲]

در ۲۱ جولای سال ۲۰۱۵ «پیتر والا[۳]» یکی دیگر از توسعه‌دهندگان بیت‌کوین که در گذشته با مایک هرن در گوگل مشغول به کار بوده است، یک پیشنهاد هارد فورک برای افزایش سایز بلاک ارائه داد. پیتر در این قائله یکی طرفداران بلاک‌های کوچک بود. به نظر من، این پیشنهاد درواقع یک مصالحه و جوابی به فشارهای گوین بود. این پیشنهاد به شماره BIP-103 شناخته می‌شد و در آن از ولادمیر ون در لان و یک توسعه‌دهنده دیگر به نام «گرگوری مکسول[۴]» قدردانی شده بود[۵] که نشان از حمایت بالقوه آن‌ها داشت. این پیشنهاد [افزایش سایز بلاک] درواقع هارد فورکی بود که در ژانویه سال ۲۰۱۷ فعال می‌شود و سایز بلاک را هر سال و تا سال ۲۰۶۳ به مقدار ۱۷/۷ درصد افزایش می‌دهد. این پیشنهاد، هیچگونه مکانیزمی برای فعال‌سازی معرفی نمی‌کرد و به نظر می‌رسید که قصد از ارائه آن این است که به‌عنوان یک کاتالیزور برای گفتگوهای بیشتر مورد استفاده قرار بگیرد و پس از دستیابی به توافق، یک روش فعال‌سازی برای آن تعیین شود.

2 https://sourceforge.net/p/bitcoin/mailman/message/34155307/
3 Pieter Wuille
4 Gregory Maxwell
5 https://github.com/bitcoin/bips/blob/master/bip-0103.mediawiki

به نظر من ارائه این پیشنهاد حرکت معناداری بود. برنامه افزایش سایز بلاک آن کمی محافظه‌کارانه به نظر می‌رسید، ولی با این حال من فکر می‌کردم این هم بخشی از مذاکره باشد. من انتظار داشتم گوین به آن واکنش مثبت نشان دهد، مثلاً یک پیشنهادی روی آن بدهد و طرفین به تدریج با هم همسو شوند. به نظر می‌رسید دو طرف درگیر آرام آرام در حال رسیدن به یک راه‌حل مشترک هستند. در کمال تعجب گوین و طرفداران بلاک‌های بزرگ هیچ واکنش مثبتی نسبت به BIP-103 نشان ندادند. از نظر آن‌ها افزایش سایز بلاک در این پیشنهاد به‌قدری کم است که بیشتر به یک توهین شبیه است تا پیشرفت. متأسفانه به نظر نمی‌رسید BIP-103 بتواند کمکی [در رفع اختلاف‌نظرها] کند. به نظر می‌رسید تقاضا [برای فضای بلاک] توسط تراکنش‌های بیت‌کوین از ۱۷/۷ درصد افزایش سالانه که در BIP-103 ارائه شده بود بیشتر باشد. در مقابل، طرفداران بلاک‌های بزرگ می‌خواستند این افزایش طوری اجرا شود که مطمئن شوند افزایش سایز بلاک از نرخ رشد تقاضای تراکنش‌های شبکه بیت‌کوین بیشتر باشد. حالا که دوطرف درگیر در این مناقشه خواسته‌های کاملاً متناقضی با یکدیگر داشتند، آیا می‌شد به یک راه‌حل مشترک رسید؟

از نظر طرفداران بلاک‌های بزرگ، تجربه کاربران بیت‌کوین اولویت اول بود. نکته کلیدی برای آن‌ها این بود که بلاک‌های پُر در شبکه نداشته باشیم وگرنه کاربران باید مدت زمان غیرقابل پیش‌بینی برای تأیید شدن تراکنش‌شان منتظر بمانند. اگر قرار باشد [شبکه] تا این اندازه غیر قابل اعتماد شود، کدام فروشگاه حاضر می‌شود پذیرنده بیت‌کوین شود؟ اگر کاربران را وادار کنیم تا برای به دست آوردن فضای بلاک [و تأیید تراکنش‌هایشان و تعیین کارمزد] با یکدیگر رقابت کنند، برخی از کاربران را از استفاده از بیت‌کوین محروم خواهیم کرد و آن‌ها به سراغ ابزارهای دیگر خواهند رفت. این یک استراتژی وحشتناک تجاری است. یک سیستم چطور می‌تواند عمداً دست رد به سینه کاربرانش بزند و موفق هم بشود؟

از نظر طرفداران بلاک‌های کوچک این موضوع مشکلی پدید نمی‌آورد. آن‌ها معتقد بودند بلاک‌های پُر بحرانی برای شبکه پیش نخواهند آورد و چه بسا نشانه موفقیت آن هستند. آن‌ها بیان می‌کردند که بیت‌کوین در حال رواج پیدا کردن است و یک سطع تعادل جدیدی در پذیرش کاربران جدید برای آن پدید خواهد آمد که منعکس کننده محدودیت سایز بلاک است. آن‌ها غالباً ایده طرفداران بلاک‌های بزرگ مبنی بر بالا رفتن هزینه کارمزد تراکنش و در نتیجه از دست دادن کاربران را دست می‌انداختند و می‌گفتند شبیه به این موردِ متناقض است که: «کسی به آنجا نمی‌رود... چون خیلی شلوغ است.»

علاوه بر این، طرفداران بلاک‌های کوچک معتقد بودند به هر حال بلاک‌های پُر هم ضروری هستند و هم اجتناب‌ناپذیر. و برای جلوگیری از وقوع مشکل مارپیچ مرگِ کارمزد هنگامی که پاداش ساخت بلاک کم می‌شود، ضروری است. همچنین لازم است چون باید مطمئن باشیم وقتی پاداش ساخت بلاک به مقدار ناچیزی تقلیل پیدا می‌کند، ماینرها همچنان بلاک می‌سازند و زنجیره را به جلو می‌برند. همیشه باید مقداری تراکنش بیشتر از ظرفیت و در انتظار تأیید شدن داشته باشیم تا ماینرها انگیزه برای ساختن بلاک‌ها داشته باشند و این برای شبکه بیت‌کوین حیاتی است. اگر بلاک‌ها پُر نباشند و تراکنش‌هایی در انتظار تأیید شدن در بلاک‌ها نداشته باشیم و ماینرها درآمدی نداشته باشند، چطور می‌توانیم از آن‌ها انتظار داشته باشیم به کار استخراج ادامه دهند؟ در این صورت ماینرها برای صرفه‌جویی در هزینه‌های انرژی دستگاه‌های خود را خاموش خواهند کرد و برای ادامه کار منتظر می‌مانند تا تعدادی تراکنش در انتظار تأیید [توسط کاربران] ساخته شود و این کار امنیت شبکه را به شدت کاهش می‌دهد. طرفداران بلاک‌های بزرگ این استدلال را وارد نمی‌دانستند. از نظر آن‌ها پاداش ساخت بلاک برای دهه‌ها برقرار بود و چرا [ماینرها] به‌خاطر مشکلی که در ۲۰ تا ۱۰۰ سال آینده رخ خواهد داد، کاری کنند که مشتریان خود را از دست بدهند؟

طرفداران بلاک‌های کوچک همچنین معتقد بودند که بلاک‌ها در هر صورت پُر خواهند شد. اگر قرار باشد فضای بلاک [بدون محدودیت] فراهم باشد، چرا از آن استفاده نکنیم؟ هرکسی می‌تواند هر چیزی که دوست دارد مثل مجموعه موسیقی یا اسناد رمزگذاری شده را روی بلاک‌چین ذخیره کند. آن‌ها استدلال می‌کردند که تقاضا برای یک فضای ذخیره‌سازی ارزان [که به‌طور غیرمتمرکز روی نودها تکثیر شده است] بسیار بالا است [و همه خواهان آن هستند]. بنابراین افزایش محدودیت سایز بلاک بالاتر از [میزان] تقاضا، کار احمقانه‌ای است. [حتی] یک نفر هم قادر است به راحتی کل این فضا را پر کند. پاسخ به این استدلال از جانب طرفداران بلاک بزرگ به مبحث انگیزه ماینرها برمی‌گشت؛ از نظر آن‌ها ماینرها این کار را نمی‌کردند و اجازه نمی‌دادند این مقدار داده در بلاک قرار بگیرد. علاوه بر این، طرفداران بلاک‌های بزرگ اظهار می‌کردند که در طول پنج سال اول فعالیت بیت‌کوین، بلاک‌ها پُر نمی‌شدند و این مسأله مشخصاً در موفقیت [این پروژه] مؤثر بوده است. چرا باید ریسک کنیم و این شرایط را [با بلاک‌های پُر] تغییر دهیم؟

متأسفانه جامعه فعالان بیت‌کوین به اتفاق‌نظر نمی‌رسیدند و گوین هم نقشه خود را پیش می‌برد. گفته می‌شود در ژوئن سال ۲۰۱۵ گوین نظر برخی از ماینرها و استخرهای استخراج چینی را در مورد پیشنهاد [افزایش سایز بلاک خود] پرسیده است[1]. جلسه‌ای در پکن برگزار شده و گفته می‌شود در آن ماینرها با توجه به ضعیف بودن زیرساخت‌های ارتباطی و دشواری در انتشار بلاک‌هایی به این بزرگی، با افزایش سایز بلاک به ۲۰ مگابایت مخالف کرده‌اند. بنابراین گویا بر روی بلاک‌های ۸ مگابایتی با یکدیگر توافق کرده‌اند. گوین هم در پشت صحنه خود را برای اجرای برنامه خود در ماه آگوست که تنها چند هفته به آن مانده بود آماده می‌کرد.

1 https://bitco.in/forum/threads/gold-collapsing-bitcoin-up.16/page-712#post-25018

در بخش پرسش و پاسخ سایت Bitcoin XT آمده بود:

> تصمیمات بر پایه توافق بین مایک و گوین گرفته می‌شوند و در صورت بروز اختلافات جدی، تصمیم نهایی با مایک است.[1]

در بخشی از جامعه بیت‌کوین این تصور تقویت شد که همه این اتفاقات برای این است که مایک قدرت را در دست بگیرد. اصلاً مایک چه‌کاره است که باید تصمیم نهایی را بگیرد؟ کسی مشکلی با شخص مایک نداشت، [اتفاقاً] به نظر می‌رسید پسر خوبی است، ولی مشکل اصلی اینجا بود که به نظر نمی‌رسید اعلام این موضع به این روشنی، رویکرد درستی باشد. بیت‌کوینرها دوست دارند احساس کنند که کنترل در اختیار آن‌ها است، آن‌ها می‌خواهند صاحب‌اختیار [دارایی‌شان] باشند و استقلال مالی داشته باشند. این به هیچ وجه پیامی نبود که Bitcoin XT [به کاربران] مخابره کند و به نظر می‌رسید بیش از حد بر روی مایک متمرکز شده است. دومین اشتباه بزرگ طرفداران بلاک‌های بزرگ هم همین بود، Bitcoin XT بیش از آنکه پشت سر کاربران بیت‌کوین قرار گیرد، به مایک مرتبط می‌شد. شاید اگر این نرم‌افزار تمرکزش را حول گوین قرار می‌داد، احتمال موفقیتش بیشتر می‌شد.

1 https://archive.is/KoknZ#selection-311.0-311.128

فصل سوم

اولین کنفرانس مقیاس‌پذیری بیت‌کوین – مونترال

در روزهای آخر هفته، ۱۲ و ۱۳ سپتامبر سال ۲۰۱۵، کنفرانسی با عنوان «فاز اول مقیاس‌پذیری بیت‌کوین[1] ۲۰۱۵» در مونترال کانادا برگزار شد. این کنفرانس درواقع تلاشی بود برای کمک به حل منازعاتی که در آن زمان جامعه فعالان بیت‌کوین را آزار می‌داد. حداقل فرصتی بود تا شخصیت‌های برجسته هر دو طرف درگیر با یکدیگر گفتگو کنند. به نظر می‌رسید بیشتر بحث‌ها تا آن موقع از طریق انجمن‌های گفتگو انجام شده بود و تصور می‌شد احتمالاً افراد بتوانند از طریق بحث‌های رو در رو درک بهتری از دیدگاه‌های همدیگر داشته باشند، کسی هم منکر کارآمد بودن آن‌ها نبود.

مهم‌تر از همه اینکه، بازیگران اصلی هر دو طرف یعنی گوین اندریسن (به نمایندگی طرفداران بلاک‌های بزرگ) و گرگوری مکسول (به نمایندگی از طرفداران بلاک‌های کوچک) در این کنفرانس حضور داشتند. گرگوری یکی از توسعه‌دهندگان بیت‌کوین و طرفدار سرسخت و سازش‌ناپذیر بلاک‌های کوچک بود و نسبت به دیگران به هیچ وجه حاضر نبود از مواضع‌اش کوتاه بیاید. گرگوری فوق‌العاده باهوش بود و به نظر من درک عمیقی از حوزه‌های مختلفی که به بیت‌کوین ارتباط پیدا می‌کردند، از علوم کامپیوتر و

1 Scaling Bitcoin 2015 Phase 1

رمزنگاری گرفته تا نظریه بازی[1] و مشوق‌ها[2] داشت. بعضی اوقات به او جادوگر بیت‌کوین می‌گفتند. اولین مطلب عمومی او در سایت BitcoinTalk در ماه می سال ۲۰۱۱ در مورد کارمزد تراکنش بیت‌کوین و انگیزه برای استخراج بود، و در آن دلیل ضروری بودن کارمزد برای تأمین امنیت شبکه [بیت‌کوین] را توصیف می‌کرد.

گرگوری در سال ۲۰۱۴ از مؤسسان شرکت Blockstream بود، شرکتی که به نظر می‌رسید از طرفداران بلاک‌های کوچک تشکیل، و بر پایه یک مدل تجاری وابسته به بالا بودن کارمزد تراکنش [در شبکه] بنا شده بود و راه‌حل‌های بالقوه‌ای برای حل این مشکل ارائه می‌داد. مشکلی که از نظر طرفداران بلاک‌های بزرگ [اصلاً] وجود نداشت، یا به‌طور دقیق‌تر نباید وجود داشته باشد. بنابراین شرکت Blockstream برای طرفداران بلاک‌های بزرگ منفور بود. چون به نظر آن‌ها این شرکت تضاد منافع مالی، و برای کوچک نگه داشتن [سایز] بلاک‌ها انگیزه داشت. در دفاع از شرکت Blockstream می‌توان گفت، شواهد قابل توجهی وجود دارد که نشان می‌دهد بسیاری از بنیان‌گذاران و کارمندان این شرکت مدت‌ها قبل از پیش آمدن قائله سایز بلاک از ایده بلاک‌های کوچک پشتیبانی می‌کردند. به نظر می‌رسد برخی از طرفداران بلاک‌های بزرگ ترتیب علت و معلول را برعکس متوجه شده بودند. به نظر من کارکنان شرکت Blockstream به دلیل دیدگاهی که از قبل در مورد مقیاس‌پذیری بیت‌کوین داشتند به این شرکت پیوستند، نه اینکه به این شرکت بپیوندند و بعد به این دیدگاه رسیده باشند. از طرف دیگر سوگیری تأییدی و تفکر گروهی[3] مشکلاتی واقعی هستند و احتمالاً هرکدام به اندازه‌ای در این قضیه تأثیرگذار بوده‌اند. با این حال، برخلاف ادعاهای تئوری توطئه پردازان[4]، هیچ‌کس در شرکت Blockstream عمداً بدخواه نبود و قصور در استدلال‌های شناختی ناخودآگاه بود. این مسأله در مورد گوین و طرفداران بلاک‌های بزرگ هم صادق است.

1 Game theory
2 Incentives
3 groupthink
4 conspiracy theorists

گرگوری شخصاً در مباحث مربوط به این مسأله در Reddit بسیار فعال، و به یکی از چهره‌های شاخص این فضا تبدیل شده بود. از نظر او روند توسعه بیت‌کوین بسیار پیچیده و علمی و نیازمند برقرار کردن تعامل میان مسائل چالش برانگیز فنی مختلفی است. او از مشارکت توده ناآگاه [به مسائل فنی] در روند تصمیم‌گیری استقبال نکرد و آن‌ها را به تماشاگرانی با کلاه‌های بوقی در یک مسابقه اتومبیل‌رانی تشبیه می‌کرد که درباره نحوه مهندسی ماشین‌های مسابقه نظر می‌دهند.

> با استفاده از تشابه با مسابقات اتومبیل‌رانی، یک تیم فنی ماشین‌های مسابقه را فرض کنید که پیستون‌های سخت شده[1]، سیستم مدار بسته کنترل مخلوط شدن سوخت و هوا، نیتروس، و سیستم‌هایی که به تازگی ابداع شده‌اند را بر روی ماشین نصب کرده‌اند و قصد دارند برای آن یک توربوشارژر بسازند و در کنار همه این فعالیت‌ها، از پیست مسابقه نگهداری می‌کنند و بدنه ماشین را رنگ می‌کنند که چون به‌سادگی توضیح داده می‌شود [این کار] بیشتر از کارهای دیگرشان به چشم می‌آید. و در حالی که آن‌ها مشغول بحث جدی در مورد نسبت فشرده‌سازی و سوخت با اکتان بالا و اینکه احتمالاً باتوجه به تکنولوژی‌هایی که امروزه در دسترس هستند نمی‌توان به سرعتی بالاتر از سرعت فعلی رسید، یک بنده‌خدایی در حاشیه پیست با یک کلاه بوقی ایستاده و به شما می‌گوید: «بچه‌ها نگران نباشید و ترمز ماشین را حذف کنید!» و جمعیت هم با این حرف به وجد می‌آید و می‌گوید: بالاخره یکی پیدا شد که به موضوع سرعت ماشین اهمیت می‌دهد.

گرگوری به دلیل حمایت از بلوک‌های کوچک «گرگوری یک مگابایتی[2]» لقب گرفت و شاید بتوان گفت طرفداران بلاک‌های بزرگ از او بیشتر از هر کس دیگری نفرت داشتند.

1 hardened pistons
2 One Meg Greg

به دلیل علاقه شدیدی که به بحث سایز بلاک داشتم و با توجه به شرکت‌کنندگان آن، احساس کردم باید در کنفرانس کانادا شرکت کنم. من فکر می‌کردم که شاید گوین و گرگوری در فضای آزادی که فراهم می‌شود با یکدیگر درباره مسائل بحث کنند و در جهت حل اختلافات پیش روند و مشتاقانه انتظار آن را می‌کشیدم. در آن زمان من در لندن در یک شرکت مدیریت سرمایه‌گذاری به نام Ruffer کار می‌کردم و مرخصی‌های محدودی برایم باقی‌مانده بود و نمی‌توانستم کارم را ترک کنم. با این حال چون کنفرانس در آخر هفته برگزار می‌شد طوری برنامه‌ریزی کردم که بتوانم هم در کنفرانس شرکت کنم و هم اول هفته سر کارم حاضر شوم. من می‌توانستم با توضیح اهمیت این سفر به شرکتی که در آن کار می‌کردم آن را به یک سفر تحقیقی تبدیل کنم و برنامه سفر را از فشردگی در بیاورم ولی با توجه به شناختی که از دیدگاه مدیران این شرکت داشتم احساس می‌کردم نظر کلی آن‌ها نسبت به بیت‌کوین منفی است و به همین خاطر از این تصمیم منصرف شدم.

البته پنج سال بعد از اجرا شدن این کنفرانس و در زمانی که مناقشه سایز بلاک تبدیل به یک واقعه تاریخی شده بود که داشت کم کم از ذهن‌ها پاک می‌شد، شرکت Ruffer برای مشتریانش ۷۰۰ میلیون دلار آمریکا بیت‌کوین خرید که یک لحظه تاریخی در اکوسیستم تجاری کشوری مثل بریتانیای کبیر بود. چون خرید بیت‌کوین از جانب یک شرکت معروف و محافظه‌کار مثل Ruffer تأثیر قابل‌توجهی بر درک مؤسسات مالی از آن داشت.

من حدود ساعت ۲ بامداد شنبه به وقت محلی به هتل خود در کانادا رسیدم که با محل کنفرانس فاصله کمی داشت. بسیار خسته بودم ولی توانستم به یک پادکست یک ساعته درباره مناقشه سایز بلاک و بحثی میان گوین و «آدام بک[1]» گوش دهم. آدام بک تنها شخصی بود که در متن اصلی وایت‌پیپر بیت‌کوین به ایده Hashcash او که در سال ۱۹۹۷ مطرح کرده بود ارجاع داده شده بود، و او در نهایت به یکی از شخصیت‌های اصلی در

1 Adam Back

بحث سایز بلاک تبدیل شد و از طرفداران بلاک‌های کوچک بود. آدام بک رئیس شرکت Blockstream بود. در این زمان به نظر می‌رسید آدام نسبت به گوین موضع متعادل‌تری داشت و از ایده افزایش سایز بلاک در فواصل دوساله به ۲ و ۴ و در نهایت ۸ مگابایت حمایت می‌کرد (BIP-248). به نظر نمی‌رسید این پیشنهاد خیلی با چیزی که گوین می‌خواست فاصله داشته باشد، تنها موردی که آدام با آن مخالف بود افزایش مداوم تا ۸,۰۰۰ مگابایت بود که گوین از آن حمایت می‌کرد. خاطرم هست که گوین در آن در پادکست از ساتوشی نقل قول می‌کرد که گفته بود نودها می‌توانند پردازش تراکنش‌ها را در مراکز داده[1] انجام دهند. آدام پاسخ داد که امروزه عملیات استخراج متمرکزتر از زمانی است که ساتوشی در پروژه فعالیت می‌کرده است. این تمرکز در استخراج موازنه را بهم می‌زد یعنی اهمیت اجرای نود توسط کاربران به منظور حفاظت از قوانین و غیرمتمرکز نگه داشتن شبکه بیش از گذشته اهمیت پیدا کرده است. درک این نکته ضروری است که وقتی ساتوشی در پروژه فعال بوده، بین نودهایی که ماین می‌کردند و نودهایی که از قوانین شبکه محافظت می‌کردند تمایزی وجود نداشته است. آن‌ها اساساً یک چیز بوده‌اند. ولی تا سال ۲۰۱۵ اوضاع تغییر کرده بود و مزارع استخراج تخصصی بیت‌کوین مشغول فعالیت بودند.

من ساعت ۸ صبح روز شنبه به محل کنفرانس رسیدم و چند صد نفر مهمان در آنجا حضور داشتند. جو آنجا آرام و ساکت بود. به نظر می‌رسید بیشتر افراد در آنجا یکدیگر را نمی‌شناسند و ناظران کنجکاو این بحث هستند و در آن شرکت نمی‌کنند. به نظر می‌رسید واقعاً ترکیب خوبی از افراد در هر دو طرف بحث شرکت کرده‌اند و من احساس کردم این رویداد مفید و اثربخش است. بیشتر گفتگوها بر روی جنبه‌های علوم کامپیوتریِ مقیاس‌پذیری بیت‌کوین متمرکز بود و تأکید ویژه‌ای بر روش علمی و هرگونه تجزیه و تحلیل داده‌ای و آماری محدودیت‌های فنی شبکه داشت. به نظر می‌رسید که برگزارکننده اصلی این رویداد «پیندار وانگ[2]»، عضو سابق هیئت مدیره ICANN بود که در زمینه حکمرانی اینترنت تخصص داشت و از گردانندگان یکی از اولین «تأمین کنندگان

1 Data centre
2 Pindar Wong

سرویس اینترنت[1]» جهان بوده است. بیشترین تمرکز در این کنفرانس اشاره به درس‌هایی بود که می‌توان از اختلافات حکمرانی در نهادهای مسئول اینترنت، مثل گروه ویژه مهندسی اینترنت[2] (IETF) گرفت و احتمالاً از آن‌ها [برای حل اختلافات] در بیت‌کوین استفاده کرد.

دو تا از سخنرانی‌ها بیشتر از بقیه نظر من را به خود جلب کردند: یکی از آن‌ها «پیتر رایزن[3]» بود که اقتصاد سایز بلاک، و دیگری «جف گارزیک[4]» بود که پیشنهادهای مختلف ارائه شده برای سایز بلاک را مرور می‌کرد. صحبت‌های پیتر بر محور تئوری اقتصادی پشت سایز بلاک بود. او معتقد بود مشکل مارپیچ مرگِ کارمزد رخ نخواهد داد چون حتی بدون محدودیت روی سایز بلاک، یک بازار کارمزد برای تراکنش‌ها پدید خواهد آمد. هرچند او اظهار کرد که در تئوری خود تورم غیر صفر را در نظر گرفته است، که در چشم‌انداز کوتاه مدت و میان مدت مشکلی پدید نخواهد آورد. این فرض برای کسانی که روی پایداری بلند مدت سیستم متمرکز بودند، منطقی به نظر نمی‌رسید. پیتر محدودیت بلاک را شبیه به تعیین سهمیه تولید[5] [در یک اقتصاد غیر آزاد] در نظر می‌گرفت که مانع بزرگی برای بازار آزاد است.

از نظر او بازار آزاد قادر بود کارمزد تراکنش را به روش کارآمدتری تعیین کند. او سخنان خود را با اشاره به سانسور شدن کسانی که طرفدار حذف سهمیه تولید و حملات DDos به شبکه و استخرهای استخراج بیت‌کوین از طریق حذف محدودیت سایز بلاک، مثل نرم‌افزار Bitcoin XT و استخر استخراج Slushpool بودند، پایان داد. او همچنین اشاره کرد که نودهایی که از مفهوم سهمیه تولید حمایت می‌کنند در حال از بین رفتن هستند و یک چارت روی صفحه انداخت که نشان می‌داد دو درصد از نودهای شبکه بیت‌کوین در ۱۵ آگوست سال ۲۰۱۵ نرم‌افزار Bitcoin XT را اجرا می‌کردند و این رقم

1 ISP
2 Internet Engineering Task Force
3 Peter Rizun
4 Jeff Garzik
5 production quota

تا ۳۰ آگوست سال ۲۰۱۵ به ۱۵ درصد افزایش یافته است. سپس پیتر پیش‌بینی کرد که ایده سهمیه تولید شکست خواهد خورد.

> بیت‌کوین سدهای ساخته شده توسط گروه‌های ذی‌نفوذی که سعی دارند جلوی جریان عظیم تراکنش‌های شبکه را بگیرند خواهد شکست. این حرف آخر من در مورد بازار کارمزد تراکنش‌ها است.

عبارت Stream در متن بالا به وضوع اشاره‌ای داشت به شرکت Blockstream و باعث خنده حاضران شد. برخی از طرفداران بلاک‌های کوچک که حساس‌تر از بقیه بودند زیر لب غرغر کردند و معتقد بودند این کارهای تحریک‌آمیز موجب از بین رفتن روحیه همکاری در کنفرانس خواهد شد.

سخنرانی شایان ذکر بعدی، ارائه جف گارزیک با عنوان «مسائل تاثیرگذار بر روی پیشنهادهای افزایش سایز بلاک» است. جف یکی دیگر از توسعه‌دهندگان اولیه بیت‌کوین بود و همانطور که در فصل دوم توضیح دادیم، پیشنهاد حذف محدودیت سایز بلاک را چند هفته بعد از اعمال شدن آن در سال ۲۰۱۰ [توسط ساتوشی] داده بود. علی‌رغم این، جف در برخورد با مسائل مربوط به سایز بلاک همیشه میانه‌رو بود و اغلب به نظرات هر دو طرف درگیر در بحث توجه می‌کرد. به نظر می‌رسید او تلاش می‌کند خود را در موقعیتی قرار دهد تا بتواند شکاف پدید آمده بین این دو طرف را از بین ببرد و ظاهراً هیچ‌وقت از Bitcoin XT حمایت نکرده بود. با این حال، به نظر می‌رسید او علاقه دارد تا هرچه سریع‌تر تصمیمی گرفته شود و حوصله طرفداران بلاک‌های کوچک را هم نداشت. او در صحبت‌های خود تأکید کرد که محدودیت ۱ مگابایتی در معرفی و بازاریابی بیت‌کوین مشکلاتی به‌وجود خواهد آورد و باعث منصرف شدن شرکت‌ها از کار کردن با بیت‌کوین خواهد شد.

مسأله دیگر موضوعی است که من به آن مشکل Fidelity می‌گویم.
Fidelity یکی از بسیاری از شرکت‌های وال‌استریت است که قصد دارد آزمایشاتی بر روی بیت‌کوین انجام دهد و این شرکت به همراه دیگر شرکت‌های علاقه‌مند معتقدند اگر برنامه‌های اولیه خود را شروع کنند، حداکثر ظرفیت شبکه بیت‌کوین را اشغال خواهند کرد. بنابراین این موضوع باعث می‌شود این پروژه‌ها هرگز آغاز به کار نکنند و رشدی که در انتظار آن بوده‌ایم را هرگز نخواهیم دید.

بعدازظهر، کنفرانس به گروه‌های کوچکتری تقسیم شد و من و یک گروه پنج یا شش نفره به همراه گوین در یک تیم بودیم. دیگران درمورد درس‌هایی که می‌توان از اختلافات پدید آمده در پروتکل‌های رمزنگاری آموخت مانند تصمیمات بحث‌برانگیز نحوه انتخاب یک عملگر هش[1] صحبت می‌کردند و معتقد بودند نیاز به گفتمان و صبر داریم. در مورد مفهوم «اجماع کلی[2]» صحبت شد و روشی که نهاد IETF از آن استفاده کرده و شامل قضاوت «حس گروه[3]» است.

گروه‌های کاری از طریق فرآیند «اجماع کلی» تصمیم‌گیری می‌کنند. اجماع مورد نیاز در IETF نیازی به توافق میان همه طرفین درگیر ندارد اگرچه ترجیح بر این است که اینطور باشد. به‌طور کلی دیدگاه غالب یک کارگروه بر دیگر نظرات چیره می‌شود. (با این حال باید توجه داشت که «تسلط» بر اساس اندازه گروه یا قدمت آن تعیین نمی‌شود و صرفاً یک توافق کلی است) رسیدن به توافق می‌تواند با اشاره دست، زمزمه کردن یا هر وسیله دیگر مورد قبول کارگروه‌ها انجام پذیرد. توجه داشته باشید که توافق ۵۱ درصدی به معنی رسیدن به اجماع کلی نیست و یک توافق ۹۹ درصدی هم دیگر یک توافق کلی نیست. تعیین اینکه آیا یک توافق کلی بین طرفین حاصل شده است یا خیر بر عهده مسئول است.

1 hash function
2 rough consensus
3 sense of the group

سپس نوبت گوین بود که سخنرانی کند. او اساساً گفت همه این صحبت‌ها در مورد گفتگو و صبر خیلی خوب بود ولی در برخی از مواقع باید یک تصمیم نهایی گرفته شود و یک فرد یا یک فرآیند باید در جایگاه تصمیم‌گیری قرار بگیرد. از نظر او مشکل در این بود که هیچ‌کس نمی‌دانست که چه کسی و چگونه باید این تصمیم را بگیرد. آنچه می‌گفت منطقی بود، با این حال من احساس کردم او مستأصل شده و صبرش رو به اتمام است. اصلاً عجیب نبود چون او به‌عنوان یکی از افرادی که همه توجه‌ها به سمت او متمرکز بود، فشار بسیار زیادی را تحمل می‌کرد. من در آن زمان برای گوین برای شرکت در این مباحث احترام زیادی قائل بودم، چون او می‌توانست مثل مایک هِرن راه ساده‌تر را انتخاب کند و حتی به خودش زحمت شرکت در این کنفرانس را ندهد.

اولین ملاقات حضوری من با گرگوری مکسول در این کنفرانس بود. تصور من از او با خواندن مطالبی که در انجمن‌های آنلاین می‌نوشت این بود که او فوق‌العاده باهوش است، شخصیتی قوی دارد، فکری تیز دارد و تا حدودی در مقابل افرادی که درک فنی ضعیفی از برخی از مفاهیم علوم کامپیوتر مرتبط با بیت‌کوین دارند، کم صبر و تحمل است. من از دیدن شخصیت واقعی او بسیار متعجب شدم. او به نظر آرام، کنجکاو، مؤدب، متفکر، و روشن‌فکر بود و با گرگوری که من انتظارش را داشتم، بسیار تفاوت داشت.

در راهروهای کنفرانس و در یکی از جلسات استراحت متوجه شدم که گوین و گرگوری نزدیک به یکدیگر نشسته و شروع به صحبت کرده‌اند. این همان چیزی بود که بسیار از شرکت‌کنندگان در این کنفرانس امیدوار بودند ببینند، آن‌ها می‌خواستند افراد کلیدی هر دو گروه در این مورد با هم بحث کنند. باگذشت زمان تعداد افرادی که برای دیدن این مناظره دور آن‌ها جمع شده بودند بیشتر و بیشتر شد، چون می‌خواستند بحث را دنبال کنند. گفتگوی آن‌ها بر روی مسائل مورد درگیری متمرکز نبود و آرام آرام سرد شد. هر دوی آن‌ها به نظر معذب می‌آمدند، به‌خصوص گرگوری. او ترجیح می‌داد در قالب انجمن‌های آنلاین بحث کند تا همه افراد درگیر و طیف وسیعی از افراد بتوانند بحث را دنبال کنند.

بنابراین اگر قرار باشد تصمیمی برای تغییر پروتکل بیت‌کوین گرفته شود این تصمیم نباید در این فضاهای بسته گرفته شود. بنابراین این گفتگو به سرعت به پایان رسید و مطالب زیادی توسط آن‌ها مطرح نشد.

قالب و چهارچوب این کنفرانس به سمت دیدگاه طرفداران بلاک‌های کوچک و روشی که به نظر آن‌ها درست بود و کارها باید بر طبق آن پیش می‌رفت، متمایل بود. به جای [صرفاً] تصمیم‌گیری، بر علم و گفتگو تأکید شده بود و این شایستگی علمی دقیقاً روشی بود که طرفداران بلاک‌های کوچک می‌خواستند فضا به سوی آن تکامل پیدا کند. به نظر می‌رسید رویکرد طرفداران بلاک‌های بزرگ بیشتر تجاری است و آن‌ها معتقد بودند بیت‌کوین یک پروژه علمیِ نظری نیست، بلکه یک سیستم در حال کارِ جهانی است و کاربران واقعی دارد. به طور کلی، طرفداران بلاک‌های بزرگ کاربران فعال بیت‌کوین بودند و می‌خواستند استفاده از بیت‌کوین را ساده‌تر کنند و دوست نداشتند دانشمندان نظری علوم کامپیوتر که حتی از بیت‌کوین استفاده نمی‌کردند، برای آن‌ها مانعی ایجاد کنند. طرفداران بلاک‌های بزرگ، برگزارکنندگان کنفرانس را متهم می‌کردند که موضوع را بیش از حد پیچیده می‌کنند و از این رویداد برای خریدن وقت بیشتر و متوقف کردن تلاش‌های آنان استفاده می‌کنند. تا جایی که به برگزاری این کنفرانس‌ها بدبین بودند و عنوان آن‌ها را از «مقیاس‌پذیری بیت‌کوین[1]» به «متوقف کردن بیت‌کوین[2]» تغییر داده بودند.

1 Scaling Bitcoin
2 Stalling Bitcoin

فصل چهارم

دومین کنفرانس مقیاس‌پذیری بیت‌کوین - هنگ کنگ

چند ماه پس از برگزاری اولین کنفرانس افزایش ظرفیت بیت‌کوین در مونترال، مرحله دوم این مجموعه کنفرانس‌ها در هنگ کنگ و در تاریخ ۶ و ۷ دسامبر سال ۲۰۱۵ برگزار شد. هنگ کنگ به دلیل نزدیکی به چین و نزدیکی به صنعت استخراج‌کنندگان بیت‌کوین که بسیاری از آن‌ها در آنجا مستقر بودند، انتخاب شده بود. عدم تعامل بین ماینرها و توسعه‌دهندگان در آن زمان یک مشکل اساسی تلقی می‌شد و این مکان برای رفع این نگرانی انتخاب شده بود. در همین حین من تصمیم گرفته بودم از شرکت Ruffer استعفا دهم و به هنگ کنگ بروم، بنابراین زمان و مکان این کنفرانس برای من بسیار مناسب بود. من از این فرصت استفاده کردم و یک آپارتمان در شهر پیدا کردم و یک هفته کامل در منطقه بودم. بعداً مشخص شد که هنگ کنگ یکی از مهم‌ترین میدان‌های نبرد در این درگیری بوده و اگر کسی می‌خواست شاهد روند تکاملی این مناقشه باشد مطمئناً باید در آن شرکت می‌کرد.

این کنفرانس در سایبرپورت[1]، یک پردیس تجاری در ضلع غربی جزیره هنگ کنگ و مشرف به اقیانوس برگزار شد. پروژه سایبرپورت در هنگ کنگ بحث‌برانگیز بود. قرار

1 Cyberport

بود مرکز فناوری و مرکز استارتاپ‌های شهر باشد و به همین دلیل این پروژه تصویب شد. با این حال، شرکت‌های فناوری زیادی در آنجا مستقر نبودند و فضای وسیع زیادی در آنجا خالی مانده بود و منجر به مطرح شدن اتهاماتی شده بود که این پروژه درواقع لباس مبدلی برای توسعه واحدهای مسکونی است. دولت پروژه توسعه را به شرکت Pacific Century Group اعطا کرده بود، شرکتی که تحت کنترل «ریچارد لی[1]»، پسر سرمایه‌دار معروف هنگ کنگ یعنی «لی کا-شینگ[2]» بود. این پروژه بحث‌برانگیز بود چون بدون برگزاری یک مناقصه آزاد به آن‌ها اعطا و منجر به اتهامات مالی شد.

ممکن است فکر کنید ما در اینجا بیش از حد به جزئیات می‌پردازیم، ولی جالب اینجاست که این موضوع اساس تئوری‌های توطئه‌ای است که برخی از افراطی‌ترین طرفداران بلاک‌های بزرگ مطرح می‌کنند. شرکت سرمایه‌گذاری Horizon Ventures که در تصاحب لی کا-شینگ بود، در شرکت Blockstream سرمایه‌گذاری کرده بود و ارتباط آن با سایبرپورت هنگ کنگ از جانب طرفداران بلاک‌های بزرگ به‌عنوان مدرکی برای پیاده کردن یک برنامه و به قصد فلج کردن بیت‌کوین و کوچک نگه داشتن بلاک‌ها معرفی می‌شد. همین امر در مورد شرکت بیمه فرانسوی AXA هم گفته می‌شد که یکی از شاخه‌های سرمایه‌گذاری آن در شرکت Blockstream سرمایه‌گذاری کرده بود. مدیر عامل سابق AXA «هنری دو کستریس[3]» رئیس گروه هدایت جلسه Bilderberg بود که یک گروه پشت درهای بسته و متشکل از نخبگان مالی و سیاسی جهان است، و همه این‌ها خمیرمایه‌های مورد نیاز برای کسانی که به تئوری‌های توطئه اعتقاد داشتند فراهم می‌کرد. این نظریه‌های احمقانه بارها و بارها در انجمن‌های ساب‌ردیت /r/btc تکرار می‌شدند.

جو کنفرانس هنگ کنگ زنده‌تر و سنگین‌تر از مونترال بود. تنش‌ها به اندازه قابل‌توجهی بیشتر بود و به نظر نمی‌رسید به اندازه کنفرانس مونترال ثمربخش باشد و گفتگو و بحث مفیدی بین دو طرف در جریان باشد و فقط مشاجره و درگیری بین افراد بود. در اولین

1 Richard Li
2 Li Ka-Shing
3 Henri de Castries

عصر و در مهمانی افتتاحیه سعی کردم حس و حال جمعیت را به‌دست آورم. این رویداد از کنفرانس مونترال بسیار بزرگ‌تر بود و طیف گسترده‌تری از افراد در آن شرکت کرده بودند. فضا بسیار خوش‌بینانه بود، اکثریت قریب به اتفاق شرکت‌کنندگان طرفداران بلاک‌های بزرگ بودند که انتظار داشتند این مسأله طی چند ماه آینده و با افزایش سایز بلاک حل شود. بیشتر آن‌ها فکر می‌کردند استدلال‌های طرفداران بلاک‌های کوچک به تدریج در حال شکست هستند و فقط یک اقلیت کوچک با هارد فورک افزایش سایز بلاک مخالفت می‌کنند.

جلسات کنفرانس هنگ کنگ شبیه به مونترال و بیشتر فنی بودند. تفاوت اساسی آن با کنفرانس مونترال حضور افراد فعال در صنعت استخراج بیت‌کوین بود. یکی از جلساتی که همه در انتظار آن بودند، میزگرد ماینرها در بعد از ظهر دوشنبه بود که در آن هفت نفر از نمایندگان صنعت استخراج بیت‌کوین بر روی صحنه حاضر شدند. اغلب آن‌ها چینی زبان بودند، و چین در آن زمان ۶۵ درصد هش‌ریت[1] جهانی را در اختیار داشت. این جلسه با این سؤال شروع شد که آیا آن‌ها از افزایش سایز بلاک حمایت می‌کنند یا نه. جواب اکثر آن‌ها مثبت بود، هرچند بعضی از آن‌ها قائل به شرایط خاصی بودند، مثلاً معتقد بودند بهتر است این کار با احتیاط انجام شود، یا روابط بین چین و غرب باید بهبود یابد. بیشتر ترجمه چینی به انگلیسی توسط «بابی لی[2]» انجام می‌شد که در آن زمان مدیرعامل و بنیانگذار صرافی BTCC بود. بابی یکی از طرفداران دوآتشه بیت‌کوین و یکی از مروجان اصلی آن در چین بود. دو پیشنهادی که در این جلسه مورد بحث قرار گرفتند یکی BIP-101 بود که توسط نرم‌افزار Bitcoin XT پیاده‌سازی شده بود و دیگری BIP-100 بود که توسط جف گارزیک پیشنهاد شده بود و به ماینرها اجازه تعیین سایز بلاک را می‌داد. اکثریت ماینرها نسبت به BIP-100 علاقه نشان می‌دادند و جای تعجب هم نداشت چون BIP-100 قدرت و اختیار بیشتری به آن‌ها می‌داد.

1 Hashrate
2 Bobby Lee

«وانگ چونگ[1]» گرداننده یکی از بزرگترین استخرهای استخراج بیت‌کوین به نام F2Pool معتقد بود ماینرها تنها گروهی هستند که می‌توانند رأی بدهند، بنابراین تصمیم‌گیری بر عهده آنان است. وی اظهار داشت بیت‌کوین یک سیستم اثباتِ کار[2] است و گروه‌های دیگر ابزاری برای رأی دادن ندارند. با این حال او ادامه داد که سایز ۸ مگابایت برای بلاک بسیار زیاد است، چون دانلود بلاک‌ها برای نود بسیار طولانی خواهد شد که به گفته وی یک فاجعه خواهد بود.

به نظر می‌رسید بیشتر ماینرها فکر می‌کردند کنترل شبکه بر عهده آن‌ها است و تصمیم [نهایی] را آن‌ها می‌گیرند، هرچند معتقد بودند اطلاعات کافی برای یک تصمیم‌گیری درست ندارند. [از طرف دیگر] طرفداران بلاک‌های کوچک اعتقاد داشتند قدرت تصمیم‌گیری روی پروتکل بیت‌کوین در اختیار ماینرها نیست و کنترل [قوانین] شبکه در اختیار کاربران بیت‌کوین است یا باید اینطور باشد. آن‌ها می‌گفتند که اثباتِ کار صرفاً برای حل مشکل دوبار خرج کردن[3] به‌وجود آمده و ماینرها فقط روی ترتیبِ قرارگرفتن تراکنش‌های [کاربران در بلاک‌ها] کنترل دارند. با این حال، بیشتر ماینرها معتقد بودند تصمیم نهایی را آن‌ها می‌گیرند. بخشی از این باور مربوط به گرایش آن‌ها برای به دست گرفتن قدرتی بود که همه به دنبال آن هستند، و بخش دیگر آن به این دلیل بود که هر دو طرف [درگیر در این مناقشه] با آن‌ها لابی می‌کردند. اصلاً اگر قرار نبود تصمیم نهایی را آن‌ها بگیرند چرا همه به سراغ آن‌ها می‌آمدند و از آن‌ها نظرخواهی می‌کردند؟ مشخص نبود که آیا ماینرها بالاخره چنین قدرتی دارند یا نه. طرفداران سرسخت بلاک‌های کوچک معتقد بودند که ماینرها هرگز چنین قدرتی نداشته‌اند چون آن‌ها کوین‌های Bitcoin XT را نخواهند پذیرفت، در حالی که دیگران باور داشتند اگر از آستانه ۷۵ درصد فعال‌سازی بگذریم، Bitcoin XT به بیت‌کوین جدید تبدیل می‌شود چون زنجیره آن بیشترین اثباتِ کار را در خود خواهد داشت.

1 Wang Chung
2 Proof of work
3 Double spend

از نظر آن‌ها همین مفهوم اثباتِ کارِ بیشتر بود که حکمرانی بیت‌کوین را در اختیار داشت و کاربران پشت اکثریت هش‌ریت قرار می‌گرفتند. هریک از این دو دیدگاه با توجه به فرضیاتی که از نحوه رفتار کاربران داشتند، به نوعی درست بود. اگر Bitcoin XT به آستانه ۷۵ درصد می‌رسید و همه کاربران نرم‌افزار خود را به نرم‌افزاری که از بلاک‌های بزرگ پشتیبانی می‌کند به‌روزرسانی می‌کردند، در این صورت تنها یک بیت‌کوین جدید، با بلاک‌های بزرگ‌تر وجود می‌داشت. اما اگر کاربران از به‌روزرسانی نرم‌افزار خود امتناع می‌کردند، در این صورت زنجیره اصلی همچنان ادامه پیدا می‌کرد و ماینرها کنترل‌شان را از دست می‌دادند. مشکلی که در اینجا وجود دارد این است که هر دو گروه فرض را بر این گذاشته بودند که سایر کاربران نیز مانند آن‌ها رفتار خواهند کرد بدون اینکه درنظر بگیرند ممکن است آن‌ها متفاوت عمل کنند.

بعد از اتمام این جلسه، بحث دیگری با ماینرها در اتاقی در جریان بود. در این بحث صحنه‌ای در کار نبود و درواقع یک میزگرد بود. تا جایی که من مطلع هستم این میزگرد یک بخش رسمی از کنفرانس نبود. این همان چیزی بود که بسیاری از حاضران در کنفرانس می‌خواستند ببینند و همینطور که این میزگرد پیش می‌رفت افراد زیادی هم به زحمت راه خود را به این اتاق باز می‌کردند. در نهایت فکر می‌کنم ۸۰ نفر داخل آن اتاق که صندلی هم نداشت ایستاده بودند. در این میزگرد برخی از ماینرها عنوان کردند که می‌خواهند با توسعه‌دهندگان بیت‌کوین همکاری کنند و روی یک راه‌حل به توافق برسند. هرچند سال‌ها بعد از این کنفرانس مطلع شدم که منظور از این پیام به اندازه‌ای که در ظاهر به نظر می‌رسید ربطی به همکاری نداشته و بیشتر روی قدرت تصمیم‌گیری ماینرها بر روی پروتکل بیت‌کوین تأکید کرده است. ظاهراً پیام اصلی در حین ترجمه گم شده بوده چون مترجم می‌خواسته به حل اوضاع کمک کند و باعث ایجاد تقابل و دشوارتر شدن شرایط نشود. ظاهراً یکی از ماینرها گفته بوده که آن‌ها کسب و کار راه انداخته‌اند و روی آن با پول سرمایه‌گذاری کرده‌اند و آن‌ها هستند که بلاک‌ها را تولید می‌کنند و این موضوع به آن‌ها قدرت واقعی کنترل شبکه را می‌دهد، در حالی که توسعه‌دهندگان چنین نفوذی ندارند.

اکنون زمان مناسبی برای وارد کردن «راجر ور[1]» به ماجرا است، چون او هم در این کنفرانس حضور داشت. راجر خود را به‌عنوان اولین سرمایه‌گذار در استارت‌آپ‌های بیت‌کوین معرفی می‌کند. او مطمئناً سابقه موفقی در سرمایه‌گذاری در فضای بیت‌کوین و حمایت از شرکت‌های Blockchain.info، و Bitpay، و Kraken داشته است. راجر یکی از برجسته‌ترین و پیگیرترین مروجان بیت‌کوین در روزهای اول، و همیشه هوادار آن بوده است. معروف است وقتی او برای اولین بار با بیت‌کوین آشنا شد، آنچنان هیجان‌زده شده است که چندین روز در بیمارستان بستری بوده است. به طور خاص، او همیشه علاقه زیادی به جنبه کاربردی پرداخت بیت‌کوین داشته و با تشویق فروشندگان برای پذیرش بیت‌کوین در جا انداختن بیت‌کوین نقش مهمی داشته است. شاید به دلیل این اشتیاق بی حد و حصری که به بیت‌کوین داشت و به مذاق همه خوش نمی‌آمد، نام مستعار «مسیح بیت‌کوین[2]» را برای خود کسب کرد.

قبل از بیت‌کوین راجر ور شرکتی در زمینه فروش قطعات کامپیوتر به نام MemoryDealers.com داشت. پیش از آن، وی به جرم فروش غیرقانونی مواد منفجره به‌صورت آنلاین در ایالات متحده محکوم و زندانی شد. او پس از آزادی مدت زیادی در ایالات متحده باقی نماند و در سال ۲۰۱۴ رسماً از تابعیت ایالات متحده دست کشید و در آن زمان در توکیو زندگی می‌کرد. تا جایی که من می‌دانم راجر به جنبه‌های عملی و تجاری بیت‌کوین علاقه داشت و تا قبل از مناقشه سایز بلاک علاقه چندانی به جنبه‌های فنی یا علوم کامپیوتر بیت‌کوین نشان نمی‌داد. او همچنین بخاطر اطمینانی که به مشتریان صرافی Mt.Gox مبنی بر توانایی پرداخت بدهی این صرافی پس از بررسی «اظهارات بانکی متعدد» در سال ۲۰۱۳ داده بود، در جامعه بیت‌کوین شناخته شده بود. متأسفانه در آن زمان صرافی Mt.Gox ورشکسته و هزاران بیت‌کوین از دست داده بود. چند ماه بعد از ضمانت راجر و در فوریه سال ۲۰۱۴ صرافی Mt.Gox شکست بزرگی خورد. این موضوع تا حدودی به اعتبار راجر آسیب زد ولی افرادی که در این فضا مشغول هستند حافظه کوتاه مدت دارند و همواره موجی از کاربران جدید [که از این مسائل بی‌خبرند] اضافه

1 Roger Ver
2 Bitcoin Jesus

می‌شوند.در هر حال، در زمستان سال ۲۰۱۵ اتفاقات صرافی Mt.Gox مثل یک خاطره دور بود.

راجر مالک دومین ساب‌ردیت[1] بیت‌کوین یعنی r/btc/ بود و با توجه به دیدگاه‌های صریح و آزادی‌خواهانه‌اش، با روش مدیریت r/bitcoin/ که از نظر او سانسور بود بسیار مخالف بود. در این مرحله و این کنفرانس راجر به‌عنوان یکی از طرفداران بلاک‌های بزرگ شناخته نمی‌شد. بلکه او با مدیرعامل صرافی OKCoin یعنی «استار ژو[2]» روی دامنه Bitcoin.com و ظاهراً بابت یک قرارداد تقلبی، درگیری و دعوای پر سر و صدایی داشت. به نظر می‌رسید این موضوع به «ژانگ‌پنگ ژائو[3]» که در آن زمان مدیرعامل OKCoin بود و بعداً صرافی Binance را تأسیس کرد ارتباط پیدا می‌کرد. ما در اینجا به جزئیات این ماجرا نخواهیم پرداخت ولی نکته این است که در آن زمان حواس راجر معطوف به مسائل دیگری بود و به‌صورت مستقیم درگیر مناقشه سایز بلاک نبود، اگرچه بر کسی پوشیده نیست که او از طرفداران بلاک‌های بزرگ حمایت می‌کرد.

جف گارزیک دوباره بر روی صحنه رفت و درباره نقاط قوت و ضعف گزینه‌های اصلی صحبت کرد که اساساً چهار مسیر رو به جلو بودند: پیشنهاد BIP-101، پیشنهاد BIP-100 که از جانب خودش مطرح شده بود، افزایش یکباره به ۲ مگابایت که در BIP-102 مطرح شده بود، و در آخر هیچکدام از آن‌ها.

پس از سخنرانی از او درباره نحوه تصمیم‌گیری پرسیدند و او جواب داد:

> من فکر می‌کنم روند کار به این شکل است که ما در کنفرانس مونترال داده‌های ورودی را گرفتیم. اکنون در هنگ کنگ ما همه موارد مثل هزینه‌های اعتبارسنجی، پیشنهادهای مختلف و غیره را بررسی می‌کنیم. در مرحله سوم باید دوباره کار را

1 subreddit
2 Star Xu
3 Changpeng Zhao

دست بگیریم و با کسب و کارها، کاربران، ماینرها بحث و گفتگو کنیم و به یک توافق کلی برسیم. پاسخ کلی من این است که همه باید نظرات خود را اعلام کنند. همه باید بدانند جف گارزیک در این مورد چه نظری دارد، یا شرکت BitPay چگونه به مسأله فکر می‌کند. من فکر می‌کنم از طریق شفافیت و بحث و گفتگو می‌توانیم راه [درست برای تصمیم‌گیری] را پیدا کنیم. به نظر من در خفا گاوبندی کردن و بازدیدهای خصوصی افراد مختلف راهی به جایی نمی‌برد. این کار را باید به‌صورت عمومی به انجام برسانیم و روش اپن-سورس[1] به این شکل است.

در پایان کنفرانس جف دوباره به صحنه بازگشت. او این بار درباره پیشنهادهای مختلفی که ارائه شده بود از مخاطبان نظرخواهی کرد. او یک پیشنهاد را نام می‌برد و حاضرین در صورت موافقت با آن کف می‌زدند. وقتی که او به پیشنهاد افزایش سایز به ۲ مگابایت رسید، افراد بسیار زیادی در جمع حاضرین مشغول به کف زدن شدند. به نظر می‌رسید حدود ۷۰ درصد نمایندگان با شوق و ذوق کف می‌زدند. با این حال اقلیت کوچکی به وضوح از این اتفاق ناراضی بودند و از حاضرین درخواست می‌کردند از کف زدن دست بکشند. آن‌ها می‌خواستند تصمیمات بر اساس شایستگی گرفته شود نه بر اساس اینکه چه کسی در یک رویداد بلندتر کف می‌زند. با این حال افراد زیادی معتقد بودند این [کار] ضرری ندارد. به نظر می‌رسید توافق شرکت‌کنندگان در این کنفرانس این است که فعلاً افزایش سایز بلاک بیشتر از ۲ مگابایت کمی خطرناک است. بسیاری از سخنرانان از جمله «جاناتان تومیم[2]» که از طرفداران بلاک‌های بزرگ بود با استدلال‌های فنی استدلال می‌کردند که افزایش سایز بلاک به ۲ مگابایت با توجه به شرایط فعلی شبکه مشکلی به‌وجود نخواهد آورد ولی اگر سایز را خیلی بیشتر از آن افزایش دهیم، زمان طولانی انتشار بلاک می‌تواند شبکه را دچار مشکل کند. به نظر می‌رسید اکثر ماینرها هم با این استدلال موافق هستند.

1 open-source
2 Jonathan Toomim

پس از این رویداد مسیر رو به جلو [همچنان] مشخص نبود. با این حال یک چیز برای من روشن شده بود؛ اینکه Bitcoin XT دیگر مرده است. دیدگاه [غالب] این بود که احتمالاً ۲ مگابایت در شرایط حال حاضر مناسب است، نه ۸ مگابایت. پیشنهاد Bitcoin XT به‌طور رسمی کنار گذاشته نشد و طرفدارانش هم هیچ‌وقت به افراطی بودن سایز پیشنهادی‌شان و فشاری که برای افزایش سایز بلاک آورده بودند اعتراف نکردند. شاید چنین اعترافی از جانب ایشان می‌توانست به بهتر شدن اوضاع کمک کند. از نظر طرفداران بلاک‌های کوچک Bitcoin XT یک شرایط بحرانی پدید آورده بود و باعث ایجاد تنش و جنجال شده بود و پیشرفت در موضوع افزایش سایز بلاک را دشوارتر کرده بود. در حالی که از نظر طرفداران بلاک‌های بزرگ، یک کاتالیزور ضروری برای ادامه بحث و گفتگو بود.

بعد از اتمام کنفرانس من و هفت یا هشت نفر از کارمندان شرکت Blockstream برای خوردن شام از جزیره هنگ کنگ به «کالون[1]» رفتیم. بیشتر بحث سر میز شام حول موضوعات کاملاً فنی بود، از جمله اینکه چگونه می‌توان امضاهای بیت‌کوین را فشرده یا با یکدیگر جمع کرد. سپس بحث به سمت گوین و تاکتیک‌های او رفت. آیا گوین نمی‌فهمد که بیت‌کوینرها دوست ندارند کسی به آن‌ها بگوید چه کاری انجام دهند؟ مردم احساس می‌کنند صاحب بیت‌کوین هستند و می‌خواهند کنترل آن به دست خودشان باشد. Bitcoin XT از بالا به پایین به آن‌ها تحمیل می‌شود و هیچ تلاشی هم نمی‌شود تا کاربران احساس کنند کنترل مسائل و تصمیم [نهایی] با آن‌ها است. از نظر آن‌ها گوین اینجا یک اشتباه بزرگ تاکتیکی مرتکب شده بود. به نظر می‌رسید همه افراد حاضر در میز شام با این مسأله موافق هستند و از اقدام اشتباه گوین متعجب شده‌اند. آن‌ها دلسوز گوین بودند و می‌خواستند گوین به توصیه‌های آن‌ها گوش کند و سعی کند با استفاده از یک روش دیگر و با همکاری بیشتر کاربران بیت‌کوین برای افزایش سایز بلاک دوباره تلاش کند تا کاربران احساس کنند بر روی پول‌شان کنترل دارند. یکی از حاضران در میز شام معتقد بود اگر گوین به کاربران می‌گفت تصمیم [نهایی] با آن‌ها است، حتماً از او حمایت

1 Kowloon

می‌کردند. با این حال به نظر می‌رسید گوین این کار را نخواهد کرد چون او معتقد نبود که تصمیم [نهایی] با کاربران بیت‌کوین است.

ما آخر شب برای برگشت به جزیره هنگ کنگ یک کشتی گرفتیم. یادم می‌آید به آسمان خراش‌های سربه فلک کشیده در مرکز هنگ کنگ، شهری که قرار بود به زودی خانه جدید من باشد نگاه می‌کردم. مرکز شهر تحت سلطه بخش خدمات مالی یا همان چیزی است که بیت‌کوینرها به آن سیستم مالی سنتی[1] می‌گویند. حس قدرتی که این ساختمان‌ها به بیننده القاء می‌کند، این بحث را جلوی دید ما قرار می‌دهد. ما فقط چند صد نفر بودیم که در یک اتاق در هنگ کنگ با یکدیگر بحث و گفتگو می‌کردیم. آیا اصلاً بیت‌کوین تا این اندازه اهمیت دارد؟ آیا می‌تواند روزی روی پای خود بایستد و سیستم مالی را به چالش بکشد؟ اگر اکنون که فقط چند صد نفر به آن اهمیت می‌دهند نتوانیم این اختلاف را حل کنیم، چطور می‌توانیم به بیت‌کوین امید ببندیم؟ من به فشارهای همه جانبه‌ای که با رشد بیت‌کوین از طرف بازیگران عمده اقتصادی و سیاسی بر بیت‌کوین وارد خواهد شد فکر می‌کردم. این فشارها در آینده به‌قدری بزرگ خواهند بود که کار مایک و گوین بسیار کوچک جلوه خواهد کرد.
من فهمیدم که قوانین شبکه باید قوی باشند. مهم نیست چه کسی سعی در تغییر قوانین دارد، یا اصلاً این تغییر کار درستی است یا نه. برای اینکه بیت‌کوین بتواند موفق شود باید تغییر قوانین آن واقعاً دشوار باشد، در غیر اینصورت قادر به ایستادگی در برابر فشارهای مؤسسات مالی عمده‌ای که مطمئناً با افزایش ارزش بیت‌کوین به سراغش خواهند آمد، نخواهد بود.

اگرچه از نظر طرفداران بلاک‌های بزرگ، افزایش سایز بلاک تغییر در قوانین بیت‌کوین نبود، بلکه درواقع پایبندی به چشم انداز اصلی بود. این تغییر به معنای واقعی و از نظر علوم کامپیوتر تغییراتی در قوانین شبکه اعمال می‌کرد، به این معنی که با افزایش سایز بلاک، قوانین شبکه آزادتر[2] می‌شدند. با این حال [طرفداران بلاک‌های بزرگ] معتقد بودند اگر

1 Legacy financial system
2 Relaxed (hard forks)

این محدودیت ادامه پیدا کند، یک تغییر عمده اقتصادی رخ خواهد داد و خللی در چشم‌انداز [اصلی] به‌وجود خواهد آمد و ما شاهد بلاک‌های پُر خواهیم بود [در حالی که تاکنون چنین چیزی وجود نداشته است].

در هر صورت باید شرایط حال حاضر[1] [شبکه] به‌گونه‌ای تعریف می‌شد. اگر بیت‌کوین بخواهد موفق شود باید ساز و کاری وجود داشته باشد تا این شرایط حال حاضر به‌شکلی بقا یابد و [بر مشکلات] غلبه کند. تا جایی که من می‌دانم، به نظر می‌رسد که این «نقطه شلینگ[2]» روی قوانین فنیِ اعتبارِ بلاک تنظیم شده بودند و هیچگونه مکانیزمی برای اطمینان از تغییرناپذیریِ تصور مردم[3] از شبکه وجود نداشت. به نظر می‌رسد فقط تغییر قوانین مربوط به اعتبارسنجی بلاک‌ها بسیار دشوار بود چون واگرایی از شرایط حال حاضر در آن بخش [یعنی موضوع اعتبار بلاک،] منجر به دوپاره شدن زنجیره خواهد شد، و عواقب سنگین اقتصادی در پی خواهد داشت.

این سیستم حکمرانی بی‌نقص نبود و باعث انعطاف‌ناپذیر شدن سیستم می‌شد، ولی تنها روشی بود که می‌توانستیم برای حفظ پایداری شبکه بکار ببندیم. این موضوع نقل قولی از وینستون چرچیل[4] را به یاد من آورد: «دموکراسی بدترین روش حکمرانی است، فقط همه روش‌های دیگر از آن بدتر هستند.» شاید سیستمی که شرایط حال حاضر در آن چیره، و ایجاد تغییر در آن بدون یک توافق قاطع و عمومی غیرممکن باشد، بدترین شکل حکمرانی در بیت‌کوین باشد ولی دیگر روش‌ها از آن بدتر هستند.

1 Status quo
2 Schelling point
3 People’s vision
4 Winston Churchill

فصل پنجم

سگویت

در اولین جلسه از روز دوم کنفرانس مقیاس‌پذیری بیت‌کوین در هنگ کنگ و در یکی از اولین سخنرانی‌ها، پیتر والا، یکی از توسعه‌دهندگان بیت‌کوین درباره موضوعی با نام «تفکیک بخش امضای دیجیتالی[1]» یا «سگویت[2]» سخنرانی کرد. سگویت راهی بود که می‌شد از طریق آن بدون نیاز به یک هارد فورک، سایز بلاک‌های را در شبکه افزایش داد. یعنی این تغییر از طریق سافت فورک انجام می‌شد و کاربرانی که نسخه نرم‌افزار پایین‌تری اجرا می‌کردند همچنان با شبکه سازگار باقی می‌ماندند. یک تراکنش بیت‌کوین از بخش‌های مختلفی تشکیل شده است، یکی از آن‌ها امضای دیجیتالی است که به صاحب کوین اجازه خرج یا منتقل کردن کوین‌ها را می‌دهد. این امضای دیجیتالی از لحاظ مقدار فضایی که اشغال می‌کند، اغلب بزرگترین بخش یک تراکنش است.

سگویت درواقع یک قالب جدید برای تراکنش‌ها بود که در آن نیازی به وارد کردن امضای دیجیتال به بلاک‌های قدیمی ۱ مگابایتی نبود. نرم‌افزار کاربرانی که نودهایشان را به‌روزرسانی کرده باشند، بلاک‌های جدیدی که حاوی این امضاهای دیجیتالی هستند را

1 Segregated Witness
2 Segwit

خواهد دید. محدودیت ۱ مگابایت از روی این بلاک‌های جدید برداشته، و با یک واحد ۴ میلیونی جدید جایگزین می‌شود. به این واحد جدید «محدودیت وزن[1]» می‌گوییم. این محدودیت وزن به اندازه ۴ برابر داده‌هایی که به امضای دیجیتال تراکنش مربوط نمی‌شدند (در واحد بایت)، به‌علاوه اطلاعات امضای دیجیتال تراکنش (در واحد بایت) تعریف شده بود. این بدان معنی است که در محاسبه [سایز تراکنش] برای داده‌های مربوط به امضای دیجیتال آن تخفیفی قائل می‌شویم، ولی در نهایت سایز بلاک بیشتر از ۲ مگابایت نخواهد شد، که البته همان چیزی بود که به نظر می‌رسید خواسته بسیاری از کاربران بود؛ افزایش سایز بلاک به حدود ۲ مگابایت.

یک توسعه‌دهنده بیت‌کوین به نام «لوک دش‌یر[2]» که در فلوریدا زندگی می‌کرد راهی کشف کرده بود که از طریق آن امکان اعمال سگویت به‌صورت یک سافت فورک بر روی شبکه بیت‌کوین امکان‌پذیر می‌شد. لوک به عنوان یکی از سرسخت‌ترین طرفداران بلاک‌های کوچک شناخته می‌شد و در کنار گرگوری مکسول بین طرفداران بلاک‌های بزرگ از چهره‌های منفور بود. او از مخالفت با جمعی که با وی همفکر نبودند هراسی نداشت. او یک کاتولیک معتقد، پدر هفت فرزند، و بسیار تندخو بود و در جامعه فعالان بیت‌کوین به پیش‌گویی می‌ماند که کسی حرف‌هایش را جدی نمی‌گیرد. با این حال کاملاً واضح بود که لوک درک فنی بسیار خوبی از بیت‌کوین دارد و شیوه تفکر غیرخطی او که باعث می‌شود چیزهایی را ببیند که دیگران نمی‌بینند، به او کمک کرده تا بتواند روشی [برای اجرای اعمال تغییرات به صورت سافت فورک] پیدا کند که به فکر توسعه‌دهندگان دیگر نرسیده بود.

سگویت برای کسانی که آن را می‌فهمیدند یک پیشنهاد هوشمندانه و دو سر برد بود. هم شبکه می‌توانست به بلاک‌های ۲ مگابایتی دست پیدا کند، هم [به‌دلیل اعمال تغییرات از راه سافت فورک] از به‌وجود آمدن مشکل ناسازگاری [بین نودهای] شبکه جلوگیری

1 Weight limit
2 Luke Dashjr

می‌شد. علاوه بر این کیف پول‌های قدیمی [با نرم‌افزار قدیمی] و جدید [که نرم‌افزار خود را به‌روز کرده بودند] همچنان می‌توانستند با یکدیگر تعامل داشته باشند و به‌روزرسانی [نرم‌افزار بیت‌کوین] کاملاً اختیاری بود و کاربران می‌توانستند نرم‌افزار خود را به‌روز، و از قابلیت‌های سگویت استفاده کنند، یا به روال گذشته از شبکه استفاده کنند. [چون بخش امضای دیجیتال تراکنش‌ها در سگویت به قسمت دیگری منتقل شده است،]کیف پول‌های قدیمی، این بخش از داده تراکنش را در اختیار نخواهند داشت، با وجود این آن‌ها تراکنش‌های جدید [سگویتی] را از شبکه دریافت می‌کنند و اگر [این تراکنش توسط یک ماینر] داخل بلاک قرار گرفته باشد، برای آن‌ها معتبر است. همچنین سگویت باعث می‌شد ظرفیت تراکنش [شبکه] سریع‌تر از روش افزایش سایز بلاک با استفاده از هارد فورک بالا رود، چون در این صورت نیازی نیست انتظار بکشیم تا همه [نودها نرم‌افزار خود را] به‌روزرسانی کنند و قادر خواهیم بود به سرعت از فضای اضافه شده به بلاک استفاده کنیم.

سگویت نه تنها به نفع بیت‌کوین، بلکه به نظر می‌رسید خواه عمدی خواه ناخواسته، یک حرکت تاکتیکی هوشمندانه از جانب طرفداران بلاک‌های کوچک در مناقشه سایز بلاک بود. این پیشنهاد به‌قدری خوب بود که هیچگونه استدلال معتبری علیه آن وجود نداشت. گوین مجبور به پشتیبانی از پیشنهاد سگویت بود و تا حدودی هم این کار را انجام داد[1]. اگر کنفرانس‌های مقیاس‌پذیری بیت‌کوین توطئه‌ای در خفا و به هدف وقت خریدن و در نهایت [آماده‌سازی و] اعلام این ایده بوده، می‌توانم بگویم [آن‌ها] کارشان را خوب انجام دادند ولی من در اینجا این اتهام را [علیه کسی] مطرح نمی‌کنم. [با برگزاری این کنفرانس‌ها] طرفداران بلاک‌های بزرگ تلاش برای اعمال هاردفورک را موقتاً متوقف می‌کردند و فرصتی کلیدی برای گروه مقابل پیش می‌آمد. به یاد دارم که در آن زمان با برخی از طرفداران پیش‌کسوت بلاک‌های بزرگ صحبت می‌کردم و آن‌ها به من گفتند که معتقدند این پیشنهاد [افزایش سایز بلاک] بسیار هوشمندانه است و آن‌ها مغلوب شده‌اند.

1 https://twitter.com/gavinandresen/status/800405563909750784

هرچند این‌ها همه روی کاغذ بودند. شاید در یک دنیای فرضی، جایی که همه سگویت را می‌فهمیدند و در عین حال منطقی رفتار می‌کردند، سگویت یک اقدام فوق‌العاده بود. دعوا بر سر سایز بلاک بود و سگویت این محدودیت را رفع می‌کرد و [سایز بلاک را افزایش می‌داد]، بنابراین دیگر بحثی باقی نمی‌ماند. ولی در واقعیت داستان از این قرار نبود. سگویت بسیار پیچیده بود و تقریباً هیچ‌کس از آن سردر نمی‌آورد. این اولین جایی بود که طرفداران بلاک‌های کوچک هوش مخالفان خود، یا حداقل توانایی آن‌ها در درک جنبه‌های علوم کامپیوتر را بیش از حد ارزیابی کرده بودند. با درنظر گرفتن اتفاقات گذشته شاید بهتر بود نام آن را چیزی مانند «افزایش بلاک به ۲ مگابایت» می‌گذاشتند.

اما این پیشنهاد عنوانی رمزآلود و مبهم داشت و برای طرفداران بلاک‌های بزرگ که یک راه روشن و قابل فهم [برای افزایش سایز بلاک] می‌خواستند، بسیار مشکوک به نظر می‌رسید. به نظر می‌رسید طرفداران بلاک‌های بزرگ فهمیده بودند که این حرکت از جانب دشمن آن‌ها است و بر راه [پیشنهادی] خود اصرار داشتند. این جنگ بر سر به دست آوردن کنترل [شبکه] بود و آن‌ها خواهان به‌دست گرفتن کنترل [شبکه] بودند. آن‌ها فکر می‌کردند سگویت هم مکانیزمی برای خریدن وقت بیشتر و توقف اجرای افزایش بلاک‌های بزرگ‌تر است. بنابراین بدون اینکه آن را بفهمند، با آن مخالفت کردند.

همزمان با جلب توجه جامعه فنی به سگویت، سوءتفاهم‌ها و سوءبرداشت‌های طرفداران بلاک‌های بزرگ نسبت به آن بالا گرفت. این سوءتفاهم‌ها و شایعات شامل (و نه لزوماً مختص) موارد زیر بود:

- سگویت یک افزایش سایز بلاکِ واقعی نیست، بلکه فقط تراکنش‌ها را فشرده [و در بلاک ذخیره] می‌کند. (این درست است که نودهایی قدیمی [و به‌روزرسانی نشده] همچنان بلاک‌ها را ۱ مگابایتی می‌بینند، ولی این موضوع در شرایط هارد

فورک هم صادق است چون نودهای قدیمی هنوز قانون ۱ مگابایت را اعمال می‌کنند. در سگویت نودهایی که نرم‌افزار خود را به‌روزرسانی کرده باشند بلاک‌های بزرگ‌تر از ۱ مگابایت را می‌بینند که خواسته طرفداران بلاک‌های بزرگ هم احتمالاً همین بوده است)

- بیت‌کوین بر پایه زنجیره‌ای از امضاهای دیجیتالی است و سگویت این زنجیره را از هم پاره، و در نتیجه یک مشکل امنیتی به‌وجود می‌آورد.
- اگر یک ماینر که نرم‌افزار خود را به سگویت به‌روزرسانی نکرده است یک بلاک تولید کند، این بلاک برای نودهایی که به‌روز شده‌اند معتبر نیست و رد خواهد شد. این مسأله خطر فورک شدن زنجیره را بالا می‌برد. (این فقط در صورتی اتفاق می‌افتد که ماینر از نرم‌افزاری استفاده کند که عمداً به قصد فورک کردن زنجیره طراحی شده باشد)
- اگر کاربری نرم‌افزار خود را به سگویت به‌روزرسانی کرده باشد، قادر به انتقال بیت‌کوین به کاربری که نرم‌افزار خود را به‌روزرسانی نکرده است، نخواهد بود.
- سگویت برگشت‌پذیر است و در این صورت هرکس می‌تواند بیت‌کوین‌هایی که در آدرسهای سگویتی هست را بدزدد. (لغو سگویت فقط از طریق یک هارد فورک امکان‌پذیر است)

بسیاری از این سوءتفاهم‌ها بی‌معنی بودند و نمی‌شد به راحتی برای آن‌ها جوابیه نوشت. به نظر می‌رسید این افراد اصول پایه‌ای تراکنش‌های بیت‌کوین را هم درک نکرده بودند و سوءتفاهم‌ها هم از همین نشأت می‌گرفت. برای مثال اغلب به عبارت «آدرس با الگوی سگویت[1]» اشاره می‌شد، ولی سگویت یک الگوی جدید یا متفاوت برای آدرس‌ها ارائه نمی‌کرد. اگر این افراد از ساز و کار تراکنش‌های بیت‌کوین سر در نمی‌آورند، توضیح ساز و کار سگویت قطعاً غیرممکن بود.

1 SegWit format address

سگویت به‌قدری پیچیده بود که به نظر می‌رسید حتی جف گارزیک هم آن را درک نکرده است. او معتقد بود که دو «بخش مجزا[1]» برای بازار کارمزد به‌وجود خواهد آمد: یکی برای بلاک‌های ۱ مگابایتی و یکی برای بلاک‌های جدید که محدودیت وزن ۴ میلیون برای آن‌ها تعیین شده بود[2]. در حقیقیت [اینطور نبود]، سایز بلاک و وزن بلاک به‌گونه‌ای ساخته شده بودند که با یکدیگر سازگار باشند و [از نظر کارمزد] تفاوتی با یکدیگر نداشته باشند، بنابراین فقط یک بازار برای پیشنهاد تراکنش خواهیم داشت. تقصیر جف هم نبود چون سگویت پیچیده، و درک کامل آن بسیار دشوار بود و همین موضوع نقطه ضعف اساسی آن بود. اگرچه از نظر فنی سگویت راه درستی برای ادامه مسیر بود ولی به دلیل پیچیدگی‌هایی که داشت، توضیح آن به جامعه فعالان بیت‌کوین بسیار دشوار بود.

گذشته از پیچیدگی، استدلال‌های معتبری هم علیه سگویت وجود داشت. برای دستیابی به مزایای سگویت و افزایش فضای بلاک، کاربران باید کیف پول‌هایشان را برای پشتیبانی از قالب جدید تراکنش‌ها به‌روز کنند. این موضوع باعث می‌شود افزایش سایز بلاک زمان بیشتری نسبت به روش هارد فورک ببرد، چون آن روش نیازی به تغییر الگوی تراکنش‌ها نداشت. لازم به ذکر است که به محض استفاده برخی کاربران از سگویت، فضای بلاک برای افرادی که کیف‌پول خود را به‌روز نکرده باشند آزاد می‌شود و [آن‌ها هم از مزایای آن برخوردار می‌شوند].

از نظر بسیاری از طرفداران بلاک‌های کوچک، ترغیب کاربران به به‌روزرسانی و پشتیبانی از قالب جدید تراکنش‌ها، خود بخشی از سگویت بود. سگویت علاوه بر افزایش سایز بلاک و ارائه قالب جدید برای تراکنش‌ها، چند مشکل[3] [نرم‌افزاری] دیگر را هم برطرف می‌کرد که از بین آن‌ها می‌توان به مشکل «تغییرپذیری تراکنش[4]» و مقیاس‌پذیری غیرخطی عملگرهای `sighash` اشاره کرد. (برای کسب اطلاعات بیشتر در مورد مشکل

1 Two buckets
2 https://www.slideshare.net/jgarzik/bitcoin-status-report-onchain-scaling-aug-2016
3 bug
4 Transaction alleability

تغییرپذیری تراکنش به پیوست مراجعه کنید. - م) من در اینجا خیلی وارد جزئیات نمی‌شوم ولی به‌طور خلاصه تغییرپذیری تراکنش اساساً به این دلیل به‌وجود می‌آمد که شناسه یک تراکنش بیت‌کوین[1] می‌توانست قبل از تأیید و وارد شدن به بلاک‌چین بیت‌کوین، تغییر کند و همچنان معتبر باشد. این امر در گذشته باعث بروز مشکلاتی برای برخی از کیف پول‌ها و پذیرندگان بیت‌کوین شده بود، چون نمی‌توانستند پرداخت‌ها را ردیابی کنند. این درواقع یک اشکال [نرم‌افزاری] بود و توسعه شبکه تراکنش‌ها روی لایه دومِ زنجیره اصلی بیت‌کوین معروف به «شبکه لایتنینگ[2]»، وابسته به برطرف شدن این مشکل بود.

[مشکل] مقیاس‌پذیری غیرخطی عملگرهای sighash یعنی با افزایش تعداد ورودی‌های یک تراکنش، تعداد عملیات هش لازم برای اعتبارسنجی این تراکنش با مربع[3] آن‌ها افزایش می‌یابد و رابطه آن‌ها خطی[4] نیست. این مسأله مانعی برای مقیاس‌پذیری شبکه بیت‌کوین] از راه بلاک‌های بزرگ‌تر بود، چون مهاجمان می‌توانستند تراکنش‌هایی بسازند که زمان اعتبارسنجی آن‌ها به‌قدری طولانی باشد که کل شبکه از کار بایستد. درواقع یکی از دلایل اصلی که طرفداران بلاک‌های کوچک برای مخالفت با افزایش سایز بلاک مطرح می‌کردند همین بود، چون مهاجمان می‌توانستند از این نقطه ضعف استفاده کنند. یک فرد مهاجم می‌توانست بلاکی بسازد که شامل تعداد زیادی از این تراکنش‌های بزرگ باشد، به‌طوری که اعتبارسنجی آن برای یک کامپیوتر معمولی ساعت‌ها طول بکشد.

بنابراین برای بسیاری از طرفداران بلاک‌های کوچک حل این مشکل، پیش شرط افزایش سایز بلاک بود. آن‌ها طرفداران بلاک‌های بزرگ را به دلیل ساده‌لوحی، درنظر نگرفتن این مشکل، و نخواندن دست افرادی که مترصد ضربه زدن به شبکه بیت‌کوین هستند، مورد تمسخر قرار می‌دادند. برعکس طرفداران بلاک‌های بزرگ معتقد بودند که بیت‌کوین تقریباً نابود نشدنی و آسیب‌ناپذیر است. طرفداران بلاک‌های کوچک مستحکم بودن

1 Transaction ID
2 Lightning network
3 quadratical
4 linear

سیستم را نتیجه سخت‌کوشی و دقت تیم توسعه می‌دانستند، اما این موضوع تا اندازه‌ای که باید مورد توجه جامعه فعالان بیت‌کوین قرار نمی‌گرفت. بیشتر طرفداران بلاک‌های بزرگ معتقد بودند که رفع این اشکالات نباید در اولویت باشد و افزایش سایز بلاک کلید [حل مشکلات] است.

از این‌ها که بگذریم، با اعمال سگویت این اشکالات هم برطرف می‌شدند و این موضوع از نظر طرفداران بلاک‌های کوچک کاملاً منطقی بود. با استفاده از سگویت قادر بودیم محدودیت ۱ مگابایتی را بر روی تراکنش‌هایی که مشکل مقیاس‌پذیری [ورودی‌ها را] داشتند حفظ کنیم و در عین حال فضای بیشتری به تراکنش‌های جدیدی که این مشکل را نداشتند اختصاص دهیم. سگویت از نظر فنی و مهندسی فوق‌العاده بود. دوباره تکرار می‌کنم که اشکال آن پیچیدگی بود؛ بیشتر کاربران بیت‌کوین تصوری از این مشکلات نداشتند و به آن‌ها اهمیتی نمی‌دادند. بیت‌کوین موضوعی فراتر از مهندسی و علوم کامپیوتر است، علاوه بر این [مسائل فنی] بیت‌کوین یک سیستم اجتماعی، یک سیستم پرداخت مستقیم فعال، یک سیستم اقتصادی، و یک سیستم مالی هم هست. با درنظر گرفتن این زوایای دید مختلف نسبت به بیت‌کوین، سگویت تا حدودی اهمیت خود را از دست می‌داد.

اگرچه ایده سگویت در دسامبر سال ۲۰۱۵ در کنفرانس هنگ کنگ ارائه شد، اما کار توسعه، تحلیل، تست [نرم‌افزاری]، و بحث و گفتگو درباره آن به اتمام نرسیده بود. بالاخره و بعد از ۱۰ ماه انتظار طولانی سگویت در نوامبر سال ۲۰۱۶ به نرم‌افزار `Bitcoin Core` اضافه شد. هرچند اضافه شدن آن به `Bitcoin Core` به معنی این نبود که کاربران می‌توانند از سگویت استفاده کنند. این یک تغییر یا به‌طور دقیق‌تر سخت‌گیرانه‌تر شدن قوانین پروتکل، و به عبارت دیگر یک سافت فورک بود. این یعنی به یک روش برای فعال‌سازی [قوانین جدید بر روی شبکه] نیاز است. مکانیزم فعال‌سازی انتخاب شده این بود که ماینرها باید حمایت خود را از طریق سیگنال [قرار داده شده در سربرگ بلاک‌ها] اعلام کنند. اگر ۹۵ درصد از ۲,۰۱۶ بلاک در یک دوره تنظیم سختی شبکه حاوی سیگنال

حمایت ماینرها بودند، سافت فورک سگویت بعد از گذشت یک «دوره تنفس[1]» دو هفته‌ای فعال می‌شد. اگر فعال‌سازی بعد از گذشت ۱۲ ماه انجام نمی‌شد، تلاش برای فعال‌سازی آن لغو می‌شد.

از نظر طرفداران بلاک‌های بزرگ این روش فعال‌سازی مناسب نبود و دلیل آن‌ها هم این بود که تحت هیچ شرایطی نخواهیم توانست به یک توافق ۹۵ درصدی برسیم. چون فقط یک ائتلاف کوچک ۵ درصدی بین ماینرها کافیست تا فرآیند اعمال این تغییر متوقف شود. بعضی از این طرفداران بلاک‌های بزرگ، معتقد بودند انتخاب آستانه فعال‌سازیِ ۹۵ درصد تاکتیکی است برای ایجاد وقفه در اعمال تغییرات، و آستانه ۷۵ درصدی پیشنهاد شده توسط Bitcoin XT را بیشتر می‌پسندیدند. طرفداران بلاک‌های بزرگ تمایل داشتند تا سیگنال‌های [آماده بودن] ماینرها را به عنوان یک رأی در روند تصمیم‌گیری ببینند. با درنظر گرفتن این مسأله به نظر می‌رسید رسیدن به توافق ۹۵ درصدی امکان‌پذیر نباشد. از طرف دیگر طرفداران بلاک‌های کوچک معتقد بودند سیگنال‌های ماینرها فقط به معنی اعلام آمادگی یا ابزاری برای تأمین امنیت هرچه بیشتر شبکه است. از نظر آن‌ها کاربران در مورد اعمال قوانین جدید تصمیم‌شان را گرفته بودند و سیگنال ماینرها فقط برای اطمینان از امنیت شبکه در شرایط گذار به قوانین جدید است و فرآیندی برای رأی‌گیری سیاسی از ماینرها نیست.

علاوه بر این آستانه ۹۵ درصدی هم از هوا نیامده بود و سه سافت فورک آخر پروتکل هم بر اساس همین آستانه ۹۵ درصدی بر روی شبکه فعال شده بودند: BIP-66 (که قالب امضاهای دیجیتال تراکنش را به الگوی DER محدود می‌کرد) و در جولای ۲۰۱۵ فعال شد، BIP-65 (قابلیت CLTV[2]) که در دسامبر ۲۰۱۵ فعال شد، BIP-112، BIP-68، و BIP-113 که سه سافت فورک مختلف بودند و با یکدیگر در جولای ۲۰۱۶ بر روی شبکه فعال شدند. برای سگویت هم تصمیم بر آن بود که از همین روش فعال سازی (با

1 Grace period
2 Check Lock Time Verify

اندکی تغییرات) استفاده شود. لازم به ذکر است که فعال‌سازی سافت فورک‌های قبلی که پیشتر به آن‌ها اشاره کردیم هم بی‌نقص پیش نرفته بود. فعال‌سازی BIP-66 در جولای سال ۲۰۱۵ باعث به‌وجود آمدن شکافی در زنجیره[1] بیت‌کوین شد که تا چند بلاک ادامه پیدا کرد، چون ماینرها علی‌رغم اعلام سیگنال آمادگی، هنوز نرم‌افزار خود را [به نسخه مورد نیاز] برای این سافت فورک به‌روز نکرده بودند. اعمال سافت فورک جولای ۲۰۱۶ هم بیشتر از حد انتظار طول کشید و جامعه فعالان بیت‌کوین مجبور شد برای جلب حمایت مدیران استخرهای استخراج[2] و اعلام سیگنال آمادگی، با آن‌ها لابی کند. سرعت به‌روزرسانی نرم‌افزار استخرهای استخراجی که از طرفداران بلاک‌های بزرگ بودند کندتر بود، شاید به این دلیل که سگویت را درک نکرده بودند و دل خوشی هم از Bitcoin Core نداشتند.

با توجه با تاریخچه فوق و تنش جدیدی که در جامعه فعالان بیت‌کوین به وجود آمده بود، در زمان انتشار نرم‌افزار سگویت هیچ‌کس از اینکه آیا ماینرها آن را بر روی شبکه فعال می‌کنند یا نه، اطمینان نداشت. درواقع یکی از استخرهای استخراج بیت‌کوین به نام ViaBTC حتی قبل از انتشار نرم‌افزار اعلام کرده بود که از این سافت فورک پشتیبانی نخواهد کرد[3]. سگویت اگرچه از نظر فنی و مهندسی یک جادوگری بود، اما نتوانست در این درگیری کاری در کاهش تنش‌ها از پیش ببرد.

1 Chain-split
2 Mining pools
3 https://bitcoinmagazine.com/articles/segregated-witness-officially-introduced-with-release-of-bitcoin-core-1477611260

(تلاش می‌کنیم به مرور فصل‌های بعدی این کتاب را ترجمه و به آن اضافه کنیم)

پیوست

مشکل تغییرپذیری تراکنش‌ها

ساختار و نحوه قرار گرفتن اطلاعات تراکنش‌ها در بلاک‌های بیت‌کوین از همان ابتدا موجب بوجود آمدن یک مشکل در بیت‌کوین شده بود که به مشکل «تغییرپذیری تراکنش‌ها[1]» معروف بود. یکی از رویدادهای مهمی که به باور برخی از کارشناسان به‌دلیل وجود این مشکل به وقوع پیوست، رخداد هَک صرافی «مت.گاکس[2]» است. این اتفاق در فوریه سال ۲۰۱۴ رخ داد و در نهایت باعث بسته شدن و ورشکستگی این صرافی شد. در این حادثه هکرها ۸۵۰,۰۰۰ بیت‌کوین به سرقت بردند.

مشکل تغییرپذیری تراکنش‌ها چیست؟

تراکنش‌های بیت‌کوین از دو بخش عمده تشکیل می‌شوند. بخش اول حاوی اطلاعات پایه‌ای تراکنش است و در آن مشخص می‌شود کدام کوین‌ها از کجا و به چه آدرسی منتقل می‌شوند و اطلاعاتی از این قبیل. بخش دوم به «گواهی[3]» معروف است و شامل داده‌های رمزنگاری و امضای دیجیتالی است و ثابت می‌کند کسی که می‌خواهد این کوین‌ها را جابه‌جا کند واقعاً صاحب آن‌ها است.

1 Transaction malleability
2 Mt.Gox
3 Witness

این امضای دیجیتالی مشکلی دارد که به اشکال تغییرپذیری[1] معروف است. مشکل این است که بعد از ساختن این امضای دیجیتالی می‌توان آن را کمی تغییر داد، و این تغییر اعتبار آن را خدشه‌دار نمی‌کند. این مسأله به این معنی است که شناسه[2] این تراکنش می‌تواند توسط نودهایی که تراکنش را به نودهای ماینرهای بیت‌کوین می‌رسانند، (در بین راه) تغییر کند.

این مسأله به خودی خود مشکلی پیش نمی‌آورد. تراکنش‌ها با وجودی که امضای دیجیتال و بالتبع شناسه آن‌ها تغییر کرده است، همچنان معتبرند و بیت‌کوین‌ها را بین ارسال و دریافت‌کننده جابه‌جا می‌کنند. هرچند یک مشکل دیگر پدید خواهد آمد؛ اینکه دیگر نمی‌توان تراکنش‌های جدیدی را برپایه تراکنش‌هایی که هنوز تأیید نشده‌اند[3] بسازیم. تراکنش‌های جدید باید شناسه تراکنشی که به آن وابسته هستند را بدانند، یعنی این شناسه باید تغییرناپذیر باشد. بنابراین با وجود مشکل تغییرپذیری تراکنش‌ها ساخت پروتکل‌های لایه دوم[4] مثل لایتنینگ[5] بسیار دشوار خواهد بود.

راه‌حل برطرف کردن این مشکل

یک راه‌حل طرح شده برای حل این مشکل این بود که داده امضای دیجیتال از بقیه داده‌های تراکنش حذف شود. این موضوع در سال ۲۰۱۲ میلادی توسط «راسل کانر[6]»، «مت کورالو[7]»، «لوک دش‌یر[8]»، و «گرگوری مکسول[9]» و «تی‌مس[10]» مدیر سایت

1 Malleability bug
2 TxId
3 Unconfirmed Transactions
4 Second layer
5 Lightning
6 Russell O'Connor
7 Matt Corallo
8 Luke Dashjr
9 Gregory Maxwell
10 Theymos

«بیت‌کوین‌تاک[1]» در کانال «آی‌آرسی[2]» توسعه بیت‌کوین مورد بحث قرار گرفت ولی در آن زمان روش موجهی برای پیاده‌سازی و اعمال آن بر روی شبکه پیدا نشد.

یک سال بعد و در آگوست سال ۲۰۱۳ میلادی این موضوع دوباره بر سر زبان‌ها افتاد و «پیتر تاد[3]» و گرگوری مکسول برنامه‌نویسان بیت‌کوین، مجدداً درباره روش حل این مشکل در کانال آی‌آرسی بیت‌کوین به بحث پرداختند. این بار آن‌ها کمی در پیدا کردن روش حل این مشکل پیشرفت کرده بودند. مکسول نوشت: «من پیشنهاد می‌کنم شناسه تراکنش را بدون احتساب امضای دیجیتال تراکنش محاسبه کنیم».

یک ماه بعد، مکسول و استاد معروف رمزنگاری دکتر «آدام بک[4]» دوباره درباره این مشکل در کانال آی‌آرسی بیت‌کوین با یکدیگر به بحث پرداختند. در این گفتگو آدام بک روش حذف امضای دیجیتال برای محاسبه شناسه تراکنش را مجدداً پیش کشید. هرچند مکسول این بار در پاسخ به این روش عنوان کرد: «جدا کردن بخش امضای دیجیتال می‌تواند مشکل را حل کند ولی این تغییر به یک «هارد فورک[5]» اساسی نیاز دارد و اجرای آن بسیار مشکل است.»

در ماه آگوست سال ۲۰۱۴ میلادی شرکت بلاک‌استریم[6] توسط آدام بک و گرگوری مکسول، همچنین با همراهی «آستین هیل[7]» و چند تن از برنامه‌نویسان پروتکل بیت‌کوین مثل دکتر «پیتر والا[8]» تاسیس شد. این شرکت می‌خواست روی« زنجیره‌های جانبی[9]» تمرکز کند. زنجیره‌های جانبی که می‌توانستند به شبکه بیت‌کوین وصل[10] شوند.

1 Bitcointalk.org
2 IRC
3 Peter Todd
4 Adam Back
5 Hard fork
6 Blockstream
7 Austin Hill
8 Pieter Wuille
9 Sidechains
10 Pegged

در اوایل سال ۲۰۱۵ میلادی مهندسان شرکت بلاک‌استریم تصمیم گرفتند ویژگی جدیدی را در نمونه اولیه زنجیره جانبی خود که «المنت[1]» نام داشت پیاده‌سازی کنند. این ویژگی با جدا کردن داده‌های مربوط به امضای دیجیتال از دیگر داده‌های عمومی تراکنش، مشکل تغییرپذیری تراکنش را به‌طور قطعی حل می‌کرد. نامی که برای آن انتخاب کردند هم «سگویت[2]» بود.

هارد فورک‌ها[3] و سافت فورک‌ها[4]

بخش‌هایی از کتاب «اختراع بیت‌کوین» برای توضیح مفاهیم پیش‌نیاز در این قسمت آورده شده است.

تا اینجا متوجه شدیم که نرم‌افزار بیت‌کوین چگونه قوانینی را که افراد روی آن‌ها توافق دارند در شبکه اعمال می‌کند و فهمیدیم که افراد چگونه قوانینی را که موافق آن هستند با استفاده از انتخاب نسخه نرم‌افزار اجرا می‌کنند.

همچنین توضیح دادیم که چطور ماینرها درهنگام تولید بلاک قوانین شبکه را رعایت می‌کنند و باید بلاک‌ها را به گونه‌ای تولید کنند که مورد قبول کاربران باشد، در غیر این صورت باید ریسک رد شدن بلاک و از دست رفتن پاداش بلاک را بپذیرند.
درنهایت، می‌دانیم که نرم‌افزار بیت‌کوین طولانی‌ترین زنجیره‌ای که بیشترین حجم انباشته اثباتِ کار را در خود جای داده باشد به عنوان زنجیره معتبر می‌پذیرد، و می‌دانیم که چند شاخه شدن زنجیره‌ها (یا به‌اصطلاح فورک‌ها) به دلایلی که در فصل ۶ کتاب «اختراع بیت‌کوین» به تفصیل توضیح داده شده اتفاق می‌افتند.

1 Element
2 SegWit (Segregated Witness)
3 Hard Fork
4 Soft Fork

حالا بیایید به فورک‌هایی که به عمد ایجاد می‌شوند بپردازیم. فورکِ عمدی زمانی‌ست که تعدادی از ماینرها و/یا کاربران با قوانین جاری بیت‌کوین موافق نباشند و تصمیم بگیرند آن را تغییر دهند. به‌طور کلی دو نوع فورک برای تغییر قوانین وجود دارد: سافت فورک، که با قوانین قبل سازگاری دارد[1] و هارد فورک که با قوانین قبل سازگار نیست[2]. ببینیم این فورک‌ها چطور اتفاق می‌افتند و مثال‌هایی از آنها را مطرح کنیم.

سافت فورک‌ها

یک سافت فورک ایجاد تغییر در قوانین اجماع بیت‌کوین است، به صورتی که تغییرات با قوانین قبلی شبکه سازگاری داشته باشد. یعنی چه؟ این یعنی اگر شما یک نود قدیمی را اجرا کنید که به‌روزرسانی نشده باشد، بلاک‌هایی که با قوانین جدید ساخته شده‌اند همچنان برای نود شما معتبر هستند. برای یک نود که با فورک جدید به‌روزرسانی شده است تمام بلاک‌هایی که قبلا نامعتبر بوده‌اند هنوز هم نامعتبر هستند اما حالا بعضی از بلاک‌های معتبر ممکن است برای این نود نامعتبر باشند. اجازه دهید با یک مثال این موضوع را روشن‌تر کنیم:

۱۲ سپتامبر ۲۰۱۰ قانون جدیدی به نرم‌افزار بیت‌کوین معرفی شد: سایز بلاک‌ها حداکثر می‌تواند ۱ مگابایت باشد. این قانون برای مقابله با اسپم‌ها در بلاک‌چین اعمال شد. قبل از این قانون، بلاک‌ها با هر سایزی قابل قبول (معتبر) بودند. با قانون جدید تنها بلاک‌های با اندازه کوچکتر از ۱ مگابایت پذیرفته می‌شدند. اگر شما یک نود قدیمی را اجرا می‌کردید که به‌روزرسانی نشده بود بلاک‌های کوچکتر همچنان برای آن معتبر بودند، پس شما تحت تاثیر قرار نمی‌گرفتید.

استفاده از سافت فورک‌ها برای به‌روزرسانی قوانین شبکه باعث بروز اختلال در شبکه نمی‌شود. چون به صاحبان نودها این امکان را می‌دهد که داوطلبانه و به مرور زمان نرم‌افزار

1 Backwards compatible
2 Backwards incompatible

نود خود را به‌روزرسانی کنند. اگر این کار را هم انجام ندهند، می‌توانند همچنان مثل گذشته به فعالیت خود ادامه دهند. فقط ماینرها که بلاک‌ها را تولید می‌کنند باید نرم‌افزار نود خود را به‌روز کنند تا بلاک‌های تولیدشده از قوانین جدید پیروی کنند. وقتی یک ماینر قانونِ محدودیت ۱ مگابایت را در فورک جدید به‌روزرسانی می‌کرد، سایز تمام بلاک‌های بعدی او حداکثر ۱ مگابایت بود و ممکن بود کاربرانی که نسخه‌های قدیمی نرم‌افزار را اجرا می‌کردند اصلاً از قضیه خبردار نمی‌شدند.

هارد فورک‌ها

هارد فورک نقطه مقابل سافت فورک است. در یک هارد فورک تغییری که با قوانین گذشته سازگار نیست در شبکه اعمال می‌شود و بلاک‌هایی که قبلاً نامعتبر بودند حالا در شبکه معتبر خواهند بود. در یک هارد فورک نودهای قدیمی که به‌روزرسانی نشده‌اند دیگر نمی‌توانند بلاک‌هایی را که تحت قوانین جدید ایجاد شده‌اند بررسی کنند. به همین دلیل تا نرم‌افزار خود را به‌روزرسانی نکنند در زنجیره قبلی باقی خواهند ماند. یکی از نمونه‌های هارد فورک افزایش سایز بلاک‌ها از ۱ مگابایت به سایز بیشتری بود. چون بلاک بزرگ‌تر از ۱ مگابایتی که بر اساس قانون قبلی نامعتبر بود، بعد از اعمال هارد فورک و بر اساس قوانین جدید معتبر است.

هارد فورک‌هایی که در آن‌ها همه نودهای شبکه روی تغییرات جدید با یکدیگر هم رأی هستند، در شبکه مشکلی ایجاد نمی‌کنند. همه نودها باید سریعاً نرم‌افزار خود را به‌روزرسانی کنند. اگر کسی در جریان نباشد و از ایجاد تغییرات در قوانین اطلاع نداشته باشد، دیگر بلاک‌های جدید را دریافت نخواهد کرد و اگر خوش‌شانس باشد متوجه می‌شود که نرم‌افزار ازکار افتاده است و وادار به ارتقاء نرم‌افزار خود خواهد شد.

هارد فورک‌ها درعمل به این سادگی پیش نمی‌روند. در یک سیستم آنارشیستی و غیرمتمرکز، نمی‌توان همه را وادار به قبول قوانین جدید کرد. در اگوست ۲۰۱۷، افرادی که از شرایط بیت‌کوین در زمینه پرداخت‌های ارزان (با کارمزد کم) ناراضی بودند،

تصمیم گرفتند برای ایجاد زنجیره‌ای با بلاک‌های بزرگ‌تر یک فورک ایجاد کنند. چون قانون بیت‌کوین تولید بلاک‌هایی کمتر از ۱ مگابایت بود (با توجه به سافت فورک سال ۲۰۱۰)، این افراد تصمیم گرفتند زنجیره جدیدی ایجاد کنند که در آن اندازه بلاک‌ها بزرگتر باشد. این فورک با نام Bitcoin Cash شناخته می‌شود.

هارد فورکی مثل Bitcoin Cash که از چهارچوب قوانین بیت‌کوین خارج شده است و از جانب همه نودها و ماینرها پذیرفته نمی‌شود، یک بلاک‌چین جدید ایجاد می‌کند که قسمتی از تاریخچه آن با زنجیره اولیه مشترک است، اما از نقطه‌ای که زنجیره آن از زنجیره بیت‌کوین جدا شده است، کوین‌هایی که در آن تولید می‌شوند دیگر بیت‌کوین نیستند و بنابراین توسط هیچ نودی در شبکه بیت‌کوین پذیرفته نخواهند شد.

اینکه چه چیزی بیت‌کوین «است» و چه چیزی بیت‌کوین «نیست» در طی یک سال بعد از فورک Bitcoin Cash بحث داغی بود. بعضی از افرادی که طرفدار Bitcoin Cash بودند، اعتقاد داشتند که بیت‌کوین باید براساس آنچه که ساتوشی ۱۰ سال پیش در مقاله اولیه خود نوشته است، تعریف شود، و برای اثبات نظر خود جملاتی از مقاله را گلچین کرده بودند. اما یک سیستم مبتنی بر اجماع براساس مشاجره‌هایی که در شبکه‌های اجتماعی شکل می‌گیرند کار نمی‌کند، بلکه براساس انتخاب افراد در اجرای نرم‌افزاری خاص، برای اجرای قوانین مشخصی عمل می‌کند.

درمورد این فورک، اکثریت افرادی که نودهای مهمی از نظر اقتصادی اجرا می‌کردند (مثل کیف پول‌ها، صرافی‌ها و پذیرندگان بیت‌کوین) نمی‌خواستند نرم‌افزار خود را با چیزی که گروه کمتری از آن حمایت می‌کنند و تیم کم‌تجربه‌تری آن را توسعه داده است عوض کنند. همین‌طور میزان توان هشِ شبکه ناچیز آن نشان می‌داد افراد کمتری خواهان تغییر این قوانین هستند. همچنین افراد فکر می‌کردند که چنین «ارتقاءای» ارزش برهم زدن اکوسیستم را ندارد. مشکل هارد فورک‌ها این است که آنها زمانی موفقیت‌آمیز هستند که همه آن را بپذیرند، ولی اگر اختلاف نظر به‌وجود بیاید، دو کوین متفاوت ایجاد

می‌شود. پس بیت‌کوین همان بیت‌کوین باقی ماند و Bitcoin Cash، کوین جداگانه‌ای شد.

امروزه تعداد زیادی فورک بیت‌کوین ایجاد شده است، مثلBitcoin Gold و Bitcoin Diamond وBitcoin Private، که توان هشِ شبکه ناچیزی امنیت آنها را تامین می‌کند و توسعه‌دهندگان کمتری مشغول توسعه آن‌ها هستند و تقریبا فعالیت اقتصادی ندارند. بسیاری از آنها به طور واضحی مصداق کلاه‌برداری، یا پروژه‌های تحقیقاتی سطح پایینی هستند. صدها کوین شبیه به بیت‌کوین وجود دارند که کدهای مشابهی دارند اما تاریخچه حساب (مجموعه UTXO) آن‌ها از بیت‌کوین جدا است، مثل Litecoin و Dogecoin.

کتاب The Blocksize War تألیف Jonathan Bier و تهیه شده در بخش تحقیق و پژوهش شرکت BitMEX است.

ترجمه فارسی این کتاب توسط مترجمان ناشناس، و بازبینی و صفحه‌بندی ویراست اول آن توسط سایت منابع فارسی بیت‌کوین و به سرپرستی الف.آزاد انجام شده است.

منابع فارسی بیت‌کوین
ویراست اول
بهار ۱۴۰۰