



مناقشه سائز بلاک بیت کوین

بررسی جنگ داخلی که بین سالهای ۲۰۱۷-۲۰۱۵ به هدف
به دست گرفتن کنترل قوانین پروتکل بیت کوین رخ داد

"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

قوانین پروتکل بیت کوین شبیه به قوانین شطرنج است؛ می‌توانید تغییرشان دهید ولی کسی با شما بازی نخواهد کرد.

@100trillionUSD (PlanB)

سخنی با خوانندگان

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

بیت کوین مجموعه‌ای از قوانین شفاف است و در قالب یک پروتکل و نرم‌افزار اپن سورس^۱ ارائه می‌شود، اما تغییر یا ارتقاء این قوانین چگونه انجام می‌پذیرد؟ استخراج‌های ماین بیت کوین با توان هش بالا بلاک‌های زنجیره بیت کوین را می‌سازند، توسعه‌دهندگان بیت کوین پیشنهادهای فنی ارائه می‌کنند و مسئول نگهداری و ارتقاء نرم‌افزار بیت کوین هستند، و در نهایت کاربران بیت کوین با اجرای فول‌نود از قوانین شبکه حفاظت می‌کنند. هر کدام از این بازیگران تا کجا برای تغییر قوانین شبکه بیت کوین آزادی عمل و اختیار دارند؟

یک پاسخ کلی به این سؤال این است که سه‌گانه استخراج‌های ماین، توسعه‌دهندگان، و کاربران بیت کوین بر اساس قوانین طراحی شده بر پایه نظریه بازی^۲ 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 به قدری متفاوت باشد که رسیدن به توافق غیرممکن شود، در نهایت تغییر و ارتقاء قوانین شبکه از چه راهی امکان پذیر می شود؟

بهترین روش برای بررسی دقیق این موضوع بررسی تاریخ درگیری های پیش آمده بین سال های ۲۰۱۷ - ۲۰۱۵ برای افزایش سایز بلاک است.

قبلاً مطلبی تحت عنوان «مروری بر مناقشه افزایش سایز بلاک (UASF)» در سایت منابع فارسی بیت کوین منتشر شده است که به بررسی تاریخچه مختصر این درگیری ها می پردازد. این کتاب ترجمه کتابی است که اخیراً با عنوان "The Blocksize War" توسط بخش تحقیق و پژوهش شرکت BitMEX منتشر شده است و در آن اتفاقات و رویدادهای این جنگ داخلی میان طرفداران بیت کوین از یک موضع بی طرف به تفصیل مورد بررسی قرار می گیرند.

مجوز ترجمه این کتاب به زبان فارسی از نویسنده آن آقای «جاناتان بی پر»^۱ کسب شده است و ایشان با انتشار ترجمه فارسی این کتاب به صورت رایگان موافقت کرده اند. اگر قصد حمایت از نویسنده را دارید می توانید نسخه انگلیسی این کتاب را [از سایت آمازون](#) خریداری کنید.

سایت منابع فارسی بیت کوین

بهار ۱۴۰۰

1 Jonathan Bier

فصل ۱

جرقه اول

در روز شنبه ۱۵ آگوست سال ۲۰۱۵ میلادی واقعه‌ای رخ داد که بسیاری از فعالان فضای بیت کوین را غافلگیر کرد. دو نفر از برجسته‌ترین و معتبرترین توسعه‌دهندگان بیت کوین در آن زمان یعنی «مایک هرن^۱» و «گوین اندریسن^۲» یک نسخه جدید از نرم‌افزار بیت کوین (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 بیت کوین 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 تیترا زد:

جنگ‌های بیت کوین 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 به نظر می‌رسید این جنگ، محدود به یک مسأله مشخص و جزئی؛ یعنی حداکثر سائز مجاز بلاک در بلاک چین بیت کوین باشد. نرم‌افزار Bitcoin XT پیشنهادی برای افزایش فضای موجود در بلاک‌ها ارائه می‌داد. در سال ۲۰۱۵ محدودیت سائز 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 سائز بلاک به ۸,۰۰۰ مگابایت می‌رسید، هر دو سال آن را دوبرابر کند. هدف این بود که همگام با افزایش محبوبیت بیت کوین، بلاک‌ها هم بزرگ‌تر شوند و از طرف دیگر با توجه به محدودیت ۱ مگابایتی، بلاک‌ها اغلب پر می‌شدند. طرفداران افزایش سائز بلاک معتقد بودند که بیت کوین 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 بیت کوین 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 سائز بلاک می‌توانست اکوسیستم بیت کوین 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 سائز بلاک است و ارتباط مستقیم با ذات و تعریف بیت کوین دارد و اساساً به چهار موضوع زیر مرتبط است:

۱. مقدار فضای موجود در هر بلاک بیت کوین - 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 بیت کوین از چه روشی تغییر کنند - آیا تغییر قوانین مربوط به بخش اعتبارسنجی بلاک‌های بیت کوین 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^۱ راه‌اندازی شده توسط کاربران عادی - تأثیر نودهای راه‌اندازی شده توسط کاربران عادی بیت کوین بر اعمال قوانین پروتکل بیت کوین تا چه اندازه است.

۴. ترجیحات زمانی^۲ - آیا بیت کوین به‌مانند یک شرکت نوپا^۳ 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 سائز بلاک بود. تقریباً همگان توافق داشتند که سائز ۱ مگابایتی بلاک بسیار کوچک است. اما هیچگونه اتفاق نظری بر روی تعیین سائز بلاک و نحوه تغییر آن وجود نداشت. همچنین به نظر می‌رسید اکثریت کاربران معتقدند که افزایش سائز 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»^۴ 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 کوین 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 کوین کارشان را اقدامی خصمانه یا عملی ناشایست تلقی می‌کردند.

Bitcoin XT پیاده‌سازی نرم‌افزاری BIP-101^۱ و یکی از ده‌ها پیشنهاد افزایش ساینز بلاک بود. این پیشنهاد اولین بار به‌طور رسمی توسط کوین 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»^۲ و «علامت‌دهی ماینرها»^۳. 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 ۱,۰۰۰ 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 «دورهٔ تنفس»^۴ معروف است، قوانین جدید بر روی شبکه اعمال و سرانجام ساینز 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»^۵ بسیار بحث‌برانگیز بود. دلیل اصلی آن این بود که این ارتقاء، با قوانین موجود در شبکه ناسازگار بود. اساساً به این معنی که هر کس که یک نود بیت‌کوین اجرا و قوانین شبکه را تأیید

1 Bitcoin Improvement Proposal

2 Flag day

3 Miner signaling

4 Grace period

5 Small block

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»^۱ 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 ساینز 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 گم‌کنی 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 اساسی 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.

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.

1 Hard fork

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

ما معتقدیم دیگر وقت آن رسیده است که دیدگاه خود را به روشی شفاف و روشن بیان کنیم. بعد از صحبت های طولانی با توسعه دهندگان اصلی، استخراج کنندگان، تیم های فنی خودمان، و دیگر شرکت های فعال، به این نتیجه رسیده ایم که افزایش محدودیت سائز بلاک برای موفقیت بیت کوین ضروری است.

ما از نرم افزاری که BIP-101 پیاده سازی کرده است حمایت می کنیم. استدلال های کوین اندریسن مبنی بر لزوم بلاک های بزرگ تر و کارآمد بودن نرم افزاری که تهیه شده است، در حالی که از نامتمرکز بودن شبکه بیت کوین محافظت شود - ما را قانع کرده است. اکثر ماینرها همین امروز از بلاک های ۸ مگابایتی مطرح شده در BIP-101 پشتیبانی می کنند و ما احساس می کنیم زمان آن فرا رسیده است که همه فعالان پشت این پیشنهاد با یکدیگر متحد شوند.

شرکت های ما تا ماه دسامبر ۲۰۱۵ برای بلاک های بزرگ تر آماده خواهند شد و ما نرم افزاری که برای این منظور تهیه شده است را اجرا خواهیم کرد. با رشد جامعه کاربران بیت کوین، ضروری است برای تضمین ثبات شبکه به دنبال اجماع محکمی باشیم و اکنون بیش از هر زمان دیگری به آن نیاز داریم. ما متعهد می شویم که تا ماه دسامبر ۲۰۱۵ در سیستم ها و نرم افزارهای خود از BIP-101 استفاده کنیم و دیگران را هم تشویق می کنیم به ما بپیوندند.^۱

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

این نامه توسط مدیران عامل شرکت‌های BitPay ،Blockchain.info ،Circle ،Xapo ،Bitnet ،itBit ،Kncminer و BitGo امضاء شده بود. این‌ها نه تنها 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 بیت کوین بود. این نامه شرایط را ملتهب‌تر کرد. از یک طرف برای صنعت بسیار مهم بود که با مسائل موجود در توسعه بیت کوین 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 بیت کوین به صورت 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^۱ معروف بود، معتقد بودند کوین باید بیشتر تلاش خود را معطوف به لابی کردن با کاربران بیت کوین 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 کوین 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 کوین بود تا به توسعه‌دهندگان که با او مخالفت می‌کردند نشان دهد که اصلاً مهم نیستند و شرکت‌های 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.

1 Small blockers

اکنون زمان مناسبی است تا کمی درباره کوین اندریسن صحبت کنیم. خالق بیت کوین «ساتوشی ناکاموتو»^۱ است. به طور دقیق تر، ساتوشی سیستم را طراحی کرد، نرم افزار پیاده سازی آن را که پر از اشکالات نرم افزاری بود نوشت، و مقاله معرفی^۲ آن را هم تألیف کرد. ساتوشی کمتر از ۲ سال بعد از راه اندازی شبکه و در ماه دسامبر سال ۲۰۱۰ میلادی پروژه را ترک کرد. بعد از این مرحله او دیگر مشارکتی در کُد بیت کوین نداشت و فعالیت او در انجمن های گفتگوی آنلاین هم متوقف شد. کوین توضیح می دهد که از نظر او چگونه هدایت پروژه به او سپرده شد:

با گذشت زمان ساتوشی به روش کُد نویسی من اعتماد کرد و سرانجام کار عجیبی از او سر زد. او از من پرسید آیا با قرار گرفتن آدرس ایمیل ام بر روی صفحه اصلی سایت بیت کوین موافق هستم یا نه. و من هم موافقت کردم ولی نمی دانستم او بعد از اضافه کردن آدرس ایمیل من، آدرس ایمیل خود را حذف می کند. هر کس می خواست در مورد بیت کوین اطلاعاتی به دست بیاورد به من ایمیل ارسال می کرد. ساتوشی آرام آرام از رهبری پروژه کناره گیری کرد و من را در جایگاه رهبری پروژه قرار داد.^۳

از قرار معلوم زمانی که ساتوشی پروژه را به کوین اندریسن تحویل داده است، سورس کد^۴ پروژه بر روی سایت «سورس فورج»^۵ قرار گرفته و در ژانویه سال ۲۰۱۱ نام دو نفر یعنی خود ساتوشی و کوین به عنوان نگهدارنده^۶ ذکر شده است. البته روایت کوین از وقایع مورد مناقشه است و مخالفان وی ادعا می کنند که هیچ سندی از جانب ساتوشی مبنی بر ادعای تحویل پروژه به او وجود ندارد. به ویژه ادعای «رهبر پروژه»^۷ بودن او بعید و غیرمستند به نظر می رسد. بیت کوین رهبر ندارد. کوین مخزن^۸ نرم افزار بیت کوین در

1 Satoshi Nakamoto

2 Whitepaper

3 https://www.huffingtonpost.co.uk/entry/gavin-andresen-bitcoin_n_3093316

4 Source code

5 Sourceforge

6 Maintainer

7 Leader of the project

8 Repository

سورس فورج و بعداً «گیت‌هاب»^۱ را کنترل می‌کرد تا اینکه چندین سال بعد یعنی در آوریل سال ۲۰۱۴ آن را به «ولادیمیر ون در لان»^۲ تحویل داد. کنترل مخزن نرم‌افزار البته به معنی کنترل بیت کوین 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 کوین مبنی بر تحویل گرفتن پروژه از ساتوشی درست باشد ولی ادعای رهبری پروژه کمی اغراق‌آمیز به نظر می‌رسد.

با این حال تمرکز بر روایت بحث برانگیز تحویل پروژه از ساتوشی به کوین، یا نقش فنی او در رابطه با مخزن نرم‌افزار بیت کوین 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 کوین در این فضا داشت در واقع به دلیل 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 کوین 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 بیت کوین که نسبت به کسانی که دانش فنی پایین‌تری داشتند کم‌تحمل‌تر بودند، یا ترجیح می‌دادند پشت صحنه بمانند. نفوذ او بر کامیونیتی فنی بیت کوین به دلیل شخصیت او بود، نه اینکه ساتوشی پروژه را به او تحویل داده است.

کوین همچنین در چند سال اول پروژه به‌طور قابل‌توجهی به آن کمک کرد. در سال ۲۰۱۰ و ۲۰،۰۰۰ بیت کوین به ارزش ۵۰ دلار خریداری و آن‌ها را از طریق یک

1 Github

2 Wladimir Van Der Laan

وبسایت بین مردم تقسیم کرد. فقط کافی بود آن‌ها یک پازل captcha را حل کنند تا ۵ بیت کوین به صورت 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 بیت کوین را درک نمی‌کردند و بعید بود برای خرید آن پولی خرج کنند، چون هنوز اعتمادی به آن نداشتند ولی می‌توانستند از این راه به راحتی بیت کوین به دست بیاورند. کوین در سال ۲۰۱۲ یکی از بنیانگذاران بنیاد بیت کوین^۱ و یکی از اعضای هیات مدیره آن شد. یکی از مسئولیت‌های اصلی این بنیاد علاوه بر فعالیت‌های مختلفی که داشت، پرداخت پول به کوین برای کار در زمینه توسعه بیت کوین بود. بنابراین کوین اولین توسعه‌دهنده بیت کوین بود که برای این کار پول دریافت می‌کرد. او تا اواسط سال ۲۰۱۷ و با سمت «محقق ارشد^۲» در بنیاد باقی ماند.

احترامی که اعضای جامعه بیت کوین برای کوین قائل بودند بر کسی پوشیده نیست. بسیاری او را «فرد اصلی» پروژه می‌دانستند. البته اختلافات فزاینده‌ای در سطح جامعه فنی بیت کوین وجود داشت که غالباً از چشم یک ناظر عادی دور می‌ماند. افراد زیادی اعتقاد داشتند کوین 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 بیت کوین داشت مورد قضاوت قرار دهیم. این موضوع بخاطر حمایت شخص کوین مثل بمب صدا کرد و گرنه 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 بیت کوین بود که وقت آزاد خود را در شرکت گوگل (پروژه ۲۰ درصد^۳) به بیت کوین اختصاص داده بود. با این حال، مایک به اندازه کوین درگیر توسعه نرم‌افزار اصلی^۴ بیت کوین نبود. او برخلاف کوین که

1 Bitcoin foundation

2 Chief scientist

3 20 percent free time project at Google

4 Reference implementation

محافظه کار، میانه رو و به دنبال برقراری اجماع میان کاربران بود، فردی بود که در تصمیماتش خطر می کرد و محافظه کار نبود. مایک کارهای زیادی در نرم افزار Bitconij انجام داد که یک کتابخانه با زبان جاوا^۱ برای کار کردن با پروتکل بیت کوین بود. همین کار او باعث شد امکان تولید کیف پول های قابل نصب بر روی موبایل فراهم شود که مسلماً در آن زمان کمک بزرگ و چشمگیری به فضای بیت کوین محسوب می شد.

با شدت گرفتن قائله در ماه آگوست سال ۲۰۱۵، جنگی شدید و خشن در شبکه های اجتماعی در جریان بود. دو بستر اصلی برای بحث در مورد بیت کوین در آن زمان انجمن های گفتگوی سایت BitcoinTalk و سابردیت^۲ /r/bitcoin بود. بحث و مناظره مدتی بود که در این دو بستر در گرفته بود ولی انتشار Bitcoin XT آنها را تند و آتشین تر کرد. در کل بیشتر مطالبی که منتشر می شد در حمایت از بلاک های بزرگ تر بود. پیام هواداران بلاک های بزرگ روشن و ساده بود: بیت کوین به ظرفیت بیشتری نیاز داشت. از نظر یک ناظر عادی استدلال هایی که با این دیدگاه غالب مخالف بودند، معمولاً بسیار پیچیده و تا حدی گیج کننده بودند. علاوه بر این به نظر می رسید 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 بحث های طولانی خسته شده بودند، انجمن های گفتگوی آنلاین پر شده بودند از مطالبی که از بلاک های بزرگ و نرم افزارهای ناسازگار با سیستم فعلی شبکه حمایت می کردند. آنقدر پست های تکراری وجود داشت که یافتن سایر اخبار در حوزه بیت کوین کار دشواری شده بود و کار مدیران این انجمن ها و مدیریت مطالب چند برابر شده بود. مدیریت مطالب در این انجمن ها باعث می شد طرفداران بلاک های بزرگ عصبانی شوند و از نظر آنها سیاست مدیریت یا به زعم آنها سانسور مطالب، از پیشرفت بیت کوین جلوگیری می کرد.

1 Java library
2 subreddit

انجمن‌های BitcoinTalk و ساب‌ردیت `/r/bitcoin` هر دو توسط یک شخص با نام کاربری «تی‌مُس^۱» کنترل می‌شدند. نام واقعی او «مایکل مارکوارت^۲» و یکی از پیش‌کسوتان فضای بیت‌کوین است و علاوه بر انجمن‌هایی که معرفی شدند سایت `bitcoin.it` (Bitcoin Wiki) را هم مدیریت می‌کرد. او همچنین اولین وب‌سایت بلاک‌اکسپلورر بیت‌کوین^۳ را ایجاد کرده است. یک صفحه اینترنتی که کاربران می‌توانستند در آن اطلاعات تراکنش‌هایشان^۴ را مشاهده کنند. این امر در اوایل برای توسعه فضا و آموزش مردم در مورد نحوه کار بیت‌کوین بسیار مهم بود. ولی در نهایت بلاک‌اکسپلورر `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 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 در نتیجه 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

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

اگر همه کارشناسان فعال در بیت کوین روی یک هارد فورک به یک اجماع همگانی برسند و اکثریت قریب به اتفاق کاربران و شرکت‌های بیت کوین نیز از آن پشتیبانی کنند، در این صورت می‌توانیم بگوییم به احتمال خیلی زیاد این شبکه / ارز جدید به تعریف جدید بیت کوین 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 بیت کوین 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 بیت کوین و ایجاد یک شبکه / ارز رقیب برای بیت کوین تهیه شده است وجود دارد. مورد دوم علناً در تضاد با قوانین تعیین شده برای سابردیت `/r/bitcoin` است. هرچند فناوری بیت کوین بدون توجه به این اتفاقات به کار خود ادامه می‌دهد، این تلاش‌ها برای فورک بیت کوین به اکوسیستم و اقتصاد بیت کوین 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 به دست 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 در واقع این افراد را به ترک این ساب‌ردیت تشویق می‌کند تا بتوانیم در مورد اخبار بیت کوین در آرامش به گفتگو پردازیم.^۱

قوانین جدید برای ساب‌ردیت بیت کوین کاملاً شفاف بود: از آنجا که کاربران روی Bitcoin XT توافق نداشتند و این نرم‌افزار با قوانین فعلی شبکه بیت کوین 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 خشمگین تر 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 به خاطر 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 چه کاره است که درباره توافق رسیدن یا نرسیدن ما تصمیم بگیرد؟ بیت کوین به همان اندازه که به او تعلق دارد مال من هم هست! اگر استدلال خوبی دارند پس چرا به سانسور متوسل می‌شوند؟ اگر بیت کوین 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 تی‌مُس وجود داشت، باید ببینیم افرادی که به اندازه کافی درگیر این بحث بودند، چه کسانی هستند. آن‌ها عموماً «آنارکو-کاپیتالیست»^۱ یا آزادیخواهانی^۲ 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 به خاطر 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»^۳ یا سیاست‌های پولی 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 به تدریج 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 «سوگیری تأییدی»^۴ به یک خطر جدی تبدیل شد.

به راحتی می‌توان تی‌مُس را مسئول این انشقاق در جامعه بیت‌کوین دانست. هرچند با بررسی توسعه دیگر 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 تی‌مُس 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 تی‌مُس 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 بیت کوین به وجود بیاورد؛ یا
۲. قبل از تشویق کاربران برای اجرای این نرم افزار 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 نرم افزار جدید را اجرا خواهند کرد و کوین جدیدی که به وجود آمده را به نام «بیت کوین» می شناسند.

این موضوع در حال حاضر تقریباً برای همه جا افتاده است که تلاش برای هارد فورک در شرایطی جز ۲ مورد ذکر شده، می تواند باعث یک انشعاب بسیار دردسرساز در زنجیره بیت کوین شود. متأسفانه در آن زمان، همگان از این ظرافت ها اطلاع نداشتند، بنابراین طرفداران بلاک های بزرگ نمی دانستند دقیقاً باید چه کار کنند. آن ها مطمئن نبودند آیا به یک اجماع عمومی میان همه کاربران نیاز دارند یا نه.

در مراحل اولیه درگیری به نظر می رسید که طرفداران بلاک های بزرگ در حال پیشرفت هستند و در جنگ پیروز خواهند شد. به نظر می رسید که آن ها یک پیام ساده و روشن دارند و اکثریت کاربران با آن ها موافق هستند. در همین حین شعارهای مبارزه با سانسور انجمن های گفتگوی آنلاین هم رفته رفته بیشتر مورد استقبال افکار عمومی قرار می گرفت.

اما از سوی دیگر، همچنین برای همگان روشن بود که پیشنهاد افزایش سائز بلاک مطرح شده در Bitcoin XT مبنی بر افزایش های ۸ مگابایتی سائز بلاک بر اساس یک برنامه مشخص و تا ۲۰ سال آینده خیلی افراطی است. اصلاً مایک هرن که بود که همچنین تصمیمی بگیرد؟ و او از کجا می دانست که قرار است در آینده دور چه اتفاقی برای فضای بیت کوین بیفتد؟ فضایی که بسیار سریع و غیرقابل پیش بینی تغییر می کرد. بسیاری از افراد معتقد بودند که بهتر است سائز بلاک به روش ساده تر و متعادل تری افزایش یابد. در حالی که تقریباً همه خواهان افزایش محدودیت سائز بلاک بودند ولی به نظر می رسید

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

صف آرای مخالفین

در روزهای ابتدایی بیت کوین یعنی از سال ۲۰۰۹ تا اوایل ۲۰۱۱، کل اکوسیستم بیت کوین فقط از نرم افزار بیت کوین^۱ تشکیل شده بود. این نرم افزار در ابتدا فقط روی سیستم عامل ویندوز قابل اجرا بود و از بخش های کیف پول، فول نود^۲، و ماینر تشکیل شده بود. خبری از کیف پول های موبایلی، پذیرش بیت کوین در فروشگاه ها، وب سایت های شرط بندی، بازارهای دارک وب^۳، تهاتر کالا، صرافی ها، و سرمایه گذاری شرکت ها نبود؛ فقط همین یک نرم افزار خیلی ابتدایی وجود داشت. تنها کاری که یک نفر می توانست در آن زمان انجام دهد این بود که چندتا کوین استخراج کند و آن ها را برای دیگران بفرستد یا دریافت کند. در آن زمان بیت کوین تقریباً بی فایده بود و به نظر نمی رسید که ارزشی یا آینده ای داشته باشد. در آن زمان فقط کسانی به فضای بیت کوین علاقه مند می شدند که قوه تخیل بالایی داشتند. آن ها باید آینده دور و مراحل تحول و توسعه این سیستم را در ذهن خود تصور می کردند و پیش فرض های مختلفی را در رابطه با چگونگی تکامل بیت کوین روی هم می گذاشتند.

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 بیت کوین 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 بیت کوین در رابطه با نحوه کار بیت کوین، 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 بیت کوین برای این افراد داشت، ممکن بود نتیجه وحشتناک و پیش‌بینی نشده باشد.

قیمت بیت کوین هم به مقدار قابل توجهی افزایش یافته بود و از چند سنت^۱ در سال ۲۰۱۰ به حدود ۲۲۰ دلار در تابستان سال ۲۰۱۵ رسیده بود. بنابراین بسیاری از طرفین درگیری با سرمایه‌گذاری زودهنگام در بیت کوین 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 بیت کوین 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 می‌کنند که درک بسیار خوبی از بیت کوین دارند و می‌توانند مسیر درست را برای ادامه راه بیت کوین تشخیص دهند، چون معتقدند بیت کوین را به خوبی در سال ۲۰۱۱ فهمیده‌اند و شاهد این ادعا هم سود بزرگی است که به دست 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 بیت کوین سرمایه‌گذاری کرده‌اند و منطق آن‌ها مبنی بر درک درست بیت کوین 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 سائز بلاک، تازه‌واردان هستند. به همین خاطر بود که این جنگ در مدت کوتاهی بالا گرفت و به سرعت جدی شد.

اکنون بهتر است کمی به تاریخچه اولیه بیت کوین بپردازیم. اولین نسخه از نرم‌افزار بیت کوین هیچگونه محدودیتی روی سائز 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 کد به مخزن نرم‌افزار^۱، [و به قوانین شبکه] اضافه کرد.

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

نرم‌افزار بیت کوین‌ای 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^۳» 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 سائز بلاک، وقتی سائز جدید کمتر از سائز 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 می کند به نام هارد فورک^۱ شناخته می شود. اگر در زنجیره بیت کوین یک هارد فورک رخ دهد، همه کاربران باید نرم افزار 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^۲. سافت فورک اعمال محدودیت ۱ مگابایتی اولین ارتقاء قوانین شبکه بیت کوین بود که از یک روش فعال سازی استفاده می کرد. این روش فعال سازی روش روز موعود نام دارد که قوانین جدید در یک شماره بلاک به خصوص فعال می شوند. ساتوشی هرگز دلیل واضحی برای اعمال این محدودیت بر روی سایز بلاک ارائه نداد. بسیاری از طرفداران بلاک های بزرگ معتقد بودند که این اقدام موقتی بوده، هرچند من هیچ گونه یادداشتی که این ادعا را تأیید کند پیدا نکرده ام.

رویداد مهم بعدی که طرفداران بلاک های بزرگ خیلی به آن ارجاع می دهند، در ۴ اکتبر سال ۲۰۱۰ رخ داد. هنوز از اعمال محدودیت ۱ مگابایتی بر روی سایز بلاک نگذشته بود که یکی از توسعه دهندگان بیت کوین به نام «جف گارزیک^۳»، پیشنهاد حذف آن و افزایش سایز بلاک را داد^۴. وی یک وصله نرم افزاری^۵ را با حذف قانون ۱ مگابایت ارائه کرد و معتقد بود با این کار می توان ظرفیت پردازش تراکنش های شبکه بیت کوین را به ظرفیت شرکت Paypal رساند. اگرچه جف می دانست که چنین موضوعی در آن زمان امکان پذیر نخواهد بود ولی از نظر او این کار از منظر بازاریابی و روایت^۶ بیت کوین اهمیت داشت. بعد از گذشت فقط ۱۵ دقیقه، تی مُس پاسخ داد و اظهار کرد: «این افزونه نود شما را با نودهای شبکه ناسازگار خواهد کرد». 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+ تی‌مُس. از این افزونه استفاده نکنید. این به ضرر شما تمام می‌شود و باعث می‌شود [نود شما] با شبکه ناسازگار شود. بعداً هر وقت 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^۱ 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 در نظر نمی‌گرفتند. می‌توان پیام ساتوشی مبنی بر استفاده نکردن از افزونه و افزایش بلافاصله سائز بلاک را به ناسازگاری با [نودهای] شبکه تفسیر کرد. سپس او موضع محتاط‌تری می‌گیرد و در ادامه راه‌حلی پیشنهاد می‌دهد که بتوان با استفاده از آن‌ها سائز 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»^۱ با خیال راحت از [مکانیزم] «بررسی پرداخت ساده»^۲ (بخش ۸ [وایت‌پیپر]) استفاده کنند که فقط به زنجیره سربرگ بلاک‌ها^۳ 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^۴ با سخت‌افزارهای خاص سپرده خواهد شد. این مزارع فقط یک نود در شبکه خود دارند و شبکه محلی^۵ 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^۱ است. (ECC بسیار فشرده است). هر تراکنش باید ۲ بار در شبکه منتشر^۲ شود، پس می‌شود ۱ کیلوبایت 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.^۳

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^۴ بدون نیاز به بررسی و تأیید همه تراکنش‌ها بتوانند اثبات دوبار خرج شدن^۵ 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 در واقع 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 [بیت کوین]، از شخصی به نام «جیمز ای دونالد»^۱ و درباره ابراز نگرانی در مورد ظرفیت شبکه بیت کوین بود.

برای شناسایی و مردود کردن به موقع یک تراکنش که [یک کوین را] دوبار خرج می‌کند، هر فرد باید [سابقه] اغلب تراکنش‌های گذشته را داشته باشد که اگر به صورت ساده لوحانه‌ای 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.^۲

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 بیت کوین به عنوان یک «تهدید برای شبکه» نام می‌برد و طراحی اصلی بیت کوین را در ماه جون سال ۲۰۱۰ طی گفتگویی با کوین اندریسن به صورت «ثابت و تغییرناپذیر»^۳ معرفی می‌کند:

ماهیت بیت کوین به گونه‌ای است که به محض انتشار نسخه ۰.۱v۷ طرح اصلی^۴ تا آخر عمر [بیت کوین] 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. راه حل، استفاده از یک اسکریپت بود که مسأله را طوری تعمیم دهد که طرفین معامله بتوانند تراکنش خود را به صورت یک «محمول»^۵ (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 اسکرپیت در واقع 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 اسکرپیت می گذارم.

سمت گیرنده تراکنش، الگوی اسکرپیت را بررسی می کند. در حال حاضر گیرنده فقط دو الگو را می پذیرد: پرداخت مستقیم و پرداخت به آدرس بیت کوین. نسخه های بعدی نرم افزار می توانند الگوهای جدیدی را برای انواع تراکنش ها اضافه کنند و نودهایی که نسخه یکسان یا بالاتر از آن را اجرا می کنند قادر به دریافت آن ها هستند. همه نودهای شبکه صرف نظر از نسخه ای که اجرا می کنند می توانند هر گونه تراکنش جدیدی را تأیید [اعتبار] و پردازش کنند و به بلاک ها اضافه کنند، حتی اگر از آن ها سر در نیاورند.

این طرح از انواع گسترده ای از تراکنش هایی که من سال ها قبل طراحی کرده ام پشتیبانی می کند. [مثل] تراکنش های تضمینی^۱، قراردادهای اوراق قرضه^۲، میانجی گری شخص ثالث^۳، چند امضائی^۴، و غیره. این ها مواردی هستند که اگر بیت کوین همه گیر شود، در آینده می خواهیم رویشان کار کنیم ولی باید در اوایل راه طراحی شوند تا مطمئن باشیم بعداً امکان پذیر هستند.

من معتقدم یک نسخه دیگر که با شبکه سازگار است هرگز ایده خوبی نخواهد بود. همه نودهای شبکه باید در مرحله ارزیابی اسکرپیت به نتایج یکسانی برسند و بخش زیادی از طراحی به این وابسته است. بنابراین یک نسخه جدید نرم افزار 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.^۱

ساتوشی در طول دو سال اول حضور خود در فضای بیت کوین 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 به دلیل تجربه شبکه [در دنیای واقعی و] در عمل، بیشتر از ساتوشی آن زمان درباره شبکه بیت کوین می‌دانیم. طرفداران بلاک‌های کوچک اغلب مدعی بودند بیت کوین 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 به وجود نمی‌آورد. هرچند بیت کوین 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 بیت کوین نقشی ایفا کرده‌اند.

به نظر می‌رسد ساتوشی در بحثی که در سال ۲۰۱۵ در گرفته 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 سائز بلاک را از طریق گروه ایمیلی^۱ 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 بیت کوین ادعا می‌کنند که از دیدگاه اصلی من پیروی می‌کنند ولی این کاملاً از حقیقت به دور است. هنگامی که من بیت کوین را طراحی کردم، آن را به گونه‌ای طراحی کردم که تغییرات آتی در قوانین اجماع بدون توافق اکثریت قریب به اتفاق [کاربران] دشوار باشد. بیت کوین طوری طراحی شده است که از نفوذ رهبران کاریزماتیک مصون باشد، خواه اسم آن‌ها کوین 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 در واقع نقض می‌کند.

آن‌ها از نوشته‌های قدیمی من برای تعریف چستی بیت کوین 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^۲ و تأثیرات آن بر شبکه را پیش‌بینی نکرده بودم. تبدیل بیت کوین به یک سیستم پولی 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 به جای صرفاً اعتماد به نوع دوستی [دیگران]، نودهای خودشان را اجرا کنند.

اگر دو توسعه‌دهنده بتوانند بیت کوین را فورک کنند و در مواجهه با انتقادات فنی گسترده و با استفاده از تاکتیک‌های عوام‌فریبانه در بازتعریف «بیت کوین» موفق باشند، من چاره‌ای ندارم جز اینکه اعلام کنم پروژه بیت کوین شکست خورده است. قرار بود بیت کوین هم از نظر فنی و هم از نظر اجتماعی قوی باشد. وضعیت کنونی بسیار ناامید کننده است.^۱

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^۲ 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 بیت کوین نتوانسته از روزهای اولیه خود و وابستگی به یک فرد فاصله بگیرد. بیت کوین 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 اختلاف نظر شدیدی در مورد مسائل مربوط به مقیاس‌پذیری، کارمزد تراکنش‌ها و انگیزه‌های صنعت استخراج بیت کوین در درازمدت پدید آمد. همه با هم محترمانه رفتار می‌کردند ولی به نظر می‌رسید یک اختلاف نظر 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 بیت کوین آمده «کارمزد تراکنش به انگیزه جدید ماینرها [برای ادامه کار] تبدیل خواهد شد»^۱. البته Vandroiy در تاریخ ۲۲ آپریل سال ۲۰۱۱ پرسش چالش برانگیزی مطرح کرد:

همه ماینرهای کوچک مستقل قصد دارند سودآوری خود را به حداکثر برسانند. تصمیم آن‌ها در انتخاب 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 افت 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^۲ و در نتیجه آن کاهش سختی^۳ می‌شود، و این حلقه تکرار می‌شود. با این استدلال، سختی شبکه احتمالاً تا نزدیک صفر کاهش یابد.^۴

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

با تحلیل نظر vandroy 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 ماریپیج مرگ کارمزد»^۱ رخ خواهد داد. ولی بازار کارمزد [در بیت کوین] 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 بیت کوین بود یا نه، بسیار بحث‌برانگیز بود. با خواندن این رشته مطالب^۲ 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 بیت کوین به وجود نخواهد آورد. حتی به نظر می‌رسید در ابتدا مایک هرن هم با مشکل ماریپیج مرگ 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 ماریپیج مرگ فرض را بر این می‌گذارد که من همه تراکنش‌ها را بدون در نظر 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 صرف نظر 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.^۳

به نظر می‌رسید اکثر افرادی که فکر می‌کردند مسأله ماریپیج مرگ کارمزد مشکل ساز 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 سائز بلاک از پایین آمدن کارمزد تراکنش جلوگیری خواهد کرد. بنابراین این محدودیت در سائز بلاک باعث ایجاد «مازاد تولیدکننده»^۱ 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 هرن به اهمیت مشکل مارپیچ مرگ کارمزد پی برده بود، ولی به جای محدودیت سائز بلاک، «قراردادهای تضمینی»^۲ را به عنوان یک راه حل بالقوه پیشنهاد کرد.

اولین مورد از تبلیغات عمومی روی موضوع سائز بلاک ویدیویی بود که توسط توسعه‌دهنده بیت‌کوین و از طرفداران بلاک‌های کوچک یعنی «پیتر تاد»^۳ تهیه شد. در ماه مه سال ۲۰۱۳ او یک ویدیو که به صورت حرفه‌ای تولید شده بود روی یوتوب^۴ منتشر کرد. او در این ویدئو استدلال کرد که محدودیت سائز بلاک الزامی است، تا همه کاربران بیت‌کوین بتوانند همه تراکنش‌ها را تأیید کنند و بیت‌کوین به صورت غیرمتمرکز باقی بماند. در این ویدئو گفته می‌شد «به هر کس که می‌خواهد نرم‌افزاری که استفاده می‌کنید را تغییر دهد و محدودیت ۱ مگابایتی بلاک را افزایش دهد اعتنا نکنید»

پیتر تاد همچنین به دلیل اینکه حامی اصلی قابلیت‌های «جایگزینی تراکنش با کارمزد»^۵ 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

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>

5 Replace by Fee (RBF)

که همان ورودی^۱ را خرج و کارمزد بالاتری پرداخت می‌کند، جایگزین کنند. ماینرهایی که از این قابلیت پشتیبانی می‌کنند ترجیح می‌دهند تراکنشی که کارمزد بالاتری پرداخت می‌کند را انتخاب کنند. در مقابل ماینرهایی که از این قابلیت پشتیبانی نمی‌کردند و در عوض قابلیتی به نام «انتخاب تراکنشی که اول دیده شده^۲» را به کار 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، کوین، و طرفداران بلاک‌های بزرگ با قابلیت RBF مخالف بودند، در حالی که طرفداران بلاک‌های کوچک از آن حمایت می‌کردند. اختلاف نظرهایی که در مقوله RBF و سایز بلاک وجود داشت، با هم یک تفاوت اساسی داشتند؛ موضوع محدودیت سایز بلاک به پروتکل بیت کوین 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 بیت کوین و جنبه‌های دیگر 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 ماریچ مرگ کارمزد بود.

مخالفان RBF اظهار می‌کردند که این [قابلیت] به تجربه کاربری کاربران آسیب می‌رساند و احتمال رخ دادن مشکل دوبار خرج شدن^۳ را بیشتر می‌کند، در حالی که مدافعان آن ادعا 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 [بیت کوین] با این واقعیت نداریم. انتقاد طرفداران بلاک‌های بزرگ به این قابلیت این بود

1 Transaction input

2 First seen safe (FSS)

3 Double spend

که از نظر آن‌ها ماینرها با توجه به وابستگی به کاربران بیت کوین، 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 بیت کوین وابسته است. اگر صنعت استخراج بین چند بازیگر محدود و به صورت 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 قابل توجهی بر اکوسیستم، و به طور 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»^۲ 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 سائز 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؛
- 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 آوریل سال ۲۰۱۵ یک رویداد رسمی از طرف «بنیاد بیت کوین»^۱، با عنوان DevCore در لندن برگزار شد. کوین هم در این رویداد شرکت داشت و آمده بود تا سخنرانی خود را با عنوان «چرا به زنجیره بزرگ‌تری [از لحاظ ساینز بلاک] نیاز داریم» ارائه کند. من هم در این همایش شرکت کرده بودم. کوین خیلی خوش برخورد بود و از بحث درباره این موضوع استقبال می‌کرد. کوین به من تأکید کرد که ۱ مگابایت خیلی کم و مضحک است، و خیلی از صفحات وب بیشتر [از ۱ مگابایت] هستند. از نظر او، تاریخچه فناوری اطلاعات نشان از رشد نمایی و سریع‌تر و بزرگ‌تر شدن همه چیز می‌داد. چند بار به «قانون مور»^۲ به عنوان نمونه‌ای برای نشان دادن چگونگی بهبود سیستم‌ها در گذر زمان اشاره شد، و اینکه چطور در آینده بلاک‌های بیت کوین بزرگ‌تر خواهند شد و به ساینز گیگابایت خواهند رسید و هیچگونه مشکل فنی در زمینه مقیاس‌پذیری پیش نخواهد آمد. کوین آهسته به من گفت که ساینز مطلوب او ۲۰ مگابایت است ولی اگر [مخالفان] با او همراه شوند حاضر است کوتاه بیاید و به ۸ مگابایت راضی شود. چند روز بعد یعنی در ۱۸ آوریل سال ۲۰۱۵ مایک و کوین یک جلسه پرسش و پاسخ در لندن برگزار کردند. وقتی بحث ساینز بلاک پیش آمد، کوین گفت:

1 Bitcoin foundation

2 Moore's law

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 کوین 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 کوین گستاخانه است و از این حرف‌ها خوششان نمی‌آمد. از نظر آن‌ها مسئولیت [تصمیم‌گیری برای] بیت کوین در اختیار کوین نبود؛ اگر قرار بود او از اختیاراتش استفاده و [سرخود] تغییراتی در بیت کوین ایجاد کند، پس بیت کوین برای چه به وجود آمده است؟ با ذکر P2SH او موضوع بحث برانگیزی که در ارتقاء قوانین بیت کوین به صورت سافت فورک در سال ۲۰۱۲ رخ داده بود را پیش کشید که در آن پیشنهادهای [فنی] مختلفی ارائه شده بود و کوین 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، کوین را تحت فشار قرار می‌دهد تا قضیه سائز بلاک موضع محکم‌تری بگیرد، در حالی که کوین کمی از این کار خودداری می‌کرد. حتی مایک از کوین می‌خواست دسترسی دیگر توسعه‌دهندگان بیت کوین را از مخزن کُد بیت کوین در گیت‌هاب^۳ مسدود کند و خودش کنترل مخزن را بر عهده بگیرد. از گفتگوی بیشتر با آن‌ها به نظر می‌رسید کوین در نهایت همانطور که مایک می‌خواست، موضع محکم‌تری بگیرد. هر دوی آن‌ها آشکارا فکر می‌کردند این موضوع تعیین‌کننده خواهد بود. ولی در آن زمان نمی‌دانستم چه زمانی کوین این کار را خواهد کرد و چه اقدام خاصی انجام خواهد داد.

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

در روز ۴ می سال ۲۰۱۵ کوین در وبلاگ خود مطلبی با عنوان «زمان پیاده‌سازی بلاک‌های بزرگ‌تر فرا رسیده است»^۲ 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 کوین وقت آن رسیده بود که برای پیاده‌سازی بلاک‌های بزرگ‌تر [در شبکه بیت کوین] فشار بیاورد. در روز ۷ می سال ۲۰۱۵ «ولادمیر ون در لان»^۳ نگهدارنده اصلی^۴ پروژه Bitcoin Core روی گیت‌هاب، یادداشت زیر را در قالب یک ایمیل به گروه ایمیلی بیت کوین 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 ذاتی عملی و سیاسی که باید برای برنامه‌ریزی یک هارد فورک در نظر گرفت را نادیده می‌گیرد.

Bitcoin Core نام پیاده‌سازی نرم‌افزار مرجع بیت کوین 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 هرن انتخاب^۵ و به‌عنوان نام جدید مورد استفاده قرار گرفت و اکنون کمی کنایه‌آمیز به نظر می‌رسد. کوین قبلاً مالکیت مخزن پروژه بیت کوین روی گیت‌هاب را به ولادمیر سپرده بود تا بتواند بیشتر روی جنبه تحقیقاتی بیت کوین تمرکز کند. این اتفاق هم طنزآلود است، چون به نظر می‌رسد کوین 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 دهد در مقایسه با کار طاقت‌فرسای نگهداری از پروژه بیت کوین، مهم‌تر به نظر می‌رسید و این‌طور نبود که کوین از قدرت کناره‌گیری کرده باشد. بعدها طرفداران بلاک‌های بزرگ‌تر، تصمیم کوین برای واگذاری کنترل پروژه به ولادمیر را به‌عنوان یک اشتباه مهم تلقی کردند.

2 <https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg07472.html>
3 Wladimir Van Der Laan
4 Lead maintainer
5 <http://archive.is/kwqw0>

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 بیت کوین با تغییر دادن مخزن نرم‌افزار تعیین نمی‌شوند، بلکه توسط نرم‌افزاری که کاربران بیت کوین 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 اختلاف نظر «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 کوین در جریان بود، این هارد فورک در Bitcoin Core ادغام¹ نخواهد شد و گزینه‌های کوین تا حدودی محدود است. در تاریخ ۲۹ می سال ۲۰۱۵ کوین 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 بیت کوین 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.

1 Merge

اگر به زودی به یک توافق نرسیم، در این صورت من برای بررسی یا تهیه افزونه‌های نرم‌افزاری^۱ برای پروژه Bitcoin-Xt که مایک به راه 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 [بیت کوین] و صرافی‌ها و سرویس‌های تأمین کننده خدمات کیف پول 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 به جای 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 به دست 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] به عنوان 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»^۲ [که پیشتر توضیح دادم] موفقیت آمیز باشد، 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 و گرنه عقب می‌مانند، همچنین به آن‌ها

1 patches

2 Bigger blocks now

فرصتی داده شود تا قبل از این اتفاق [یعنی اعمال قوانین جدید، نرم افزار خود را] به روزرسانی کنند.

زیرا اگر نتوانیم در این مرحله به توافق برسیم، اختیار نهایی برای تعیین اجماع، کُدی است که اکثریت پذیرندگان [بیت کوین] و صرافی‌ها و ماینرها اجرا می‌کنند.^۲

در ۲۱ جولای سال ۲۰۱۵ «پیتر والا^۳» یکی دیگر از توسعه‌دهندگان بیت کوین 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 در واقع یک مصالحه و جوابی به فشارهای کوین 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] در واقع 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.

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 کوین 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 کوین و طرفداران بلاک‌های

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>

بزرگ هیچ واکنش مثبتی نسبت به BIP-103 نشان ندادند. از نظر آن‌ها افزایش سایز بلاک در این پیشنهاد به قدری کم است که بیشتر به یک توهین شبیه است تا پیشرفت. متأسفانه به نظر نمی‌رسید BIP-103 بتواند کمکی [در رفع اختلاف نظرها] کند. به نظر می‌رسید تقاضا [برای فضای بلاک] توسط تراکنش‌های بیت کوین 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 بیت کوین 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 بیت کوین اولویت اول بود. نکته کلیدی برای آن‌ها این بود که بلاک‌های پُر در شبکه نداشته باشیم و گرنه 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 بیت کوین 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 بیت کوین 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 بیت کوین در حال رواج پیدا کردن است و یک سطح تعادل جدیدی در پذیرش کاربران جدید برای آن پدید خواهد آمد که منعکس‌کننده 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 مورد 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 مرگ 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] به خاطر 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؟ هر کسی 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 به طور 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 اتفاق نظر نمی‌رسیدند و گوین هم نقشه خود را پیش می‌برد. گفته می‌شود در ژوئن سال ۲۰۱۵ گوین نظر برخی از ماینرها و استخراج‌های استخراج چینی را در مورد پیشنهاد [افزایش ساینز بلاک خود] پرسیده است.^۱ جلسه‌ای در پکن برگزار شده و گفته می‌شود در آن ماینرها با توجه به ضعف بودن زیرساخت‌های ارتباطی و دشواری در انتشار بلاک‌هایی به این بزرگی، با افزایش ساینز 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.

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.^۲

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 چه کاره است که باید تصمیم نهایی را بگیرد؟ کسی مشکلی با شخص مایک نداشت، [اتفاقاً] به نظر می‌رسید پسر خوبی است،

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

2 <https://archive.is/KoknZ#selection-311.0-311.128>

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 صاحب اختیار [دارایی‌شان] باشند و استقلال مالی داشته باشند. این به هیچ وجه پیامی نبود که Bitcoin XT [به کاربران] منخبره 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.

فصل سوم

اولین کنفرانس مقیاس پذیری بیت کوین - مونترال

در روزهای آخر هفته، ۱۲ و ۱۳ سپتامبر سال ۲۰۱۵، کنفرانسی با عنوان «فاز اول مقیاس پذیری بیت کوین ۲۰۱۵» در مونترال کانادا برگزار شد. این کنفرانس در واقع تلاشی بود برای کمک به حل منازعاتی که در آن زمان جامعه فعالان بیت کوین را آزار می داد. 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 کوین اندریسن (به نمایندگی طرفداران بلاک‌های بزرگ) و گرگوری مکسول (به نمایندگی از طرفداران بلاک‌های کوچک) در این کنفرانس حضور داشتند. گرگوری یکی از توسعه‌دهندگان بیت کوین 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 بیت کوین ارتباط پیدا می‌کردند، از علوم کامپیوتر و رمزنگاری گرفته تا نظریه بازی^۱ و مشوق‌ها^۲ داشت. بعضی اوقات به او جادوگر بیت کوین می‌گفتند. اولین مطلب عمومی او در سایت BitcoinTalk در ماه می سال ۲۰۱۱ در مورد کارمزد تراکنش بیت کوین و انگیزه برای استخراج بود، و در آن دلیل ضروری بودن کارمزد برای تأمین امنیت شبکه [بیت کوین] 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 کوچک‌نگه 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 سائز 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 بیت کوین 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^۳ مشکلاتی واقعی هستند و احتمالاً هر کدام به اندازه‌ای در این قضیه تأثیرگذار بوده‌اند. با این حال، برخلاف ادعاهای تئوری توطئه پردازان^۴، هیچ‌کس در شرکت Blockstream عمداً بدخواه نبود و قصور در استدلال‌های شناختی ناخودآگاه بود. این مسأله در مورد کوین 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 بیت کوین 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^۱، 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 به سادگی 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 با توجه 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^۲» 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 سائز بلاک داشتم و با توجه به شرکت کنندگان 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 باقی مانده 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 فشرده‌گی 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 سائز 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 قابل توجهی 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 سائز بلاک و بحثی میان گوین و «آدام بک»^۱ 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 کوین 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 کوین می‌خواست فاصله داشته باشد، تنها موردی که آدام با آن مخالف بود افزایش مداوم تا ۸,۰۰۰ مگابایت بود که کوین از آن حمایت می‌کرد. خاطریم هست که کوین در آن پادکست از ساتوشی نقل قول می‌کرد که گفته بود نودها می‌توانند پردازش تراکنش‌ها را در مراکز داده^۱ 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 بیت کوین 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 کامپیوتری مقیاس‌پذیری بیت کوین 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^۲»، 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^۱ 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^۲ (IETF) گرفت و احتمالاً از آنها [برای حل اختلافات] در بیت کوین استفاده کرد.

دو تا از سخنرانی‌ها بیشتر از بقیه نظر من را به خود جلب کردند: یکی از آنها «پیتر رایزن»^۳ بود که اقتصاد سایز بلاک، و دیگری «جف گارزیک»^۴ 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 ماریپیج مرگ 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^۵ [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 بیت کوین 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 بیت کوین 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 پیش بینی کرد که ایده سهمیه تولید شکست خواهد خورد.

بیت کوین 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 وضوح 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 ساینز بلاک» است. جف یکی دیگر از توسعه‌دهندگان اولیه بیت کوین بود و همانطور که در فصل دوم توضیح دادیم، پیشنهاد حذف محدودیت ساینز 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 ساینز 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 بیت کوین مشکلاتی به وجود خواهد آورد و باعث منصرف شدن شرکت‌ها از کار کردن با بیت کوین 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.

بعد از ظهر، کنفرانس به گروه‌های کوچکتری تقسیم شد و من و یک گروه پنج یا شش نفره به همراه کوین در یک تیم بودیم. دیگران در مورد درس‌هایی که می‌توان از اختلافات پدید آمده در پروتکل‌های رمزنگاری آموخت مانند تصمیمات بحث‌برانگیز نحوه انتخاب یک عملگر هش^۱ صحبت می‌کردند و معتقد بودند نیاز به گفت‌وگو و صبر داریم. در مورد مفهوم «اجماع کلی»^۲ صحبت شد و روشی که نهاد IETF از آن استفاده کرده و شامل قضاوت «حس گروه»^۳ 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 هرن 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، کم‌صبر 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 بیت کوین 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 بیت کوین یک پروژه علمی نظری نیست، بلکه یک سیستم در حال کار جهانی است و کاربران واقعی دارد. به طور کلی، طرفداران بلاک‌های بزرگ کاربران فعال بیت کوین بودند و می‌خواستند استفاده از بیت کوین را ساده‌تر کنند و دوست نداشتند دانشمندان نظری علوم کامپیوتر که حتی از بیت کوین 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 بدین بودند و عنوان آنها را از «مقیاس‌پذیری بیت کوین^۱» به «متوقف کردن بیت کوین^۲» تغییر داده بودند.

1 Scaling Bitcoin
2 Stalling Bitcoin

فصل چهارم

دومین کنفرانس مقیاس پذیری بیت کوین - هنگ کنگ

چند ماه پس از برگزاری اولین کنفرانس افزایش ظرفیت بیت کوین 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 استخراج کنندگان بیت کوین 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^۱، یک پردیس تجاری در ضلع غربی جزیره هنگ کنگ و مشرف به اقیانوس برگزار شد. پروژه سایبرپورت در هنگ کنگ بحث‌برانگیز بود. قرار بود مرکز فناوری و مرکز استارت‌آپ‌های 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 در واقع لباس تبدلی برای توسعه واحدهای مسکونی است. دولت پروژه توسعه را به شرکت Pacific Century Group اعطا کرده بود، شرکتی که تحت کنترل «ریچارد لی^۲»، پسر سرمایه‌دار معروف هنگ کنگ یعنی «لی کا-شینگ^۳» 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 بیت کوین 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^۴» 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 قابل توجهی بیشتر بود و به نظر نمی‌رسید به اندازه کنفرانس مونترال ثمربخش باشد و گفتگو و بحث

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

مفیدی بین دو طرف در جریان باشد و فقط مشاجره و درگیری بین افراد بود. در اولین عصر و در مهمانی افتتاحیه سعی کردم حس و حال جمعیت را به دست آورم. این رویداد از کنفرانس مونترال بسیار بزرگ تر بود و طیف گسترده تری از افراد در آن شرکت کرده بودند. فضا بسیار خوش بینانه بود، اکثریت قریب به اتفاق شرکت کنندگان طرفداران بلاک های بزرگ بودند که انتظار داشتند این مسأله طی چند ماه آینده و با افزایش سایز بلاک حل شود. بیشتر آن ها فکر می کردند استدلال های طرفداران بلاک های کوچک به تدریج در حال شکست هستند و فقط یک اقلیت کوچک با هارد فورک افزایش سایز بلاک مخالفت می کنند.

جلسات کنفرانس هنگ کنگ شبیه به مونترال و بیشتر فنی بودند. تفاوت اساسی آن با کنفرانس مونترال حضور افراد فعال در صنعت استخراج بیت کوین 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 بیت کوین بر روی صحنه حاضر شدند. اغلب آن ها چینی زبان بودند، و چین در آن زمان ۶۵ درصد هشریت^۱ جهانی را در اختیار داشت. این جلسه با این سؤال شروع شد که آیا آن ها از افزایش سایز بلاک حمایت می کنند یا نه. جواب اکثر آن ها مثبت بود، هرچند بعضی از آن ها 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^۲» انجام می شد که در آن زمان مدیرعامل و بنیانگذار صرافی BTCC بود. بابی یکی از طرفداران دو آتشفشان بیت کوین 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 نرم افزار Bitcoin XT پیاده سازی شده بود و دیگری BIP-100 بود که توسط جف گارزیک پیشنهاد شده بود و به ماینرها اجازه تعیین سایز بلاک را می داد. اکثریت ماینرها نسبت به BIP-100 علاقه نشان می دادند و جای تعجب هم نداشت چون BIP-100 قدرت و اختیار بیشتری به آن ها می داد.

1 Hashrate
2 Bobby Lee

«وانگ چونگ^۱» گرداننده یکی از بزرگترین استخرهای استخراج بیت کوین به نام F2Pool معتقد بود ماینرها تنها گروهی هستند که می‌توانند رأی بدهند، بنابراین تصمیم‌گیری بر عهده آنان است. وی اظهار داشت بیت کوین یک سیستم اثبات کار^۲ است و گروه‌های دیگر ابزاری برای رأی دادن ندارند. با این حال او ادامه داد که سائز^۳ 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 تصمیم‌گیری [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 بیت کوین در اختیار ماینرها نیست و کنترل [قوانین] شبکه در اختیار کاربران بیت کوین است یا باید اینطور باشد. آنها می‌گفتند که اثبات کار صرفاً برای حل مشکل دوبار خرج کردن^۳ به وجود آمده و ماینرها فقط روی ترتیب قرار گرفتن تراکنش‌های [کاربران در بلاک‌ها] کنترل دارند. با این حال، بیشتر ماینرها معتقد بودند تصمیم‌گیری 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 تصمیم‌گیری 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 بیت کوین جدید تبدیل می‌شود چون زنجیره آن بیشترین اثبات کار را در خود خواهد داشت.

1 Wang Chung
2 Proof of work
3 Double spend

از نظر آن‌ها همین مفهوم اثبات کار بیشتر بود که حکمرانی بیت کوین 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 بیت کوین 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 در نظر 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 در واقع 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 بیت کوین 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 بیت کوین تأکید کرده است. ظاهراً پیام اصلی در حین ترجمه گم شده بوده چون مترجم می‌خواست 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»^۱ به ماجرا است، چون او هم در این کنفرانس حضور داشت. راجر خود را به عنوان اولین سرمایه گذار در استارت آپ های بیت کوین معرفی می کند. او مطمئناً سابقه موفقیت در سرمایه گذاری در فضای بیت کوین و حمایت از شرکت های Blockchain.info، و Bitpay، و Kraken داشته است. راجر یکی از برجسته ترین و پیگیرترین مروجان بیت کوین در روزهای اول، و همیشه هوادار آن بوده است. معروف است وقتی او برای اولین بار با بیت کوین آشنا شد، آنچنان هیجان زده شده است که چندین روز در بیمارستان بستری بوده است. به طور خاص، او همیشه علاقه زیادی به جنبه کاربردی پرداخت بیت کوین داشته و با تشویق فروشندگان برای پذیرش بیت کوین در جا انداختن بیت کوین نقش مهمی داشته است. شاید به دلیل این اشتیاق بی حد و حصری که به بیت کوین داشت و به مذاق همه خوش نمی آمد، نام مستعار «مسیح بیت کوین»^۲ را برای خود کسب کرد.

قبل از بیت کوین راجر ور شرکتی در زمینه فروش قطعات کامپیوتر به نام MemoryDealers.com داشت. پیش از آن، وی به جرم فروش غیرقانونی مواد منفجره به صورت 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 می کرد. تا جایی که من می دانم راجر به جنبه های عملی و تجاری بیت کوین علاقه داشت و تا قبل از مناقشه سائز بلاک علاقه چندانی به جنبه های فنی یا علوم کامپیوتر بیت کوین نشان نمی داد. 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 بیت کوین شناخته شده بود. متأسفانه در آن زمان صرافی Mt.GOX ورشکسته و هزاران بیت کوین 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 بی خبرند] 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^۱ 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»^۲ روی دامنه Bitcoin.com و ظاهراً بابت یک قرارداد نقلی، درگیری و دعوی پر سر و صدایی داشت. به نظر می‌رسید این موضوع به «ژانگ پنگ ژائو»^۳ 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 سائز 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،

1 subreddit
2 Star Xu
3 Changpeng Zhao

پیشنهادهای مختلف و غیره را بررسی می‌کنیم. در مرحله سوم باید دوباره کار را 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 گاویندی کردن و بازدیدهای خصوصی افراد مختلف راهی به جایی نمی‌برد. این کار را باید به صورت عمومی به انجام برسانیم و روش اپن-سورس^۱ به این شکل است.

در پایان کنفرانس جف دوباره به صحنه بازگشت. او این بار درباره پیشنهادها 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] ضروری ندارد. به نظر می‌رسید توافق شرکت کنندگان در این کنفرانس این است که فعلاً افزایش سایز بلاک بیشتر از ۲ مگابایت کمی خطرناک است. بسیاری از سخنرانان از جمله «جاناتان تومیم^۲» 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 به وجود 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 به طور رسمی کنار گذاشته نشد و طرفدارانش هم هیچ وقت به افراطی بودن سائز پیشنهادی شان و فشاری که برای افزایش سائز بلاک آورده بودند اعتراف نکردند. شاید چنین اعترافی از جانب ایشان می توانست به بهتر شدن اوضاع کمک کند. از نظر طرفداران بلاک های کوچک Bitcoin XT یک شرایط بحرانی پدید آورده بود و باعث ایجاد تنش و جنجال شده بود و پیشرفت در موضوع افزایش سائز بلاک را دشوارتر کرده بود. در حالی که از نظر طرفداران بلاک های 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» رفتیم. بیشتر بحث سر میز شام حول موضوعات کاملاً فنی بود، از جمله اینکه چگونه می توان امضاهای بیت کوین را فشرده یا با یکدیگر جمع کرد. سپس بحث به سمت کوین و تاکتیک های او رفت. آیا کوین نمی فهمد که بیت کوینرها دوست ندارند کسی به آنها بگوید چه کاری انجام دهند؟ مردم احساس می کنند صاحب بیت کوین هستند و می خواهند کنترل آن به دست خودشان باشد. Bitcoin XT از بالا به پایین به آنها تحمیل می شود و هیچ تلاشی هم نمی شود تا کاربران احساس کنند کنترل مسائل و تصمیم [نهایی] با آنها است. از نظر آنها کوین اینجا یک اشتباه بزرگ تاکتیکی مرتکب شده بود. به نظر می رسید همه افراد حاضر در میز شام با این مسأله موافق هستند و از اقدام اشتباه کوین متعجب شده اند. آنها دلسوز کوین بودند و می خواستند کوین به توصیه های آنها گوش کند و سعی کند با استفاده از یک روش دیگر و با همکاری بیشتر کاربران بیت کوین برای افزایش سائز بلاک دوباره تلاش کند تا کاربران احساس کنند بر روی پول شان کنترل دارند. یکی از حاضران در میز شام معتقد بود اگر کوین به کاربران می گفت تصمیم [نهایی] با آنها است، حتماً از او حمایت

می کردند. با این حال به نظر می رسد کوین این کار را نخواهد کرد چون او معتقد نبود که تصمیم [نهایی] با کاربران بیت کوین است.

ما آخر شب برای برگشت به جزیره هنگ کنگ یک کشتی گرفتیم. یادم می آید به آسمان خراش های سربه فلک کشیده در مرکز هنگ کنگ، شهری که قرار بود به زودی خانه جدید من باشد نگاه می کردم. مرکز شهر تحت سلطه بخش خدمات مالی یا همان چیزی است که بیت کوینرها به آن سیستم مالی سنتی^۱ می گویند. حس قدرتی که این ساختمانها به بیننده القاء می کند، این بحث را جلوی دید ما قرار می دهد. ما فقط چند صد نفر بودیم که در یک اتاق در هنگ کنگ با یکدیگر بحث و گفتگو می کردیم. آیا اصلاً بیت کوین تا این اندازه اهمیت دارد؟ آیا می تواند روزی روی پای خود بایستد و سیستم مالی را به چالش بکشد؟ اگر اکنون که فقط چند صد نفر به آن اهمیت می دهند نتوانیم این اختلاف را حل کنیم، چطور می توانیم به بیت کوین امید ببندیم؟ من به فشارهای همه جانبه ای که با رشد بیت کوین از طرف بازیگران عمده اقتصادی و سیاسی بر بیت کوین وارد خواهد شد فکر می کردم. این فشارها در آینده به قدری بزرگ خواهند بود که کار مایک و کوین 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 بیت کوین بتواند موفق شود باید تغییر قوانین آن واقعاً دشوار باشد، در غیر اینصورت قادر به ایستادگی در برابر فشارهای مؤسسات مالی عمده ای که مطمئناً با افزایش ارزش بیت کوین به سراغش خواهند آمد، نخواهد بود.

اگرچه از نظر طرفداران بلاک های بزرگ، افزایش سائز بلاک تغییر در قوانین بیت کوین نبود، بلکه در واقع پایبندی به چشم انداز اصلی بود. این تغییر به معنای واقعی و از نظر علوم کامپیوتر تغییراتی در قوانین شبکه اعمال می کرد، به این معنی که با افزایش سائز بلاک، قوانین شبکه آزادتر^۲ می شدند. با این حال [طرفداران بلاک های 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] به وجود 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^۲ [شبکه] به گونه‌ای تعریف می‌شد. اگر بیت کوین بخواهد موفق شود باید ساز و کاری وجود داشته باشد تا این شرایط حال حاضر به شکلی بقا یابد و [بر مشکلات] غلبه کند. تا جایی که من می‌دانم، به نظر می‌رسد که این «نقطه شلینگ»^۳ روی قوانین فنی اعتبار بلاک تنظیم شده بودند و هیچگونه مکانیزمی برای اطمینان از تغییرناپذیری تصور مردم^۴ 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^۵ 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 بیت کوین باشد ولی دیگر روش‌ها از آن بدتر هستند.

2 Status quo

3 Schelling point

4 People's vision

5 Winston Churchill

فصل پنجم

سگویت

در اولین جلسه از روز دوم کنفرانس مقیاس‌پذیری بیت کوین در هنگ کنگ و در یکی از اولین سخنرانی‌ها، پیتر والا، یکی از توسعه‌دهندگان بیت کوین درباره موضوعی با نام «تفکیک بخش امضای دیجیتال^۱» یا «سگویت^۲» سخنرانی کرد. سگویت راهی بود که می‌شد از طریق آن بدون نیاز به یک هارد فورک، سائز 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 بیت کوین از بخش‌های مختلفی تشکیل شده است، یکی از آن‌ها امضای دیجیتال است که به صاحب کوین اجازه خرج یا منتقل کردن کوین‌ها را می‌دهد. این امضای دیجیتال از لحاظ مقدار فضایی که اشغال می‌کند، اغلب بزرگترین بخش یک تراکنش است.

سگویت در واقع 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 امضاها دیجیتال 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^۱» می‌گوییم. این محدودیت وزن به اندازه ۴ برابر داده‌هایی که به امضای دیجیتال تراکنش مربوط نمی‌شدند (در واحد بایت)، به علاوه 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 بیت کوین به نام «لوک داش‌یر^۲» که در فلوریدا زندگی می‌کرد راهی کشف کرده بود که از طریق آن امکان اعمال سگویت به صورت یک سافت فورک بر روی شبکه بیت کوین 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 بیت کوین به پیش‌گویی می‌ماند که کسی حرف‌هایش را جدی نمی‌گیرد. با این حال کاملاً واضح بود که لوک درک فنی بسیار خوبی از بیت کوین 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 [به دلیل اعمال تغییرات از راه سافت فورک] از به وجود 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 [سگویی] 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 عمده خواه ناخواسته، یک حرکت تاکتیکی هوشمندانه از جانب طرفداران بلاک‌های کوچک در مناقشه سایز بلاک بود. این پیشنهاد به قدری خوب بود که هیچ‌گونه استدلال معتبری علیه آن وجود نداشت. کوین 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 سائز بلاک بود و سگویت این محدودیت را رفع می‌کرد و [سائز 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 سر در 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 در نظر 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 سائز 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 به دست 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 سائز بلاک 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 می کنند. در سگویت نودهایی که نرم افزار خود را به روزرسانی کرده باشند بلاک های بزرگ تر از ۱ مگابایت را می بینند که خواسته طرفداران بلاک های بزرگ هم احتمالاً همین بوده است)

- بیت کوین بر پایه زنجیره ای از امضاهای دیجیتالی است و سگویت این زنجیره را از هم پاره، و در نتیجه یک مشکل امنیتی به وجود می آورد.
- اگر یک ماینر که نرم افزار خود را به سگویت به روزرسانی نکرده است یک بلاک تولید کند، این بلاک برای نودهایی که به روز شده اند معتبر نیست و رد خواهد شد. این مسأله خطر فورک شدن زنجیره را بالا می برد. (این فقط در صورتی اتفاق می افتد که ماینر از نرم افزاری استفاده کند که عمداً به قصد فورک کردن زنجیره طراحی شده باشد)
- اگر کاربری نرم افزار خود را به سگویت به روزرسانی کرده باشد، قادر به انتقال بیت کوین به کاربری که نرم افزار خود را به روزرسانی نکرده است، نخواهد بود.
- سگویت برگشت پذیر است و در این صورت هر کس می تواند بیت کوین هایی که در آدرسهای سگویی هست را بدزدد. (لغو سگویت فقط از طریق یک هارد فورک امکان پذیر است)

بسیاری از این سوء تفاهم ها بی معنی بودند و نمی شد به راحتی برای آنها جوابیه نوشت. به نظر می رسد این افراد اصول پایه ای تراکنش های بیت کوین را هم درک نکرده بودند و سوء تفاهم ها هم از همین نشأت می گرفت. برای مثال اغلب به عبارت «آدرس با الگوی سگویت^۱» اشاره می شد، ولی سگویت یک الگوی جدید یا متفاوت برای آدرس ها ارائه نمی کرد. اگر این افراد از ساز و کار تراکنش های بیت کوین سر در نمی آورند، توضیح ساز و کار سگویت قطعاً غیر ممکن بود.

1 SegWit format address

سگویت به قدری پیچیده بود که به نظر می‌رسید حتی جف گارزیک هم آن را درک نکرده است. او معتقد بود که دو «بخش مجزا»^۱ برای بازار کارمزد به وجود خواهد آمد: یکی برای بلاک‌های ۱ مگابایتی و یکی برای بلاک‌های جدید که محدودیت وزن ۴ میلیون برای آن‌ها تعیین شده بود.^۲ در حقیقت [اینطور نبود]، سایز بلاک و وزن بلاک به گونه‌ای 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 بیت کوین 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 کیف پول 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^۳ [نرم‌افزاری] دیگر را هم برطرف می‌کرد که از بین آن‌ها می‌توان به مشکل «تغییرپذیری تراکنش»^۴ 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 Transactionalleability

تغییرپذیری تراکنش به پیوست مراجعه کنید. - م) من در اینجا خیلی وارد جزئیات نمی‌شوم ولی به‌طور خلاصه تغییرپذیری تراکنش اساساً به این دلیل به‌وجود می‌آید که شناسه یک تراکنش بیت‌کوین^۱ 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 در واقع یک اشکال [نرم‌افزاری] بود و توسعه شبکه تراکنش‌ها روی لایه دوم زنجیره اصلی بیت‌کوین معروف به «شبکه لایت‌نینگ»^۲، وابسته به برطرف شدن این مشکل بود.

[مشکل] مقیاس‌پذیری غیرخطی عملگرهای siphash یعنی با افزایش تعداد ورودی‌های یک تراکنش، تعداد عملیات هش لازم برای اعتبارسنجی این تراکنش با مربع^۳ آن‌ها افزایش می‌یابد و رابطه آن‌ها خطی^۴ نیست. این مسأله مانعی برای مقیاس‌پذیری شبکه بیت‌کوین] از راه بلاک‌های بزرگ‌تر بود، چون مهاجمان می‌توانستند تراکنش‌هایی بسازند که زمان اعتبارسنجی آن‌ها به قدری طولانی باشد که کل شبکه از کار بایستد. در واقع 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، به طوری 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، در نظر 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 سخت کوشی و دقت تیم توسعه می دانستند، اما این موضوع تا اندازه‌ای که باید مورد توجه جامعه فعالان بیت کوین قرار نمی گرفت. 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 می شدند 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 بیت کوین تصویری از این مشکلات نداشتند و به آن‌ها اهمیتی نمی‌دادند. بیت کوین موضوعی فراتر از مهندسی و علوم کامپیوتر است، علاوه بر این [مسائل فنی] بیت کوین یک سیستم اجتماعی، یک سیستم پرداخت مستقیم فعال، یک سیستم اقتصادی، و یک سیستم مالی هم هست. با در نظر گرفتن این زوایای دید مختلف نسبت به بیت کوین، 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 «دورهٔ تنفس^۱» 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 کفایت تا فرآیند اعمال این تغییر متوقف شود. بعضی از این طرفداران بلاک‌های بزرگ، معتقد بودند انتخاب آستانه فعال‌سازی 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 در نظر 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^۲) 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 فعال‌سازی (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^۱ 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^۲ 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 دل‌خوشی 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. در واقع یکی از استخرهای استخراج بیت‌کوین به نام ViaBTC حتی قبل از انتشار نرم‌افزار اعلام کرده بود که از این سافت فورک پشتیبانی نخواهد کرد^۳. سگویت اگرچه از نظر فنی و مهندسی یک جادوگری بود، اما نتوانست در این درگیری کاری در کاهش تنش‌ها از پیش‌برد.

1 Chain-split

2 Mining pools

3 <https://bitcoinmagazine.com/articles/segregated-witness-officially-introduced-with-release-of-bitcoin-core-1477611260>

فصل ششم

شبکه لایتنینگ^۱

سگویت با رفع مشکل تغییر پذیری تراکنش^۲، کاربران را قادر به ساختن تراکنش‌هایی می‌کرد که واسطه‌های خرابکار [در شبکه بیت کوین] امکان تغییر آن را نداشتند. حل این مشکل پیش‌نیاز پیاده‌سازی شبکه لایتنینگ (تکنولوژی مقیاس‌پذیری بیت کوین روی لایه دوم) بود چون با وجود این مشکل، پیاده‌سازی لایتنینگ بیش از حد پیچیده می‌شد.

شبکه لایتنینگ برای اولین بار در مقاله‌ای از «جوزف پون^۳» و «تاج درایجا^۴» در فوریه سال ۲۰۱۵ منتشر شد. چند ماه بعد مقاله مشابهی در تشریح راه‌حل‌های لایه-دوم توسط «کریستیان دکر^۵» منتشر شد.^۶ در این مقاله ساز و کار یک شبکه پرداخت لایه-دوم، روی [زنجیره اصلی] بیت کوین شرح داده شده بود. مفاهیم مشابه سال‌ها در فضای بیت کوین به بحث گذاشته شده بودند. در واقع به نظر می‌رسد این ایده از ابتدا توسط خود ساتوشی مطرح شده باشد.^۷ شبکه لایتنینگ اساساً با ادغام پرداخت‌ها منجر به کاهش تعداد تراکنش‌های

1 Lightning network

2 Transaction malleability

3 Joseph Poon

4 Thaddeus Dryja

5 Christian Decker

6 https://link.springer.com/chapter/10.1007/978-3-319-21741-3_1

7 <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002417.html>

بیت کوینی می‌شود. تراکنش‌های [روی زنجیره اصلی] بیت کوین برای باز کردن کانال‌های پرداخت^۱ مورد استفاده قرار می‌گیرند و [این کانال‌ها] پس از راه‌اندازی موجب تسهیل پرداخت‌هایی به تعداد بالا [و بدون نیاز به تراکنش‌های بیت کوینی] می‌شوند. افراد مختلف می‌توانند با یکدیگر کانال‌های پرداخت باز کنند و شبکه‌ای متشکل از کانال‌ها را تشکیل دهند. سپس پرداخت‌ها می‌توانند مسیر خود را در میان کانال‌های پرداختی که به یکدیگر متصل هستند پیدا کنند و به گیرنده نهایی برسند.

[بکارگیری] این ساختار لایه-دوم برای ساختن یک سیستم پرداخت جهانی ارزان، به اعتقاد برخی از طرفداران بلاک‌های کوچک بسیار منطقی‌تر بود. سیستم‌های پرداخت مبتنی بر [لایه اول] بلاک‌چین عموماً همه تراکنش‌ها را به همه [نودها] ارسال می‌کنند، به گونه‌ای که هر وقت شخصی پرداختی انجام می‌دهد، باید تراکنش [پرداخت] خود را برای همه اعضای شبکه ارسال کند. سپس همه اعضا باید این تراکنش [دریافت شده] را پردازش کنند تا ببینند آیا متعلق به آن‌ها است یا نه. این سیستم خصوصاً برای پرداخت‌های خرد بسیار ناکارآمد محسوب می‌شود. چرا تراکنش فردی که می‌خواهد در فرانسه یک فنجان قهوه بخرد باید توسط بنگاهی که در ژاپن بلیت کنسرت می‌فروشد بررسی شود؟ اساساً پرداخت‌های روی لایه اول بلاک‌چین بیت کوین به این شکل کار می‌کردند و از نظر طرفداران بلاک‌های کوچک این روش اصلاً منطقی نبود؛ [آن‌ها معتقد بودند] لایه اول فقط به‌عنوان زیرساختی برای یک سیستم پولی^۲ مورد نیاز است. شبکه لایت‌نینگ کارآمدتر است و ساختار شبکه پرداخت^۳ آن منطقی‌تر است. بجای انتشار یک تراکنش [پرداخت] به همه، می‌توان این تراکنش را شبیه به معماری نظیر-به-نظیر^۴، مستقیماً به دریافت‌کننده ارسال کرد. اگر یکی از طرفین معامله تقلب کند و بخواهد پولی سرقت کند، طرف مقابل می‌تواند یک تراکنش روی [لایه اول] بلاک‌چین منتشر کند و پول خود را پس بگیرد. بنابراین [در این صورت] بلاک‌چین و سازوکار اجماع برپایه اثبات کار بیت کوین، به‌عنوان یک سرویس برای حل اختلاف به کار گرفته می‌شود. ولی

1 Payment channels
2 Monetary system
3 Payment network
4 peer-to-peer

اگر هر دو طرف معامله صادق باشند و خیال تقلب در معامله نداشته باشند، نیازی به این ریزه کاری‌ها و بکارگیری فرآیند اثبات کار [روی لایه اول] نخواهد بود.

نگرانی اصلی طرفداران بلاک‌های بزرگ این بود که شبکه لایت‌نینگ بهانه‌ای برای افزایش ندادن سائز بلاک باشد و آن را برنمی‌تابیدند. [از نظر آن‌ها] مسأله سائز بلاک مشکل امروز [شبکه] بود، در حالی که شبکه لایت‌نینگ بسیار پیچیده بود، نیاز به تست و اثبات شدن داشت، و در بهترین حالت سال‌ها طول می‌کشید آماده شود و مورد استفاده قرار گیرد. از نظر آنان خیلی مهم بود که فروشندگان پذیرنده بیت کوین شوند و طی سال ۲۰۱۵ از این نظر موفقیت‌های بزرگی حاصل شده بود. در سال ۲۰۱۵ شرکت‌های Expedia, Overstock, TierDirect, Newegg, Dell, Rakuten امکان پرداخت با بیت کوین را برای مشتریان خود فراهم کردند. در ماه آوریل سال ۲۰۱۵ فروشگاه بازی‌های ویدیویی Steam شروع به پذیرش پرداخت‌های بیت کوین کرده بود. این فروشگاه‌ها بیت کوین را بر روی لایه اول بلاک‌چین دریافت می‌کردند و از شبکه لایت‌نینگ استفاده نمی‌کردند. اگر [مسیر پرداخت] بیت کوین به سمت شبکه لایت‌نینگ می‌رفت، روشی که این فروشندگان برای دریافت بیت کوین از مشتریان‌شان پیاده‌سازی کرده بودند به دلیل هزینه‌های بالا و زمان طولانی تأیید شدن تراکنش‌ها، ناکارآمد می‌شد. این برای شبکه بیت کوین یک فاجعه به بار می‌آورد و این فروشندگان احتمالاً از پذیرش بیت کوین دست می‌کشیدند و دیگر هیچ‌گاه به آن باز نمی‌گشتند. شبکه لایت‌نینگ هرچقدر هم که از نظر فنی و معماری پیشرفته باشد، اهمیتی نخواهد داشت. سرانجام بسیاری از این پذیرندگان دست از پذیرش بیت کوین کشیدند و طرفداران بلاک‌های بزرگ تا حدود زیادی درست می‌گفتند. مفهوم «اجازه ندهید یک چیز عالی دشمنی برای یک چیز خوب شود»^۱ در اینجا مصداق پیدا می‌کند. افزایش ندادن سائز بلاک به وضوح یک تصمیم بد تجاری بود و از دست دادن این پذیرندگان موجب استیصال طرفداران بلاک‌های بزرگ می‌شد.

1 Do not let the perfect be the enemy of the good

اگرچه بیت کوین از نظر طرفداران بلاک‌های کوچک یک کسب و کار تجاری، و رقیب سیستم‌های پرداخت مثل ویزا^۱، مستر کارت^۲، و یا پی‌پال^۳ نبود. بیت کوین از نظر آن‌ها شکل جدیدی از پول و مستعد تحول آفرینی در جامعه و اقتصاد بود. بیت کوین رقیب بانک‌های مرکزی بود. طرفداران بلاک‌های کوچک در کل هیچ مشکلی با تبدیل شدن بیت کوین به یک سیستم پرداخت سریع و ارزان نداشتند، فقط از نظر آن‌ها این مسأله در اولویت دوم قرار می‌گرفت و اولویت اول آن‌ها [بیت کوین به‌عنوان] شکل جدیدی از یک پول قابل اتکا بود.

این فقط یک اختلاف نظر ساده نبود، اولویت اول طرفداران بلاک‌های کوچک اجرای یک حرکت استراتژیک هوشمندانه بود و اولویت اول طرفداران بلاک‌های بزرگ را ساده‌لوحانه ارزیابی می‌کردند. پرداخت با بیت کوین در مقایسه با برخی دیگر از روش‌های متمرکز پرداخت مانند کارت اعتباری یا ارسال بین بانکی^۴، سریع و ارزان بود. با این حال، اگر بیت کوین محبوبیت پیدا کند، این سرویس‌های پرداخت به راحتی می‌توانند هزینه و زمان [انتقال پول] را کاهش دهند. در واقع از نظر معماری فناوری اطلاعات^۵، چیزی مانع این امر نخواهد بود و شبکه‌های پرداخت متمرکز کارآمدتر [از سیستم‌های پرداخت غیرمتمرکز] هستند. سیستم‌های متمرکز فناوری اطلاعات نسبت به بیت کوین یا هر سیستم غیرمتمرکز دیگری، به مراتب توانایی پردازش تراکنش‌های بیشتری را دارند و این کار را سریع‌تر و ارزان‌تر انجام می‌دهند. دلیل اینکه این سیستم‌های پرداخت متمرکز تا به امروز این کار را انجام نداده‌اند، نبود رقابت و مسائل مرتبط به مسائل حقوقی است که به‌سادگی قابل رفع هستند. این [ضعف که امروزه در سیستم‌های پرداخت متمرکز وجود دارد] به دلیل وجود نواقص اساسی در فناوری پایگاه‌های داده متمرکز نیست. اگر بیت کوین تمرکز خود را بر روی [ایجاد] یک شبکه پرداخت کم هزینه که در آن زمان مورد تأیید همگان بود می‌گذاشت، با اطمینان می‌توان گفت می‌توانست در مدت کوتاهی سهمی از بازار [پرداخت در دنیا] را بدست آورد. اگر چه این مزیت در طولانی مدت پایدار

1 VISA
2 Mastercard
3 Paypal
4 Bank wire
5 IT

نمی‌ماند. در مقابل، مؤسسات مالی سنتی قادر به رقابت با شکل جدیدی از پول که قابلیت انتقال به صورت الکترونیکی داشت و غیرقابل سانسور بود، نبودند. این موضوع می‌توانست عامل ارزش پایدار در بلندمدت باشد. به نظر می‌رسید اختلاف نظرها همچنان روی ترجیحات زمانی^۱ افراد بود.

از نظر طرفداران بلاک‌های کوچک، مسأله انتخاب بین یک شبکه پرداخت و یک سیستم پولی قوی نبود که طرفداران بلاک‌های بزرگ اولی و طرفداران بلاک‌های کوچک دومی را ترجیح دهند، مسأله این بود که ایده ایجاد شبکه پرداخت سریع و ارزان نخواهد توانست در بلند مدت مزیت رقابتی پایداری بوجود آورد. فناوری‌های برپایه تکنولوژی بلاک‌چین ویژگی‌های موردنیاز برای رسیدن به این هدف را ندارند و مقیاس‌پذیر نیستند. آن‌ها استدلال می‌کردند که تنها راه برای رسیدن به هر دو هدف این است که از راهکارهای لایه-دوم مثل شبکه لایتنینگ استفاده شود.

شبکه لایتنینگ مثل سگویت پیچیده بود و موجب سردرگمی افراد شد. ادعاهای غلطی در مورد شبکه لایتنینگ وجود داشت مبنی بر اینکه کوین‌های قفل شده در شبکه لایتنینگ در معرض «خطر اعتبار»^۲ قرار می‌گیرند، یا اینکه شبکه لایتنینگ «گسترش اعتبار»^۳ در بیت کوین را به مشکل بزرگتری تبدیل می‌کند. پیچیدگی بالای شبکه لایتنینگ قطعاً یک مشکل بود، و مسائل و نگرانی‌های موثقی درباره آن وجود داشت. یک سؤال این بود که چگونه می‌توان اطمینان پیدا کرد که کانال‌ها برای تسهیل در پرداخت از نقدینگی کافی برخوردار هستند. در شبکه لایتنینگ کاربران باید برای ایجاد انگیزه در تأمین نقدینگی، برای تراکنش‌ها کارمزد پرداخت کنند و مشخص نبود آیا این موضوع می‌تواند شرایط تبدیل شدن به یک شبکه پرداخت مطمئن و ارزان را فراهم کند یا نه. شبکه لایتنینگ همچنین در مقایسه با پرداخت بر روی بلاک‌چین بیت کوین مشکلات دیگری داشت، برای نمونه گیرنده تراکنش باید آنلاین بود و با فرستنده تعامل می‌کرد، در حالی که

1 Time preferences
2 Credit risk
3 Credit expansion

پرداخت روی بلاک چین بیت کوین چنین پیش نیازی ندارد. همچنین برای اطمینان از نقدینگی کافی و جلوگیری از به سرقت رفتن دارایی‌شان، کاربران شبکه لایت‌نینگ همواره ملزم به کنترل و مدیریت کانال‌های پرداخت خود بودند. طرفداران بلاک‌های کوچک هم این مشکلات را جدی می‌گرفتند. با این حال [آنها معتقد بودند] که این مشکلات در نهایت با استفاده راهکارهای خودکاری که سرویس‌های واسطه و کیف پول‌های خلاق بکار می‌گیرند، حل می‌شود و نیازی نیست کاربران بطور مستقیم با آنها درگیر شوند. همچنان این مسأله به ترجیحات زمانی باز می‌گردد و ممکن است سال‌ها طول بکشد تا این سیستم‌ها آماده استفاده افراد شوند و جا بیافتند.

طرفداران بلاک‌های بزرگ می‌توانستند به حق مدعی شوند که طرفداران بلاک‌های کوچک در واقع خوره‌های باهوش علوم کامپیوتر هستند و به راهکارهای پیچیده و بدون نقص (از نظر فنی) گرایش دارند ولی این روش‌ها کاربردی نیستند. گفته می‌شد طرفداران بلاک‌های کوچک در کی از مسائل تجاری ندارند و نمی‌توانند ببینند که حل این مشکلات نیاز به راهکارهای ساده‌تری دارد. با بررسی شبکه لایت‌نینگ در حال حاضر، به نظر می‌رسد طرفداران بلاک‌های بزرگ در مورد آن حق داشتند. در زمان نگارش این کتاب اگرچه شبکه لایت‌نینگ در حال جلب توجه کاربران بیشتری است و فناوری آن به سرعت در حال پیشرفت است، اما فروشندگان محدودی پذیرنده لایت‌نینگ هستند. پذیرندگان بیت کوین در پایان سال ۲۰۱۵ بیشتر از پذیرندگان امروز لایت‌نینگ به نظر می‌رسیدند. با این حال من همچنان به شبکه لایت‌نینگ خوشبین هستم و فکر می‌کنم ممکن است در طولانی مدت موفق شود.

فصل هفتم

بیت کوین کلاسیک^۱

در اواخر سال ۲۰۱۵ این مناقشه به طور قابل توجهی در حال شدت گرفتن بود. حتی یک موج از حملات منع سرویس^۲ به نودهای Bitcoin XT صورت گرفت. در ۲۸ دسامبر سال ۲۰۱۵ یکی از کاربران ردیت^۳ به نام `/u/tl212` نوشت:

به من حمله DDOS کردند. این حمله به قدری بزرگ بود که تأمین کننده اینترنت محل من را از کار انداخت. بخاطر کارهای این جنایتکاران جمعیت ساکن پنج شهر دسترسی به اینترنت خود را برای چند ساعت از دست دادند. این موضوع قطعاً باعث می شود از اجرا کردن نودها منصرف شوم.^۴

این اقدام بسیار تهاجمی و غیرقابل توجیه بود. گزارش های قابل توجهی از حملات شدید و از کار انداختن کامل ISP وجود داشت. به نظر می رسد این حملات تأثیر مخربی بر شبکه Bitcoin XT داشتند و می توان گفت تا حدودی در کارشان موفق بودند. من هیچکدام از طرفداران بلاک های کوچک که هویت واقعی آنها شناخته شده بود را نمی شناسم که از

1 Bitcoin Classic

2 Distributed denial of service (DDos) attack

3 Reddit

4 https://www.reddit.com/r/bitcoinxt/comments/3yewit/psa_if_youre_running_an_xt_node_in_stealth_mode

چنین عمل غیر اخلاقی دفاع کند، اگرچه برخی از طرفداران ناشناس بلاک‌های کوچک در سایت BitcoinTalk به عنوان یک «ضد حمله»^۱ از آن یاد می‌کردند. این حمله اهمیت یک شبکه بزرگ، توزیع شده، و نظیر-به-نظیر را برای همگان آشکار کرد، و این چیزی بود که Bitcoin XT در این مرحله برای خود فراهم نکرده بود. هرگز مشخص نشد چه کسی عامل این حملات بوده است، اگرچه ماه‌ها بعد شایعاتی درباره گرداننده یک Botnet (شبکه‌ای از کامپیوترها که برای انجام حملات منع سرویس به کار گرفته می‌شوند. -م) منتشر شد که به صورت ناشناس به او بیت کوین پرداخت کرده‌اند تا این حملات را ترتیب دهد. رفتار مهاجمان حتی در نظر طرفداران بلاک‌های کوچک غیر اخلاقی بود و بسیاری از آن‌ها معتقد بودند نتیجه عکس دارد و باعث رویگردان شدن افراد از دیدگاه‌های آنان می‌شود. به نظر من اگر فرض را بر این بگذاریم که این حملات ردگم کنی نبوده و از جانب طرفداران بلاک‌های کوچک انجام شده باشد، یک نمونه نادر از اشتباهات تاکتیکی گروه طرفداران بلاک‌های کوچک است. هدف از این مناقشه ترغیب افراد هرچه بیشتر به گروه مورد نظر بود و چنین اقدام‌های تهاجمی ثمربخش نبود. تا آنجا که من اطلاع دارم چنین حمله‌ای در طول این مناقشه تکرار نشد.

در تاریخ ۳ ژانویه سال ۲۰۱۶، «برایان آرمسترانگ»^۲ مدیر عامل شرکت «کوین بیس»^۳ (یکی از بزرگترین صرافی‌های مبادلات ارزهای دیجیتال که سرمایه‌گذاری بزرگی روی آن انجام گرفته است)، مطلبی در حمایت از بلاک‌های بزرگ در وبلاگ خود منتشر کرد. برایان همچنین از کوین پشتیبانی می‌کرد و نظرات بحث‌برانگیزی در مورد نحوه ارتقاء [پروتکل بیت کوین] داشت.

خوشبختانه در بیت کوین یک مکانیزم برای ارتقاء [پروتکل] وجود دارد که به زیبایی طراحی شده است. اگر «رأی» اکثریت ماینرهای بیت کوین برای اعمال تغییرات خاصی روی شبکه مثبت باشد، بنابراین طبق تعریف، این نسخه به بیت کوین جدید تبدیل خواهد شد. تعداد آراء هریک از ماینرها وابسته به توان

1 Counter attack
2 Brian Armstrong
3 Coinbase

محاسباتی (یا همان هش‌ریت. -م) آنها است (بنابراین راهی برای جعل رأی وجود ندارد).^۱

این دیدگاه که بیت کوین با زنجیره‌ای که بیشترین هش‌ریت را در خود جا داده است تعریف می‌شود، از نظر طرفداران بلاک‌های کوچک اشتباه بود. از نظر آنها این نودهای بیت کوین بودند که قوانین را [بر روی شبکه] اعمال می‌کردند و بلاک‌ها فقط در صورت رعایت این قوانین معتبر محسوب می‌شدند. از نظر طرفداران بلاک‌های کوچک این موضوع یکی از حیاتی‌ترین ویژگی‌های شبکه بیت کوین بود. اگر ماینرها قوانین شبکه را [به شکلی که برایان توضیح داده بود] تغییر می‌دادند، بلاک‌چین بیت کوین دوپاره و به دو زنجیره متفاوت تقسیم، و یک کوین جدید ایجاد می‌شد. [از بین این دو،] کوینی که از قوانین اصلی شبکه پیروی کند، بیت کوین خواهد بود.

از نظر طرفداران بلاک‌های کوچک فول نودهای بیت کوین در [محافظت و] اعمال قوانین پروتکل نقش بسیار مهمی داشتند، در حالی که طرفداران بلاک‌های بزرگ اینگونه فکر نمی‌کردند. از نظر طرفداران بلاک‌های بزرگ اکثر کاربران فول نود ندارند و معمولاً از نودهای سبک^۲ استفاده می‌کنند. (مانند نرم‌افزارهای کیف پول بیت کوین که همه بلاک‌ها را بررسی نمی‌کنند. با نود کم‌حجم^۳ اشتباه گرفته نشود. -م) با این حال حتی اگر از دیدگاه طرفداران بلاک‌های بزرگ به مسأله نگاه کنیم، کاربران حتی اگر فول نود نداشته باشند از نرم‌افزار کیف پول بیت کوین استفاده می‌کنند. همه کیف پول‌های بیت کوین بخشی از قوانین پروتکل بیت کوین را بررسی و اعتبارسنجی می‌کنند. بیت کوین بجز قانون ساینز بلاک، قوانین و قواعد مختلف دیگری هم دارد. مثل الگوی تراکنش‌ها، امضاهای تأیید خرج کردن، ساختار درخت مرکل^۴، الگوی سربرگ بلاک‌ها و غیره. مطمئناً منظور برایان و دیگر طرفداران بلاک‌های بزرگ این نبود که هر چیزی، مثلاً یک زنجیره هش بدون اطلاعات تراکنش‌ها [بدون رعایت قوانین شبکه و] صرفاً بخاطر هش‌ریت بالا

1 <https://blog.coinbase.com/scaling-bitcoin-the-great-block-size-debate-d2cba9021db0>
2 Light nodes
3 Pruned nodes
4 Merkle tree

می تواند به عنوان بیت کوین تعریف شود. حتی در جهان بینی طرفداران بلاک های بزرگ که در آن افراد از نودهای سبک استفاده می کردند هم بلاک ها باید از برخی قوانین پیروی می کردند.

شاید بهتر است استدلال برایان را اینگونه تفسیر کنیم که دست ماینرها در تغییر قوانین پروتکل باز است، به استثنای قوانینی که از جانب کیف پول ها به آنها تحمیل می شود. از این زاویه ایده بلاک های بزرگ منطقی تر می شود. ممکن است محدودیت ساینز بلاک از این قوانین خارج شده باشد ولی کیف پول ها مجموعه های مختلفی از قوانین را بر روی شبکه اعمال می کنند. بنابراین در مرز بین قوانینی که ماینرها می توانستند تغییر دهند و آنچه که نمی توانستند تغییر دهند، یک منطقه خاکستری وجود داشت و طرفداران بلاک های کوچک با این مسأله مخالفت می کردند. آنها می خواستند قوانین شبکه [که غیر قابل تغییر بودند] از دیگر قوانین کاملاً متمایز باشند، تا در تعیین طولانی ترین زنجیره معتبر [که بیت کوین با آن تعریف می شود] کوچکترین شک و شبهه ای وجود نداشته باشد.

من اغلب سعی می کردم نظر طرفداران بلاک های بزرگ را در این مورد جویا شوم. مثلاً از آنها می پرسیدم: اگر ماینرها مازاد بر سقف ۲۱ میلیون، برای خود بیت کوین خلق کنند و آن زنجیره اثبات کار بیشتری داشته باشد، باز هم فکر می کنید این زنجیره معرف بیت کوین خواهد بود؟ اغلب پاسخ آنها این بود که: «ماینرها هرگز چنین کاری نخواهند کرد»، یا «بیت کوین بر پایه مشوقها^۱ و نظریه بازی^۲ بنا شده و اگر ماینرها چنین کاری کنند، قیمت بیت کوین سقوط خواهد کرد»، یا «نظریه بازی در بیت کوین به گونه ای طراحی شده است که ماینرها هرگز چنین کاری نخواهند کرد». من به آنها می گفتم اگر ماینرها چنین کاری کنند، این زنجیره برای نودها و کیف پول ها نامعتبر خواهد بود و در صورتی که ماینرها از برنامه تولید بیت کوین تخطی کنند، نودها و کیف پول ها بلاک های

1 Incentives

2 Game theory

تولید شده در این زنجیره نامعتبر را دریافت نخواهند کرد. طرفداران بلاک‌های بزرگ معمولاً در جواب به این مسأله ادعا می‌کردند «نودها اهمیتی ندارند». بیت کوین برای آن‌ها یعنی بلندترین زنجیره‌ای که بیشترین اثبات کار را در خود جای داده باشد، خواه برای نودها معتبر باشد خواه نامعتبر. اگر کاربری بخواهد بخشی از شبکه بیت کوین باشد، شاید بهتر باشد نرم‌افزار نود خود را به‌روزرسانی کند تا مطمئن شود زنجیره‌ای که بیشترین اثبات کار را در خود جای داده است را دنبال می‌کند. خواه از قوانین تخطی شده باشد، خواه نشده باشد.

برای من مشخص نبود کدامیک از طرفین درست می‌گویند. به نظر من این موضوع به رفتار عموم کاربران بیت کوین بستگی داشت؛ اگر همه مثل طرفداران بلاک‌های بزرگ رفتار می‌کردند و نرم‌افزار نود خود را برای پیروی از قوانین جدید [خواه درست، خواه نادرست] به‌روزرسانی می‌کردند، حرف آن‌ها درست بود. اما اگر همه شبیه به طرفداران بلاک‌های کوچک رفتار می‌کردند و در مقابل تغییر و به‌روزرسانی نرم‌افزار نود خود مقاومت می‌کردند و سرسختی نشان می‌دادند، طرفداران بلاک‌های کوچک درست می‌گفتند. این سؤال بی‌جواب مانده بود و هیچ‌کس نمی‌دانست پاسخ درست به آن چیست. به نظر می‌رسید در هر دو طرف این مناقشه افراط‌گرایانی بودند که از جواب به این سؤال اطمینان داشتند ولی مسأله این بود که آن‌ها روی اعتقادات خود تعصب داشتند. این افراد الگوی ذهنی برای خود ساخته بودند که در آن تصور می‌کردند عموم کاربران درست مثل آن‌ها رفتار خواهند کرد. البته در واقعیت موضوع متفاوت بود چون افراد مختلف عقاید و دیدگاه‌های مختلفی دارند، بنابراین رفتار متفاوتی از خود نشان خواهند داد. به نظر می‌رسید تقریباً اکثریت کاربران باید برای تحقق نظرات طرفداران بلاک‌های بزرگ با آن‌ها موافقت می‌کردند، در حالی که طرفداران بلاک‌های کوچک فقط به توافق یک اقلیت قابل توجه نیاز داشتند. اگر از این زاویه به موضوع نگاه می‌کردیم، به نظر من طرفداران بلاک‌های کوچک درست می‌گفتند. بعضی از افراد حاضر بودند نرم‌افزار نود خود را به‌روزرسانی کنند و بعضی دیگر تمایلی به این کار نداشتند، بنابراین احتمالاً شاهد یک شکاف^۱ در زنجیره خواهیم بود.

1 Split

دیدگاه‌های متفاوت در مورد نقش فول نودها در [محافظة و] اعمال قوانین شبکه منجر به سردرگمی بیشتر همگان شد. طرفداران بلاک‌های کوچک اغلب ابراز می‌کردند که با افزایش سایز بلاک مخالف هستند، چون این امر هزینه راه‌اندازی یک نود را زیاد می‌کند و در نتیجه تعداد فول نودهای شبکه کاهش می‌یابد و این موضوع موجب متمرکز شدن شبکه می‌شود. طرفداران بلاک‌های بزرگ این مسأله را به اشتباه تفسیر می‌کردند و فکر می‌کردند طرفداران بلاک‌های کوچک نگران این هستند که به تعداد کافی «نودهای بازفرستنده»^۱ (که مسئول انتشار تراکنش‌ها و بلاک‌ها در یک شبکه نظیر-به-نظیر هستند)، در شبکه وجود نداشته باشد و در نتیجه شبکه ارتباطی بین نودها بسیار ضعیف و به چند مرکز بزرگ محدود [و متمرکز] شود. اما طرفداران بلاک‌های کوچک در کل نگران وقوع چنین تمرکزی نبودند. آن‌ها بیشتر نگران این بودند که کاربران کمتری قادر به اجرای فول نودهای بیت کوین باشند و با توجه به اینکه این فول نودها وظیفه اعمال قوانین شبکه را بر عهده دارند، این موضوع می‌تواند مکانیزم اعتبارسنجی و محافظت از قوانین شبکه را از حالت غیرمتمرکز خارج کند. به نظر می‌رسید طرفداران بلاک‌های بزرگ این نگرانی را درک نمی‌کردند و معتقد بودند لزومی ندارد عموم کاربران بیت کوین قادر باشند این فول نودها را اجرا کنند. خطر افزایش هزینه راه‌اندازی فول نود در اثر افزایش سایز بلاک و در نتیجه کاهش تعداد کاربرانی که قادر به اجرای فول نودها هستند، طرفداران بلاک‌های بزرگ را نگران نمی‌کرد و به این موضوع اهمیتی نمی‌دادند. این دیدگاه‌های متفاوت اساساً باعث می‌شد طرفین دعوا بجای گفتگو و رسیدن به درک متقابل فقط درگیر بحث و درگیری با یکدیگر شوند.

این سردرگمی اغلب با یک تصور غلط در مورد نحوه کار بیت کوین همراه بود. برای نمونه، افراد زیادی معتقد بودند که حمله ۵۱ درصدی ماینرها می‌تواند به سرقت دارایی کاربران بیت کوین منجر شود، حتی اگر فردی که این حمله را انجام می‌دهد امضای دیجیتال معتبری برای ارائه در اختیار نداشته باشد. ماینرها قادر به انجام چنین کاری نیستند، حداقل در دنیای بلاک‌های کوچک چنین چیزی ممکن نیست. نهایت کاری که ماینرها

1 Relay nodes

می‌توانند در شرایط حمله ۵۱ درصدی انجام دهند این است که یک تراکنش که امضای دیجیتال معتبری برای آن دارند را دوباره خرج^۱ کنند. البته این بدان معنا نیست که همه طرفداران بلاک‌های بزرگ این مسأله را درک نمی‌کردند، آن‌ها تا حدودی از این قضایا اطلاع داشتند. هرچه باشد این حوزه جدیدی از علوم بود که داشت برای اولین بار مورد کاوش قرار می‌گرفت. هر دو طرف درگیری در این مورد اطمینان کافی نداشتند و رسیدن به تفاهم هم زمان بر بود. شفاف نبودن این مسأله موجب شد طرفداران بلاک‌های بزرگ در دستیابی به اهداف‌شان ناموفق باشند. اگر طرفداران بلاک‌های بزرگ بجای ایجاد سردرگمی دوباره وجود چنین قوانینی، فقط بر حذف محدودیت ساینز بلاک تمرکز می‌کردند، احتمال موفقیت‌شان بیشتر می‌شد.

به نظر می‌رسد آخرین جمله وایت‌پیپر بیت‌کوین بر دیدگاه برایان مبنی بر اینکه زنجیره بیت‌کوین با هش‌ریت تعریف می‌شود صحه می‌گذاشت. این جمله به شرح زیر است:

آن‌ها توسط توان پردازنده^۲ خود رأی می‌دهند و با ساختن بلاک‌های جدید بر روی بلاک‌های معتبر و ادامه دادن آنها، و رها کردن بلاک‌های نامعتبر و ادامه ندادن آنها نظرشان را ابراز می‌کنند. با این مکانیزم اجماع می‌توان هر قانون و مشوقی که لازم باشد را به اجرا درآورد.

این نقل قول اغلب توسط طرفداران بلاک‌های بزرگ مطرح می‌شد. با این حال مشخص نیست ساتوشی اصلاً چنین دیدگاهی داشته است یا نه. چون در همان وایت‌پیپر آمده: ما این سناریو که یک مهاجم تلاش کند با سرعت بیشتری زنجیره دیگری غیر از زنجیره اصلی بسازد را در نظر می‌گیریم. حتی اگر این امر محقق شود، سیستم در معرض تغییرات خودسرانه قرار نخواهد گرفت و نمی‌توان از «هیچ» ارزشی خلق کرد، و این مهاجم نمی‌تواند پولی که به او تعلق ندارد را تصاحب کند. نودها یک

1 Double spend

2 CPU power

تراکنش نامعتبر را به عنوان پرداخت^۱ نخواهند پذیرفت، و نودهایی که قوانین شبکه را دنبال می کنند هرگز بلاکی که شامل این تراکنش نامعتبر باشد را نخواهند پذیرفت. این مهاجم فقط می تواند برای پس گرفتن پولی که به تازگی خرج کرده تلاش کند^۲. (اشاره به مفهوم دوبار خرج کردن. - م)

در نقل قول بالا ساتوشی به صورت شفاف بیان می کند که نودها قوانین خاصی را [بر روی شبکه] اعمال می کنند. مهم است که مطالب وایت پیپر را با توجه به بستر معنایی آن مورد قضاوت قرار دهیم. مطلبی که بالاتر از ساتوشی نقل قول شد در درجه اول مربوط به یک راه حل بالقوه برای مشکل دو بار خرج کردن بود. نوآوری اصلی بیت کوین این نبود که کاربران برای اعمال قوانین بر روی شبکه نودهایی اجرا کنند، بلکه سیستم استخراج بر پایه اثبات کار بود. از طرفی طرفداران بلاک های کوچک دلیل می آورند که جمله آخر وایت پیپر به این معنی است که ماینرها ترتیب تراکنش ها را تعیین می کنند. در هر صورت این دو نقل قول از ساتوشی تا حدودی با یکدیگر متناقض به نظر می رسند.

به نظر می رسد از نظر بسیاری از افراد، دیدگاه های اساساً متفاوتی در مورد نحوه کار بیت کوین وجود دارد. با این حال این موضوع لزوماً به صورت مستقیم اثری بر مناقشه سائز بلاک نداشت. مهم تر از همه، آنچه طرفداران بلاک های بزرگ واقعاً می خواستند، بلاک های بزرگ تر بود. آن ها می خواستند ماینرها روی سائز بلاک اختیار تام داشته باشند، خواه این اختیار شبیه به روش BIP-100 باشد که در آن ماینرها برای تعیین سائز بلاک رأی می دهند، خواه با برداشتن محدودیت سائز بلاک از قوانین پروتکل بیت کوین. در عوض، در فضای پیرامون این مسأله سردرگمی ایجاد شد، چون طرفداران بلاک های بزرگ اغلب ادعا می کردند که اکثریت هش ریت شبکه قادر به انجام تقریباً هر کاری هستند و کسی هم نمی تواند جلوی آن ها را بگیرد. این عدم تمرکز و عدم شفافیت به گروه طرفداران بلاک های بزرگ آسیب رساند و کار جذب حمایت کاربران بیت کوین را برای آن ها سخت تر کرد. اینکه بعد از حمایت اکثریت ماینرها و در صورت رخ دادن

1 payment

2 <https://bitcoin.org/bitcoin.pdf>

هارد فورک افزایش سایز بلاک، کاربران نرم‌افزار جدیدی که از قوانین جدید پیروی می‌کند را نصب خواهند کرد به نظر من منطقی بود. در این مورد استدلال طرفداران بلاک‌های بزرگ قابل پذیرش بود. اما اینکه بگوییم همه نرم‌افزار جدید را دانلود و نصب می‌کنند تا بلندترین زنجیره‌ای را که کوین‌های بعضی از افراد را سرقت کرده و به ماینرها داده دنبال کنند، بی‌معنی بود. اگر چنین چیزی اتفاق می‌افتاد، من مطمئنم طرفداران بلاک‌های بزرگ به سرعت از ادعای خود مبنی بر مؤثر نبودن نودهای اعمال کننده قوانین بر شبکه دست می‌کشیدند. بنابراین شاید تفاوتی که در دیدگاه‌ها به نظر می‌رسید آنچنان که به نظر می‌رسید عمیق نبود. طرفداران بلاک‌های بزرگ فقط به دنبال بلاک‌هایی با سایز بیشتر بودند. این استدلال که بیت کوین توسط بلندترین زنجیره دارای اثبات کار تعریف می‌شود را ساخته بودند چون فکر می‌کردند برای رسیدن به هدف به آن‌ها کمک می‌کند.

برایان در مطلب وبلاگ خود به تصمیم شرکت Coinbase برای ادامه حمایت از نرم‌افزار Bitcoin XT اشاره کرد:

من فکر می‌کنم Bitcoin XT یکی از چندین پیشنهاد خوبی است که از آن رضایت خواهیم داشت ولی این موضوع نیاز به تفسیر و تعبیر بیشتر ندارد. (ما روی سرورهای اصلی خود انواع نودها را راه‌اندازی کرده‌ایم؛ XT، Bitcoin Core و یک گونه دیگر که خودمان آن را نوشته‌ایم و جوابگوی مقیاس کار ما است و احتمالاً در آینده گونه‌های دیگر مثل BitcoinUnlimited را هم به زیرساخت‌های خود اضافه خواهیم کرد.)

قبل از این مطلب و توضیحاتی که برایان در وبلاگ خود نوشته بود، او توئیت‌هایی در حمایت از Bitcoin XT نوشته بود که اکنون حذف شده‌اند. تقریباً بلافاصله بعد از آن Coinbase از لیست کیف پول‌های توصیه شده در وبسایت Bitcoin.org حذف شد. این وبسایت در آن زمان یکی از منابع اصلی بیت کوین به شمار می‌رفت، و توسط

شخص ساتوشی راه اندازی شده بود^۱. این اقدام تهاجمی بسیار شبیه به سیاست مدیریت مطالب سابر دیت بیت کوین بود. این مسأله طرفداران بلاک های بزرگ را خشمگین کرد و آن ها معتقد بودند که این کار کود کانه و تفرقه برانگیز است. از طرف دیگر طرفداران بلاک های کوچک اظهار می کردند که شرکت Coinbase قصد دارد از بیت کوین به یک آلت کوین تبدیل شود. بنابراین آن ها معتقد بودند نباید در وب سایت بیت کوین لیست شود چون موجب سردرگمی کاربران خواهد شد. این موضوع درست به مانند قائله سانوسر سابر دیت بیت کوین، باعث شد طرفداران بلاک های بزرگ عزم خود را هرچه بیشتر جزم کنند و باعث عمیق تر شدن شکاف میان طرفین دعوا شد.

در اواخر دسامبر، همه از ادامه حمایت برایان از Bitcoin XT متعجب به نظر می رسیدند، چون به نظر می رسید این پیشنهاد افزایش سایز بلاک با توجه به اینکه اغلب استخراج های ماینینگ اعلام کرده بودند که سایز ۸ مگابایت بیش از حد زیاد است، تقریباً دیگر به فراموشی سپرده شده باشد. برایان در همان مطلبی که در وبلاگ منتشر شده بود، تصویری از یک جدول اکسل^۲ آورده بود که ماینرها و ترجیحات آن ها را روی سایز بلاک نشان می داد. این تصویر نشان می داد که سه استخراج استخراج بزرگ اول با پیشنهاد Bitcoin XT مخالف هستند. نظرات آن ها در مورد سایز بلاک بعد از شش ماه که از موافقت آن ها با سایز ۸ مگابایت می گذشت، تغییر کرده بود. به نظر می رسید یک افزایش سایز ساده و محافظه کارانه به ۲ مگابایت در دستور کار قرار گرفته بود و هر روز احتمال وقوع آن بیشتر می شد.

در ۱۴ ژانویه سال ۲۰۱۶ یک اتفاق مهم دیگر در مناقشه سایز بلاک رخ داد. مایک هرن اصلی ترین طرفدار Bitcoin XT از عدم پیشرفت در مسأله سایز بلاک چنان ناامید شد

1 <https://github.com/bitcoin-dot-org/Bitcoin.org/commit/7d1cdd94651461ff13ad4ed10b05b2374690fac2>

2 Excel

که اعلام کرد بیت کوین یک پروژه ناموفق است و تمام کوین‌های خود را خواهد فروخت^۱. مایک اینگونه ابراز عقیده کرد:

در نتیجه جنگ داخلی شاهد حذف نام Coinbase (بزرگترین و شناخته‌شده‌ترین استارت‌آپ بیت کوین در ایالات متحده آمریکا) از وبسایت رسمی بیت کوین بودیم، چون آن‌ها در طرف «نادرستی» از دعوا ایستاده بودند و به همین خاطر از حضور در انجمن‌های گفتگوی آنلاین فعالان بیت کوین منع شدند. وقتی بخشی از یک جامعه به طرز شریانه‌ای با افرادی که میلیون‌ها کاربر را با این ارز آشنا کرده‌اند رفتار می‌کنند، شما متوجه می‌شوید که اوضاع تا چه حد بهم ریخته است.

ابراز عقیده خشمناک و ترک بیت کوین از سوی مایک هرن در بسیاری از رسانه‌ها منتشر شد و به نظر می‌رسد باعث سقوط ۱۰ درصدی قیمت بیت کوین از ۴۳۲ دلار به حدود ۳۸۸ دلار آمریکا شد. دو روز بعد از اعلامیه مایک هرن و در ۱۶ ژانویه سال ۲۰۱۶ «جیهان وو»^۲ پیام زیر را توییت کرد:

مایک هرن بازنده نظرات نژادپرستانه و غیرمنصفانه‌ای درباره بیت کوین‌های چینی ابراز کرده بود. برای همین است که نتوانست از پشتیبانی کافی برخوردار شود^۳.

جیهان یکی از مهم‌ترین و تاثیرگذارترین بازیگران صنعت استخراج بیت کوین بود. او یکی از مدیران عامل و یکی از بنیانگذاران شرکت Bitmain، یک شرکت چینی بود که ماشین‌آلات استخراج بیت کوین تولید می‌کرد و مزرعه استخراج خود را داشت و استخراج بیت کوین را مدیریت می‌کرد. جیهان عصبانیت خود از مایک هرن که به آن شکل از پروژه کناره‌گیری کرده بود را پنهان نمی‌کرد، هرچند انتقادات او نسبت به مایک هرن تا حدودی عجیب است چون طولی نکشید که جیهان خود به یکی از افراد

1 <https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.h81ihjioy>

2 Jihan Wu

3 <https://twitter.com/JihanWu/status/688300019003162626>

کلیدی در گروه طرفداران بلاک‌های بزرگ تبدیل شد. ادعای جیهان در مورد نژادپرستی مایک به نظر من عجیب بود، چون این مسأله در تمام برخوردهایی که من با مایک داشتم سابقه نداشت. از طرف دیگر بعضی از اعضای گروه طرفداران بلاک‌های بزرگ برخی اظهارات ضد چینی را مستقیماً به خود من ابراز کرده بودند. برای مثال آن‌ها حمایت نکردن از XT را به وفاداری چینی‌ها به وضعیت ظالمانه موجود نسبت می‌دادند و شاهد آن‌ها حمایت گسترده‌ای بود که از حزب کمونیست چین می‌شد. این تعبیر از دلایل حمایت نشدن از XT به نظر من مضحک و ناپسند، و ناشی از سوگیری تاییدی بود که آن زمان در فضا بیداد می‌کرد. ممکن است مایک چنین دیدگاهی را مطرح کرده باشد ولی از نظر من خیلی بعید است. روز بعد مایک در انجمن‌های گفتگو مطلبی نوشت و در آن اظهار کرد که او یک مکالمه تلفنی پرتنش با ماینرهای چینی داشته است. به احتمال زیاد گفتگو میان آن‌ها خوب پیش نرفته و ممکن است همین امر موجب مطرح شدن اتهامات نژادپرستی شده باشد. وی در همان پست توضیح می‌دهد که چرا محدودیت ۸ مگابایتی برای سایز بلاک در XT تعیین شده؛ چون هشت در چین عدد شانس است.

چرا هشت؟ چون با کلمات چینی «رفاه» یا «ثروت» هم‌آوایی دارد.

این موضوع همواره در جامعه فعالان چینی مطرح شده است. بنابراین بدیهی است که این انتخاب بر اساس تحقیق و بررسی علمی نبوده است. مسلماً تعیین متغیرهای ثابت پروتکل بیت‌کوین بر پایه قافیه و هم‌آوایی کلمات خجالت‌آور است ولی با وجود این ما به توافق رسیدیم و این کار را انجام دادیم.

وقتی توسعه‌دهندگان Bitcoin Core پیشنهاد BIP-101 (که اکنون تغییر کرده است) را رد کردند، من و کوین با هم XT را منتشر کردیم. اینجا نظر ماینرها تغییر کرد و اعلام کردند که بجز نرم‌افزار Bitcoin Core هرگز نرم‌افزار دیگری را اجرا نخواهند کرد و این تصمیم آن‌ها نهایی است. قبلاً چنین شرطی مطرح نشده بود. از صحبت‌هایی که شخصاً با آن‌ها کرده‌ام (من تماس‌های

تلفنی مختلفی با ماینرهای سراسر جهان، از جمله ماینرهای چینی داشته‌ام) و اظهارات عمومی آن‌ها روشن شد که وفاداری آن‌ها به Bitcoin Core بی‌قید و شرط است و مهم نیست که ما چه تغییراتی در XT ایجاد کنیم، آنها هرگز آن را اجرا نخواهند کرد. بنابراین ادامه دادن موضوع بی‌معنی بود.^۱

می‌توان گفت مطرح شدن این مسائل آخرین میخ بر تابوت XT بود و طرفداران بلاک‌های بزرگ می‌بایست یک راه‌حل جدید پیدا می‌کردند. تلاش بعدی برای رسیدن به بلاک‌های بزرگ‌تر، Bitcoin Classic بود.^۲ این پیشنهاد، سایز بلاک را به یکباره به ۲ مگابایت افزایش می‌داد و نسبت به XT که شامل افزایش سایز به ۸,۰۰۰ مگابایت می‌شد، معتدل و منطقی‌تر بود. این بار به جای مایک، کوین توسعه‌دهنده اصلی این پروژه بود. جف گارزیک هم از این پیشنهاد حمایت می‌کرد و نام او در سایت Classic به‌عنوان توسعه‌دهنده درج شده بود. با توجه به رویکرد بسیار معتدل‌تری که Classic نسبت به XT داشت به نظر می‌رسید شانس موفقیت بیشتری هم داشته باشد.

به نظر می‌رسید تقریباً همه ماینرها و بازیگران اصلی فعال در بیت کوین با افزایش یکباره سایز بلاک به ۲ مگابایت موافق هستند. از طرف دیگر با توجه به سرنوشت XT یک ناکامی در سابقه تلاش برای حذف محدودیت سایز بلاک ثبت شده بود و طرفداران بلاک‌های بزرگ قصد داشتند دوباره همان روش را امتحان کنند. این موضوع موجب امیدواری طرفداران بلاک‌های کوچک شده بود. یکی از ماینرهای بیت کوین به نام «جاناتان تومیم»^۳ در کنفرانس مقیاس‌پذیری بیت کوین که در هنگ کنگ برگزار شد گفته بود که سایز ۲ مگابایت مطمئن است و از مدافعان Bitcoin Classic بود. طرفداران بلاک‌های کوچک نام این کوین را ToomimCoin گذاشتند^۴ و همانطور که

1 <https://news.ycombinator.com/item?id=10920902>

2 <https://archive.is/6QvMJ>

3 Jonathan Toomim

4 <https://bitcointalk.org/index.php?topic=1330553.0>

Bitcoin XT به مایک هرن مرتبط بود، تلاش می کردند Classic را به تومیم ارتباط دهند. نرم افزار Bitcoin Classic در ۱۰ فوریه سال ۲۰۱۶ منتشر شد.^۱

روش فعال سازی Bitcoin Classic تقریباً شبیه به Bitcoin XT بود و هیچگونه اصلاحی روی آن صورت نگرفته بود. قبل از تشویق کاربران برای نصب و اجرای نرم افزار، هیچ تلاشی برای رسیدن به یک اجماع گسترده میان کاربران صورت نگرفته بود. در واقع طرفداران بلاک های بزرگ مایل به انجام این کار نبودند. آن ها نه تنها بلاک هایی با سایز بزرگ تر می خواستند، بلکه از روش فعال سازی مورد حمایت طرفداران بلاک های کوچک هم بیزار بودند. این امر به دلیل عدم اعتماد، خشم ناشی از سانسور، و سایر رفتارهای پرخاشگرانه ای بود که از طرف طرفداران بلاک های کوچک سر می زد. بنابراین Bitcoin Classic آستانه فعال سازی ۷۵ درصدی XT را حفظ کرد. این کار به نظر من یک اشتباه تاکتیکی بود. اگر آن ها یک روش فعال سازی متعادل تر با ویژگی های ایمنی بهتری انتخاب می کردند، فرصتی برای طرفداران بلاک های بزرگ پدید می آمد که در جبهه طرفداران بلاک های کوچک تفرقه پدید آورند و پیروز این میدان شوند.

به طور کلی طرفداران بلاک های کوچک به چند دلیل با آستانه ۷۵ درصدی مخالفت می کردند. از نظر آن ها موضوع ارتقاء قوانین شبکه مسأله ای نبود که به رأی گذاشته شود و نشانه ای که در سربرگ بلاک^۲ قرار می گرفت صرفاً مکانیزمی امنیتی برای اطمینان از آمادگی ماینرها و فعال سازی قوانین جدید در شبکه بود. در آوریل سال ۲۰۱۲، سافت فورک P2SH با استفاده از آستانه ۵۵ درصدی فعال شد. با این حال همچنان ۴۵ درصد ماینرها تا چند ماه بعد از فعال سازی، بلاک های نامعتبر می ساختند. از نظر آن ها این مسأله مشکل ساز بود و برای همین از آن زمان به بعد از آستانه ۹۵ درصدی استفاده می شود. اما از نظر طرفداران بلاک های بزرگ نشانه گذاری در سربرگ بلاک به معنی رأی گیری از ماینرها بود و در چنین سناریویی ۷۵ درصد یک اکثریت قاطع بود، در حالی که از نظر

1 <https://github.com/bitcoinclassic/bitcoinclassic/releases/tag/v0.11.2.cl1>

2 Block header

آن‌ها آستانه ۹۵ درصدی یک هدف دست‌نیافتنی بود. علاوه بر این طرفداران بلاک‌های بزرگ تصور می‌کردند که آستانه ۷۵ درصدی برای به جلو بردن طولانی‌ترین زنجیره بلاک‌چین کفایت می‌کند. از نظر آن‌ها ۵۱ درصد هشریت برای به دست گرفتن کنترل شبکه کافی بود و آستانه ۷۵ درصدی یک حاشیه امن غیرضروری پدید می‌آورد.

من معتقدم طرفداران بلاک‌های کوچک با اصل موضوع رأی‌گیری و نظرسنجی از ماینرها مخالفتی نداشتند. با این حال نظرسنجی از ماینرها و نشانه‌گذاری در سربرگ بلاک‌ها به قصد اعمال تغییرات در قوانین اجماع شبکه، از یکدیگر متمایز هستند. طرفداران بلاک‌های کوچک نشانه‌گذاری در سربرگ بلاک‌ها را به عنوان بخش مهمی در امنیت شبکه در نظر می‌گرفتند و معتقد بودند ترکیب فعال‌سازی مطمئن تغییرات بر روی شبکه و رأی‌گیری از ماینرها با هم، بی‌مورد و خطرناک است.

طرفداران بلاک‌های بزرگ در این مرحله از درگیری متوجه نبودند که این روش فعال‌سازی به‌طور قابل توجهی شانس آن‌ها را برای افزایش سائز بلاک کاهش می‌دهد. شبیه به این بود که یک نفر در حالی که دستانش از پشت بسته شده‌اند به جنگ برود. طرفداران بلاک‌های بزرگ تلاش می‌کردند تا سائز بلاک را افزایش دهند. قانون فعلی این بود که بلاک‌ها باید ۱ مگابایت یا کمتر باشند و آن‌ها می‌خواستند قانون را تغییر دهند طوری که بلاک‌ها ۲ مگابایت یا کمتر باشند. قانون بلاک‌های کوچک زیرمجموعه‌ای از قانون بلاک‌های بزرگ‌تر بود و این موضوع شرایط را نامتقارن می‌کرد. اگر هارد فورک فعال می‌شد و بلاک‌چین به دو زنجیره جداگانه شکافته می‌شد، زنجیره بلاک‌های ۱ مگابایتی همچنان برای نودهایی که از قانون بلاک‌های بزرگ‌تر پیروی می‌کردند معتبر بودند، در حالی که زنجیره بلاک‌های ۲ مگابایتی برای نودهایی که از قانون قدیمی پیروی می‌کردند نامعتبر بود. اگر زنجیره بلاک‌چین بیت کوین در نتیجه این درگیری‌ها دوپاره می‌شد، این شرایط نامتقارن برای طرفداران بلاک‌های کوچک یک مزیت ایجاد می‌کرد. این بدان معنی است که اگر زنجیره بلاک‌های کوچک از زنجیره بلاک‌های بزرگ جلو

می افتاد، زنجیره بلاک‌های بزرگ به کلی در واقعه‌ای که به «نابود شدن^۱» معروف است، از بین می‌رفت. این موضوع مخصوصاً در شرایطی که اکثریت ماینرها بر روی زنجیره بلاک‌های بزرگ کار کنند تهدید بزرگی به نظر نمی‌رسد، ولی در هر صورت این شرایط باید از نقطه نظر دوپاره شدن احتمالی زنجیره در نظر گرفته شود. اگر به‌طور تصادفی و بعد از ساخته شدن اولین بلاک بزرگ‌تر از ۱ مگابایت، زنجیره بلاک‌های کوچک‌تر جلو بیفتد، می‌تواند زنجیره بلاک‌های بزرگ‌تر را به سرعت از بین ببرد. این امر می‌توانست تأثیرات مخربی روی جبهه طرفداران بلاک‌های بزرگ داشته باشد، چون ماینرها از ساختن بلاک بزرگ بعدی هراس پیدا می‌کردند.

اگر از منظر بازارهای مالی به مسأله نگاه کنیم، اهمیت این شرایط نامتقارن حتی بیشتر هم می‌شود چون باعث می‌شود سرمایه‌گذاران مالی از زنجیره بلاک‌های کوچک‌تر حمایت کنند و کوین‌های زنجیره بلاک‌های بزرگ‌تر خود را بفروشند. این امر می‌تواند موجب پایین رفتن قیمت کوین‌های زنجیره بلاک‌های بزرگ‌تر و بالا رفتن قیمت کوین‌های زنجیره بلاک‌های کوچک‌تر شود، که در نتیجه باعث می‌شود ماینرها انگیزه بیشتری برای تغییر موضع و ادامه کار بر روی زنجیره بلاک‌های کوچک‌تر داشته باشند تا بتوانند پاداش بیشتری برای ساختن بلاک دریافت کنند. این امر در نهایت می‌تواند منجر به از بین رفتن کامل زنجیره بلاک‌های بزرگ‌تر شود و سود کلانی برای سرمایه‌گذاران فراهم کند.

این مشکل یک راه‌حل ساده داشت؛ برای حل آن قوانین جدید باید به گونه‌ای اعمال می‌شد که اولین بلاک ساخته شده بعد از فعال شدن قوانین جدید بزرگ‌تر از ۱ مگابایت باشد، در این صورت یک شکاف کامل در زنجیره به وجود می‌آید و هر دو زنجیره در مقابل از بین رفتن آسیب‌پذیر نبودند. با این حال وقتی در مورد این موضوع با طرفداران بلاک‌های بزرگ بحث می‌کردم، به من می‌گفتند که این مسأله مشکلی به وجود نخواهد آورد زیرا اکثریت ماینرها از زنجیره بلاک‌های بزرگ‌تر حمایت می‌کنند. همچنین طرفداران بلاک‌های بزرگ معتقد بودند که بیت‌کوین را اکثریت هش‌ریت تعریف می‌کند، و

1 wipeout

قراردادن چنین «نقطه کنترلی^۱» در نرم افزار بیت کوین این دیدگاه را تضعیف می کند. به نظر می رسد ایدئولوژی آنها در طرفداری از بلاک های بزرگ باعث آسیب پذیرتر شدن زنجیره مورد حمایت آنها می شد. با این حال وقتی داشتیم با یکی از افراد برجسته تیم طرفداران بلاک های کوچک درباره این موضوع گفتگو می کردم به من گفت بهتر است این قضیه را مسکوت نگه دارید و توضیح داد وقتی دشمن تصمیم دارد عمل اشتباهی مرتکب شود بهتر است حواسش را پرت نکنید و اجازه دهید کارش را تمام کند. برخی از طرفداران بلاک های کوچک ترجیح می دادند این ابزار بالقوه را به عنوان یک مکانیزم اضطراری برای روز مبادا نگه دارند تا اگر زنجیره بلاک های بزرگ تر با این مشکل راه اندازی شده بود از آن استفاده کنند. در ادامه این درگیری سرانجام طرفداران بلاک های بزرگ تر از این مسأله درس گرفتند و با استفاده از روش قرار دادن یک نقطه کنترلی، بلاک چین بیت کوین را به دو زنجیره مجزا تبدیل کردند. هرچند این مسأله تا تابستان سال ۲۰۱۷ از آنها زمان برد.

پیشنهاد Bitcoin Classic نقطه ضعف دیگری داشت که در کنار مسئله عدم تقارن که پیشتر توضیح دادیم باعث وخیم تر شدن شرایط می شد؛ این نقطه ضعف پنجره فعال سازی مستمر^۲ ۷۵ درصدی بود. (البته XT هم از این قاعده مستثنی نبود) همانطور که قبلاً ذکر شد، برای فعال کردن سافت فورک ها در شبکه بیت کوین از آستانه فعال سازی ۹۵ درصدی استفاده می شد، ولی پنجره فعال سازی در دوره های ۲ هفته ای و ثابت در نظر گرفته می شد. (دوره های بازتنظیم سختی شبکه به عنوان پنجره های فعال سازی قوانین جدید بر روی شبکه بکار گرفته می شوند. -م) اما Bitcoin Classic از روش پنجره فعال سازی مستمر ۷۵ درصدی استفاده می کرد، به این معنی که اگر ۷۵۰ بلاک از ۱,۰۰۰ بلاک گذشته در سربرگ خود نشانه مخصوص حمایت از اعمال تغییرات را قرار داده بودند، قوانین جدید بر روی شبکه فعال می شد. بیا بیاید فرض کنیم که ماینرها نرم افزار خود را به مرور به روزرسانی می کنند، همچنان که در سافت فورک های گذشته هم وضعیت به همین شکل بوده است. از آنجا که آنها فقط ۴ هفته برای به روزرسانی نرم افزار خود مهلت

1 Checkpoint
2 Rolling

داشتند یعنی در زمان تولید اولین بلاک بزرگ، تقریباً ۲۵ درصد ماینرها هنوز مشغول به کار بر روی زنجیره بلاک‌های کوچکتر هستند. اگر از پنجره علامت‌دهی ثابت به‌جای مستمر استفاده می‌شد، حتی با انتخاب آستانه ۷۵ درصدی اطمینان پیدا می‌کردیم که حداقل ۷۵ درصد هش‌ریت شبکه نرم‌افزار خود را به‌روزرسانی کرده‌اند. اما اوضاع از این بدتر بود. فردی یک تجزیه و تحلیل آماری درباره علامت‌دهی ماینرها در سربرگ بلاک‌ها انجام داد و در محاسبات خود فرض را بر این گذاشت که ماینرها با سرعت پایینی اقدام به به‌روزرسانی نرم‌افزار خود کنند. بر اساس نتایج مشخص شد Bitcoin Classic احتمالاً قبل از اینکه ۷۵ درصد ماینرها نرم‌افزار خود را به‌روزرسانی کرده باشند به آستانه اعلام آمادگی ۷۵ درصدی در سربرگ بلاک‌ها خواهد رسید. محتمل‌ترین سناریو این بود که در زمان فعال‌سازی نسبت آن‌ها ۷۱ به ۲۹ باشد^۳.

بنابراین استفاده از روش پنجره فعال‌سازی مستمر تقریباً ایجاد شکاف در زنجیره بیت‌کوین را تضمین می‌کرد. طرفداران بلاک‌های بزرگ اصرار داشتند با دستانی که از پشت بسته شده و چشم‌بندهایی که چشمان‌شان را پوشانده است، وارد کارزار شوند. صرف‌نظر از تعداد افرادی از هریک از این دو گروه طرفداری می‌کردند، احتمالاً این درگیری با پیروزی گروه طرفداران بلاک‌های کوچک به پایان می‌رسید.

به نظر می‌رسید این پنجره فعال‌سازی مستمر کاملاً غیرضروری است و برخی از توسعه‌دهندگان بیت‌کوین بارها این موضوع را به گوین گوشزد کردند. با این حال این مسأله گوین را نگران نمی‌کرد چون از نظر او این روش فعال‌سازی از حمایت قاطعی برخوردار بود. بنابراین این موضوع مسأله مهمی نبود. شاید بهتر بود گوین کمی محتاط‌تر برخورد می‌کرد و اهمیت این موضوع را در نظر می‌گرفت، چون در این صورت می‌توانست بدون زحمت اضافه شانس اعمال موفقیت‌آمیز تغییرات پیشنهاد شده را بیشتر کند و به‌طور بالقوه افراد بیشتری را به جمع حامیان خود اضافه کند. بالاخره ممکن بود

³ <https://bitcoinmagazine.com/articles/bitcoin-classic-hard-fork-likely-to-activate-at-hashrate-support-1457020892>

گوین در پیش‌بینی سطح حمایتی که از Bitcoin Classic می‌شد در اشتباه باشد و معتقدم بهتر بود جانب احتیاط را رعایت می‌کرد. امتناع او از شنیدن نظرات منتقدان او را از گوین‌ای که قبلاً می‌شناختم متمایز می‌کرد، او در گذشته محتاط‌تر بود و از خود تعصب نشان نمی‌داد. استیصال از شرایط تا حدودی بر قدرت تصمیم‌گیری او تأثیر گذاشته بود و کاسه صبر او در حال لبریز شدن بود. شاید گوین حق داشت خسته شود و همه این نگرانی‌ها که از جانب طرفداران بلاک‌های کوچک مطرح می‌شد فقط تاکتیک‌هایی برای خریدن وقت و جلوگیری از افزایش سایز بلاک بود. طرفداران بلاک‌های کوچک در این کار استاد بودند. اینطور نبود که طرفداران بلاک‌های کوچک بگویند «فقط این دو مورد را برطرف کنید تا ما از Classic پشتیبانی کنیم». اگر گوین این مشکلات را برطرف می‌کرد، همین افراد به سراغ مشکلات دیگری که در Classic پیدا کرده بودند می‌رفتند. به عنوان مثال، درخواست می‌کردند که سربرگ بلاک‌ها تغییر کند تا کیف پول‌ها و نودهای سبک به موقع از رخ دادن هارد فورک مطلع شوند. این یکی از ویژگی‌های ایمنی بود که طرفداران بلاک‌های کوچک اغلب خواستار آن بودند. در یک درگیری معمولاً هر دو طرف تا حدودی حق دارند ولی این حقیقت که سرانجام طرفداران بلاک‌های بزرگ بعضی از این مشکلات را برای رفع نگرانی‌ها برطرف کردند نشان می‌دهد ادعای زیان‌بار بودن روش فعال‌سازی طرفداران بلاک‌های بزرگ تا حدودی حقیقت داشته است.

با وجود این نقاط ضعف بالقوه فاجعه‌باری که در روش فعال‌سازی Bitcoin Classic وجود داشت، هر روز به مقبولیت آن اضافه می‌شد. تقریباً همه شرکت‌های سرمایه‌گذاری تحت حمایت سیلیکون ولی^۱ در سانفرانسیسکو مانند Coinbase از Bitcoin Classic پشتیبانی می‌کردند. نقاط ضعف Bitcoin Classic بیش از حد تئوریک و فنی بود، برای عموم افراد قابل درک نبود و بین آن‌ها به بحث گذاشته نمی‌شد. در این مرحله سرعت طرفداران بلاک‌های بزرگ زیاد شده بود و داشتند در این درگیری پیروز می‌شدند. استخراج‌های بیشتری مانند گروه Bitfury و شرکت‌های فعال در زمینه بیت‌کوین حمایت خود از Bitcoin Classic را اعلام می‌کردند.^۲ با این حال تعداد بلاک‌هایی که

1 Silicon Valley

2 <https://twitter.com/valeryvavilov/status/688054411650818048>

علامت مخصوص پشتیبانی از Bitcoin Classic را در سربرگ خود داشتند نسبتاً کم بود و به نظر نمی‌رسید تعداد زیادی از کاربران بیت کوین نودهای Classic را اجرا می‌کنند.

در فوریه سال ۲۰۱۶ رویدادی با عنوان میزگرد ساتوشی^۱ برگزار شد. این دومین رویداد از مجموعه رویدادهای سالانه بود که تا سال ۲۰۲۰ ادامه پیدا کرد و فرصتی برای پیشگامان صنعت بلاک‌چین فراهم می‌آورد تا در مورد موضوعات مختلف بحث و گفتگو کنند. دستور کار این دوره از این رویداد تحت تأثیر موضوع سائز بلاک قرار گرفته بود. من در این رویداد حضور نداشتم بنابراین نمی‌توانم تجربه مستقیم خود را از این رویداد ارائه کنم. برایان آرمسترانگ به همراه همکار آن زمان خود، خالق لایت کوین^۲ «چارلی لی^۳»، برادر «بابی لی^۴» در این رویداد شرکت کردند. پس از اتمام کنفرانس، برایان مطلبی در وبلاگ خود نوشت و از چندین توسعه‌دهنده Bitcoin Core انتقاد و حمایت خود را از Bitcoin Classic اعلام کرد. تا جایی که به خاطر می‌آورم انتقاداتی که در آن نسبت به توسعه‌دهندگان Bitcoin Core مطرح شده بود خیلی تند بود، ولی به سرعت آن را حذف و متن معتدل‌تری به جای آن گذاشتند.

به نظر من شاید بزرگترین خطری که در حال حاضر بیت کوین را تهدید می‌کند از قضا همان چیزی است که در گذشته بیشترین کمک را به آن کرده است و آن چیزی نیست جز توسعه‌دهندگان Bitcoin Core.

...

آن‌ها از ضریب هوشی بسیار بالایی برخوردارند اما بعد از ملاقاتی که آخر هفته گذشته با آن‌ها داشتم مسائلی توجه من را به خود جلب کرد که من را نسبت به تیم

1 Satoshi Roundtable
2 Litecoin
3 Charlie Lee
4 Bobby Lee

آن‌ها بسیار نگران می‌کند. بعضی از آن‌ها مهارت‌های ارتباطی بسیار ضعیفی از خود نشان می‌دهند و رفتار بالغانه‌ای ندارند و همین باعث شده توسعه‌دهندگان جدید به این فضا اضافه نشوند. آن‌ها راه‌حل‌های «قابل قبول» را نمی‌پذیرند و فقط پذیرای راه‌حل‌های «از هر نظر کامل» هستند. و اگر یک راه‌حل کامل برای مسأله‌ای پیدا نشود ترجیح می‌دهند حتی به قیمت در معرض خطر قرار دادن بیت کوین، هیچ کاری نکنند.

...

ما باید برای کار بر روی پروتکل بیت کوین یک تیم جدید تشکیل دهیم. تیمی که از پیوستن توسعه‌دهندگان جدید استقبال کند، در موقعیت‌های مناسب اهل مصالحه باشد، و برای مقیاس‌پذیر شدن پروتکل، همواره به آن کمک کند. طی یکی دو ماه آینده بیشتر در این مورد خواهید شنید.

...

اگر می‌خواهید از موفقیت بیت کوین اطمینان حاصل کنید، پیشنهاد می‌کنم در اولین فرصت نرم‌افزار Bitcoin Classic را نصب کنید.

...

من همچنین از مرورگرهای وب مثل زدم. تیم Chrome و Safari رقبای سرسختی هستند اما با یکدیگر در کنفرانس‌ها شرکت، و در زمینه استانداردها با IETF همکاری می‌کنند. بسیاری از شرکت‌های رقیب دیگر هم در این کنفرانس حضور داشتند. اما با یکدیگر سر جنگ و دعوا نداشتند. همه ما در یک صنعت مشغول به کار هستیم و از بسیاری از جهات با هم دوست هستیم. این موضوع در مورد تیم‌های مختلفی که بر روی پروتکل بیت کوین مشغول به کار هستند هم

صدق می‌کند. با ارائه گزینه‌های بیشتر در بازار پیشرفت حاصل خواهد شد، نه پسرفت^۱.

موارد فوق خلاصه‌ای از بحث برانگیزترین قسمت‌های مطلب برایان است که به وضوح نشان دهنده کینه روزافزون او نسبت به برخی از توسعه‌دهندگان Bitcoin Core و همچنین تمایل او به رهایی بیت‌کوین از این افراد بود.

برایان مثالی از تیم‌های رقیب مرورگرهای وب مثل Chrome و Safari را پیش کشیده بود. البته این موضوع برای طرفداران بلاک‌های کوچک روشن کننده این مسأله بود که برایان هنوز قضیه را درک نکرده است. مرورگرهای وب چیزی به نام سیستم اجماع جهانی^۲ نداشتند. از نظر طرفداران بلاک‌های کوچک این یک مناقشه میان تیم‌های رقیب نبود، بلکه رقابتی بود میان قوانین اجماع شبکه و در نتیجه کوین‌هایی که در بازار قیمت داشتند و جریان اقتصادی بین آن‌ها جاری بود، و تمام پیچیدگی‌هایی که ممکن بود شکاف در زنجیره بلاک چین بیت‌کوین پدید آورد. از نظر آن‌ها Bitcoin Classic اصلاً یک تیم رقیب به حساب نمی‌آمد چون در واقع همان کد Bitcoin Core بود که فقط چندتا از متغیرهای آن تغییر کرده بودند. Bitcoin Core رقابتی داشت که با استفاده از روش کدنویسی خود، پروتکل بیت‌کوین را پیاده‌سازی کرده بودند و هیچگونه وابستگی به کد Bitcoin Core نداشتند. آن‌ها به زبان‌های برنامه‌نویسی مختلف نوشته شده بودند، برای نمونه می‌توان به BTCD و Libbitcoin اشاره کرد. طرفداران بلاک‌های بزرگ بین کوین‌های رقیب و تیم‌های رقیب تمایزی قائل نبودند و این یکی از اشتباهات مهم آن‌ها بود. از نظر طرفداران بلاک‌های کوچک آن‌ها بلاک‌های بزرگتری می‌خواستند ولی نمی‌دانستند بیت‌کوین چگونه کار می‌کند، یا نمی‌دانستند چطور باید یک هارد فورک را بر روی شبکه اجرا کرد، بنابراین مستأصل می‌شدند و همه تقصیرها را به گردن تیم توسعه‌دهندگان Bitcoin Core می‌انداختند.

1 <https://blog.coinbase.com/what-happened-at-the-satoshi-roundtable-6c11a10d8cdf>

2 Global consensus system

علیرغم پشتیبانی کم ماینرها از Bitcoin Classic، فضا در فوریه سال ۲۰۱۶ به گونه‌ای بود که احساس می‌شد ماینرها اعلام آمادگی خواهند کرد و احتمال فعال‌سازی بسیار بالا است. در همین حال پشتیبانی Coinbase از Bitcoin Classic موجب معروف شدن هرچه بیشتر آن شده بود. با توجه به مشکلاتی که در روش فعال‌سازی انتخاب شده وجود داشت و بی‌توجهی طرفداران بلاک‌های بزرگ به آنها، به نظر می‌رسید بیت‌کوین به سمت یک بحران بزرگ پیش می‌رود و یک شکاف در زنجیره بلاک‌چین آن به وقوع خواهد پیوست. در این مقطع از درگیری، طرفداران بلاک‌های بزرگ‌تر در موقعیت مستحکم‌تری نسبت به گذشته قرار داشتند، در حالی که طرفداران بلاک‌های کوچک هنوز ترفندهایی در آستین داشتند. به نظر می‌رسید بیت‌کوین در آستانه یک شکست فاجعه‌بار قرار گرفته است.

فصل هشتم

میزگرد هنگ کنگ^۱

در ۲۰ فوریه سال ۲۰۱۶ با گروهی از دوستانم در ارتفاعات اطراف هنگ کنگ پیاده‌روی می‌کردیم. نزدیک عصر به بالای صخره Lion رسیده بودم و داشتم از منظره زیبایی که مشرف به جزیره بود لذت می‌بردم. در حالی که منتظر بودم بقیه اعضای گروه به من برسند، تلفن همراهم را باز کردم و به ساب‌ردیت `/r/btc` رفتم و به یک مطلب برخوردم که از برگزاری یک نشست میان ماینرها و توسعه‌دهندگان بیت کوین درباره موضوع مقیاس‌پذیری در هنگ کنگ خبر می‌داد^۲. با دیدن عکس‌ها به نظر می‌رسید این نشست در مکان کنفرانس مقیاس‌پذیری دوم که در سایبرپورت هنگ کنگ برگزار شده بود، برقرار باشد. مشتاق بودم تا این نشست را از دست ندهم برای همین قبل از رسیدن دوستانم بالافاصله از کوه پایین آمدم و با یک تاکسی خود را به محل برگزاری رساندم. من به این رویداد دعوت نشده بودم ولی با توجه به اینکه آن‌ها می‌خواستند در مورد قوانین پروتکل بیت کوین بحث و تصمیم‌گیری کنند، و از آنجا که بیت کوین یک شبکه آزاد^۳ است، من

1 Hong Kong Roundtable

2 https://www.reddit.com/r/btc/comments/46oa1r/feb_20_hk_coreminer_conference_pics_will_be

3 Open network

معتقد بودم به اندازه دیگران حق شرکت در آن را دارم. فکر می‌کردم منصفانه نبود مرا به آنجا راه ندهند و با اعتماد به نفسی که داشتم بالاخره راهم را به داخل باز کردم.

من حدود ساعت ۴ عصر به آنجا رسیدم. این نشست در یک اتاق کوچک برگزار می‌شد و تعداد شرکت‌کنندگان حدود ۳۰ تا ۴۰ نفر بود که در گروه‌های کوچکی با یکدیگر آهسته صحبت می‌کردند. توسعه‌دهندگان که از ایالات متحده آمریکا آمده بودند با آدم‌بک در یک سمت اتاق و ماینرها در سمت دیگر مشغول به صحبت با یکدیگر بودند. توسعه‌دهندگان حاضر در نشست «کوری فیلدز»^۱ که از آمریکا آمده بود (که قبلاً با کوین در بنیاد بیت کوین همکاری می‌کرد)، «جانسون لا»^۲ (که در هنگ کنگ مستقر بود و در توسعه سگویت نقش داشت. - م)، لوک دش‌یر، «مت کورالو»^۳ (که از بنیانگذاران شرکت بلاک‌استریم و مستقر در آمریکا بود)، و پیتر تاد بودند. در صحبتی که با آن‌ها داشتم به من می‌گفتند برای بالابردن آگاهی ماینرها نسبت به شبکه بیت کوین و گفتگوی دوستانه با آن‌ها به هنگ کنگ آمده‌اند. آن‌ها همچنین می‌خواستند ماینرها را از اجرای Bitcoin Classic منصرف کنند. اگرچه بعضی از آن‌ها بسیار مشتاق به اجرای هارد فورک بودند و تهدید کرده بودند که از Classic استفاده خواهند کرد.

کاملاً واضح بود که تنش در فضای اتاق بسیار زیاد شده است. به سمت دیگر اتاق حرکت کردم. جیهان وو و «میکره ژان»^۴ دو نفر از بنیانگذاران شرکت Bitmain پشت میز کنار یکدیگر نشسته بودند و افراد مختلف فعال در صنعت استخراج بیت کوین دور آن‌ها جمع شده بودند و برای شروع بحث و گفتگو آماده می‌شدند. جیهان بیشتر از بقیه آشفته به نظر می‌رسید و اطرافیانش او را به آرامش دعوت می‌کردند. ناگهان جیهان چنین چیزی گفت: «ما از Classic پشتیبانی خواهیم کرد؛ Bitcoin Core هم یا هارد فورک را اجرا می‌کند یا دیگر از آن استفاده نخواهیم کرد!» اطرافیان او نگران به نظر می‌رسیدند و سعی می‌کردند دوباره او را آرام کنند. قرار بود گفتگوها چند دقیقه بعد دوباره آغاز شود.

1 Cory Fields
2 Johnson Lau
3 Matt Corallo
4 Micree Zhan

جیهان صحبتش را با صدای بلند اینگونه آغاز کرد که ماینرها هارد فورک ۲ مگابایتی را اجرا خواهند کرد. او ادامه داد: «اگر Bitcoin Core بخواهد بخشی از بیت کوین باشد باید این هارد فورک را انجام دهد.» یکی از توسعه‌دهندگان گفت «سگویت ۲ مگابایت است و توسعه‌دهندگان Bitcoin Core در حال آماده‌سازی آن هستند.» جیهان گفت «نه! ما به یک هارد فورک ۲ مگابایتی نیاز داریم، نه سگویت». احساس استیصال در اتاق بسیار زیاد بود و به من گفتند قبل از رسیدن من هم اوضاع به همین شکل بوده است و آن‌ها فقط حرف‌های خود را تکرار می‌کردند. کاملاً مشخص بود که این دو گروه به یکدیگر اعتماد ندارند.

به نظر می‌رسید هر دو طرف دعوا با یکدیگر موافق هستند که بلا تکلیفی روی Bitcoin Core و هارد فورک در نهایت به ضرر بیت کوین است. یک طرحی مطرح شد که اگر حاضرین جلسه مواردی که بر روی آن‌ها توافق دارند را به اطلاع عموم برسانند و برای آن برنامه‌ای اعلام کنند، به نفع بیت کوین خواهد بود. به خاطر دارم کسی می‌گفت این کار به بازار آرامش می‌دهد و باعث افزایش قیمت خواهد شد. تنها چیزی که همه بر روی آن توافق داشتند بالا رفتن قیمت بیت کوین بود. بنابراین قرار شد بر روی متنی که مسیر حرکت رو به جلوی بیت کوین را مشخص می‌کند به توافق برسند و آن را به اطلاع عموم برسانند. ولی دقیقاً نمی‌دانم این ایده چطور شکل گرفت.

در طول این مذاکرات آدام بک و چند تن از توسعه‌دهندگان از طریق تلفن و نرم‌افزارهای پیام‌رسان با همکاران خود در شرکت بلاک‌استریم در آمریکا در تماس بودند. آن‌ها حتماً از کارهای آدام عصبانی بودند، پیام‌های خشن برای او می‌فرستادند و عاجزانه از او درخواست می‌کردند این کار را ادامه ندهد. من می‌توانم تصور کنم آن‌ها احتمالاً چه پیام‌هایی برای او ارسال می‌کردند. آن‌ها احتمالاً استدلال می‌کردند که بیت کوین قرار است پولی باشد که عاری از سیاست‌زدگی است و قوانین آن نباید در مذاکرات پشت درهای بسته تعیین شود. آن‌ها همچنین نگران بودند که آدام و دیگر توسعه‌دهندگان حاضر

در این نشست حاضر به اجرای هارد فورک شوند در حالی که آن‌ها اطمینان داشتند سگویت بهترین راه برای ادامه مسیر است. آن‌ها به روشنی بیان کردند که عضوی از این توافق‌نامه نخواهند بود ولی گفتگو بدون توجه به این موضوع ادامه پیدا کرد چون توسعه‌دهندگان حاضر در نشست معتقد بودند این تنها راه متوقف کردن Bitcoin Classic است.

بیشتر گفتگوها حول زمان‌بندی و ترتیب انجام کارها بود. جیهان اعتماد نداشت و درخواست می‌کرد که هارد فورک قبل از سگویت اجرا شود. توسعه‌دهندگان می‌گفتند نمی‌توانند قول هارد فورک را بدهند چون کنترل Bitcoin Core در اختیار آن‌ها نیست و کنترل Bitcoin در اختیار Bitcoin Core نیست. آن‌ها فقط می‌توانستند قول نوشتن کُد هارد فورک را بدهند. برخی از ماینرها تکرار می‌کردند که کُد هارد فورک باید در نسخه Bitcoin Core منتشر شود و بحث بر روی این موضوع زمان زیادی از جلسه گرفت.

«سمسون مو»^۱ که در آن زمان در صرافی بابی لی به نام BTCC کار می‌کرد نیز در جلسه حضور داشت. به خاطر می‌آورم که او یکی از هواداران ایده نگارش متن مشترک بود و بخشی از متن هم توسط خود او نوشته شده بود. در آن زمان سمسون از طرفداران بلاک‌های کوچک بود و به نظر می‌رسید از تمسخر طرفداران بلاک‌های بزرگ لذت می‌برد. این باعث شده بود وی در کنار گرگوری مکسول، آدام بک، لوک دشر از چهره‌های منفور نزد طرفداران بلاک‌های بزرگ باشد. در آوریل سال ۲۰۱۷ یعنی حدود یک سال بعد از این نشست، او به عنوان رئیس بخش استراتژی^۲ به شرکت بلاک‌استریم پیوست.

1 Samson Mow

2 CSO

ساعت ۴ صبح بود و چانه‌زنی روی انتخاب کلمات متن همچنان ادامه داشت. حتی این متن به اشتباه روی سایت Medium منتشر شد ولی بعداً بدلیل عدم رضایت یکی از طرفین آن را حذف کردند. تا جایی که می‌دانم این جلسه از حدود ساعت ۱۰ صبح روز شنبه آغاز شده بود. همه افراد در اتاق بسیار خسته و عصبانی بودند و استرس زیادی داشتند که موجب می‌شد تصمیمات اشتباه بگیرند. به نظر می‌رسید آن‌ها راهی جز توافق کردن با یکدیگر ندارند. با بالاگرفتن استیصال بالاخره بر روی متن به توافق رسیدند ولی همه از آن ناراضی بودند. در واقع می‌توان گفت تقریباً همه با قسمتی از متن مخالف بودند. با این حال حدود ساعت ۵ صبح کسی توان ادامه بحث را نداشت. این تاکتیک معمولاً در مذاکرات بین‌المللی با هدف اجبار طرفین برای رسیدن به توافق مورد استفاده قرار می‌گیرد.

هنگامی که سرانجام دو طرف روی متن توافق کردند، همه به شکل یک دایره در وسط اتاق جمع شدند و به قصد نمایش توافق در حالی که دست‌های خود را به سمت یکدیگر دراز کرده بودند، یک عکس یادگاری گرفتند. همه، بجز آدام بک و مت کورالو که حتی در حین عکس‌برداری از این صحنه معروف، همچنان مشغول بازیابی و بررسی متن بودند. چهره‌ها از عکس حذف شده بودند و فقط دست‌ها دیده می‌شدند. به نظر می‌رسید ماینرها از این توافق رضایت دارند و در هنگام عکس‌برداری لبخند به چهره داشتند. برخلاف آن‌ها چهره توسعه‌دهندگان ناراضی و خسته بود و به دوربین نگاه نمی‌کردند.

متن اصلی توافق به شرح زیر است:

ما به همکاری با کل جامعه توسعه‌دهندگان پروتکل بیت کوین ادامه خواهیم داد تا بر اساس پیشرفت‌های سگویت، یک هارد فورک قابل اطمینان توسعه داده شود. توسعه‌دهندگان Bitcoin Core حاضر در این نشست، ظرف سه ماه پس از انتشار سگویت این هارد فورک را آماده می‌کنند و در Bitcoin Core ادغام می‌کنند و اجرای آن را به کاربران توصیه می‌کنند. انتظار می‌رود این هارد فورک شامل ویژگی‌هایی باشد که این روزها در جوامع فنی مورد بحث قرار می‌گیرند، از جمله

افزایش بخشی از بلاک که ارتباطی به داده‌های مربوط به امضای دیجیتال تراکنش ندارد به ۲ مگابایت، به صورتی که سایز بلاک از ۴ مگابایت بیشتر نشود. این هارد فورک در صورت اجماع گسترده میان کاربران بیت کوین اجرا خواهد شد. اگر این هارد فورک با استقبال کاربران بیت کوین مواجه شود احتمالاً حوالی ماه جولای ۲۰۱۷ اجرا خواهد شد. ما ماینرها در نهایت از نسخه‌ای از نرم‌افزار Bitcoin Core استفاده خواهیم کرد که هر دو بخش سگویت و هارد فورک در آن آماده شده باشند.

این توافق‌نامه برای هر دو طرف مفید بود. در آن قید شده بود که «هارد فورک فقط در صورت پشتیبانی گسترده همه کاربران بیت کوین اجرا خواهد شد». این مسأله برای طرفداران بلاک‌های کوچک بسیار مهم بود، چون می‌توانستند برای توجیه مسائلی که ممکن بود پیش بیاید از آن استفاده کنند. آن‌ها متعهد به اجرای هارد فورک نبودند و تصمیم در مورد این مسأله بر دوش کاربران بیت کوین گذاشته شده بود. آن‌ها زمان زیادی صرف بحث و گفتگو بر روی این موضوع کرده بودند. به نظر می‌رسد طرفداران بلاک‌های بزرگ این قسمت از توافق را کاملاً نادیده می‌گرفتند و اهمیتی به آن نمی‌دادند. حتی به نظر می‌رسد امروزه همچنان بیشتر طرفداران بلاک‌های بزرگ آن را نادیده می‌گیرند. ماینرهایی که توافق‌نامه را امضاء کردند متعهد شدند از نرم‌افزار Bitcoin Core استفاده کنند و بدین ترتیب آن‌ها موفق شدند از پیشرفت Bitcoin Classic جلوگیری کنند. این برای طرفداران بلاک‌های کوچک یک موفقیت کلیدی بود. از نظر آن‌ها یا دست کم برخی از آن‌ها از وقوع یک بحران جلوگیری شده بود. تا آنجا که به طرفداران بلاک‌های بزرگ حاضر در جلسه مربوط بود، توسعه‌دهندگان متعهد شده بودند کُد مربوط به هارد فورک را بنویسند و ماینرها با اجرای نرم‌افزار جدید، هارد فورک را بر روی شبکه اعمال کنند.

ما نسخه سگویت را زمانی اجرا خواهیم کرد که بخش نرم‌افزاری هارد فورک در یکی از نسخه‌های Bitcoin Core منتشر شده، و آماده اجرا باشد.^۱

جیهان اصرار داشت این بخش در متن توافق نامه گنجانده شود. من در آن زمان متوجه این موضوع نبودم، اما بسیاری از طرفداران بلاک‌های بزرگ آن را اینگونه تفسیر می‌کردند که ماینرها فقط در صورتی سگویت را اجرا خواهند کرد که کُد مربوط به هارد فورک مورد نظر آن‌ها در یکی از نسخه‌های نرم‌افزار Bitcoin Core منتشر و آماده اجرا باشد. یکی از مهم‌ترین نگرانی‌های جیهان در این نشست این بود که توسعه‌دهندگان Bitcoin Core کُد مربوط به بخش هارد فورک را درون نرم‌افزار قرار ندهند و حق داشت چون متن توافق نامه آن‌ها را متعهد به انجام آن نکرده بود. بنابراین جیهان برای کسب اطمینان اصرار داشت این بخش در متن توافق گنجانده شود. از نظر او، این بدان معنی بود که سگویت تا زمانی که بخش مربوط به هارد فورک در نرم‌افزار Bitcoin Core آماده و منتشر نشود، فعال نخواهد شد. برای او مهم نبود که در متن توافق نامه آمده که سگویت سه ماه قبل از هارد فورک آماده خواهد شد، چون او قصد داشت این سه ماه را صبر کند و بعد از آماده شدن بخش هارد فورک، نرم‌افزار سگویت را اجرا کند. جیهان می‌خواست با کارت سگویت بازی کند تا به هدف خود یعنی هارد فورک برسد. اگر کُد هارد فورک آماده نمی‌شد، او متعهد به اجرای سگویت نبود.

طرفداران بلاک‌های کوچک که در نشست حاضر بودند به این قسمت از متن توافق توجهی نمی‌کردند. آن‌ها معتقد بودند ماینرها در هر صورت بعد از آماده شدن سگویت آن را اجرا می‌کنند، چون تنها راه درست همین بود. از نظر آن‌ها این درست نبود که از سگویت به عنوان وسیله‌ای برای رسیدن به هارد فورک استفاده شود و برای همین این

¹ <https://medium.com/@bitcoinroundtable/bitcoin-roundtable-consensus-266d475a61ff>

بخش از توافق برای آنها بی معنی بود. آنها هرگز قصد نداشتند ماینرها را متعهد به پذیرش سگویت کنند چون معتقد بودند آنها به هر حال آن را اجرا خواهند کرد.

این توافق نه تنها باعث بهتر شدن اوضاع نشد بلکه باعث افزایش بی اعتمادی میان طرفین شد. هریک از طرفین تفسیر متفاوتی از متن توافق داشتند و می توانستند طرف مقابل را به نقض آن متهم کنند. این موضوع دوباره مسائل ژئوپلیتیک را برای من تداعی کرد، اینکه چگونه دیپلمات‌ها ساعت‌های متمادی تا نیمه‌های شب و با علم به موضع آشتی‌ناپذیر دولت‌های متبوع‌شان، برای توافق بر روی یک متن تلاش می‌کنند. شاید مشهورترین نمونه آن قطعنامه شماره ۲۴۲ شورای امنیت سازمان ملل متحد باشد که در نوامبر سال ۱۹۶۷ تصویب شد.

خروج نیروهای مسلح اسرائیل از سرزمین‌های اشغالی درگیری‌های اخیر.^۱

مشخص نبود منظور آن تمام سرزمین‌های اشغالی است یا بخشی از آن. البته که این عدم شفافیت تا حدودی عمدی بود، چون در غیر این صورت دو طرف هرگز با این قطعنامه موافقت نمی‌کردند. گرچه این قطعنامه در کوتاه‌مدت برای دیپلمات‌ها یک دستاورد محسوب می‌شد، اما به نظر نمی‌رسید منجر به یک صلح پایدار شود، زیرا طرفین طی دهه‌های آتی یکدیگر را به نقض آن متهم کردند. این روش مناسبی برای پیشرفت و تصمیم‌گیری در مورد مسائل بیت‌کوبین نبود. با در نظر گرفتن این مسائل من به این نتیجه رسیدم که رسیدن به یک راه حل مسالمت‌آمیز در مناقشه سائز بلاک، به گونه‌ای که هر دو طرف از آن رضایت داشته باشند متأسفانه بسیار بعید است. هضم این مسأله با توجه به اینکه فقط شش سال از عمر بیت‌کوبین می‌گذشت، کمی دشوار بود. چطور ممکن بود فقط بعد از گذشت شش سال یک نفر بتواند مناقشه بر سر سائز بلاک را با یکی از حل‌نشدنی‌ترین درگیری‌های سیاسی مذهبی کره زمین مقایسه کند؟ بیت‌کوبین و دین ویژگی‌های مشترک بسیاری دارند، و صد البته ادیان دائماً در حال انشعاب از یکدیگر

1 <https://unispal.un.org/unispal.nsf/0/7D35E1F729DF491C85256EE700686136>

هستند. با این تفاوت که ادیان یک ثروت مادی نیستند و نمی‌توان آن‌ها را با یکدیگر معامله کرد. این مسأله باعث جذاب‌تر شدن ماهیت این درگیری می‌شد.

پس از امضای توافق‌نامه و انتشار آن، گام بعدی برای افرادی که در جلسه حاضر بودند این بود که آن را به طرفداران خود ارائه کنند. این مرحله اصلاً خوب پیش نرفت. طرفداران بلاک‌های بزرگ معتقد بودند ماینرهای حاضر در این جلسه با پذیرش این متن، ترسو بودن خود را ثابت کرده‌اند. دست کشیدن از Bitcoin Classic و التزام به اجرای Bitcoin Core دقیقاً برعکس آن چیزی بود که طرفداران بلاک‌های بزرگ می‌خواستند. آن‌ها معتقد بودند این یک حربه جدید از جانب طرفداران بلاک‌های کوچک است و Bitcoin Core تحت هیچ شرایطی کُند مربوط به هارد فورک را منتشر نخواهد کرد. طرفداران بلاک‌های کوچک هم به همان اندازه ناراضی بودند. گرگوری مکسول، رئیس وقت بخش فنی و یکی از بنیانگذاران شرکت بلاک‌استریم یعنی همان شرکتی که آدام بک ریاست آنجا را برعهده داشت، به روشنی نظر خود را در مورد افراد حاضر در جلسه هنگ کنگ بیان کرد و گفت آن‌ها «دوستی خاله خرسه» دارند.

قضیه از این قرار است؛ چند نفر از کسانی که دوستی خاله خرسه دارند چند ماه قبل برای یادگیری و آموزش مسائل مورد بحث به چین می‌روند و خود را تا ساعت ۳-۴ صبح در یک اتاق محبوس می‌کنند تا اینکه کار به جایی می‌رسد که از جانب خودشان قول دهند بعد از سگویت، یک پیشنهاد برای اجرای هارد فورک آماده کنند. آن‌ها به تلاش بیهوده خود برای متعهد ماندن به متن توافق ادامه می‌دهند (حتی اگر این توافق را تحت اجبار پذیرفته باشند و حتی اگر استخراج f2pool بلافاصله آن را نقض کرده باشد)، و در عین حال سعی می‌کنند به اعتقادات خود وفادار باشند و احترام خود را نزد جامعه فنی بیت‌کوین از دست ندهند.^۱

1 <https://bitcointalk.org/index.php?topic=1330553.msg14835202#msg14835202>

دستیابی به توافق روی این مسأله روز به روز دشوار تر می‌شد، هرچه بیشتر می‌گذشت افراد لجبازتر و سخت‌گیرتر می‌شدند. به تدریج موضوع به کلی از انتخاب یک مسیر برای پیشرفت بیت کوین منحرف شد و متأسفانه هدف طرفین این شده بود که دیگری را شکست دهد و پیروز میدان باشد. هرچه درگیری طولانی‌تر می‌شد و بحث‌ها ادامه می‌یافت، اطمینان طرفین از اهدافی که برای خود برگزیده بودند بیشتر، و احتمال حل و فصل مسالمت‌آمیز قائله کمتر می‌شد.

بیشتر بیت‌کوینرها معتقد بودند این توافق‌نامه و رویدادهایی که در آن جلسه در هنگ کنگ رخ داده، اشتباه و خجالت‌آور است. به نظر من (که ممکن است خیلی‌ها با آن موافق نباشند) این نشست یک دستاورد مهم داشت. Bitcoin Classic در آن زمان بسیار محبوب شده بود، تقریباً همه فعالان اصلی صنعت بیت‌کوین از آن حمایت می‌کردند و به نظر می‌رسید ماینرها هم به‌زودی به جمع طرفداران آن بپیوندند و این مسأله می‌توانست برای بیت‌کوین یک بحران جدی پدید آورد. توافق هنگ کنگ ما را از لبه پرتگاه دور کرد.

فصل نهم

ساتوشی قلابی

دوشنبه ۲ می سال ۲۰۱۶ گوین اندریسن با یک خبر همه را شوکه کرد و این روز را به یک روز پر هیجان در تاریخ بیت کوین تبدیل کرد. وی با انتشار مطلبی در وبلاگ خود اعلام کرد شکی ندارد که فردی استرالیایی به نام «کریگ استیون رایت» همان ساتوشی ناکاموتو است. گوین ادعا کرد که اثبات رمزنگاری این موضوع را در لندن دیده است.

من معتقدم کریگ استیون رایت شخصی است که بیت کوین را اختراع کرده است.

من چند هفته پیش برای ملاقات با دکتر رایت به لندن رفتم. پس از رد و بدل شدن چند ایمیل میان ما متقاعد شدم که به احتمال زیاد او همان فردی است که در طول سال ۲۰۱۰ و اوایل سال ۲۰۱۱ با او در ارتباط بوده‌ام. پس از کمی معاشرت با او دیگر می‌توانم بگویم شک ندارم که کریگ رایت ساتوشی است.

بخشی از ملاقات ما صرف اعتبارسنجی امضاها و دیجیتالی پیام‌هایی بود که کلید آن‌ها فقط می‌توانست در اختیار ساتوشی باشد. اما حتی قبل از اینکه من شاهد امضا شدن و اعتبارسنجی کلیدها روی یک کامپیوتر دستکاری نشده باشم، مطمئن بودم که در کنار پدر بیت کوین نشسته‌ام.

من در طول این ملاقات با فردی برجسته، صاحب‌نظر، با برنامه، سخاوتمند، و به دنبال حفظ حریم خصوصی روبرو شدم و او با ساتوشی که شش سال پیش با او همکاری می‌کردم مطابقت دارد. او بسیاری ابهامات از جمله اینکه چرا از پروژه کناره‌گیری کرده را برطرف و به من گفت از سال ۲۰۱۱ مشغول به چه کاری بوده است. ولی من به حریم خصوصی دکتر رایت احترام می‌گذارم و تصمیم با خود او است که چه مقدار از این مسائل را با دیگران به اشتراک بگذارد. ما دوست داریم برای خود قهرمان بسازیم اما اگر این افراد با ایده‌آل‌های دست‌نیافتنی ما همخوانی پیدا نکنند، از آن‌ها متنفر می‌شویم. شاید بهتر بود ساتوشی ناکاموتو اسم رمز یکی از پروژه‌های «سازمان امنیت ملی»^۱ آمریکا، یا یک هوش مصنوعی بود که از آینده آمده تا به پیشرفت پول ما کمک کند. ولی او هیچکدام از این‌ها نیست. او یک انسان معمولی مثل بقیه آدم‌ها است. امیدوارم او بتواند اتفاقاتی را پس از معرفی شدن او به دنیا رخ خواهد داد نادیده بگیرد و به کارهایی که انجام دادن آن‌ها او را خوشحال می‌کند یعنی یادگیری، تحقیق، و نوآوری پردازد.

من بسیار خوشحالم که دست او را فشردم و از او بابت بخشیدن بیت کوین به دنیا تشکر کردم.

در وهله اول بسیاری از افراد به این نتیجه رسیدند که حتماً کوین را هک کرده‌اند، زیرا این یک ادعای باورنکردنی بود و از کوین بعید بود چنین چیزی بگوید. به همین دلیل

1 National Security Agency (NSA)

دسترسی او برای اعمال تغییرات روی مخزن^۲ نرم افزار Bitcoin Core از او سلب شد. کوین همچنان می توانست در فرآیند توسعه کُد بیت کوین مشارکت داشته باشد اما دسترسی ادغام تغییرات و به روزرسانی مخزن اصلی نرم افزار را نداشت.

با این حال، چند ساعت بعد فیلمی از کوین در شهر نیویورک بیرون آمد که در آن کوین این ادعاها را تکرار می کرد. اگرچه این ادعاها دور از ذهن به نظر می رسیدند، اما من نمی توانستم بپذیرم کوین در مورد چنین مسأله مهمی اشتباه کند. ولی با وجود این ادعای کوین را باور نمی کردم. تصمیم گرفتم منتظر بمانم تا پیامی که کریگ رایت با استفاده از یکی از کلیدهای خصوصی ساتوشی امضا کرده است را شخصاً بازبینی کنم. تصور من این بود که این مدارک خیلی زود منتشر خواهند شد و ممکن است لازم باشد جامعه بیت کوین با واقعیت بازگشت ساتوشی کنار بیاید. بلافاصله توجه من به مناقشه سائز بلاک جلب شد. پیش خودم فکر کردم شاید کوین به دلیل استقبال نشدن از Bitcoin Classic مستأصل شده و این کار را انجام داده است. من فکر می کردم مناقشه سائز بلاک این مسأله را تحریک کرده باشد. به گمان من شاید این کلیدهای خصوصی سالها در اختیار کوین بوده اند و حالا او قصد دارد کریگ رایت را به عنوان فرد اصلی ماجرا معرفی کند. ساتوشی/کریگ هم می توانست از Bitcoin Classic طرفداری کند. البته شک داشتم کوین دست به چنین اقدام خراب کارانه ای بزند.

چند ساعت بعد و به وقت عصر هنگ کنگ کریگ رایت مطلبی را در وبلاگ خود منتشر کرد. با کمال تعجب این مطلب پر از جملات و عکسهای گیج کننده و بی ربط بود. من مانند بسیاری از بیت کوینرهای دیگر سراسیمه متن را بالا و پایین می کردم و به دنبال پیام و امضاها می گشتم. تهیه آن بسیار ساده است. پس کجاست؟ من نرم افزار خود را باز کرده، و آماده بازبینی صحت امضاها شده بودم. بعد از حدود پنج دقیقه بالا و پایین کردن این متن بالاخره فهمیدم داستان از چه قرار است. این مطلب بی ارزش و پر از مزخرفات

گیج کننده بود. هیچ پیام و امضایی از طرف ساتوشی در کار نبود، و به نظر می‌رسید که همه این‌ها یک حقه است. ممکن است کوین فریب خورده باشد.

به نظر می‌رسد در قسمتی از مطلب کریگ امضایی از ساتوشی وجود داشته است. با این حال همانطور که کاربر سایت ردیت به نام r/Joukeh اشاره کرد، این امضا از روی یکی از تراکنش‌های موجود روی بلاک چین بیت کوین که ساتوشی امضا کرده بوده، برداشته شده است. هیچ پیامی مبنی بر اینکه کریگ رایت ساتوشی است در کار نبود. به نظر می‌رسید کریگ رایت صرفاً یک امضا را از روی بلاک چین عمومی بیت کوین برداشته و آن را در کنار مطالب بی‌ربط دیگر در وبلاگ خود منتشر کرده است.

همزمان با بیانیه کوین، سه خبر در رسانه‌های خبری *The Economist*، *BBC* و *Wired* توسط روزنامه‌نگارانی منتشر شد که مدعی بودند امضاهایی که ثابت می‌کرد کریگ رایت ساتوشی است را در لندن دیده‌اند. این پوشش خبری ضعیف در مورد بیت کوین برای من جدید نبود چون همیشه به همین صورت بود. اگرچه باید جانب انصاف را در مورد مجله *Wired* رعایت کنم چون گزارش اولیه آن‌ها با چاشنی شک و شبهه نوشته شده بود. چند سال پیش در مارس سال ۲۰۱۴ مجله *Newsweek* مدعی شد که ساتوشی را پیدا کرده است. این داستان به همان اندازه احمقانه بود؛ به نظر می‌رسید تهیه کننده این خبر نام ساتوشی را در دفترچه تلفن عمومی جستجو و سپس بدون هیچ مدرک دیگری مدعی پیدا کردن ساتوشی شده است.

در روز ۶ مه سال ۲۰۱۶، ولادمیر ون در لان (مسئول نگهداری از مخزن نرم‌افزار بیت کوین) درباره تصمیم سلب دسترسی کوین به مخزن نرم‌افزار و اینکه چرا دسترسی او مجدداً برقرار نشده است، توضیحاتی ارائه داد.

وقتی از ما پرسیده می‌شود که آیا ما باید مسئولیت نگهداری از مخزن بیت کوین را دوباره به کوین بازگردانیم، جواب من و بسیاری از افراد دیگر یک «نه» قاطعانه است. یکی از دلایل این است که این کار هیچ فایده‌ای ندارد، زیرا او در این سمت فعال نبود و مشارکتی در آن نداشت. علاوه بر این خیلی از افراد معتقدند اگر راه‌مان را از هم جدا کنیم بهره‌وری بیشتری خواهیم داشت.

کوین چند روز بعد از انتشار این مطلب در وبلاگ کریگ، دوباره در نشستی که در شهر نیویورک به همراه «پیندار وونگ^۱» و بنیانگذار پروژه اتریوم «ویتالیک بوتترین^۲» برگزار شده بود ادعای خود را مبنی بر اینکه کریگ رایت ساتوشی است تکرار کرد. این موضوع با توجه به بی‌اساس بودن شواهد و مدارکی که کریگ رایت ارائه کرده بود، خیلی تعجب برانگیز بود. کوین هرگز حرف خود را پس نگرفت اگرچه بعداً اعتراف کرد که احتمالاً در لندن گیج شده بوده است. اصلاً معلوم نبود چرا کوین باید به لندن پرواز می‌کرد چون این کار به راحتی از طریق ایمیل قابل انجام بود. کوین مدعی بود این کار باید حضوری انجام می‌شد، چون کریگ رایت می‌خواست امکان انکار این موضوع را داشته باشد و شخص دیگری بجز او امکان منتشر کردن این مدارک را نداشته باشد. این معضل می‌توانست به راحتی با استفاده از رمزنگاری حل شود: کوین می‌توانست با استفاده از کلید عمومی ساتوشی یک پیام خصوصی را رمزنگاری کند و اگر کریگ رایت کلید خصوصی ساتوشی را در اختیار داشت، می‌توانست این پیام را رمزگشایی کند. با این روش کوین مطمئن می‌شد که کلیدهای خصوصی ساتوشی در اختیار کریگ است، و از طرف دیگر کریگ حق انکار موجه را برای خود محفوظ نگه می‌داشت چون می‌توانست ادعا کند که پیام از طرف کوین درز پیدا کرده است.

این رسوایی ضربه بزرگی به اعتبار کوین زد و یک پیروزی بزرگ برای طرفداران بلاک‌های کوچک بود. کوین به طرفداران بلاک‌های بزرگ زخمی کاری وارد کرده بود و هیچ کس هم جز خود او مقصر نبود. کریگ خود یکی از طرفداران بلاک‌های بزرگ

1 Pindar Wong

2 Vitalik Buterin

بود و شاید این امر باعث شد تا گوین این اشتباه را مرتکب شود. طرفداران بلاک‌های کوچک از شانسی که آورده بودند متعجب بودند. جوک‌هایی در بین جامعه طرفداران بلاک‌های کوچک پخش می‌شد که شاید کریگ خود ساتوشی است و با این شیرین کاری‌ها می‌خواهد به اعتبار طرفداران بلاک‌های بزرگ آسیب برساند. من شخصاً کمی برای گوین متأسف شدم. فشار روحی زیادی بر او وارد می‌شد و بالاخره هر کسی ممکن است مرتکب اشتباه شود.

تقریباً همه طرفداران بلاک‌های کوچک روی این موضوع اجماع داشتند که کریگ رایت در گذشته هم تقلب‌های زیادی کرده بوده، و معتقد بودند هیچ مدرکی مبنی بر ساتوشی بودن کریگ رایت وجود ندارد. با این حال به نظر می‌رسد طرفداران بلاک‌های بزرگ به طرز قابل توجهی به دو گروه تقسیم شده بودند. به عنوان مثال یکی از برجسته‌ترین طرفداران بلاک‌های بزرگ، راجر ورا اظهار می‌کرد که فکر می‌کند کریگ رایت ساتوشی است.

من فکر می‌کنم شواهد کافی برای اثبات این مسأله وجود دارد.

طرفداران بلاک‌های کوچک در خلوت خود از این رخدادها رضایت داشتند. از طرفی فکر می‌کردند حربه‌هایی که برای خریدن وقت به کار بسته بودند کارآمد بوده، و اتفاقات اخیر هم موجب علنی شدن نادانی طرف مقابل درگیری شده بود. از طرف دیگر برخی از افراد محافظه‌کار هشدار می‌دادند که نباید طرفداران بلاک‌های بزرگ را دست کم گرفت.

طی دو سال بعد کریگ به عنوان بخشی از جامعه طرفداران بلاک‌های بزرگ مورد استقبال قرار گرفت و در کنفرانس‌های آن‌ها سخنرانی و در رویدادهای اجتماعی آن‌ها شرکت می‌کرد. از نظر بسیاری از طرفداران بلاک‌های کوچک کریگ شخصیتی تهاجمی داشت و به نظر می‌رسید دانش او از پروتکل بیت‌کوین خیلی کم است. خیلی از آن‌ها معتقد بودند

ظاهر او و طرز صحبت کردن او شبیه به کلاه برداران است. کریگ از طرفداران بلاک‌های بزرگ بود و دیدگاه‌های او در این زمینه شبیه به افراد افراطی در گروه طرفداران بلاک‌های بزرگ بود. به عنوان مثال او می‌گفت سگویت «آشغال»^۱ است یا اظهار می‌کرد در شبکه چیزی به عنوان «نودی که ماین نمی‌کند»^۲ (فول نودی که صرفاً با اعمال قوانین شبکه بر روی تراکنش‌ها و بلاک‌ها از قوانین پروتکل بیت کوین محافظت می‌کند. - م) نداریم، و فقط ماینرها در شبکه به عنوان نود محسوب می‌شوند. کریگ رایت و نظراتش باعث خوشحالی عده‌ای از جامعه طرفداران بلاک‌های بزرگ شد، در حالی که گروه دیگری از آن‌ها معتقد بودند که او با اظهارنظرها و کارهایش به آن‌ها خسارت وارد می‌کند. ولی این افراد نمی‌توانستند کاری از پیش ببرند چون بسیاری از رهبران گروه طرفداران بلاک‌های بزرگ او را در میان خود پذیرفته بودند.

همچنین شواهد زیادی در مورد تقلب و فریب کاری آقای رایت وجود داشت و طرفداران بلاک‌های کوچک به آن‌ها اشاره می‌کردند. به عنوان مثال، او در سال ۲۰۱۵ مطلبی که در سال ۲۰۰۸ در وبلاگ خود منتشر کرده بود را پس از هشت سال ویرایش کرد تا به نظر برسد او در آن زمان در حال نوشتن مقاله‌ای در مورد ارزهای دیجیتال است، در حالی که این بخش مربوط به ارزهای دیجیتال در آرشیو اینترنتی وبلاگ او در سال ۲۰۱۴ وجود نداشت. طرفداران بلاک‌های بزرگ با پذیرفتن کریگ رایت در جمع خود، به نهضت خود آسیب بزرگی وارد کردند. این کار باعث شد تا افرادی که هنوز تصمیم قاطع برای پیوستن به یکی از این گروه‌ها نگرفته بودند یا همچنان بی‌طرف بمانند یا به گروه طرفداران بلاک‌های کوچک پیوندند. اصلاً هدف اصلی طرفین درگیر در مناقشه سائز بلاک این بود که حمایت این افراد بی‌طرف را جلب کنند و آن‌ها را برای پیوستن به گروه خود ترغیب کنند. افراد حامی کریگ رایت در گروه طرفداران بلاک‌های بزرگ (یا بهتر است بگوییم بیشتر آن‌ها) بالاخره در نوامبر ۲۰۱۸، یعنی بعد از پایان یافتن مناقشه سائز بلاک راه خود را از او جدا کردند.

1 shit

2 Non-mining nodes

ما اینجا می‌توانیم وارد جزئیات بیشتری از کارهای گذشته کریگ رایت شویم: سابقه پرونده‌های دادرسی، ادعاهای دروغین، و ویرایش مطالبی که در گذشته منتشر کرده است. و برای همه این موارد دلایل اثبات شده‌ای وجود دارد. در عوض اجازه دهید فقط به این نکته اشاره کنیم که کریگ مطمئناً در مناقشه سائز بلاک نقش مهمی بازی کرد؛ به شهرت گوین لطمه جبران‌ناپذیری وارد کرد و در یکی از پرچالش‌ترین موقعیت‌ها در طول این درگیری، به کمک طرفداران بلاک‌های کوچک آمد.

فصل دهم

DAO و انشعاب زنجیره اتریوم

در تابستان سال ۲۰۱۶، پروژه‌ای با عنوان «دائو»^۱ (سازمان خودمختار غیرمتمرکز)^۲ توجه بسیاری از افراد فعال در جامعه ارزهای دیجیتال را به خود جلب کرد. دائو یک قرارداد هوشمند بود که بر روی زنجیره اتریوم^۳ ساخته می‌شد و به شکل یک صندوق سرمایه‌گذاری مستقل کار می‌کرد. برخلاف صندوق‌های سرمایه‌گذاری سنتی که معمولاً از بالا به پایین و بر اساس ضوابط قانونی مدیریت می‌شدند، تصمیمات سرمایه‌گذاری در دائو بر اساس رأی کاربران و برپایه قوانین پیاده شده در گُدهای نرم‌افزاری یک قرارداد هوشمند مدیریت می‌شد.

اتریوم توسط «ویتالیک بوتترین»^۴ یکی از بیت‌کوینرهای قدیمی، و در سال ۲۰۱۳ پدید آمد. این پروژه در سال ۲۰۱۴ سرمایه‌ای برای خلق یک کوین جمع‌آوری، و در سال ۲۰۱۵ آغاز به کار کرد. در این مرحله یعنی سال ۲۰۱۶ فقط یک سال از عمر آن می‌گذشت و افراد فعال در جامعه اتریوم مشغول انجام پروژه‌های بلندپروازانه‌ای بودند.

1 The DAO
2 Decentralized Autonomous Organization
3 Ethereum
4 Vitalik Buterin

گفته می‌شود ویتالیک در ابتدا قصد داشته بستر قرارداد هوشمند خود را بر روی زنجیره بیت کوین ایجاد کند، ولی بیت کوین برای کاری که او قصد انجامش را داشت به اندازه کافی انعطاف پذیر نبود. این مسأله به ساختار و گد نرم‌افزاری بیت کوین محدود نمی‌شود، بلکه جامعه طرفداران بلاک‌های کوچک مانند گرگوری مکسول و لوک دشر هم اعتقاد داشتند این انعطاف‌پذیری یک خطر بالقوه امنیتی برای بیت کوین است. بر همین اساس، ویتالیک و بسیاری از فعالان جامعه اتریوم به گروه طرفداران بلاک‌های بزرگ گرایش داشتند.

مناقشه ساینز بلاک در پروژه اتریوم هم موضوع مهمی بود. بیت کوین برای جامعه فعالان اتریوم یک تکنولوژی قدیمی، انعطاف‌ناپذیر، و در قید و بند بلاک‌های کوچک ۱ مگابایتی بود. از طرف دیگر اتریوم رویکرد بسیار انعطاف‌پذیرتری را برگزیده بود. ساینز بلاک‌ها می‌توانست به انتخاب ماینرها تغییر کند (این موضوع در اتریوم به «محدودیت گاز» معروف است که بر اساس آن یک بلاک محدود به ساینز داده‌ای که در خود جا داده است نیست، بلکه محدودیت بلاک بر اساس قدرت محاسباتی لازم برای پردازش توابع مختلفی که در آن قرار گرفته است محاسبه می‌شود). در حالی که کارمزد تراکنش‌ها در بیت کوین افزایش می‌یافت، هزینه تراکنش در شبکه اتریوم بسیار پایین بود. این استراتژی بازاریابی اتریوم بسیار موفقیت‌آمیز بود و بسیاری از بیت‌کوینرها تمرکز خود را بر روی اتریوم معطوف کردند و معتقد بودند اتریوم کوین جوان، پویا، و آینده‌داری است. کوچ بیت‌کوینرها به اتریوم از نظر برخی از طرفداران بلاک‌های بزرگ مشکلی بود که توسط طرفداران بلاک‌های کوچک ایجاد شده بود. طرفداران بلاک‌های کوچک به قدری لجباز هستند که باعث می‌شوند صبر بیت‌کوینرها تمام شود و از بیت‌کوین رانده شوند^۱. بیت‌کوین سهم بازار خود را از دست خواهد داد. ممکن است فروشندگان بجای بیت‌کوین، پذیرنده اتریوم شوند و در این صورت بیت‌کوین قطعاً شکست خواهد خورد. اگرچه درست است که محدودیت ساینز بلاک باعث کوچ برخی از بیت‌کوینرها به پروژه‌های

1 Gas limit

2 https://www.reddit.com/r/btc/comments/4u0cuq/congratulation_small_blockers_this_is_a_direct

دیگر شد، اما این تنها دلیل موفقیت آلت کوین‌ها^۱ نبود. فرصت کسب درآمد عامل اصلی این روند بود. موفقیت اتریوم موجی از کپی برداری و پروژه‌های ایجاد کوین را پدید آورده بود. این کوین‌ها اغلب مشکلات احتمالی مقیاس پذیری بیت کوین که به اندازه کافی در مورد آن‌ها تبلیغ شده بود را برجسته، و ادعا می‌کردند که کوین جدید آن‌ها می‌تواند این مسائل را حل کند. به نظر می‌رسید این مسائل برای طرفداران بلاک‌های کوچک اهمیتی نداشت. آن‌ها به توسعه یک سیستم پول تحول‌آفرین علاقه‌مند بودند و به نظر می‌رسید آلت کوین‌هایی که مدعی بودند در یک ثانیه قادر به پردازش ۴۰,۰۰۰ تراکنش هستند ارتباطی به این هدف نداشتند.

از قضا، اگرچه این آلت کوین‌ها برخی از طرفداران بلاک‌های بزرگ را کلافه می‌کرد، اما در عین حال برای آن‌ها وسوسه‌انگیز بود. برای آن‌ها ساده‌تر این بود که به کلی از خیر بیت کوین بگذرند و به جای ادامه این نبرد خسته‌کننده بر روی این آلت کوین‌ها تمرکز کنند. این گرایش آن‌ها به آلت کوین‌ها برای گروه طرفداران بلاک‌های کوچک منفعت بسیار زیادی داشت. فضای آلت کوین‌ها در خلال این مناقشه به سرعت رشد کرد و هواداران آن‌ها تمرکز خود را بر روی جذب سرمایه‌گذاری برای خلق کوین و کسب درآمد از افزایش قیمت آن گذاشته بودند. اگر آن‌ها وقت خود را بر روی آلت کوین‌ها صرف نمی‌کردند، ممکن بود در بیت کوین باقی بمانند و در مناقشه ساینز بلاک شرکت فعال داشته باشند، و با توجه به تعداد بالای این افراد غلبه بر آن‌ها کار بسیار دشواری می‌شد. در طول دوره دو ساله مناقشه ساینز بلاک، یک تغییر اساسی در اکوسیستم پدید آمد و فضا از بیت کوین به سمت ارزهای دیجیتال^۲ رفت. در این شرایط این استدلال که بیت کوین باید به مذاق همگان خوش بیاید به کلی بی‌معنی شد. متناسب با همه نیازهای افراد یک آلت کوین وجود داشت.

1 Alternative coins (altcoins)

2 Crypto currency

به هر حال، به قضیه دائو برگردیم. فروش جمعی^۱ دائو از تاریخ ۳۰ آوریل ۲۰۱۶ آغاز شد و تا ۲۵ مه ۲۰۱۶ ادامه داشت. این پروژه توجه بسیاری را به خود جلب، و بیش از ۱۵۰ میلیون دلار سرمایه جذب کرد. این مقدار سرمایه در آن زمان پول بسیار زیادی بود، بیشتر از ۱۴ درصد همه اترهای^۲ موجود درون دائو قرار گرفت. برخی از سرمایه‌گذاران آن را یک سرمایه‌گذاری بدون ریسک در نظر گرفتند، زیرا آن‌ها تصور می‌کردند هر وقت اراده کنند می‌توانند سرمایه خود را از این صندوق سرمایه‌گذاری خارج کنند.

اتریوم به‌عنوان یک پروژه جوان به‌هیچ‌وجه آماده چیز پیچیده‌ای مثل دائو نبود. اما جامعه فعالان اتریوم به آزمایش کردن چیزهای جدید علاقه‌مند بود. اصلاً دلیل اصلی جذب آن‌ها به پروژه اتریوم همین موضوع بود. آن‌ها از بیت‌کوین محافظه‌کار خسته شده بودند.

همانطور که بعداً معلوم شد، دائو در سطوح مختلفی نقص داشت. ایجاد پروژه‌های جدید سرمایه‌گذاری موجب پدید آمدن انواع مختلفی از توکن‌های دائو^۳ شد که هر کدام مخاطرات و ویژگی‌های خاص خود را داشتند. این بدان معنی است که توکن‌های دائو قابلیت تعویض‌پذیری^۴ نداشتند و با قیمت‌های متفاوتی از یکدیگر معامله می‌شدند؛ مسأله‌ای که صرافی‌ها و جامعه فعالان به‌درستی آن را درک نکرده بودند. مدل انگیزه‌های اقتصادی این پروژه هم چندان منطقی به نظر نمی‌رسید. به‌عنوان مثال، در زمان تصمیم‌گیری برای یک سرمایه‌گذاری افراد انگیزه پایینی برای رأی «مخالف» داشتند، چون افرادی که رأی مخالف داده بودند برخلاف افرادی که رأی آن‌ها ممتنع بود، در پروژه‌هایی که در نهایت تصویب می‌شد شرکت داده می‌شدند. علاوه بر این هیچ مکانیزم الزام‌آوری برای پروژه‌های موفق وجود نداشت تا دائو را از سود خود منتفع کنند، و گد نرم‌افزاری که در قرارداد هوشمند نوشته شده بود لزوماً هدف تبلیغ شده را پیاده‌سازی نمی‌کرد. چند هفته پس از اتمام فروش توکن در ۱۷ ژوئن سال ۲۰۱۶^۵، (یک تاریخ مهم دیگر در تاریخ

1 crowdsale

2 ETH

3 DAO tokens

4 fungibility

5 <http://archive.is/76EZY>

ارزهای دیجیتال) یک هکر توانست یک حفره امنیتی در کُد نرم‌افزار پیدا کند که به او اجازه می‌داد به صندوق اتریوم دائو^۱ دسترسی پیدا کند و بخشی از دارایی آن را به یک «دائو کوچک»^۲ که کنترل قابل توجهی بر روی آن داشت، منتقل کند.

این رویداد آغازگر «مناقشه دائو»^۳ بود، نبردی برای بازیابی اتریوم‌های «دزدیده» شده توسط هکر. متأسفانه فرآیند بازیابی سرمایه دزدیده شده موفقیت‌آمیز نبود، بنابراین فکری به ذهن جامعه فعالان اتریوم رسید؛ آن‌ها می‌توانستند قوانین پروتکل اتریوم را به منظور بازیابی سرمایه به سرقت رفته تغییر دهند. این موضوع برای برخی از افراد بحث‌برانگیز بود و افراد زیادی با آن مخالف بودند چون معتقد بودند این کار شبیه به مداخلات دولتی در بانک‌ها است. دلیل اصلی پیوستن افراد به ارزهای دیجیتالی این بود که آن‌ها قصد داشتند خود را از سیستم‌هایی که دولت‌ها در آن‌ها مداخله می‌کنند، مانند مداخلات دولتی سال ۲۰۰۸ و ۲۰۰۹ که در فروپاشی اقتصادی دنیا رخ داد، دور نگه دارند. اصلاً چرا باید پروژه دائو را از دیگر پروژه‌ها مستثنی کنیم؟ چرا باید در حالی که بسیاری از سرمایه‌گذاران در پروژه‌های کوچکتر و قراردادهای هوشمند اتریوم در گذشته ضرر کرده بودند، این پروژه را نجات می‌دادند؟ شاید پروژه دائو بیش از حد بزرگ بود و نمی‌بایست شکست می‌خورد، یا شاید به دلیل منافع شخصی توسعه‌دهندگان و اعضای تاثیرگذار جامعه فعالان اتریوم بود که بر روی قوانین شبکه کنترل داشتند و مبالغ زیادی را بر روی پروژه دائو سرمایه‌گذاری کرده بودند. از نظر بسیاری، این مسائل فساد و مشکلات موجود در سیستم‌های مالی سنتی را مثل یک آینه نشان می‌داد، مشکلاتی که افراد برای فرار از آن‌ها به پروژه دائو روی آورده بودند.

در ۲۴ ژوئن سال ۲۰۱۶، پیشنهاد شد که به منظور مسدود کردن دارایی تحت کنترل هکرها، یک سافت فورک بر روی پروتکل اتریوم اعمال شود^۴. حدود ۴ روز بعد مشخص شد که سافت فورک پیشنهادی نقص دارد و به طور بالقوه‌ای شبکه اتریوم را در معرض

1 DAO's Ethereum funds

2 Child DAO

3 DAO Wars

4 <http://archive.is/7UUrY>

حملات اساسی DOS قرار می‌دهد. بنابراین ایده سافت فورک را رها کردند و تصمیم بر آن شد که تنها راه بازیابی دارایی به سرقت رفته این است که یک هارد فورک بر روی شبکه اعمال شود. این اتفاقات با توجه به اینکه بیت کوین درست در میانه مناقشه سائز بلاک قرار داشت، بسیار قابل توجه بود. در حالی که Bitcoin Classic به‌عنوان یک هارد فورک احتمالی روی شبکه بیت کوین مطرح بود، اتریوم در حال برنامه‌ریزی برای اعمال یک هارد فورک بحث‌برانگیز بر روی شبکه خود بود. مناقشه بر روی سائز بلاک بیت کوین عملاً برای چند ماه متوقف شد، چون همه روی اتریوم تمرکز کرده بودند. برای اندازه‌گیری سطح پشتیبانی عمومی از هارد فورک یک رأی‌گیری با استفاده از کوین ترتیب داده شد؛ افراد می‌توانستند با استفاده از کوین‌های خود رأی دهند که آیا از هارد فورک پشتیبانی می‌کنند یا نه. اکثریت ۹۵ درصد آراء از هارد فورک حمایت کردند^۱. هرچند بسیاری از افراد معتقد بودند این نظرسنجی نماینده آراء همه افراد جامعه فعالان اتریوم نبوده است چون توسط افرادی برگزار شده که از اجرای هارد فورک حمایت می‌کردند و ممکن است افراد مخالف در آن شرکت نکرده باشند. علاوه بر این افراد کمی از دارندگان اتریوم، شاید حدود ۶ درصد در این رأی‌گیری شرکت کرده بودند^۲. همچنین از ماینرها هم نظرسنجی شد و گفته می‌شود بیشتر از ۹۰ درصد آن‌ها از اجرای هارد فورک حمایت کرده بودند.

اجرای هارد فورک برای چهارشنبه ۲۰ ژوئیه سال ۲۰۱۶ برنامه‌ریزی شده بود. برای اینکه این رویداد را از دست ندهم این روز و روز بعد را از محل کارم مرخصی گرفتم. من همچنین یک کامپیوتر جدید خریداری کرده بودم تا بتوانم هر دو نرم‌افزار اتریوم را بر روی دو کامپیوتر مجزا اجرا کنم؛ یکی را به نرم‌افزار به‌روزرسانی شده برای هارد فورک، و دیگری را به نسخه قدیمی اختصاص دادم. با نزدیک شدن هارد فورک احتمالی، مانند یک طرفدار متعصب واقعی در منزل بودم و هر دو نرم‌افزار را اجرا کرده بودم. همچنین پنجره‌های زیادی از وب‌سایت‌های مختلف بر روی مرورگر من باز بود که در آن‌ها قیمت اتریوم را با توجه به اتفاقاتی که در حال رخ دادن بود دنبال می‌کردم. من به همراه بسیاری

1 <https://futurism.com/the-dao-heist-undone-97-of-eth-holders-vote-for-the-hard-fork>

2 <https://medium.com/coinmonks/the-dao-is-history-or-is-it-47a6f457338a>

دیگر از علاقه‌مندان به ارزهای دیجیتالی مشتاقانه منتظر رسیدن بلاک شماره ۱,۹۲۰,۰۰۰ و وقوع هارد فورک بودیم^۱.

در ابتدا به نظر می‌رسید هارد فورک با موفقیت انجام شده باشد. بلاک‌های جدید به زنجیره ارتقاء یافته اضافه می‌شدند، در حالی که زنجیره قدیمی متوقف شده بود و پیشرفتی نداشت. برخی از طرفداران بلاک‌های بزرگ اعلام پیروزی کردند و معتقد بودند که این درسی برای بیت کوین است؛ آن‌ها ادعا می‌کردند که یک هارد فورک بحث‌برانگیز موجب ایجاد شکاف در زنجیره بیت کوین نخواهد شد. حدود یک ساعت بعد از اعمال هارد فورک، بلاک‌های جدید به زنجیره اصلی اتریوم، که دنباله‌رو قوانین قدیمی بودند اضافه شد. سپس بعد از تنظیم مجدد سختی شبکه^۲ در این زنجیره (که در شبکه اتریوم بسیار سریع‌تر از بیت کوین انجام می‌شود)، بلاک‌ها با سرعت بیشتری به انتهای آن اضافه می‌شدند. در حالی که در ابتدا به نظر می‌رسید زنجیره هارد فورک ۹۸ درصد از هش‌ریت را در اختیار دارد، پس از مدتی این مقدار تغییر کرد و هش‌ریت زنجیره اصلی توانست به پنج تا ده درصد از توان هش کل شبکه دست یابد. حالا زنجیره قوانین اصلی (که حاوی قوانین قدیمی شبکه بود) به یک نام نیاز داشت. با توجه به اینکه از قبل محصولی به نام Bitcoin Classic داشتیم، چرا اسم این زنجیره را Ethereum Classic نگذاریم؟

حدود سه روز پس از هارد فورک، صرافی‌ها شروع به لیست کردن اتریوم کلاسیک کردند. «پولونیکس^۳» یکی از صرافی‌هایی که در آن زمان در آلت کوین‌ها پیشرو بود، در تاریخ ۲۳ جولای سال ۲۰۱۶ اتریوم کلاسیک را در صرافی خود لیست کرد^۴. سپس قیمت اتریوم کلاسیک شروع به افزایش کرد. تا جایی که به یاد دارم قیمت آن از حدود دو درصد قیمت اتریوم شروع شد تا جایی که در تاریخ ۲۵ ژوئیه به ۵۰ درصد قیمت اتریوم رسید. قیمت اتریوم کلاسیک بسیار پرنوسان بود. ماینرها هم همیشه قیمت را دنبال می‌کنند. با افزایش قیمت اتریوم کلاسیک، ماینرهای بیشتری سراغ آن می‌رفتند تا از

1 <http://archive.is/PaGgM>
2 Difficulty adjustment
3 Poloniex
4 <http://archive.is/xfvMY>

پاداش ساختن بلاک بالاتر آن بهره‌مند شوند. اینجا بود که طرفداران بلاک‌های کوچک استدلال می‌کردند که اوضاع پیچیده‌تر از چیزی است که طرفداران بلاک‌های بزرگ فکر می‌کنند: شاید تعریف پروتکل بر عهده ماینرها نباشد، شاید ماینرها فقط از معامله‌گران و سرمایه‌گذاران تبعیت می‌کنند تا سود خود را به حداکثر برسانند.

اتریوم کلاسیک با افزایش قیمت برای معامله‌گران و ماینرها جذاب‌تر می‌شد. به نظر می‌رسید ماینرها فقط می‌خواستند سود خود را به حداکثر برسانند. اینجا بود که بسیاری از افراد دریافتند که یک هارد فورک بحث‌برانگیز فقط به علوم کامپیوتر و مسأله هش‌ریت مربوط نمی‌شود، بلکه مسأله بازارهای مالی هم در آن دخیل است. این نوع رویدادها برای دلالتان مالی و معامله‌گران فرصتی بود تا بین سکه‌های مختلفی که در نتیجه فورک زنجیره‌ها پدید می‌آید، به تجارت و کسب سود پردازند.

یکی از شخصیت‌های تاثیرگذار در فضای ارزهای دیجیتال که از اتریوم کلاسیک حمایت می‌کرد، «بری سیلبرت»^۱ بود. او از طرفداران بلاک‌های کوچک نبود بلکه به نظر می‌رسید فقط برای کسب سود از اتریوم کلاسیک پشتیبانی می‌کند.

اولین ارز دیجیتالی که بعد از بیت‌کوین خریدار اتریوم کلاسیک (ETC) است. با قیمت ۵۰ سنت از نظر ریسک سرمایه‌گذاری مناسب است و من از فلسفه پیدایش آن حمایت می‌کنم.^۲

بری سیلبرت یک سال زودتر «گروه ارز دیجیتال»^۳ را تاسیس کرده بود و یکی از بزرگترین سرمایه‌گذاران در این فضا بود. همچنین او به دلیل برنده شدن در حراج بیت‌کوین‌های مصادره شده از بازار «جاده ابریشم»^۴ توسط مقامات ایالات متحده آمریکا، بسیار شناخته شده بود. از او در ادامه داستان بیشتر خواهیم گفت. با این حال، به نظر

1 Barry Silbert

2 <https://twitter.com/BarrySilbert/status/757628841938472961>

3 Digital Currency Group

4 Silk Road

می‌رسید او در آن زمان ناخواسته در حال کمک کردن به گروه طرفداران بلاک‌های کوچک است.

محبوبیت اتریوم کلاسیک و پیشی گرفتن هشریت آن هیچگونه خطری برای اتریوم به وجود نمی‌آورد و باعث نمی‌شود همه نودهای به‌روزرسانی شده بر اساس هارد فورک از بلاک‌های زنجیره طولانی‌تر اتریوم کلاسیک پیروی کنند. ویتالیک باهوش‌تر از این حرف‌ها بود. ساختار هارد فورک اتریوم به گونه‌ای طراحی شده بود که در آن یک نقطه بدون بازگشت برای شکاف در زنجیره تعبیه شده بود. به طوری که هر دو زنجیره صرفنظر از مقدار اثبات کاری که در آن‌ها است بتوانند در کنار یکدیگر ادامه پیدا کنند. این قابلیت به «محافظت از پاک شدن»^۱ معروف است و چیزی است که من قبل از رخداد هارد فورک، با توسعه‌دهندگان اتریوم درباره آن بحث کرده بودم. امروزه، تصمیم Bitcoin Classic مبنی بر استفاده نکردن از این قابلیت، بسیار ساده‌لوحانه‌تر به نظر می‌رسد.

صرافی کوین بیس اتریوم را در تاریخ ۲۱ ژوئیه سال ۲۰۱۶ و فقط یک روز بعد از اجرای هارد فورک لیست کرد.^۲ این شرکت از حامیان Bitcoin Classic بود و مدیرعامل آن، برایان آرمسترانگ معتقد بود هارد فورک اتریوم بدون رخ دادن انشعاب در زنجیره و با موفقیت انجام خواهد شد. شاید به این دلیل که این هارد فورک از حمایت قوی ماینرها برخوردار است. این شرکت در نتیجه این برداشت غلط، اقدامات لازم برای حفاظت از دارایی کاربران خود را انجام نداد. بنابراین این شرکت در برابر چیزی به نام «حمله انتشار دوباره»^۳، آسیب‌پذیر بود. در چند روز اول پس از انشعاب، هنگام برداشت اتریوم از صرافی کوین بیس، این احتمال وجود داشت که کوین بیس دو نسخه از این تراکنش را ارسال کند. یکی به شبکه اتریوم، و دیگری به شبکه اتریوم کلاسیک. در مقابل،

1 Wipeout protection

2 <https://blog.coinbase.com/coinbase-adds-support-for-ethereum-b8046cf486d0>

3 Replay attack

صرافی‌های «کراکن»^۱ و «پولونیکس»^۲ اقداماتی برای جداسازی کوین‌های خود و در نتیجه جلوگیری از این رخدادها انجام داده بودند. برخی از معامله‌گران با تجربه در این فضا توانستند از این وضعیت کسب درآمد کنند. آن‌ها کوین‌های اتریوم و اتریوم کلاسیک خود را از هم جدا می‌کردند و اتریوم‌های خود را به کوین بیس واریز می‌کردند. آن‌ها بدون نیاز به معامله کردن اتریوم می‌توانستند آن را از صرافی برداشت کنند و امیدوار بودند با توجه به مشکل «حمله انتشار دوباره» و بدون صرف هزینه، به صورت رایگان اتریوم کلاسیک دریافت کنند. من در آن زمان با چند نفر صحبت کردم که ادعا می‌کردند با موفقیت توانسته‌اند این کار را انجام دهند و سود قابل توجهی هم کسب کرده‌اند. سرانجام کوین بیس متوجه این اشکال شد و آن را رفع کرد و زیان‌ها را از ترازنامه خود جبران کرد.

در مورد مناقشات دائو، بازیابی وجوه به سرقت رفته در زنجیره اتریوم موفقیت‌آمیز بود. ولی موضوع در مورد وجوه به سرقت رفته در زنجیره اتریوم کلاسیک پیچیده‌تر از این بود و مناقشه دائو همچنان ادامه داشت. مسائل دیگری در زنجیره اتریوم کلاسیک مطرح بود، از جمله اینکه توکن‌های بازیابی شده دائو به چه کسی می‌رسد. ولی این موضوع از حوصله داستان ما خارج است.

در پایان ژوئیه سال ۲۰۱۶، نشست دیگری بین ماینرها و توسعه‌دهندگان بیت کوین این بار در کالیفرنیا ترتیب داده شد. برای جلوگیری از گرفتاری دوباره در دام اتهام به توافق پشت درهای بسته، همه شرکت‌کنندگان ملزم بودند بیانیه زیر را قبل از حضور در این نشست امضا کنند:

شرکت‌کنندگان در این نشست به این موضوع واقف هستند که چون قوانین اجماع بیت کوین توسط کاربران بیت کوین و بر اساس نرم‌افزاری که برای اجرا انتخاب

1 Kraken
2 Poloniex

می‌کنند تعیین می‌شود، بنابراین تغییرات پیشنهادی باید با در نظر گرفتن نظرات همه افراد فعال در جامعه بیت کوین و به صورت علنی مورد بحث و تبادل نظر قرار گیرد. بنابراین هیچگونه توافق یا اجماعی در این رویداد صورت نخواهد گرفت.^۱

لطفاً توجه داشته باشید که من در این جلسه حضور نداشتم. با این حال یادداشت‌های جلسه توسط «برایان بیشاپ»^۲ که یکی از توسعه‌دهندگان بیت کوین است در اختیار عموم قرار گرفته است.^۳ برایان کار فوق‌العاده‌ای انجام می‌داد و متن بسیاری از وقایع و بحث‌های مربوط به مناقشه ساینز بلاک را رونویسی و منتشر می‌کرد. یکی از شرکت‌کنندگان در این نشست جیهان وو بود که برای دیدار با توسعه‌دهندگان بیت کوین به ایالات متحده پرواز کرده بود. نام اشخاص در این متن مشخص نشده، با وجود این کسانی که با شخصیت‌های اصلی این فضا آشنایی دارند در بسیاری از موارد می‌توانند حدس بزنند که گوینده هر بخش چه کسی بوده است. تاریخ این نشست هم تصادفی انتخاب نشده بود بلکه مصادف بود با اواخر ماه جولای، درست زمانی که قرار بود گد نرم‌افزاری هارد فورک طبق توافق‌نامه هنگ کنگ منتشر شود.

تأثیر انشعاب زنجیره اتریوم به دو کوین مستقل بر هارد فورک احتمالی بیت کوین بر این نشست کاملاً مشهود بود و بیشتر بحث حول درس‌هایی بود که می‌شد از این رخداد آموخت. شرکت‌کنندگان در این جلسه به این نتیجه رسیده بودند که یک هارد فورک باعث ایجاد انشعاب در زنجیره بیت کوین خواهد شد:

انشعابی که در زنجیره اتریوم به وجود آمد، نشان داد این اتفاق برای هارد فورک‌های احتمالی بیت کوین هم خواهد افتاد. در مورد بیت کوین از این دو حالت خارج نیست؛ یا باید ایجاد شدن چندین زنجیره مختلف و حملات از جنبه‌های

1 <https://www.coindesk.com/no-scaling-agreements-industry-bitcoin-meetup>

2 Brian Bishop

3 <https://diyhpl.us/wiki/transcripts/2016-july-bitcoin-developers-miners-meeting/cali2016/>

مختلف را بپذیریم، یا فقط روی زنجیره اصلی باقی بمانیم و سعی کنیم فورک‌ها و انشعاب‌های در اقلیت را از بین ببریم.

سپس یکی از توسعه‌دهندگان تلاش کرد وضعیت را تبیین کند و توضیح دهد که چرا علیرغم توافق هنگ کنگ اجرای یک هارد فورک در کوتاه‌مدت امکان‌پذیر نیست:

بسیاری از امضاءکنندگان توافق هنگ کنگ یک هفته را در نیویورک سپری، و خیلی بر روی طراحی نرم‌افزار کار کردند. ما در مورد چگونگی اجرای یک هارد فورک با یکدیگر بحث کردیم. ما در مورد روش اجرای این موضوع بحث کردیم، روشی که ما را درگیر مخاطراتی که اتریوم به تازگی تجربه کرده است نکند. ما درباره اهمیت یکپارچگی بیت کوین و اهمیتی که برای ارزش بیت کوین در طولانی مدت دارد در هنگ کنگ صحبت کردیم. هیچ تمایلی برای انجام هر کاری که بحث برانگیز باشد وجود ندارد، چه در هنگ کنگ، و چه در نیویورک. قبل از اجرای هر نوع هارد فورکی نیاز به توافق همگانی داریم و باید با کمترین درگیری و مخالفتی انجام شود. مسلماً نتیجه پژوهش‌ها و بحث‌هایی که تاکنون پیرامون این موضوع انجام شده است باید به طور گسترده‌ای در دسترس عموم قرار گیرد، اما مطمئناً نگرانی‌های زیادی حتی از نظر افرادی که بیرون از این اتاق هستند وجود دارد؛ که رسیدن به چنین توافقی گسترده‌ای برای اجرای یک هارد فورک بسیار دشوار خواهد بود. من می‌خواهم به این نکته اشاره کنم که هارد فورک‌ها باعث ایجاد اختلالات شدیدی در بازارها می‌شوند. آن‌ها کار پذیرندگان، بازارها، و کل اکوسیستم را مختل می‌کنند و ما باید این مسأله را در نظر بگیریم. مادامیکه دلیل بسیار مهمی برای یک هارد فورک وجود نداشته باشد، هزینه‌های اجرای آن بیشتر از فواید آن خواهد بود. ما به دنبال راه‌حلی برای حل مشکلات بیت کوین، بدون نیاز به یک هارد فورک هستیم.

در ادامه لوک دش‌پیر، که یکی از امضاءکنندگان توافق‌نامه هنگ کنگ بود توضیح داد که به تعهد خود عمل کرده و برخی از قسمت‌های کُد نرم‌افزاری هارد فورک را نوشته است.¹

یکی از توسعه‌دهندگان حاضر در نشست که احتمالاً در جلسه هنگ کنگ حضور نداشته، از رفتار خود برای تضعیف تلاش‌های توسعه‌دهندگان برای تولید کُد نرم‌افزاری هارد فورک عذرخواهی کرد. او گفت وقتی ماینرها اظهار کردند که از اجرای سگویت جلوگیری خواهند کرد، از نظر او ادامه کار بر روی هارد فورک کار درستی نبوده است. این فرد ابراز نگرانی کرد که اجرای هارد فورک موجب شود تا افزایش سایز بلاک از طریق سگویت از راه خود منحرف شود. وی همچنین از اظهارنظرهای عمومی در مورد جلوگیری از اجرای سگویت به قصد هارد فورک شکایت کرد و گفت این اظهارنظرها اساساً تهدیدهایی هستند که باعث هرچه دشوارتر شدن اجرای هارد فورک می‌شوند.

من می‌خواهم از شما و توسعه‌دهندگان بخاطر تضعیف تلاش‌هایشان در تهیه کُد نرم‌افزاری هارد فورک که در نشست هنگ کنگ متعهد به آن شده بودند، عذرخواهی کنم. من این کار را به این خاطر انجام دادم که تلاش‌های آنها در نیویورک درست پس از انتشار برخی از اظهارنظرهای عمومی در مورد جلوگیری از اجرای سگویت برای انجام هارد فورک، صورت پذیرفت. در این فضا من نسبت به پیشنهادها اجرای هارد فورک که مقیاس‌پذیری بیت کوین از راه سگویت را مختل می‌کنند، احساس خوبی ندارم. از حال و هوایی که بیان نظراتم به‌وجود آورد پشیمانم. از این بابت و نظراتم متاسفم.

سپس فردی به این اظهارنظر پاسخ داد. وی احتمالاً جیهان وو است که با زیرکی به موضوع مشکل برقراری ارتباط که هر دو طرف درگیر آن بودند، اشاره کرد. جیهان سپس تلویحاً اظهار کرد که او نیز احساس خطر کرده و هر دو طرف از این نظر مقصر هستند.

¹ <https://github.com/luke-jr/bips/blob/bip-mmhf/bip-mmhf.mediawiki>

فکر می‌کنم باید این موضوع را روش‌کنم. قضیه جلوگیری از اجرای سگویت از آنجا شروع شد که متعهد ماندن به توافق‌نامه هنگ کنگ زیر سؤال رفت. ما نمی‌توانیم به درستی با یکدیگر ارتباط برقرار کنیم و از این نظر مسیر نادرستی را در پیش گرفته‌ایم. شاید هر دو طرف نمی‌خواهند تحت فشار کاری را انجام دهند. شاید هر دو طرف نمی‌خواهند تهدید شوند.

بعد از این نشست من با یکی از طرفداران بلاک‌های کوچک که شخصیت معروفی بود و در آن نشست شرکت کرده بود، صحبت کردم. او به من گفت که جیهان موافقت کرده است که به محض انتشار سگویت به فعال شدن آن بر روی شبکه کمک کند، و ماینرها از اتفاقاتی که برای اتریوم افتاده ترسیده‌اند و نمی‌خواهند روش‌های خطرناک را آزمایش کنند. تعهد جیهان به فعال‌سازی سگویت یک مقدار خوش‌بینانه بود و امکان داشت او یک روایت کاملاً متفاوت از ماجرا داشته باشد. تصور اینکه هر دو طرف همچنان درگیر مشکل برقراری ارتباط با یکدیگر باشند اصلاً کار سختی نبود.

انشعاب در زنجیره اتریوم نقش بسیار کلیدی در مناقشه سائز بلاک بازی کرد، حتی مهم‌تر از ماجرای شرم‌آور کریگ رایت. این موضوع باعث شد ابتکار عمل در دست طرفداران بلاک‌های کوچک قرار بگیرد و ماینرها از رخ دادن اتفاقات مشابه در بیت‌کوین هراس داشته باشند. قبل از انشعاب اتریوم، ماینرها مایل بودند روشی را امتحان کنند ولی به نظر می‌رسید این دیدگاه تغییر کرده باشد. فعال شدن Bitcoin Classic در کوتاه‌مدت خیلی بعید به نظر می‌رسید. از قضا اگرچه اکثر طرفداران بلاک‌های کوچک دوست ندارند این را بپذیرند ولی ممکن است اتریوم موجب نجات بیت‌کوین شده باشد. با این حال، تا پایان جنگ زمان زیادی باقی‌مانده بود. حافظه تاریخی افراد در این فضا بسیار کوتاه است و درس‌هایی که از انشعاب اتریوم به دست آمده بود کم‌کم داشت از خاطره‌ها محو می‌شد.

فصل یازدهم

کنفرانس سوم مقیاس پذیری بیت کوین در میلان

هیجان در اتریوم اوضاع را کمی برای بیت کوین آرام کرده بود. از نظر طرفداران بلاک‌های کوچک، اجرای هارد فورک برای افزایش سایز بلاک از دستور کار خارج شده بود. در تاریخ ۸ و ۹ اکتبر سال ۲۰۱۶ کنفرانس سوم مقیاس‌پذیری بیت کوین در میلان برگزار شد. طرفداران بلاک‌های کوچک مشتاق بودند که قائله در این کنفرانس ختم شود و دو طرف بتوانند با تمرکز بر روی مسائل با اهمیت و دوری از بحث‌های بی‌مورد برای ادامه کار تصمیم بگیرند. بنابراین این کنفرانس برای تمرکز بر روی سایر مسائل مربوط به مقیاس‌پذیری، مثل شبکه لایت‌نینگ و سیستم رمزنگاری و «امضاهاى شنور»^۱ برنامه‌ریزی شده بود. هیچ سخنرانی درباره محدودیت سایز بلاک انجام نشد و نیازی نبود برای پیدا کردن افراد تصمیم‌گیرنده اصلی یا جلسات مهم مدام از این اتاق به آن اتاق برویم. این کنفرانس بیشتر متأثر از گروه طرفداران بلاک‌های کوچک بود و در مورد موضوع سایز بلاک بحثی به میان نیامد. مجموعه برنامه‌های این کنفرانس از نشستی برای حل مشکل بحران سایز بلاک، به یک کنفرانس فنی بیت کوین تغییر شکل داده بود.

1 Schnorr signatures

البته در این کنفرانس تعداد کمی از طرفداران بلاک‌های بزرگ هم شرکت داشتند. آن‌ها شامل راجر وور و گروهی از افرادی بودند که از یک پیشنهاد جایگزین برای هارد فورک شبکه بیت‌کوین، به نام Bitcoin Unlimited حمایت می‌کردند. با توجه به عدم موفقیت Bitcoin Classic، این پیاده‌سازی جدید داشت کم‌کم به‌عنوان انتخاب اصلی طرفداران بلاک‌های بزرگ‌تر مورد توجه قرار می‌گرفت. این موضوع در فصل‌های بعدی با جزئیات بیشتری مورد بحث قرار خواهد گرفت. بسیاری از طرفداران بلاک‌های بزرگ یک تی‌شرت خاص به تن داشتند که روی آن نوشته شده بود «Hard Fork Cafe». این بخشی از کمپین تبلیغاتی آن‌ها برای اجرای هارد فورک بود. من در این کنفرانس با برخی از طرفداران بلاک‌های بزرگ صحبت کردم و از اینکه به آن‌ها اجازه سخنرانی در این مراسم داده نشده بود، گله‌مند بودم. آن‌ها معتقد بودند که این کنفرانس یک‌جانبه برنامه‌ریزی شده و جانب انصاف در مورد آن‌ها رعایت نشده است.

راجر وور به همراه دوستان خود «جری چان»^۱ و «جیک اسمیت»^۲ در گروه طرفداران بلاک‌های بزرگ، یک رویداد اجتماعی را به جای برنامه عصر شنبه کنفرانس ترتیب داده بودند. این مراسم را «مهمانی آزادی بیان» نامیده بودند که شامل غذا و نوشیدنی رایگان بود و به شرکت‌کنندگان آن تی‌شرت‌های رایگان با شعار Hard Fork Cafe می‌دادند. همچنین این مراسم شامل سخنرانی‌هایی بود که ارائه آن‌ها در کنفرانس اصلی صرفاً به دلیل موضوع‌شان ممنوع بود. تا آنجا که من به یاد می‌آورم همه ماینرهای چینی حاضر در کنفرانس میلان، به جای شرکت در کنفرانس رسمی در این رویداد اجتماعی جانبی شرکت کردند. شاید تمرکز و تحلیل این وقایع از نظر برخی از افراد از اهمیت بالایی برخوردار نباشد ولی با این حال من فکر می‌کنم این وقایع نشان‌دهنده استیصال طرفداران بلاک‌های بزرگ است آن‌ها احساس می‌کردند در جامعه و فضایی که برای آن‌ها بسیار مهم است نادیده گرفته می‌شوند و صدای آن‌ها خفه می‌شود. آن‌ها صدای خود و احساس مالکیت بر بیت‌کوین را از دست داده بودند. این رویداد فریاد آن‌ها برای جلب توجه بود، آن‌ها می‌خواستند همچنان در این فضا مطرح باشند. یک شکاف اجتماعی میان جامعه

1 Jerry Chan

2 Jake Smith

فعالان بیت کوین در حال ایجاد شدن بود و مشخص بود ماینرهای چینی (حداقل آنها که با جیهان وو در ارتباط بودند) به کدام سمت گرایش دارند.

روز دوشنبه یعنی یک روز بعد از کنفرانس، یک جلسه کوچکتر میان توسعه‌دهندگان بیت کوین در شهر میلان برگزار شد. عصر همان روز پیامی از طرف جیهان وو به گروه توسعه‌دهندگان رسید مبنی بر اینکه او بر خلاف وعده‌ای که ظاهراً در ماه جولای داده بوده، قصد حمایت از سگویت را ندارد. شایعات درباره دلایل احتمالی این تصمیم جیهان در جامعه فعالان بیت کوین پیچید. گفته می‌شد که جیهان از مطرح نشدن بحث درباره هارد فورک در کنفرانس میلان دلخور شده است چون فکر می‌کرده که این موضوع از دستور جلسه برنامه کنفرانس حذف شده و انتظار چنین چیزی را نداشته است. همچنین گفته می‌شد او از اینکه توسعه‌دهندگان برای انتقال او از فرودگاه به جلسه‌ای که در ماه ژوئیه با آنها برگزار شده بود ماشین ارسال نکرده بودند ناراحت شده و احساس کرده که به او بی‌احترامی شده است. من مطمئن نیستم که این شایعات تا چه اندازه دقیق بودند چون آنها را از طریق واسطه‌هایی در گروه طرفداران بلاک‌های کوچک می‌شنیدم. مطمئنم این شایعات کمی و بر علیه جیهان تحریف شده بودند ولی حتماً تا اندازه‌ای حقیقت داشته‌اند.

من چند ماه بعد به جزئیات بیشتری از رویدادهایی که در اواخر سال ۲۰۱۶ برگزار شده بودند پی بردم و متوجه شدم که چرا ماینرها تصمیم دارند از سگویت پشتیبانی نکنند. جیک اسمیت در آن تابستان به دیدار ماینرهای بزرگ از جمله جیهان وو در چین رفته بود. او ظاهراً در این ملاقات‌ها جیهان و سایر ماینرها را متقاعد کرده بود که از سگویت پشتیبانی نکنند. او در آن زمان شریک شرکت راجر وری یعنی Bitcoin.com و از طرفداران سرسخت بلاک‌های بزرگ بود. او قبلاً در شرکت Bitmain کار می‌کرده و به همین دلیل ارتباطات خوبی با ماینرهای چینی داشت. او در جامعه فعالان چینی بیت کوین فرد شناخته شده‌ای بود و در شهر پکن اقامت داشت و به زبان چینی مسلط بود. بر اساس گزارش جلسه او با یکی از ماینرهایی که به گروه طرفداران بلاک‌های کوچک گرایش

داشت به آن‌ها گفته که Bitcoin Core قابل اعتماد نیست و سگویت خطرناک است. اگرچه با توجه به منبع این خبر هر کس آن را بشنود باید کمی نسبت به آن مشکوک باشد. این رویداد یکی دیگر از نمونه‌هایی است که طرفین درگیری سعی داشتند با ماینرها تعامل و لابی‌گری کنند: از گوین و مایک در تابستان سال ۲۰۱۵، تا کنفرانس مقیاس‌پذیری در دسامبر سال ۲۰۱۵، تا توافق هنگ کنگ در فوریه سال ۲۰۱۶، تا نشست کالیفرنیا در جولای ۲۰۱۶، و در نهایت سفرها و ملاقات‌های جیک در آگوست ۲۰۱۶.

بعد از نشست میلان من به هنگ کنگ بازگشتم و با برخی از ماینرهای آنجا صحبت کردم. من متوجه شدم دیدگاه آن‌ها کاملاً تغییر کرده است. پیش از این، آن‌ها از سیگنال‌های متناقض توسعه‌دهندگان بیت کوین خسته شده بودند و مایل بودند این قائله هرچه زودتر تمام شود. ولی حالا که ماینرهای چینی به این جنگ پیوسته بودند، ماینرهای هنگ کنگی هم ماجرا را درک کرده بودند و موضع گرفته بودند. بارزترین نمونه آن جیهان وو بود که خود را به‌عنوان بازیگر اصلی گروه طرفداران بلاک‌های بزرگ معرفی می‌کرد، در حالی که به نظر می‌رسید ماینرهای دیگری که در صنعت استخراج فعال بودند موضع متفاوتی دارند، مثل گرداننده استخراج F2Pool، «واگ چون»^۱. شرکت Bitmain و شخص جیهان وو نفوذ قابل توجهی بر صنعت استخراج بیت کوین داشتند. شرکت Bitmain دارای مزرعه و استخراج ماینینگ بود و علاوه بر آن ۷۵ درصد سهم بازار تولید تجهیزات استخراج بیت کوین را در اختیار داشت. بنابراین همه گردانندگان مزارع استخراج با توجه به نیازی که به تجهیزات ماینینگ داشتند، از جیهان طرفداری می‌کردند. این به معنای حمایت از دیدگاه او در جنگ سائز بلاک و به طور بالقوه استفاده از استخراج ماینینگ شرکت Bitmain و اعلام پشتیبانی از نرم‌افزار Bitcoin Unlimited است.

همچنین شایعاتی در میان طرفداران بلاک‌های کوچک وجود داشت مبنی بر اینکه شرکت Bitmain مقادیر زیاد و غیرضروری از ماشین‌آلات تولید دستگاه‌های استخراج بیت کوین

1 Wang Chun

و قطعاتی که در ساخت آن‌ها به کار می‌رود مثل خازن‌ها^۱ را خریداری کرده و قصد دارد با تولیدکنندگان این قطعات قراردادهای انحصاری امضا کند. شرکت Bitmain همچنین از حق ثبت اختراع برای محافظت از سلطه خود در بازار استفاده می‌کرد، تا جایی که از کارمند سابق خود «یانگ ژوژینگ»^۲ به دلیل راه‌اندازی یک شرکت رقیب و نقض یکی از اختراعات ثبت شده توسط Bitmain شکایت کرد. این اتفاقات موجب تثبیت موقعیت این شرکت در بازار شد. خواه این اقدام‌های نافی رقابت در بازار را غیراخلاقی بدانیم خواه معتقد باشیم کاملاً قانونی هستند، این کارها در نهایت بر روی مناقشه ساینز بلاک اثر داشتند و موجب شدند اغلب ماینرها به گروه طرفداران بلاک‌های بزرگ بپیوندند. اعمال شرکت Bitmain همچنین در قوی‌تر شدن خصومت‌ها نسبت به این شرکت و افزایش تعداد دشمنان آن تأثیر به‌سزایی داشتند.

در تاریخ ۱ نوامبر سال ۲۰۱۶، نسخه Bitcoin Core 0.13.1 چند هفته پس از کنفرانس و بعد از چندین بار به تعویق افتادن، سرانجام منتشر شد. این نسخه شامل پارامترهای لازم برای فعال‌سازی سگویت بود. سرانجام ماینرها قادر بودند نرم‌افزارهای خود را به‌روزرسانی و پشتیبانی خود را از سگویت اعلام کنند. با این حال با توجه به خبری که از جانب جیهان وو منتشر شده بود، چشم‌انداز آینده بسیار نامعلوم بود. پس از گذشت بیش از یک سال از شروع مناقشه ساینز بلاک و علیرغم نبردهای مختلف و شخصیت‌های متفاوتی که درگیر این جنگ بودند، همچنان که به اواخر سال ۲۰۱۶ نزدیک می‌شدیم جنگ بر سر ساینز بلاک ادامه داشت.

1 capacitor
2 Yang Zuoxing

فصل دوازدهم

نرم افزار Bitcoin Unlimited

در اواخر تابستان ۲۰۱۶ و به دلیل موفق نشدن Bitcoin Classic در کسب پشتیبانی فعالان بیت کوین، طرفداران بلاک‌های بزرگ به Bitcoin Unlimited که روشی برای هارد فورک و افزایش سایز بلاک بود گرایش پیدا کردند. ممکن بود افراد تصور کنند که این روش محدودیت سایز بلاک را به کلی از بین می‌برد و اجازه می‌دهد بلاک‌های نامحدود ساخته شوند. اگر چنین بود احتمالاً Bitcoin Unlimited پیشنهاد بسیار موفقی از آب درمی‌آمد. با این حال اگر با دقت بیشتری مورد تجزیه و تحلیل قرار می‌گرفت، مشخص می‌شد نه تنها این پیشنهاد افزایش سایز بلاک بسیار پیچیده است، بلکه از نظر فنی نقایص زیادی دارد. حمایت از پیشنهادی تا این حد پیچیده و ضعیف، یکی دیگر از خطاهای مهم استراتژیک طرفداران بلاک‌های بزرگ بود. طرفداران بلاک‌های کوچک در محافل خود از این موضوع خوشحال بودند ولی همچنان تأکید داشتند که این مسأله مسکوت بماند، در واقع طرفند آن‌ها این بود که طرفداران بلاک‌های بزرگ را با این نرم‌افزار ضعیف سرگرم نگه دارند. Bitcoin Classic فقط یک نرم‌افزار نبود، بلکه یک سازمان رسمی بود که رئیس و اعضای آن بر اساس قانون انتخابات تعیین می‌شدند.

ایده اصلی پشت Bitcoin Unlimited این بود که ماینرها و کاربران پارامترهای مربوط به محدودیت سایز بلاک را به نرم‌افزار خود اضافه کنند. این پارامترها شامل: ۱. اندازه «حداکثر تولید»^۱ (فقط برای ماینرها): یک محدودیت برای سایز بلاک که هیچ ماینری حق ساختن بلاک بزرگ‌تر از آن را نخواهد داشت؛ ۲. «اندازه مفرط سایز بلاک»^۲: اندازه بلاکی که توسط ماینرها و نودهای کاربران پذیرفته خواهد شد؛ و ۳. «عمق پذیرش»^۳: تعداد تأییدهایی^۴ که یک بلاک (حتی اگر سایز آن از اندازه مفرط سایز بلاک یا همان EB بزرگ‌تر باشد) باید قبل از پذیرفته شدن داشته باشد. منتقدان این روش ادعا می‌کردند که هر کسی قوانین دلخواه خود را تعیین خواهد کرد و این مسأله منجر به واگرایی شبکه خواهد شد. این پیشنهاد افزایش سایز بلاک با هسته اجماع بیت کوین، یعنی ادامه یافتن زنجیره معتبری که بیشترین اثبات کار را در خود جای داده، متفاوت است. گذشته از این با توجه به تعریف مفهوم عمق پذیرش یا همان AD، ماینرها می‌توانند ابتدا سعی کنند تا زنجیره معتبر کوتاه‌تری بسازند اما اگر در این مسابقه پیروز نشوند، می‌توانند به چند بلاک جلوتر بروند و بر روی زنجیره طولانی‌تری که به یکباره معتبر شده است کار کنند. Bitcoin Unlimited مثل پیشنهاد های Classic و XT از یک روش فعال‌سازی برخوردار نبود؛ فرض بر این بود که این نسخه بعد از به‌روزرسانی ماینرها به بیت کوین جدید تبدیل شود. بنابراین بسیاری از افراد معتقد بودند که از پیشنهادهای قبلی افراطی‌تر است.

من برای کسب اطلاعات بیشتر در مورد Bitcoin Unlimited خیلی مشتاق بودم، برای همین در اوایل دسامبر سال ۲۰۱۶ در یک رویداد تبلیغاتی Bitcoin Unlimited در شنزن چین شرکت کردم. سخنرانان این تور تبلیغاتی و رویداد، راجر وریکی از مبلغان دو آتشه Bitcoin Unlimited، جیک اسمیت، چند تن از کارمندان Bitcoin.com، اعضای سازمان Bitcoin Unlimited، چند تن از توسعه‌دهندگان Bitcoin Unlimited، و مدیرعامل استخراج ViaBTC «هایپو یانگ»^۵ بودند.

1 Maximum generation (MG)
2 Excessive blocksize (EB)
3 Acceptance Depth (AD)
4 Confirmations
5 Haipo Yang

این رویداد با سخنرانی راجر و آغاز شد و ترجمه چینی آن هم برای حاضرین فراهم بود. او بسیار واضح و قانع کننده صحبت می کرد و موارد زیر بیان شد:

- او اولین فردی بوده که در استارت آپ های بیت کوین سرمایه گذاری کرده است.
- از سال ۲۰۰۹ که بیت کوین راه اندازی شد تا سال ۲۰۱۵ بلاک ها پر نبوده اند و کارمزد تراکنش ها پایین بوده است. Bitcoin Core دارای یک استراتژی آگاهانه برای پر بودن بلاک ها است که یک تغییر عمده اقتصادی محسوب می شود.
- عامل موفقیت بیت کوین تا اینجا کارمزد پایین تراکنش است.
- همیشه قرار بر این بوده که ساینز بلاک افزایش پیدا کند و این موضوع صراحتاً توسط همه مطرح می شد، اما اکنون افراد جدیدی از راه رسیده اند و مانع آن می شوند.
- سانسور گسترده ای روی Reddit وجود دارد و نمی توان روی پیشنهادهای افزایش ساینز بلاک بحث و تبادل نظر کرد. Bitcoin Core به حق تصمیم گیری افراد احترام نمی گذارد.
- Bitcoin Core از کدهای کامپیوتری سر در می آورد ولی از اقتصاد چیزی نمی داند.
- Bitcoin Core می خواهد بیت کوین کارمزد تراکنش بالایی داشته باشد و تبدیل به یک شبکه تسویه بین بانکی شود، در حالیکه ساتوشی همانطور که در وایت پیپر اظهار کرده، می خواهد بیت کوین یک پول نقد الکترونیکی بدون واسطه باشد.
- در صورتی که ساینز بلاک افزایش پیدا نکند و استفاده از بیت کوین آسان نشود، آلت کوین هایی در انتظار نشستند تا بر اثر شبکه ای^۱ بیت کوین غلبه کنند [و جای آن را بگیرند].

من قبلاً هم این موارد را از راجر و شنیده بودم. اینکه او می توانست این پیام ها را بارها و بارها به صورت بی امان در سراسر جهان تکرار کند، واقعاً چشمگیر بود. او اعتقاد راسخی

1 Network effect

داشت و حرف‌های او بر شنوندگان اثر می‌گذاشت. او یکی از فعال‌ترین افراد در اردوگاه طرفداران بلاک‌های بزرگ بود.

راجر سخنرانی خود را با این جمله پایان داد که ماینرها و کاربران باید نرم‌افزار خود را از Bitcoin Core به Bitcoin Unlimited تغییر دهند. هرچند او هرگز به جزئیات مکانیزم‌های جدیدی که در Bitcoin Unlimited وجود داشت وارد نشد. چند روز بعد یک رویداد با ساختار مشابه در هنگ کنگ حول Bitcoin Unlimited برگزار شد. من به یاد می‌آورم که با خود فکر می‌کردم که چقدر شرم‌آور است که راجر بجای اینکه مثل گذشته افراد و فروشندگان جدید را با بیت کوین آشنا کند، تمام انرژی خود را صرف این درگیری داخلی کرده است.

سخنران بعدی رویداد شنزن، جری چان بود. جری در مورد ایده «اجماع نوظهور»¹ صحبت کرد، بر اساس این ایده قوانین در یک سیستم ظهور می‌کنند و توسط توسعه‌دهندگان از بالا به پایین تحمیل نمی‌شوند. یک نگرانی وجود داشت که اگر ماینرها و نودها قوانین خود را تعیین کنند زنجیره به چند شاخه منشعب خواهد شد و این سیستم برای رفع این نگرانی طراحی شده بود. وی توضیح داد که تحت این مدل، ماینرها آزادند که محدودیت ساینز بلاک را خود تعیین کنند و با توجه به سیستم EC، همگان روی یک زنجیره واحد توافق پیدا خواهند کرد. جری مثال‌های مختلفی از طرز کار این سیستم در طبیعت آورد:

مسائل خودشان را سازمان می‌دهند و می‌توان در طبیعت نشانه‌هایی از این را دید. مولکول‌های آب خود را به شکل دانه‌های برف در می‌آورند، چرا؟ خدا دلیل آن نیست، به این دلیل است که مولکول‌های آب به گونه‌ای مرتب شده‌اند که یک شش ضلعی را تشکیل، و شبیه به دانه‌های برف شوند. پرنده‌گان را در نظر بگیرید، آیا کسی به آن‌ها آموخته است تا پرنده جلویی را دنبال کنند؟ نه. آن‌ها در طول پرواز صدها کیلومتری خود می‌توانند به معنای واقعی کلمه به خواب بروند و

1 Emergent consensus (EC)

همچنان با یکدیگر تصادف نکنند. تیم Bitcoin Core می‌خواهد شما به این موضوع باور داشته باشید که اگر ماینرها یا کاربران بیت کوین تصمیمی بگیرند، اتفاقات ناگواری خواهد افتاد. تحت سیستم اجماع نوظهور، به طور طبیعی یک محدودیت برای سایز بلاک پدید خواهد آمد.

البته توصیف جری مبنی بر اینکه قوانین کنونی بیت کوین از بالا و توسط Bitcoin Core اعمال می‌شوند، برداشت نادرستی از دیدگاه طرفداران بلاک‌های کوچک بود. در دنیای طرفداران بلاک‌های کوچک، قوانین توسط نودهایی که کاربران اجرا کرده‌اند تعیین می‌شود. این قوانین بسیار سفت و سخت هستند و تغییر آن‌ها نیاز به اجماع گسترده در سطح جامعه فعالان و کاربران بیت کوین دارد. به نظر می‌رسید طرفداران بلاک‌های بزرگ هرگز قادر به بیان دقیق این دیدگاه نبوده‌اند، یا به این دلیل که آن را درک نمی‌کردند، یا مطرح شدن آن به ضرر پیشنهادهای افزایش سایز بلاک آن‌ها تمام می‌شد.

مشخص نبود این مسأله که به نظر می‌رسد در طبیعت اغلب سیستم‌ها بدون برنامه‌ریزی یا توافق بر روی قوانین، به یک ساختار مشترک می‌رسند و با یکدیگر هماهنگ می‌شوند، چه ارتباطی با بیت کوین پیدا می‌کند. بیت کوین در این مرحله به موفقیت دست پیدا کرده بود و شبکه آن ۷ سال بدون هیچ مشکلی کار کرده بود و توانسته بود بر همه مشکلات غلبه کند. به نظر می‌رسید این امر باعث بوجود آمدن درجه‌ای از غرور کاذب در جامعه فعالان بیت کوین شده بود، زیرا افراد نسبت به پایداری سیستم بیش از حد خوشبین بودند. هنگامی که از طرفداران Bitcoin Unlimited در مورد برخی از نقاط ضعف احتمالی آن سؤال می‌شد، آن‌ها اغلب پاسخ می‌دادند که بیت کوین آسیب‌ناپذیر است و چیزی نمی‌تواند مانع آن شود. از نظر من این استدلال که Bitcoin Unlimited به دلیل مقاوم بودن بیت کوین درست کار خواهد کرد و آسیب رساندن به بیت کوین تقریباً غیرممکن است، بسیار بی‌اساس بود.

علاوه بر سه پارامتری که قبلاً توضیح دادیم Bitcoin Unlimited پارامتر دیگری به نام «دریچه چسبناک»^۱ داشت. وقتی یک نود به مقدار پارامتر «عمق پذیرش» یا همان AD خود می‌رسید، همه بلاک‌های دریافت شده را فارغ از سائز آن‌ها به مدت ۲۴ ساعت می‌پذیرفت. دلیل این امر این بود که نود مورد نظر پس از افزایش سائز بلاک و ساخته شدن زنجیره‌ای از بلاک‌های بزرگ، از بلاک‌هایی که ساخته شده‌اند عقب نماند. یک پیامد ناخواسته، طنزآلود، و معیوب این مسأله این بود که اگر در ۲۴ ساعت آینده یک افزایش سائز بلاک مجدد رخ می‌داد، نودهایی با «اندازه سائز مفرط بلاک» یا همان EB پایین‌تر، زنجیره بلاک‌های بزرگ‌تر را دنبال خواهند کرد و نودهایی که «عمق پذیرش» پایین‌تری دارند روی زنجیره بلاک‌های کوچکتر می‌مانند. به نظر می‌رسد Bitcoin Unlimited پیاده‌سازی ضعیفی داشت و به همه سناریوهای ممکن فکر نشده بود. این مسأله نشان می‌داد که طرفداران بلاک‌های بزرگ در این مرحله تا چه اندازه مستأصل بودند.

Bitcoin Unlimited نقایص دیگری هم داشت، از جمله چیزی به نام «حمله متوسط اندازه سائز مفرط بلاک»^۲. از آنجا که پارامتر اندازه سائز مفرط بلاک یکی از قوانین اجماع بود و مقداری که ماینرها انتخاب می‌کردند در بلاک‌های آن‌ها گنجانده می‌شد، مهاجمان می‌توانستند توزیع مقادیر EB را روی شبکه ببینند. این به یک ماینر متخاصم اجازه می‌دهد تا مقدار متوسط «اندازه سائز مفرط بلاک یا همان EB» را روی متوسط اندازه سائز مفرط بلاک (که از پارامترهای شبکه بدست می‌آورد) تنظیم کند، به عنوان مثال می‌تواند زنجیره و هش‌ریت شبکه را به دو انشعاب با اندازه‌های اتفاقی تقسیم کند و این یک نقطه ضعف اساسی بود. وقتی این سؤالات از طرفداران Bitcoin Unlimited پرسیده می‌شد، آن‌ها معمولاً استدلال می‌کردند که ماینرها احمق نیستند و اجازه نخواهند داد چنین اتفاقی بیفتد. همچنین آن‌ها مدعی می‌شدند که ماینرها و کاربران می‌توانند برای جلوگیری از رخ دادن این اتفاق یک «اندازه سائز مفرط بلاک» یکسان انتخاب کنند. اگرچه به نظر می‌رسد توافق ماینرها و کاربران برای تعیین یک اندازه یکسان و به قصد جلوگیری از

1 Sticky gate

2 Median EB attack

انشعاب زنجیره، شبیه به مدل امنیتی مورد حمایت گروه طرفداران بلاک‌های کوچک بود که معتقد به توافق بر روی مجموعه‌ای از قوانین بودند. برای افزایش محدودیت سائز بلاک در Bitcoin Unlimited لازم بود تنظیمات اندازه سائز مفرط بلاک یا همان EB روی مقدار بالاتری تنظیم شود تا این آسیب‌پذیری خود را نشان دهد.

Bitcoin Unlimited همچنین تغییرات دیگری در نرم‌افزار خود ایجاد کرده بود که ارتباط مستقیمی با محدودیت سائز بلاک نداشت. توسعه‌دهندگان Bitcoin Unlimited سیستمی برای انتشار سریع‌تر بلاک‌ها به نام xThin، شبیه به مفهوم «بلاک‌های فشرده»^۱ در Bitcoin Core ایجاد کرده بود. ایده‌های دیگری هم قرار بود در آینده پیاده‌سازی شوند مثل «اعتبارسنجی موازی بلاک‌ها»^۲ و «تراکنش‌های انعطاف‌پذیر»^۳. تراکنش‌های انعطاف‌پذیر مانند سگویت قالب جدیدی برای تراکنش‌ها تعریف می‌کردند و گفته می‌شد می‌توانند مشکل تغییرپذیری تراکنش‌ها را حل کنند. برنامه این بود که تراکنش‌های قدیمی به کلی ممنوع شوند (یعنی تعیین صفر برای محدودیت سائز بلاک‌هایی که شامل تراکنش‌های قدیمی هستند) و سپس همه کاربران مجبور به استفاده از الگوی جدید تراکنش شوند. جالب است که این روش پیشنهادی بسیار تهاجمی‌تر از سگویت بود که توسعه‌دهندگان Bitcoin Unlimited با آن مخالفت می‌کردند. سگویت اساساً محدودیت ۱ مگابایتی قدیمی را برای تراکنش‌هایی که از الگوی قدیمی استفاده می‌کردند حفظ می‌کرد و فضای بیشتری برای تراکنش‌های جدید اضافه می‌کرد.

بنابراین به نظر می‌رسید که بسیاری از این ویژگی‌ها و پیشنهادهای اصلاً به دلیل مصالح فنی نبوده‌اند. در عوض به فرهنگ، خودپرستی، و تمایل به درگیر شدن با بیت‌کوین ارتباط پیدا می‌کردند. در این مرحله بیشتر طرفداران بلاک‌های بزرگ از طرفداران بلاک‌های کوچک و توسعه‌دهندگان Bitcoin Core متنفر بودند. آن‌ها از این استنباط که گروه طرفداران بلاک‌های کوچک بیت‌کوین را کنترل می‌کنند تنفر داشتند و می‌خواستند بخشی

1 Compact blocks

2 Parallel block validation

3 Flexible transaction

از بیت کوین باشند. به دلیل تمایل به درگیری بیشتر با بیت کوین، حوزه فعالیت Bitcoin Unlimited گسترده‌تر از صرفاً تعیین ساینز بلاک تعریف شد و شامل حوزه‌های متفاوتی بود. در نهایت ثابت شد که این اشتباه بود و در نهایت منجر به سقوط Bitcoin Unlimited شد. پس از پایان جنگ بر سر ساینز بلاک سرانجام برخی از طرفداران Bitcoin Unlimited این اشتباهات را پذیرفتند.

زمانی که Bitcoin Unlimited مورد توجه اغلب گروه‌های مختلف طرفدار بلاک‌های بزرگ بود، چند نفر از ما معتقد بودیم BU باید بجای تلاش برای افزایش ساینز بلاک از روش «اجماع نوظهور» بر روی یک افزایش ساینز بلاک ساده و برپایه Bitcoin Core تمرکز کند. ما همچنین می‌خواستیم BU را فعلاً از پیاده‌سازی نسخه «بلاک‌های ضعیف» خود منصرف کنیم. مسأله مهم این بود که با کمترین دردسر بتوانیم ساینز بلاک را افزایش دهیم و از Bitcoin Core جدا شویم. اصرار BU برای اضافه کردن بخشی از کدهای نرم‌افزاری پیچیده بجای تمرکز بر موضوع افزایش ساینز بلاک نتیجه معکوس داشت، چون کد BU اشکالات زیادی داشت و در کار نودها اختلال بوجود می‌آورد. این امر باعث شد این تصور در جامعه فعالان ایجاد شود که نمی‌توان روی توسعه‌دهندگان BU حساب کرد یا به اندازه کافی در توسعه و تست نرم‌افزار مهارت ندارند.

فرد دیگری از طرفداران بلاک‌های بزرگ گفته بود:

معتقدم [طرح] قضیه «اجماع نوظهور» اشتباه بزرگی بود.

جالب اینکه Bitcoin Unlimited علیرغم نقاط ضعف امنیتی بالقوه‌ای که داشت، از پشتیبانی طیف وسیعی از طرفداران بلاک‌های بزرگ، از برایان آرمسترانگ در Coinbase، تا جیهان وو، کوین اندریسن، و راجر وور برخوردار بود. به نظر می‌رسید هیچ‌یک از این افراد به ظرایف پارامترهای جدید توجه نمی‌کردند. آن‌ها فقط می‌خواستند

بلاک‌ها بزرگ‌تر شوند. حمایت استخرهای استخراج از جمله BTC.TOP و GBMiners و ViaBTC از Bitcoin Unlimited رو به افزایش بود و به نظر می‌رسید تعداد نودهایی که آن را اجرا می‌کنند هم رو به افزایش است. اولین استخری که از آن پشتیبانی کرد ViaBTC بود، استخر استخراجی که شرکت Bitmain روی آن سرمایه‌گذاری کرده بود و به نظر می‌رسید تا حد زیادی تحت تأثیر جیهان وو باشد. همچنین استخر BTC.TOP هم احتمالاً توسط Bitmain کنترل می‌شد. در آغاز سال ۲۰۱۷ حدود ۱۵ تا ۲۰ درصد از هش‌ریت پشتیبانی خود از Bitcoin Unlimited را اعلام کردند. شرکت Bitmain استخرهای استخراج دیگری مثل استخر Antpool را بطور مستقیم مدیریت می‌کرد و این استخر هم از مارس سال ۲۰۱۷ شروع به اعلام پشتیبانی از Bitcoin Unlimited کرد و پشتیبانی از Bitcoin Unlimited به ۴۵ تا ۵۵ درصد کل هش‌ریت شبکه رسید، سطحی که تقریباً در طول سال ۲۰۱۷ بدون تغییر ماند.

چند تن از توسعه‌دهندگان بیت‌کوین و از طرفداران بلاک‌های بزرگ برخی از ماینرها را متهم به جعل پشتیبانی از Bitcoin Unlimited می‌کردند. آن‌ها مسئولین استخرهای استخراج را متهم می‌کردند که همچنان بلاک‌ها را با استفاده از Bitcoin Core تولید می‌کنند و فقط با تغییر پارامترهایی در تنظیمات استخر استخراج خود از Bitcoin Unlimited اعلام پشتیبانی می‌کنند. آن‌ها توانسته بودند با بررسی تراکنش‌های موجود در بلاک‌ها به این نتیجه برسند که تراکنش‌ها با استفاده از الگوریتم جدیدی که در Bitcoin Core پیاده‌سازی شده بود، انتخاب شده‌اند و این قابلیت در Bitcoin Unlimited وجود نداشت. این «اعلام پشتیبانی‌های جعلی^۱» به علامت‌های دروغین معروف بودند. برخی از طرفداران بلاک‌های کوچک معتقد بودند این اعلام پشتیبانی‌های جعلی حتی مخرب‌تر از خود Bitcoin Unlimited هستند. اعلام پشتیبانی ماینرها از قوانین اجماعی که بر روی شبکه اعمال می‌کنند، مکانیزمی برای ارتقاء موفق قوانین شبکه بیت‌کوین است. اعلام پشتیبانی دروغین روشی بود که به‌روزرسانی قوانین شبکه را خطرناک‌تر می‌کرد. در واقع اعلام پشتیبانی دروغین از Bitcoin Unlimited را می‌توان

1 Fake votes

یک حمله به Bitcoin Unlimited در نظر گرفت، زیرا می‌تواند موجب فعال‌سازی ناموفق آن شود. به نظر می‌رسید طرفداران بلاک‌های بزرگ به این موضوع توجهی ندارند و با افزایش پشتیبانی هش‌ریت از Bitcoin Unlimited هیجان‌زده می‌شدند. از نظر آن‌ها این مسأله به پیشرفت Bitcoin Unlimited کمک می‌کرد و اعلام پشتیبانی ماینرها خواه جعلی، خواه واقعی، یک پیام مهم سیاسی با خود به همراه داشت.

در تاریخ ۳۰ ژانویه سال ۲۰۱۷ یکی از ماینرهایی که نرم‌افزار Bitcoin Unlimited را اجرا می‌کرد، یک بلاک بزرگ‌تر از ۱ مگابایت تولید کرد. به احتمال زیاد این اولین بلاک بالای ۱ مگابایت بود که از اثبات کار کافی برخوردار است. این بلاک احتمالاً در نتیجه یک خطا یا بطور تصادفی تولید شد، چون هیچ‌گونه هماهنگی آشکاری در پشت آن وجود نداشت. این بلاک برای همه نودهای سراسر شبکه نامعتبر بود و به عنوان یک بلاک نامعتبر از جانب آن‌ها رد شد. طرفداران بلاک‌های کوچک از این رخداد به‌عنوان نمونه‌ای یاد می‌کردند که توضیح می‌داد چرا قبل از اجرای هارد فورک نیاز به توافق عمومی میان کاربران بیت‌کوین داریم. طرفداران بلاک‌های بزرگ مثل راجر ورسعی می‌کردند این رخداد را لاپوشانی کنند و ادعا می‌کردند «بلاک‌های منتفی»^۱ شده همواره در شبکه ایجاد می‌شوند بدون اینکه پذیرند این بلاک نه‌تنها منتفی شده بلکه بی‌اعتبار است و توسط نودهای شبکه پس زده شده است.

در مارس سال ۲۰۱۷ اتفاقی افتاد که به اعتبار Bitcoin Unlimited لطمه بزرگی وارد کرد. تعداد نودهای قابل دسترس Bitcoin Unlimited در شبکه بیت‌کوین سقوط کرد.

طبق داده‌های nodecounter همه چیز تا ساعت ۶ عصر (به وقت گرینویچ) درست کار می‌کرد و تعداد نودها ۷۷۶ عدد بود. این عدد در ساعت ۷ عصر به ۶۹۶ رسید و در ساعت ۱۱ شب به کمترین مقدار خود یعنی ۱۸۲ رسید. در ساعت ۹

1 Stale blocks

صبح اوضاع دوباره به حالت عادی بازگشت و تعداد نودها به ۶۲۵ رسید. فکر نمی‌کنم این درست باشد که بگوییم BU یک واکنش غیرعادی و سریع از خود نشان داده یا ۱۰۰٪ نودها به شبکه برگشته‌اند.

ماجرای این قرار بود که یک اشکال نرم‌افزاری DOS به بخش مربوط به xThin در Bitcoin Unlimited اضافه شده بود که هیچ ارتباطی با محدودیت ساینز بلاک نداشت. این اشکال نرم‌افزاری مورد سوءاستفاده قرار گرفته بود و باعث متوقف شدن همه نودهای Bitcoin Unlimited شده بود. این مسأله توسط طرفداران بلاک‌های کوچک برجسته شد تا مورد توجه رسانه‌های پوشش دهنده اخبار ارزهای دیجیتال قرار گیرد. این رخداد باعث شد تا طیف گسترده‌تری از طرفداران بلاک‌های بزرگ به بررسی دقیق این پروژه بپردازند. قبلاً بسیاری از افراد آن را به‌عنوان یک نرم‌افزار معمولی که از بلاک‌های بزرگ پشتیبانی می‌کند در نظر می‌گرفتند، ولی این اتفاق باعث شده بود آن‌ها سؤالات انتقادی بپرسند، از جمله: این سازمان چه کارکردی دارد و چرا باید رئیس داشته باشد؟ چرا آن‌ها بخش‌هایی از کُد نرم‌افزار که ربطی به محدودیت ساینز بلاک ندارد را تغییر داده‌اند؟ پارامتر AD به چه دردی می‌خورد؟ آیا اشکالات نرم‌افزاری کلیدی دیگری ممکن است در این نرم‌افزار وجود داشته باشد؟

بعد از این اتفاق که در مارس سال ۲۰۱۷ رخ داد، شرایط هرگز برای Bitcoin Unlimited به حالت عادی بازنگشت. این اشکال نرم‌افزاری چندان هم مهم نبود ولی طرفداران بلاک‌های کوچک توانستند با موفقیت از آن استفاده، و توجه‌ها را به سمت اشکالات دیگر Bitcoin Unlimited جلب کنند. دوره Bitcoin Unlimited یکی از بدترین دوره‌های این مناقشه برای طرفداران بلاک‌های بزرگ بود و احتمالاً آن‌ها ترجیح می‌دهند این دوره را فراموش کنند. آن‌ها خود را در تله خودخواهی، عصبانیت، و استیصال انداختند و از یک نرم‌افزار ناکارآمد پشتیبانی کردند و طرفداران بلاک‌های کوچک از این اتفاق بسیار خوشحال بودند. دوباره پس از کنار گذاشته شدن Bitcoin Unlimited، هیچ‌گونه اظهار ندامت و پشیمانی از جانب طرفداران بلاک‌های بزرگ ابراز

نشد. به نظر می‌رسید هیچ یک از آن‌ها مسئولیت این کار را به عهده نمی‌گرفتند، یا به این توجه نداشتند که چرا اصرار آن‌ها برای جا انداختن یک نرم‌افزار پر از اشکال برای بیت‌کوین خطرناک، یا بالقوه مخرب است.

در ماه مارس سال ۲۰۱۷ تنش در جامعه فعالان بیت‌کوین حتی بیشتر شده بود. اکنون تمرکز بر روی این ایده بود که طرفداران بلاک‌های بزرگ از Bitcoin Unlimited استفاده خواهند کرد و با ساختن بلاک‌های خالی و نامعتبر کردن هر بلاکی که در آن تراکنشی وجود داشته باشد، به زنجیره اصلی بیت‌کوین یعنی زنجیره بلاک‌های کوچک حمله می‌کنند. بنابراین با بکارگیری از این استراتژی در نهایت زنجیره بلاک‌های کوچکتر را از بین می‌برند. جهان و علناً ایده حمله به بیت‌کوین را مطرح کرده بود:

ممکن است نیازی نباشد به آن حمله کنیم. ولی حمله به آن همیشه یک گزینه است.

همچنین کوین چیزی شبیه به این گفته بود:

فکر خوبی است که جلوی یک فورک از بیت‌کوین که در اقلیت است را بگیریم و اجازه تأیید هیچ تراکنشی را به آن ندهیم. اجماع ناکاموتو با اتفاق نظر تفاوت دارد!

«منی روزنفلد»^۲ یکی از بیت‌کوینرهای قدیمی که تا این مرحله به مناقشه ساینز بلاک وارد نشده بود، شرایط را به این صورت توصیف می‌کند:

1 Nakamoto consensus != unanimity

2 Meni Rosenfeld

گوین اندریسن، «پیتر ریزان»^۱، و جیهان وو در مورد احتمال حمله اکثریت هشریت به زنجیره اقلیت (از راه «استخراج خودخواهانه»^۲ و حمله بلاک‌های خالی) صحبت کرده و از آن حمایت کرده‌اند.

این مایه شرمساری است و اساساً با ذات بیت کوین منافات دارد. مردم از بیت کوین استفاده می‌کنند چون آن را انتخاب کرده‌اند، نه اینکه کسی آن‌ها را مجبور به استفاده از آن کرده باشد.

آن‌ها اساساً می‌گویند که اگر بعضی از ما بخواهیم از پولی که در پروتکل فعلی Bitcoin Core تعریف شده است استفاده کنیم، آن‌ها این حق را دارند که به آن حمله کنند و ما را مجبور به استفاده از پول خودشان کنند. ولی نه تنها این کار درست نیست، بلکه مایه شرمساری است و پایه اخلاقی ندارد. حتی اگر موفق هم بشوند چیزی که ساخته خواهد شد یک پول فیات است و دیگر بیت کوین نخواهد بود.

تنها از راه ایجاد پروتکل‌های مختلف و ایجاد فرصت رقابت و تکامل در کنار یکدیگر برای تبدیل شدن به قوی‌ترین بیت کوین ممکن، می‌توان به تنوع زیستی واقعی دست پیدا کرد.

این فراتر از بحث تعیین شایستگی‌های BU در مقابل Bitcoin Core است.

این به وضوح نشان دهنده تغییر لحن طرفداران بلاک‌های بزرگ بود. آن‌ها قبلاً ادعا می‌کردند انشعابی وجود نخواهد داشت و زنجیره بلاک‌های کوچک را جدا نمی‌دیدند، در حالی که اکنون به طور جدی درباره حمله به چنین زنجیره‌ای بحث می‌کردند. اوایل آوریل من با یکی از همکاران اصلی جیهان وو در هنگ کنگ گفتگویی داشتم. او به من اطلاع داد که طرفداران بلاک‌های بزرگ بودجه‌ای ۱۰۰ میلیون دلاری برای حمله به زنجیره

1 Peter Rizun

2 Selfish mining

بلاک‌های کوچک اختصاص داده‌اند. برنامه این بود که این پول صرف انرژی برای ماین بلاک‌های خالی و نامعتبر کردن بلاک‌های حاوی تراکنش شود. وی ادعا می‌کرد اساساً این اقدام‌ها «زنجیره بلاک‌های کوچک را از بین خواهد برد». از او پرسیدم چرا او می‌خواهد زنجیره بلاک‌های کوچکتر را از بین ببرد، و او پاسخ داد طرفداران بلاک‌های کوچک «سال‌ها است که جلوی پیشرفت بیت‌کوین را گرفته‌اند و سزاوار این هستند». برنامه برای هزینه ۱۰۰ میلیون دلار صرفاً برای انتقام گرفتن از مخالفان، نشان می‌دهد که در این مرحله از درگیری در چه باتلاق بزرگی گیر افتاده بودیم. از او پرسیدم وقتی این ۱۰۰ میلیون دلار تمام شد چه اتفاقی می‌افتد؟ آیا طرفداران بلاک‌های کوچک قادر به احیای زنجیره خود نخواهند بود؟ به نظر می‌رسید او جوابی برای این سؤال نداشته باشد ولی بعد از یک مکث طولانی گفت احتمالاً آن‌ها دوباره برای فراهم کردن بودجه جدید تلاش، و دوباره حمله خواهند کرد.

با ادامه یافتن سال ۲۰۱۷ و وارد شدن این مناقشه به ماه هجدهم خود، معضلات هر دو طرف درگیر نه تنها کمتر نشد بلکه افزایش یافت. جیهان و اغلب استخرهای استخراج بیت‌کوین از سگویت پشتیبانی نمی‌کردند و دستیابی به هدف ۹۵ درصدی تقریباً غیرممکن به نظر می‌رسید. طرفداران بلاک‌های بزرگ فعال‌سازی سگویت را به عنوان یک شکست برای گروه خود می‌دیدند و قصد داشتند برای حفظ اهرم کنترلی خود مانع فعال‌سازی آن شوند. این تنها برگ برنده آن‌ها بود و نمی‌خواستند از آن دست بکشند. البته این مسأله موجب استیصال گروه بلاک‌های کوچک می‌شد، هرچند به خاطر می‌آورد که آن‌ها طرف‌صبور این مناقشه بودند و بلند مدت فکر می‌کردند. انتظار برای گروه طرفداران بلاک‌های بزرگ بقدری دردناک‌تر بود که به حمله به زنجیره بلاک‌های کوچک فکر می‌کردند.

فصل سیزدهم

صرافی‌ها

اکوسیستم ارزهای دیجیتال در طول سال‌هایی که مناقشه سائز بلاک در جریان بود، تغییر قابل توجهی کرده بود. مهم‌ترین آن‌ها ظهور و رشد چندین صرافی ارزهای دیجیتال بود که موفقیت خود را مدیون تقاضای قابل توجه بازار خرده‌فروشی منطقه آسیا-اقیانوسیه^۱ بودند. از جمله این شرکت‌ها می‌توان به BitMEX، Poloniex و شاید از همه مهمتر Bitfinex اشاره کرد. Bitfinex از نظر تعیین قیمت احتمالاً در آن زمان مهم‌ترین شرکت بود. در شرایطی که شرکت‌های مستقر در ایالات متحده و مورد حمایت سیلیکون ولی^۲ از طرفداران پروپاقرص بلاک‌های بزرگ بودند، این بازیگران جدید هنوز تصمیم قاطعی برای حمایت از یک گروه خاص نگرفته بودند. بنابراین این فرصتی برای هر دو طرف درگیری بود تا برای کسب پشتیبانی این شرکت‌ها با آن‌ها صحبت و لابی کنند. در کل منصفانه‌تر این است که بگوییم گروه طرفداران بلاک‌های کوچک در این کار موفق‌تر از گروه طرفداران بلاک‌های بزرگ بودند، اگرچه تجربه انشعاب در زنجیره اتریوم در سال ۲۰۱۶ احتمالاً اثر قابل توجهی بر روی تصمیم این شرکت‌ها داشت. این شرکت‌ها به

1 Asia Pacific

2 Silicon Valley

تازگی درگیر این مناقشه شده بودند و نگاه منطقی تری به موضوع داشتند و به نظر می‌رسید استدلال‌های گروه طرفداران بلاک‌های کوچک آن‌ها را قانع کرده است.

۱۷ مارس سال ۲۰۱۷ روز مهمی در تاریخ این مناقشه طولانی است، در این روز چندین صرافی بزرگ از جمله Kraken، Bitfinex و Bitstamp ضربه بزرگی به Bitcoin Unlimited وارد کردند. آن‌ها یک اطلاعیه مشترک صادر کردند مبنی بر اینکه Bitcoin Unlimited از نظر آن‌ها Bitcoin نیست، حتی اگر اکثریت هشریت را در اختیار داشته باشد. آن‌ها همچنین در این اعلامیه اظهار کردند «هرگونه پیاده‌سازی از نرم‌افزار بیت کوین که ناقض قوانین اجماع است» باید در مقابل «انتشار مجدد مصون» باشد. (مصونیت در برابر انتشار مجدد یعنی ارسال یک تراکنش بر روی یکی از شبکه‌ها منجر به خرج شدن دارایی بر روی شبکه دیگر نشود. - م)

از آنجا که به نظر می‌رسد Bitcoin Unlimited به وقوع یک هارد فورک منجر شود، ما تصمیم داریم فورک مربوط به Bitcoin Unlimited را با BTU (یا XBUT) شناسایی کنیم. پیاده‌سازی Bitcoin Core با شناسه BTC (یا XBT) ادامه پیدا خواهد کرد و تمام صرافی‌ها و واریز و برداشت‌ها را با شناسه BTC انجام خواهند داد، حتی اگر زنجیره BTU هشریت بیشتری داشته باشد. برخی از صرافی‌ها قصد دارند BTU را به لیست ارزهای خود اضافه کنند و همه ما سعی خواهیم کرد تا از دارایی BTU کاربران خود محافظت کنیم و راهی برای دسترسی آن‌ها به BTU‌هایشان فراهم کنیم. با این حال هیچ‌یک از امضاکنندگان این اعلامیه نمی‌توانند BTU را به لیست ارزهای خود اضافه کنند، مگر اینکه اطمینان پیدا کنیم قادر هستیم هر دو زنجیره را به‌طور مستقل و بدون هیچ دردسری در کنار یکدیگر اجرا کنیم. در نتیجه ما اصرار داریم که جامعه فعالان Bitcoin Unlimited (یا هر پیاده‌سازی دیگری که موجب نقض قوانین اجماع شبکه شود) در مقابل انتشار مجدد مصونیت دو طرفه داشته باشد.

این موضع گیری توسط برخی دیگر از بسترهای مهم معاملات ارزهای دیجیتال هم گرفته شد. صرافی Poloniex اظهار کرد که:

هر انشعاب جدید حداقل باید در مقابل انتشار مجدد مصونیت ایجاد کرده باشد.

در همان روز صرافی BitMEX موضع مشابهی گرفت:

هارد فورک Bitcoin Unlimited به احتمال زیاد بدون تغییرات نرم افزاری موفقیت آمیز نخواهد بود. در صورتی که زنجیره بیت کوین منشعب شود، ما از طرح پیشنهادی Bitstamp، BTCC، Bitfinex و دیگران پشتیبانی می کنیم. پشتیبانی از هر دو زنجیره به صورت مجزا برای هیچ صرافی و BitMEX امکان پذیر نیست. به همین دلیل تا زمانی که خطر «تنظیم مجدد بلاک ها» در صورت طولانی تر شدن زنجیره Bitcoin Core رفع نشود، و مصونیت در مقابل انتشار مجدد تراکنش ها در BU پیاده سازی نشده باشد، BU نمی تواند برای واریز و برداشت مورد استفاده قرار گیرد.

این صرافی ها مواضع خود را مشخص کرده بودند. آن ها Bitcoin Unlimited را به عنوان یک آلت کوین قبول داشتند، نه بیت کوین. آن ها از اتفاقاتی که برای اتریوم کلاسیک افتاده بود درس گرفته بودند؛ Bitcoin Unlimited تا زمانی که مصونیت در مقابل انتشار مجدد تراکنش ها پیاده سازی نشده باشد، در صرافی های آن ها لیست نخواهد شد. با خواندن آن ها می شد حدس زد که این اعلامیه ها تحت تأثیر نظرات طرفداران بلاک های کوچک است، یا حتی ممکن بود پیش نویس آن را ایشان تهیه کرده باشند. طرفداران بلاک های بزرگ ترفند نامه نگاری را در سال ۲۰۱۵ و در مورد Bitcoin XT امتحان کرده بودند و حالا نوبت طرفداران بلاک های کوچک بود تا از آن استفاده کنند.

در مورد مصونیت در مقابل انتشار مجدد تراکنش‌ها، صرافی‌ها خواستار تغییر الگوی تراکنش‌ها در کوین جدید بودند. با این کار اطمینان حاصل می‌شود که پس از انشعاب در زنجیره، تراکنش‌های ارسال شده به یک شبکه باعث جابجایی کوین‌ها بر روی شبکه دیگر نخواهند شد. این امر موجب می‌شد صرافی‌ها در انجام وظایف خود به‌عنوان متولی نگهداری از دارایی‌های مشتریان خود، موفق باشند.

در اینجا باید به یک نکته اشاره کنیم که اکوسیستم سیستم‌های معامله‌گری ارزهای دیجیتال نسبت به سال ۲۰۱۵ به طرز قابل توجهی تکامل پیدا کرده بود و فراتر از «مبادلات لحظه‌ای»^۱ بود. به عنوان مثال Bitfinex فقط یک بستر برای مبادلات ساده نبود؛ این شرکت طیف وسیعی از خدمات، از «معاملات اهرمی»^۲ بیت کوین، «معاملات آتی»^۳ و «معاملات مشتقات»^۴ بیت کوین، تا «وام»^۵ و «بازارهای بدهی»^۶ بر پایه بیت کوین را ارائه می‌داد. وقتی پیامدهای مالی یک انشعاب در زنجیره بیت کوین یا هارد فورک را در نظر بگیریم، مسأله بطور قابل توجهی پیچیده‌تر می‌شود. به عنوان مثال اگر قبل از انشعاب در زنجیره کوین آن را قرض گرفته باشید، آیا بعد از انشعاب در زنجیره این کوین باید هر دو کوین را بازپرداخت کنید؟ اگر قبل از انشعاب در زنجیره کوین «خرید اعتباری اهرمی»^۷ کرده بودید، آیا این وجه اکنون برای هر دو کوین در نظر گرفته خواهد شد یا فقط یکی از آن‌ها، و افراد چگونه می‌توانند یکی از آن‌ها را انتخاب کنند؟ این پلتفرم‌های معاملاتی با توجه به این پیچیدگی‌ها حق داشتند تا درباره یک انشعاب احتمالی نگران باشند. مدل تجاری آن‌ها بر این اساس تنظیم شده بود که آن‌ها در همه ساعات همه روزها و به صورت ۲۴/۷ آماده به کار باشند و نمی‌توانستند سیستم معاملاتی خود را خاموش کنند و منتظر درست شدن مسائل شوند. به نظر می‌رسید گروه طرفداران بلاک‌های کوچک برخی از این پیچیدگی‌ها را درک، و از آن تا حدودی برای کسب حمایت این شرکت‌ها استفاده می‌کردند.

1 Spot exchange
2 Leveraged trading
3 Futures contracts
4 Derivative contracts
5 Lending
6 Debt markets
7 Margin long

در تاریخ ۱۸ مارس سال ۲۰۱۷ یک روز پس از اعلامیه صرافی‌ها، شرکت Bitfinex تصمیم بی‌نظیری گرفت که تأثیر اساسی و پایداری بر روی مناقشه ساینز بلاک داشت. این شرکت قراردادهای آتی Bitcoin Unlimited را در مقابل Bitcoin Core در صرافی خود لیست کرد که زمان سررسید آن‌ها در پایان سال ۲۰۱۷ بود. این صرافی به کاربران خود اجازه می‌داد بیت‌کوین‌هایی که بر روی این صرافی داشتند را به دو توکن BCC (به نمایندگی Bitcoin Core) و BTU (به نمایندگی Bitcoin Unlimited) تقسیم کنند. کاربران قادر بودند این دو توکن را بر روی بستر صرافی Bitfinex معامله کنند. سرانجام این امکان برای سرمایه‌گذاران فراهم شده بود تا با به خطر انداختن سرمایه خود نظرشان را ابراز کنند. قبل از این هم وب‌سایت‌هایی وجود داشت که در آن افراد نظرات بحث‌برانگیزی در مورد مناقشه ساینز بلاک ارائه می‌دادند و کوین مورد نظر خود را انتخاب می‌کردند، هولدرهای بیت‌کوین^۱ قادر بودند پیام‌های خود را با کلید عمومی آدرس‌های بیت‌کوین‌شان امضا کنند و بر روی این سایت‌ها قرار دهند. امکان ارزیابی نظرات دارندگان بیت‌کوین از طریق این وب‌سایت‌ها فراهم بود ولی مشکل اینجا بود که دارایی کاربران این وب‌سایت‌ها در خطر نبود. ولی اکنون و با راه‌اندازی قرارداد آتی شرکت Bitfinex سرمایه آن‌ها در معرض خطر قرار گرفته بود.

این موضوع در روند این مناقشه یک تغییر اساسی پدید آورد: اکنون طرفین بجای اینکه با عصبانیت با یکدیگر بحث و جدل کنند مجبور بودند سرمایه خود را به خطر بیندازند و یکی از این دو کوین را انتخاب کنند. برخی از اعضای گروه طرفداران بلاک‌های کوچک همیشه فکر می‌کردند دست آن‌ها بسته است و آزادی عمل ندارند. آن‌ها معتقد بودند که «اکثریت اقتصادی»^۲ با آن‌ها همراه است و برای پیروزی آن‌ها فقط کفایت آزادی مالی به آن‌ها داده شود تا نظرات خود را بیان کنند. آن‌ها اغلب اعلام می‌کردند «تصمیم‌گیری را بر عهده بازار بگذارید!» حالا سرانجام حداقل در یک مقیاس محدود بازاری شکل گرفته بود. بیشتر افراد نگاه مثبتی نسبت به شرکت Bitfinex داشتند و به‌طور کلی از آن حمایت می‌کردند. تنها نکته منفی این بازار این بود که برای شرط‌بندی روی نتیجه این

1 Bitcoin holders
2 Economic majority

موضوع، افراد باید حدود ۹ ماه کنترل بیت کوین هایشان را در اختیار شرکت Bitfinex قرار می دادند. این شرکت از این نظر سابقه خوبی نداشت و در گذشته مورد حمله هکرها قرار گرفته بود. شرکت Bitfinex در سال ۲۰۱۷ این کار را برای ۴ هارد فورک پیشنهادی دیگر هم تکرار کرد و بازار معاملات آتی برای آن‌ها ایجاد کرد.

قیمت توکن Bitcoin Unlimited هیچ وقت به بالاتر از ۲۰ درصد قیمت بیت کوین نرسید. ارزش آن از ۱۵ تا ۲۰ درصد قیمت بیت کوین شروع شد و در اوایل ماه مه سال ۲۰۱۷ کاهش چشمگیری یافت و به حدود ۳ درصد قیمت بیت کوین رسید. در ادامه، قیمت این توکن انعکاس دهنده پیچ و خم‌هایی بود که در مناقشه سائز بلاک رخ می داد، مثلاً در اواخر ماه مه و اواخر ماه آگوست سال ۲۰۱۷ قیمت آن بالا رفت. قیمت این توکن چند بار دیگر بالا رفت و دلیل آن این بود که معامله گران برای برداشت بیت کوین از صرافی Bitfinex ناچار به خرید توکن Bitcoin Unlimited و ترکیب دوباره آن با توکن Bitcoin Core بودند. سرانجام در پایان سال، قرارداد آتی توکن Bitcoin Unlimited در حالی منقضی شد که این توکن به دلیل اجرا نشدن هارد فورک Bitcoin Unlimited کاملاً بی ارزش بود.

فصل چهاردهم

فناوری ASICBoost

در روز ۵ آوریل سال ۲۰۱۷ بمب خبری دیگری، اینبار از جانب طرفداران بلاک‌های کوچک منفجر شد. این بمب در واقع ایمیلی بود که گرگوری مکسول به ایمیل اعضای لیست توسعه‌دهندگان بیت کوین ارسال کرد. ما در اینجا به جزئیات نمی‌پردازیم چون بسیار فنی است. گرگوری مدعی بود که دلایل اعلام شده توسط شرکت Bitmain و شخص جیهان وو برای مخالفت با سگویت، در واقع دروغ هستند. ظاهراً شرکت Bitmain یک برنامه مخفی داشته: این شرکت یک روش برای بهیه‌سازی ماینینگ کشف کرده بود که میان‌بری در مکانیزم اثبات کار محسوب می‌شد، ولی تراکنش‌های سگویتی باعث ناکارآمدی آن می‌شدند. بنابراین در حقیقت دلیل مخالفت این شرکت با سگویت مالی بود، چون آن‌ها می‌خواستند از سودآوری خود محافظت کنند و دلایلی که به صورت عمومی مبنی بر پیچیدگی سگویت یا تلاش برای اجرای هارد فورک بیان می‌شد حقیقت نداشت. اگر ثابت می‌شد که شرکت Bitmain تا این اندازه فریبکارانه عمل می‌کند، می‌شد ادعا کرد که این شرکت برای پروتکل بیت کوین یک بازیگر خطرناک است.

من یک ماه پیش روش حمله به الگوریتم SHA2 Hashcash بیت کوین توسط ASICBOOST و همچنین روش‌های مقابله با آن را در صورتی که روزی برای شبکه بیت کوین مشکل ساز شوند توضیح دادم.

در حالی که اغلب بحث‌ها در مورد ASICBOOST متمرکز بر روش‌های اجرای آن به صورت آشکارا و علنی است، ولی روش‌های مخفیانه‌ای هم برای بکار بستن آن وجود دارد.

همانطور که داشتم یکی از روش‌های جلوگیری از پیاده‌سازی پنهانی ASICBOOST را توضیح می‌دادم، متوجه شدم مواردی که مطرح می‌کنم تقریباً توصیف کننده ساختار تعهد^۱ در سگویت هستند.

نویسندگان پیشنهاد سگویت تلاش ویژه‌ای کردند تا با هیچکدام از سیستم‌های استخراج بیت کوین ناسازگاری نداشته باشند، و حتی در یک مورد تغییراتی در طراحی آن اعمال کردند تا با آدرس‌های پرداخت اجباری^۲ در تراشه‌های استخراج، سازگار باشند.

اگر اطلاع داشتیم افرادی هستند که از روش ASICBOOST استفاده می‌کنند، تلاش می‌کردیم تا صرفاً برای تفکیک دغدغه‌ها از ایجاد ناسازگاری جلوگیری کنیم. ولی روش‌هایی که این قابلیت را به بهترین نحو و به صورت مخفیانه به خدمت می‌گیرند تقریباً با همه راه‌های افزایش قابلیت‌های تراکنش‌های بیت کوین ناسازگار هستند. به استثنای بلاک‌های بسط‌یافته^۳ (که مشکلات خاص خود را دارند).

ناسازگاری [الگوی تراکنش‌های سگویت با ASICBOOST] می‌تواند رفتارهای توجیه ناپذیر برخی از گروه‌های فعال در اکوسیستم استخراج بیت کوین را توضیح

1 Commitment structure
2 Forced payout addresses
3 Extension blocks

دهد، برای همین من شروع کردم به جستجوی شواهدی که این مسأله را تأیید می‌کنند.

مهندسی معکوس یک تراشه بکارگرفته شده در یک دستگاه استخراج خاص به ما نشان داد که قطعاً فناوری ASICBOOST در آن پیاده‌سازی شده است.

بر این اساس، من پیش‌نویس BIP زیر را ارائه می‌دهم تا به بحث گذاشته شود. این BIP به طور کلی از حمله ASICBOOST جلوگیری نمی‌کند، ولی قادر است از بکارگیری آن از روش‌های مخفیانه که با ارتقاء پروتکل بیت کوین ناسازگارند، ممانعت کند.

امیدوارم حتی آن دسته از ما که ترجیح می‌دهیم بکارگیری از ASICBOOST به کلی متوقف شود با یکدیگر متحد شویم تا بتوانیم از اقدام‌هایی که مانع روش‌های بکارگیری مخفیانه از آن می‌شوند پشتیبانی کنیم، چون این روش‌های مخفیانه به طور بالقوه جلوی بهبود و ارتقاء پروتکل بیت کوین را می‌گیرند.

ASICBOOST روشی برای کاهش میزان کاری است که یک ماینر باید برای پیدا کردن اثبات کار (POW) لازم انجام دهد. اثبات کار بیت کوین که از الگوریتم هش SHA256 استفاده می‌کند، سربرگ بلاک را قبل از انجام محاسبات به قطعات ۶۴ بایتی تقسیم می‌کند. اندازه سربرگ هر بلاک بیت کوین ۸۰ بایت است، پس به دو بخش یعنی قطعه ۱ و قطعه ۲ تقسیم می‌شود. ASICBOOST مقدار یکی از این قطعه‌ها را در طول هش کردن‌های متوالی ثابت نگه می‌دارد. بنابراین کفایت دستگاه ماینر فقط بخشی از کار را بر روی این قطعه انجام دهد و در نتیجه بهره‌وری قابل توجهی، حتی تا ۲۰ درصد بدست آورد. اولین بار «تیمو هانکه»^۱ این سیستم را در مقاله‌ای در سال ۲۰۱۶ میلادی توضیح داد.

1 Timo Hanke

برای دستیابی به این هدف دو راه وجود داشت: اینکه آشکارا بخش شماره ۱ نسخه ۱ را در سربرگ بلاک در قطعه شماره ۱ و برای ایجاد آنتروپی تغییر دهیم، در حالی که قطعه شماره ۲ طی هش‌های متوالی ثابت است. یا اینکه از راه مخفیانه این کار را انجام دهیم. روش مخفیانه بکارگیری از ASICBOOST بسیار پیچیده‌تر است و برای اجرای آن و پیدا کردن یک هش درست در چهار بایت آخر ریشه مرکلی^۲، باید با تراکنش‌های بیت کوین درگیر شد. ریشه مرکلی به دو قسمت تقسیم می‌شود و در قطعه ۱ و قطعه ۲ قرار می‌گیرد، به‌صورتی که ۴ بایت آخر آن در قطعه ۲ قرار دارد. بنابراین با استفاده مخفیانه از این روش می‌توان قطعه ۲ را در طول هش‌های متوالی ثابت نگه داشت. می‌توان با ایجاد تغییر در ترتیب قرار گرفتن تراکنش‌ها در بلاک، به این روش مخفیانه دست پیدا کرد. ارتقاء سگویت ماینرها را ملزم می‌کند تا ساختار تراکنش‌ها را در محل دیگری در بلاک قرار دهند، و تقریباً باعث می‌شود این نوع دستکاری‌ها غیرممکن شود. بنابراین سگویت سهواً مانع اجرای روش‌های مخفیانه ASICBOOST می‌شود.

در این مرحله در مورد ادعای گرگوری مبنی بر اینکه «مهندسی معکوس یک تراشه بکارگرفته شده در یک دستگاه استخراج خاص به ما نشان داد که قطعاً فناوری ASICBOOST در آن پیاده‌سازی شده است»، همچنان عدم اطمینان قابل توجهی وجود داشت. در حالی که به نظر می‌رسید اغلب طرفداران بلاک‌های کوچک این ادعا را باور کرده‌اند، اما برای من روشن نبود که شواهد کافی برای اثبات این ادعا وجود دارد یا نه. شاید طرفداران بلاک‌های کوچک متقاعد شده بودند که سگویت ایده خوبی است و شرکت Bitmain هیچ دلیل موجهی برای مخالفت با آن ندارد. یا اینکه آن‌ها به اشتباه به این نتیجه رسیده بودند که این شرکت مقاصد پلیدی را دنبال می‌کند. این ادعا به خوبی تبیین‌کننده رفتار شرکت Bitmain بود و به همین دلیل به نظر می‌رسید اغلب طرفداران بلاک‌های کوچک به آن باور داشتند. البته از سوی دیگر می‌شد رفتار جیهان وو را از زاویه دیگری تحلیل کرد که اتفاقاً خیلی محتمل به نظر می‌رسید. ممکن است او یکی از طرفداران پروپاقرص بلاک‌های بزرگ بوده و در معرض ایده‌های آنان قرار گرفته و از

1 Version bits
2 Merkle root

آن‌ها پشتیبانی می‌کرده است. تحلیل رفتارهای او از این زاویه هم می‌توانست دلایل مخالفت او با سگویت را توضیح دهد.

دو روز پس از طرح ادعای گرگوری، شرکت Bitmain در یک طومار طولانی آن را قویاً انکار کرد:

شرکت Bitmain فناوری ASICBOOST را بر روی Testnet بیت کوین آزمایش کرده است اما برخلاف ادعای گرگوری مکسول، هرگز از آن روی شبکه اصلی استفاده نکرده است. ما از کسانی که مدعی این امر نادرست هستند درخواست می‌کنیم دلایل قطعی خود را ارائه کنند چون ادعاهای بی‌اساس برای فضای بیت کوین سمی هستند.

...

شرکت Bitmain دارای حق ثبت اختراع ASICBOOST در کشور چین است. ما می‌توانیم به صورت قانونی از آن در مزارع استخراج خود در چین استفاده کنیم و از آن سود ببریم و قراردادهای استخراج ابری خود را به عموم مردم بفروشیم.

...

کارایی تجهیزات استخراج بیت کوین به سرعت کاهش می‌یابد. شرکت Bitmain دائماً مدل‌های جدید و کارآمدتری را به عموم مشتریان خود معرفی کرده است. بنابراین این اظهارات که ادعا می‌کنند پیاده‌سازی ASICBOOST موجب پدید آمدن اختلاف ۲۰ درصدی در بهره‌وری انرژی می‌شود، مغایر با مدل تجاری شرکت Bitmain و نادرست هستند.

...

دلیل اجرا نشدن سگویت این است که شرایط تعیین شده در توافق نامه هنگ کنگ، همچنان محقق نشده‌اند.

...

گرگوری مکسول اخیراً پیشنهاد کرده که تصادف^۱ ۲۳۲ را به ۲۶۴ تغییر دهیم تا بکارگیری ASICBOOST دشوارتر شود. نتیجه این کار چیزی جز ضرر برای صاحبان حق ثبت اختراع ASICBOOST و پروتکل بیت کوین در پی نخواهد داشت. دارندگان حق ثبت اختراع چیزی گیرشان نمی‌آید و پروتکل بیت کوین هم پیچیده‌تر خواهد شد.

...

وقتی گرگوری مکسول کودتا علیه کوین اندریسن را برعهده گرفت و دسترسی او به گیت‌هاب را مسدود کرد، جامعه بیت کوین ضرر بزرگی متحمل شد. اکنون وظیفه ما این است که به‌عنوان جامعه فعالان بیت کوین یک گروه توسعه‌دهنده اصلی بیت کوین پیدا کنیم که وقت خود را صرف حمله به یکی از بزرگترین سرمایه‌گذاران بیت کوین (راجر وور)، یکی از بزرگترین صرافی‌ها (کوین بیس)، و یکی از بزرگترین شرکت‌های تأمین‌کننده تجهیزات استخراج (بیت‌مین) نکند.

به اولین چیزی که باید توجه شود این است که علی‌رغم این تکذیبیه، به نظر می‌رسید شرکت Bitmain به استفاده از فناوری ASICBOOST بر روی Testnet بیت کوین و به‌صورت مخفیانه اعتراف، و بنابراین احتمالاً آن را بر روی سخت‌افزار خود پیاده‌سازی کرده است. قبل از این تکذیبیه، من مطمئن نبودم که ادعاهای مطرح شده درباره این شرکت صحت داشته باشد. از قضا از نظر من ماهیت این تکذیبیه موجب بالا رفتن احتمال درست بودن این ادعاها شد. این شرکت حتی قبل از اینکه از این فناوری به‌عنوان یک

1 collision

بهینه‌سازی قانونی در امر استخراج بیت کوین دفاع کند، پا را فراتر گذاشته و مدعی بود که دارای حق ثبت اختراع ASICBOOST در کشور چین است و در صورت تمایل می‌توانند به صورت قانونی از آن استفاده کنند. بهتر بود آن‌ها بجای دفاع از ASICBOOST و سناریوی فرضی استفاده از آن به یک تکذیبیه ساده و واضح بسنده می‌کردند. این تکذیبیه موقعیت شرکت Bitmain را تضعیف کرد و توسط گروه طرفداران بلاک‌های کوچک به عنوان شاهی برای اثبات رفتارهای خرابکارانه این شرکت مورد استفاده قرار می‌گرفت. حتی اگر شرکت Bitmain در حال حاضر از فناوری ASICBOOST به صورت مخفیانه استفاده نمی‌کرد، ولی احتمالاً آن‌ها قصد استفاده از آن را داشتند و بنابراین اصل اتهامات گرگوری تا حدودی صحت داشت: شرکت Bitmain در مخالفت با اجرای سگویت صادقانه رفتار نمی‌کرد. شاید همه این‌ها به پول مربوط بود.

با این حال شاید توضیح این مسأله ساده‌تر از این باشد. شاید شرکت Bitmain در برقراری ارتباط به زبان انگلیسی ضعیف عمل کرده و ضعیف بودن این تکذیبیه هم به همین دلیل است. وجود فرهنگ بحث و مجادله هم باعث می‌شد طرفین روی هر نکته‌ای درگیر بحث و جدل شوند. شاید منظور شرکت Bitmain این بود که آن‌ها به صورت مخفیانه از ASICBOOST استفاده نمی‌کردند، اما حتی اگر استفاده هم می‌کردند مگر چه اشکالی دارد؟ ممکن است شرکت Bitmain می‌خواسته به این نکته اشاره کند، در حالی که این شرکت از ASICBOOST استفاده نمی‌کرده است. این تکذیبیه در ادامه به بیان موضع شرکت Bitmain در مناقشه سائز بلاک پرداخته بود، اینکه آن‌ها به دلیل محقق نشدن شرایط تعریف شده در توافق‌نامه هنگ کنگ، از اجرای سگویت ممانعت می‌کنند. البته از نظر طرفداران بلاک‌های کوچک این شرایط هرگز به این شکل تعریف نشده بود که قرار باشد کاری در ازای کار دیگری انجام شود.

جالب اینکه کوین با این پیش‌فرض که شرکت Bitmain از فناوری ASICBOOST به صورت مخفیانه استفاده می‌کند به دفاع از آن پرداخت و استدلال می‌کرد این فناوری یک بهینه‌سازی قانونی با استفاده از نرم‌افزار بیت کوین است.

اتریوم نباید قوانین خود را برای بازگرداندن پول‌های دزدیده شده [در واقعه دائو] تغییر دهد، ولی اگر بیت کوین قوانین خود را برای جلوگیری از یک بهینه‌سازی تغییر دهد، اشکالی ندارد؟

البته به نظر می‌رسید که کوین نکته را نگرفته است. مسأله این نبود که بکارگیری مخفیانه ASICBOOST نامشروع است، بلکه مخالفت شرکت Bitmain با اجرای سگویت صادقانه نبود. این یعنی یکی از طرفین درگیر در مناقشه سائز بلاک انگیزه‌های ریاکارانه‌ای داشت. اگر شرکت Bitmain از ابتدا صادقانه مخالفت خود را با اجرای سگویت به دلیل ناسازگاری با این فناوری اعلام می‌کرد، داستان شکل دیگری پیدا می‌کرد.

تقریباً همزمان با رسوایی ASICBOOST، چند نفر از طرفداران بلاک‌های بزرگ ایده بلاک‌های الحاقی^۱ را به‌عنوان جایگزین سگویت پیشنهاد دادند؛ روشی برای افزایش سائز بلاک از راه سافت فورک. این پیشنهاد توسط «اندرو لی»^۲ در وبلاگ Purse.io، شرکتی که با طرفداران بلاک‌های بزرگ در ارتباط بود، مطرح شد. به نظر می‌رسید حتی راجر ورو و شرکت Bitmain هم از این ایده حمایت می‌کنند. بلاک‌های الحاقی در ابتدا توسط «جانسون لا»^۳، یکی از افرادی که در نگارش سگویت مشارکت داشت در سال ۲۰۱۳ پیشنهاد شد، ولی کلاً به فراموشی سپرده شد چون جابجایی کوین‌ها از یک بلاک الحاقی به زنجیره اصلی می‌توانست مشکل‌زا باشد. مشکلی که سگویت با آن دست به گریبان نبود.

آنچه در اینجا قابل توجه بود این بود که به نظر می‌رسید طرفداران بلاک‌های بزرگ بر روی پیشنهادی به توافق رسیده‌اند که بسیاری از نقایص سگویت را در خود داشت، چون این روش بسیار پیچیده بود و فقط برای افزایش سائز بلاک طراحی نشده بود. با این حال به نظر می‌رسید آنچه برای آن‌ها اهمیت داشت این بود که این پیشنهاد توسط Bitcoin Core طراحی نشده بود. به نظر می‌رسید در این مرحله اولویت اول طرفداران بلاک‌های

1 Extension blocks
2 Andrew Lee
3 Johnson Lau

بزرگ این بود که ایده‌های خود را توسعه دهند و از شر Bitcoin Core خلاص شوند و صرف افزایش سایز بلاک اهمیت پایین‌تری داشت.

بلاک‌های الحاقی روشی برای افزایش سایز بلاک از راه سافت فورک و در عین حال حفظ امکان بکارگیری فناوری ASICBOOST به صورت مخفیانه بود. از نظر طرفداران بلاک‌های کوچک پیشنهاد این روش از جانب شرکت Bitmain گواهی بر مجرم بودن شرکت Bitmain بود. طرفداران بلاک‌های کوچک همچنین شرکت Bitmain را متهم به تأمین مالی برای اعمال فشار برای اجرای بلاک‌های الحاقی می‌کردند و این اعمال را شاهدهی بر گناهکار بودن این شرکت در موضوع ASICBOOST می‌دیدند. درست مثل اینکه طرفداران بلاک‌های بزرگ با اجرای پیشنهادهایی که توسط Bitcoin Core پیاده‌سازی شده بود مخالفت می‌کردند، طرفداران بلاک‌های کوچک هم تعصب مشابهی داشتند و با توجه به اینکه ایده بلاک‌های الحاقی توسط شرکت Bitmain تبلیغ و تأمین مالی شده بود، با اجرای آن مخالفت می‌کردند.

حق ثبت اختراع ASICBOOST تهدید قابل توجهی برای بیت کوین بود. ممکن بود یکی از شرکت‌های استخراج بیت کوین این حق ثبت اختراع را بدست می‌آورد و مدعی حقوق انحصاری بکارگیری از این فناوری می‌شد و با توجه به برتری که استفاده از این فناوری برای این شرکت بوجود می‌آورد می‌توانست بر صنعت استخراج بیت کوین مسلط شود. گفته می‌شود تعدادی از بیت کوینرها برای کاهش این نگرانی این حق ثبت اختراع را به قیمت بسیار بالایی خریداری کرده‌اند و سپس در ماه مارس سال ۲۰۱۸ آن را در ائتلاف حق ثبت اختراعات تدافعی^۱ قرار داده‌اند، به گونه‌ای که این حق ثبت اختراع هرگز بجز در موارد لازم برای دفاع در مقابل حقوق ثبت اختراع دیگر مورد استفاده قرار نخواهد گرفت.

از حدود ماه آوریل سال ۲۰۱۸ نشانه‌هایی مبنی بر استفاده علنی^۲ از فناوری ASICBOOST در بلاک‌های زنجیره بیت کوین مشاهده شد. استفاده علنی از این فناوری بسیار ساده‌تر و

1 Defensive patent pool

2 Overt

کارآمدتر از روش مخفیانه است و با سگویت سازگار است. در ماه نوامبر سال ۲۰۱۸ شرکت Bitmain استفاده علنی از این فناوری را به سیستم‌عامل دستگاه‌های استخراج خود اضافه کرد و امروز بیش از ۷۰ درصد بلاک‌های بیت‌کوین با این روش ماین می‌شوند. در مورد حق ثبت اختراع، هرگز معلوم نشد چه کسی این حق ثبت اختراع را خریداری کرده است، و همچنین نمی‌توان به راحتی از مالک آن به هویت شخصی که آن را در اختیار ائتلاف حق ثبت اختراعات تدافعی قرار داده است پی برد. بنابراین اتفاقاتی که رخ داد کمی مبهم بود.

حتی امروز من واقعاً مطمئن نیستم که آیا شرکت Bitmain واقعاً از فناوری ASICBOOST مخفیانه^۱ روی شبکه اصلی بیت‌کوین استفاده می‌کرده است یا نه. کارشناسان در این مورد با یکدیگر اتفاق نظر ندارند. به نظر من احتمال آن ۵۰ : ۵۰ است.

به نظر می‌رسد اتهامات مربوط به ASICBOOST تأثیر بسیار کمی روی گروه طرفداران بلاک‌های بزرگ داشت. به‌طور کلی آن‌ها این اتهام‌ها را درک نمی‌کردند و به نظر آن‌ها این موضوع یکی دیگر از تبلیغات و دروغ‌هایی بود که از جانب Bitcoin Core مطرح شده بود و توجهی به آن نمی‌کردند. این اتهامات همچنین تأثیر کمی در ترغیب افراد برای پیوستن به گروه طرفداران بلاک‌های کوچک داشت، چون موضوع پیچیده‌ای بود. با این حال مطمئناً تأثیر به‌سزایی در مصمم‌تر شدن اغلب طرفداران بلاک‌های کوچک داشت، که در این مرحله معتقد بودند شرایط اضطراری است. در نهایت، مجادله بر سر ASICBOOST نقش مهم و برجسته‌ای در این درگیری بازی کرد. به نظر می‌رسد گروه طرفداران بلاک‌های کوچک مصمم به انجام اقداماتی هستند.

1 Covert

فصل پانزدهم

مخفی‌گاه اژدهایان^۱

در ۵ آوریل سال ۲۰۱۷، جوزف پون^۲ یکی از مؤلفان وایت پیپر شبکه لایتینگ به یک کانال محرمانه متعلق به گروه طرفداران بلاک‌های کوچک اشاره کرد که بسیاری از تصمیمات روابط عمومی^۳ در آنجا گرفته می‌شود:

آن‌ها یک کانال محرمانه دارند که در آن عملیات روابط عمومی و روش‌های دست انداختن دیگران^۴ را در آنجا سازمان‌دهی می‌کنند. افراد زیادی در مورد آن صحبت کرده‌اند (بیشتر از ۵ نفر) و در فضاهای عمومی مختلفی به آن اشاره می‌شود چون اساساً در آنجا تصمیمات زیادی گرفته می‌شود.

من از اینکه آن‌ها به دلیل مصاحبه کردن با مطبوعات به من حمله می‌کنند بسیار ناراحت هستم، در حالی که خود آن‌ها به صورت پنهانی درگیر حقه‌بازی هستند. و همه توسعه‌دهندگان Core خودشان می‌دانند که هر وقت مشغول مشارکت بر روی نرم‌افزار بیت کوین نباشند، به چه کاری مشغول می‌شوند.

1 Dragons' Den
2 Joseph Poon
3 Public relations
4 Trolling

من فکر می‌کنم جامعه BU هم بر روی slack خود کارهای مشابهی می‌کند. چیزی که من را بیشتر از همه چیز ناراحت می‌کند این است که اعضای برجسته Core به این دلیل به من حمله می‌کنند و به من سوءظن دارند. این برای من یک مسأله شخصی است. انگار فکر می‌کنند من خودم را فروخته‌ام ولی احتمالاً من نسبت به افراد برجسته جامعه بیت‌کوین کمترین پول را به جیب زده‌ام. این مسأله به نظر من فوق‌العاده توهین‌آمیز است.

روز بعد طرفداران بلاک‌های بزرگ ویدئویی از «برام کوهن»^۱ مخترع Bittorrent پیدا کردند که در ژانویه سال ۲۰۱۷ ضبط شده بود. در طول سخنرانی او پنجره‌ای به‌طور تصادفی با نام dragonsden روی صفحه او ظاهر شد که یک کانال بر روی اسلک Bitcoin Core بود. این کانال خصوصی بود و ۲۱ عضو داشت. از آنجا می‌شد چند تن از اعضای این کانال را شناسایی کرد. این افراد از نظر طرفداران بلاک‌های بزرگ از معروف‌ترین کسانی بودند که دیگران را دست می‌انداختند و در میان آن‌ها افرادی از مدیران ساب‌ردیت بیت‌کوین هم بودند. از نظر طرفداران بلاک‌های بزرگ این یک رسوایی بزرگ بود؛ شواهدی از هماهنگی طرفداران بلاک‌های کوچک، ارتباط بین ساب‌ردیت بیت‌کوین، توسعه‌دهندگان Bitcoin Core، و کمپین‌های تبلیغاتی وجود داشت. طرفداران بلاک‌های بزرگ هم احتمالاً از راه‌های ارتباطی مخفی برای هماهنگی و تمرکز بر فعالیت‌های مربوط به روابط عمومی استفاده می‌کردند. این موضوع به ماهیت سیاسی اوضاع مربوط می‌شد، درگیری به حدی بالا گرفته بود که طرفین ناچار به استفاده از این ابزارها بودند. این «رسوایی» برای من یک نتیجه مشخص داشت؛ باید هر طور شده به این «مخفی‌گاه اژدها» راه پیدا می‌کردم. چند هفته بعد و با کمی پرس و جو، توانستم! و خودم را به اعماق این مخفی‌گاه رساندم.

این کانال بسیار فعال بود و کاملاً بر روی مناقشه‌ساز بلاک متمرکز بود. بیشتر مسائل حول شبکه‌های اجتماعی، روابط عمومی، و اینکه چگونه به بهترین شکل ضعف دیدگاه‌ها و

1 Bram Cohen

استدلال‌های مطرح شده توسط طرفداران بلاک‌های بزرگ را بر ملا کنند. بسیاری از اعضای این کانال بسیار متعهد به نظر می‌رسیدند. گفتگوها اغلب حول روش‌های متقاعد کردن افراد مختلف برای پیوستن به گروه طرفداران بلاک‌های کوچک بود، مخصوصاً افرادی که امکان تغییر موضع‌شان بیشتر بود. همچنین در مورد موثرترین موضوعاتی که باید در رسانه‌های اجتماعی مورد توجه قرار گیرد تصمیم گرفته می‌شد و در مورد میم^۱ و ساختن آن‌ها بحث می‌کردند. این جنگ، جنگ میم‌ها هم بود، و این اژدهایان (نامی که اعضای این کانال بعضی اوقات به خود می‌دادند)، در تولید میم نقش پررنگی داشتند. بسیاری از این میم‌ها طنزآلود بودند و طوری طراحی شده بودند تا نشان دهند طرفداران بلاک‌های بزرگ درک ضعیفی از مسائل فنی بیت کوین دارند. راجر ور، کریگ رایت، و جیهان وو در مرکز اصلی توجه آن‌ها بودند. استراتژی دیگر آن‌ها افشای ارتباط راجر ور با کریگ رایت بود، اگرچه انصافاً باید گفت راجر به آن‌ها سخت نمی‌گرفت.

چیزی که مرا در مورد این کانال محرمانه تحت تأثیر قرار می‌داد شدت فعالیت در آن، حداقل در اوایل سال ۲۰۱۷ بود. این کانال در ۲۴ ساعت روز و هفت روز هفته فعال بود. مهم نبود چه ساعتی از روز باشد، در هر صورت یک موضوعی مربوط به مناقشه سائز بلاک در جریان بود.

اینکه آیا همه تاکتیک‌های این اژدهایان همیشه بر پایه اصول اخلاقی بود یا نه، جای سؤال دارد. هر دو طرف درگیر همدیگر را به حقه‌بازی متهم می‌کردند. اتهامی که به آن‌ها می‌زدند این بود که این افراد رفتارهای سمی^۲، مرموز، مخرب، فریبکارانه، و دغل‌کارانه دارند. از قضا آنچه برای من روشن بود این بود که روش‌ها و تاکتیک‌های بکار گرفته شده از هر دو طرف درگیر به طرز قابل توجهی به هم شباهت داشتند، تا جایی که می‌توانیم بگوییم دقیقاً مثل هم بودند. هر دو طرف درگیر از نظر رعایت صداقت در این جنگ سابقه خوبی نداشتند، و نمی‌توانستند در یک مورد خاص دیگری را متهم به رعایت نکردن اصول اخلاقی کنند. با وجود اینکه برخی از اقدام‌های این کانال محرمانه کمی شیطنت‌آمیز

1 Meme
2 Toxic

بود، ولی کار شرورانه‌ای از آن‌ها سر نمی‌زد. هیچ مدرکی مبنی بر انجام کارهای غیرقانونی از هیچ‌کدام از طرفین درگیر وجود نداشت، به جز در مورد حملات DDOS. هرچند من هیچ مدرکی دال بر برنامه‌ریزی شدن این عملیات در کانال مخفی‌گاه اژدهایان مشاهده نکردم.

فصل شانزدهم

لایت کوین

یک استراتژی که در کانال اژدهایان مورد بحث قرار گرفت، فعال کردن سگویت بر روی زنجیره لایت کوین؛ یکی از آلت کوین‌هایی که اغلب به‌عنوان یکی از نزدیکان بیت کوین در نظر گرفته می‌شود، بود. این به ماینرها نشان می‌داد که سگویت مشکلی ندارد و بسیاری از کاستی‌هایی که توسط طرفداران بلاک‌های بزرگ تبلیغ می‌شود، مثل مشکلات امنیتی، در حقیقت بی‌معنی هستند. نرم‌افزار سافت فورک سگویت برای لایت کوین در تاریخ ۱۲ ژانویه سال ۲۰۱۷ و با نسخه ۷۰.۱۳.۲.۱ منتشر شد. برخلاف بیت کوین که آستانه فعال‌سازی آن ۹۵ درصد بود، آستانه فعال‌سازی لایت کوین ۷۵ درصد بود. پنجره پیوسته فعال‌سازی^۱ دوهفته‌ای و دوره^۲ تنفس دوهفته‌ای لایت کوین عیناً شبیه به بیت کوین بود. بیشتر توضیحات^۳ نسخه منتشر شده را یک توسعه‌دهنده ناشناس لایت کوین به نام «شاولین فرای»^۴ نوشته بود و بخش عمده‌ای از کُد نرم‌افزاری سگویت توسط توسعه‌دهندگان بیت کوین تهیه شده بود. شاولین فرای احتمالاً عضوی از کانال اژدهایان بوده است، با این حال هویت واقعی این فرد به‌طور قطعی مشخص نبود. چارلی لی خالق لایت کوین بود و به نظر می‌رسید از طرفداران بلاک‌های کوچک باشد. همزمان به نظر

1 Rolling activation window
2 Grace period
3 Release notes
4 Shaolinfry

می‌رسید جامعه کاربران لایت کوین با اشتیاق از فعال شدن سگویت بر روی زنجیره لایت کوین پشتیبانی می‌کنند، زیرا این فرصتی بود تا یک فناوری جدید قبل از بیت کوین بر روی لایت کوین پیاده شود، و این موضوع برای آن‌ها بسیار مثبت ارزیابی می‌شد.

پشتیبانی از لایت کوین در بین ماینرهای لایت کوین به تدریج در حال افزایش بود، ولی همچنان کم بود و معلوم نبود سگویت بر روی شبکه لایت کوین فعال خواهد شد یا نه. حدود ۹ آوریل سال ۲۰۱۷ کمپینی^۱ برای فعال کردن سافت فورک از جانب کاربران^۲ (UASF) برگزار شد تا ماینرها را مجبور به فعال‌سازی سگویت کند. نیروی محرکه این کمپین استیصال کاربران لایت کوین از پیشرفت کند ماینرها بود. کاربران می‌خواستند به جای انتظار کشیدن برای علامت^۳ ماینرها و رسیدن به آستانه فعال‌سازی ۷۵ درصدی، نرم‌افزاری را اجرا کنند که قوانین جدید را در زمان مشخصی در آینده و صرف‌نظر از وضعیت علامت‌دهی ماینرها، بر روی شبکه لایت کوین اعمال کند. این مرحله از کمپین صرفاً کاربران را تشویق می‌کرد تا نشانه "UASF-Segwit-BIP148" را به گونه‌ای به شناسه نرم‌افزار فول نود لایت کوین خود اضافه کنند که در شبکه لایت کوین توسط دیگران قابل مشاهده باشد. هیچ قانون جدید روی شبکه فعال نمی‌شد، فقط کاربران قصد خود را از این طریق بیان می‌کردند.

این روش در دوران ساتوشی برای فعال کردن قوانین جدید بر روی شبکه به کار گرفته می‌شد، ولی به منظور کاهش احتمال ایجاد شکاف در زنجیره، یا مشکلاتی که ممکن بود در خلال فعال‌سازی قوانین جدید رخ دهد، از روش جایگزین علامت‌دهی ماینرها در بیت کوین استفاده می‌شود. به نظر من گرچه استفاده از این روش در بیت کوین؛ مخصوصاً برای یک ارتقاء جنجالی مثل سگویت ممکن است کمی خطرناک باشد، ولی به راحتی می‌توان از آن در لایت کوین استفاده کرد. تقریباً همه کاربران لایت کوین از سگویت پشتیبانی می‌کردند و حتی بنیانگذار این پروژه در این فضا بسیار فعال بود و از آن حمایت

1 Campaign
2 User activated softfork
3 Flagging

می‌کرد. به نظر می‌رسید روش UASF مؤثر باشد؛ به نظر می‌رسید ماینرها پیام کاربران را دریافت کرده‌اند و علامت‌های ماینرها برای فعال‌سازی سگویت بر روی زنجیره لایت کوین شروع به افزایش کرد. به نظر می‌رسید فعال‌سازی به‌زودی انجام پذیرد.

با این حال، در حدود ۱۷ آوریل سال ۲۰۱۷ هش‌ریت شبکه لایت کوین به شدت افزایش یافت. این هش‌ریت جدید برای فعال‌سازی سگویت علامت نمی‌داد و به نظر می‌رسید قصد دارد مانع فعال‌سازی آن شود. این کار بسیار شبیه به یک استراتژی آگاهانه از جانب ماینرها بود. این هش‌ریت مربوط به استخرهای LTC1BTC و LTC.TOP می‌شد که تحت کنترل «جیانگ ژوئر»^۱، از دست‌نشانده‌های جیهان وو اداره می‌شدند. در ۱۹ آوریل سال ۲۰۱۷ جیانگ ژوئر مطلبی نوشت و موضع خود را در آن توضیح داد:

اگرچه من در مورد سگویت تردیدهایی دارم (من یک هولدر لایت کوین هستم)، ولی اگر این روش برای ادامه مسیر به‌طور گسترده‌ای مورد پذیرش قرار بگیرد، مخالفتی با آن ندارم. اما من کاملاً با تاکتیک‌هایی که طرفداران سگویت برای فعال کردن آن به کار می‌برند؛ یعنی (DASF) UASF و اثبات حملهٔ DDOS، کاملاً مخالف هستم. اگر طرفداران این تاکتیک‌ها موفق به فعال‌سازی آن در لایت کوین شوند و این موفقیت منجر به تأیید آن‌ها شود، آنگاه بیت کوین و لایت کوین در مقابل خرابکاری‌های تبهکاران آسیب‌پذیر خواهند شد.

به همین دلیل من برای اطمینان از موارد زیر هش‌ریت کافی به استخراج خود اضافه می‌کنم:

اطمینان از اینکه سگویت از روش اثبات حملهٔ DDOS روی شبکه فعال نمی‌شود.

1 Jiang Zhuoer
2 Proof of DDOS

که جامعه کاربران لایت کوین صبر می کنند تا چارلی لی به چین سفر کند و با هم تصمیم بگیریم.

اکنون به نظر می رسد که جنگ بر سر مقیاس پذیری بیت کوین و همه مشاجرات مربوطه به لایت کوین منتقل شده است. در این دوره من مستقیماً با جیانگ ژوئر گفتگویی داشتم. او به من توضیح داد که بدون افزایش سایز بلاک لایت کوین از روش هارد فورک، به فعال شدن سگویت رضایت نخواهد داد. هرچند این درخواست او منطقی به نظر نمی رسد چون برخلاف بیت کوین، بلاک های لایت کوین پر نبود. جیانگ به من توضیح داد قضیه مربوط به اصول ماجرا است: توسعه دهندگان لایت کوین باید «این موضوع را روشن کنند که در صورت پر شدن بلاک ها، هارد فورک را اجرا کنند»، در غیر این صورت این مسیر اشتباه است. او سپس به من گفت که فعال کردن سگویت روی لایت کوین بازی Bitcoin Core است. او نگران بود که اگر سگویت بر روی لایت کوین فعال شود، ممکن است بر روی بیت کوین نیز فعال شود. او مشخصاً از پیشنهاد شدن روش UASF و اینکه می توان آن را در بیت کوین هم انجام داد، عصبانی بود. از نظر جیانگ روش UASF «علیه منافع ماینرها» و «اقدامی خصمانه علیه ماینرها» است. از این مکالمه مشخص بود که جیانگ و برخی از ماینرها از احتمال موفقیت UASF بسیار نگران بودند. آن ها می ترسیدند موفقیت UASF موجب از بین رفتن این تصور شود که ماینرها تا حدودی بر پروتکل بیت کوین کنترل دارند.

البته گفته های جیانگ تا حدودی حقیقت داشت. من از مکالماتی که در کانال اژدهایان در جریان بود می دانستم که طرفداران بلاک های کوچک قصد دارند از راه فعال سازی سگویت بر روی لایت کوین، به فعال شدن آن روی بیت کوین کمک کنند. طرفداران بلاک های بزرگ از این هدف خبردار شده بودند و حالا مجبور بودند برای جلوگیری از وقوع آن تلاش کنند. از طرف دیگر واضح بود که سگویت از پشتیبانی جدی جامعه کاربران لایت کوین برخوردار است، بنابراین شاید بتوان گفت تلاش های طرفداران بلاک های بزرگ تا حدودی ناشایست بود.

در تاریخ ۲۱ آوریل سال ۲۰۱۷ در اقدامی روشن در کپی برداری از بیت کوین، یک میزگرد لایت کوین با حضور اکثر استخراج کنندگان آن در چین برگزار، و توافق نامه‌ای منتشر شد:

ما معتقدیم تصمیم برای ارتقاء قوانین پروتکل لایت کوین باید بر اساس نیاز کاربران گرفته شود، در میزگردها به رأی گذاشته شود، و در نهایت توسط ماینرها فعال شود.

...

ما از یک روش فعال‌سازی در یک روز خاص^۱ UASF که روند رأی‌گیری از کاربران یا جامعه فعالان لایت کوین را طی نکرده باشد، حمایت نمی‌کنیم. این روش ارتقاء اجباری بدون رسیدن به اجماع بین جامعه فعالان، لایت کوین را در معرض رخ دادن یک شکاف در زنجیره آن قرار می‌دهد.

...

طبق رأی‌گیری انجام شده، اعضای شرکت کننده در این میزگرد در موضوع ارتقاء پروتکل لایت کوین به اتفاق آراء با برنامه زیر موافقت می‌کنند:

سافت فورک سگویت بر روی زنجیره لایت کوین اجرا می‌شود.

وقتی بیشتر از ۵۰ درصد ظرفیت بلاک مورد استفاده قرار گرفت، ما شروع به آماده‌سازی راه‌حلی برای افزایش محدودیت ۱ مگابایتی بلاک از راه سافت فورک یا هارد فورک خواهیم کرد.

1 Flag day activation

در آخر، شایان ذکر است که این بیانیه معرف نظر اعضای حاضر در این نشست است و قصد نداریم بجای عموم جامعه فعالان لایت کوین تصمیم گیری کنیم.

این توافق نامه به فعال سازی سگویت متعهد است، اما همچنین در آن مقرر می شود که بعد از پر شدن نیمی از فضای بلاک، برای بالا بردن فضای بلاک باید از روش دیگری استفاده شود. ماینرها شرط دوم را برای حفظ آبرو به این توافق نامه اضافه کرده بودند؛ سگویت فعال می شد و همچنان راه برای اجرای یک هارد فورک احتمالی در آینده باز بود. ولی در حقیقت ماینرها احتمالاً بدلیل تهدید UASF که در لایت کوین بسیار جدی بود، مجبور به فعال کردن سگویت بودند. توافق هنگ کنگ همچنان برای جیهان وو اهمیت داشت و آن ها می خواستند از این روش نشان دهند که نظرشان در مورد بیت کوین تغییر نکرده است و خواستار اجرای سگویت و یک هارد فورک برای افزایش سایز بلاک هستند. با توجه به اینکه بیشتر از ۵۰ درصد فضای بلاک ها در شبکه بیت کوین در حال حاضر پر بود، پس از نظر آن ها اجرای هارد فورک هم ضروری به نظر می رسید.

چند تناقض آشکار در این توافق به چشم می خورد. مدعی بود که تصمیمات مربوط به پروتکل باید در جلسات میزگرد گرفته شود، ولی بعداً اظهار می کرد که این جلسات قرار نیست به نمایندگی از عموم فعالان جامعه تصمیمی بگیرند و پروتکل لایت کوین در کنترل جامعه کاربران آن است. این نشان از اختلاف نظر افراد شرکت کننده در این میزگرد داشت و به نظر می رسید این جملات متناقض برای راضی نگه داشتن طرفین نوشته شده است. همچنین نشان می داد که جیهان وو و برخی از ماینرها تا چه اندازه معتقد بودند که قوانین پروتکل تحت کنترل ماینرها است. از گفتگوهایی که در این دوره با جیهان وو و جیانگ داشتم متوجه شدم که آن ها به تدریج دریافته اند که ماینرها قدرتی را که قبلاً تصور می کردند بر روی قوانین پروتکل دارند در واقع در اختیار ندارند و این موضوع برای آن ها بسیار ناامید کننده بود و تصمیم داشتند تا جایی که ممکن است به آن متوسل شوند.

سرانجام پس از هیاهوهای فراوان سگویت در می سال ۲۰۱۷ روی لایت کوین فعال شد و قیمت آن بعد از این اتفاق به شدت افزایش یافت؛ بخشی به دلیل هیجان مربوط به فعال شدن سگویت، بخشی به دلیل استراتژی برخی از طرفداران بلاک‌های کوچک به منظور افزایش قیمت و ایجاد یک فضای مثبت در مورد سگویت، ولی بیشتر از همه به دلیل منابع مالی جدیدی که با توجه به شکل گرفتن حباب ارزهای دیجیتال در سال ۲۰۱۷ به بازار وارد می‌شد، بود. برخی از اژدهایان بعد از این اتفاق به تعریف و تمجید از سگویت و اینکه قیمت لایت کوین افزایش یافته پرداختند و اظهار می‌کردند که پیش‌بینی‌های طرفداران بلاک‌های بزرگ مبنی بر اشکالات مهلک سگویت، چرند بوده است.

این اتفاق به وضوح برای طرفداران بلاک‌های کوچک یک شروع خوب در سال ۲۰۱۷ بود. آن‌ها سه پیروزی پیاپی بدست آورده بودند: صرافی‌ها، ASICBoost، و اکنون لایت کوین. وضعیت امتیازهای طرفین درگیر در تابستان سال ۲۰۱۷ سه بر صفر به نفع طرفداران بلاک‌های کوچک بود. پیشروی در این جنگ بسیار مهم بود و بیشتر مردم می‌خواستند از برنده حمایت کنند و دنباله‌رو اکثریت باشند. تأثیر تجمعی این پیروزی‌ها بسیار مهم بود و سلطه گروه طرفداران بلاک‌های کوچک در این مناقشه در حال گسترش بود.

فصل هفدهم

اعمال سافت فورک از جانب کاربران UASF

به نظر می‌رسد ایده اجرای UASF برای حل بن‌بست فعلی و فعال‌سازی سگویت از توسعه‌دهنده‌ای با نام مستعار شاولین فرای و در ایمیلی که او در تاریخ ۲۵ فوریه سال ۲۰۱۷ به لیست ایمیل بیت کوین ارسال کرده بود، نشأت گرفته شده باشد:

مشکل روش [اجرای سافت فورک بر اساس] سیگنال پشتیبانی اکثریت هش‌ریت این است که یک توجه غیرضروری را به ماینرها جلب، و به تبع آن شرایط را بی‌جهت سیاست‌زده می‌کند. ماینرها که از قبل دچار سوءبرداشت بوده‌اند و آن را با رأی‌گیری اشتباه می‌گرفتند، ممکن است برای «تصمیم‌گیری» به نیابت از جامعه فعالان بیت کوین احساس فشار کنند. این موضوع که چه کسی سیگنال آمادگی می‌دهد و چه کسی این کار را نمی‌کند به شدت مورد توجه عمومی قرار می‌گیرد و ممکن است به ماینرهایی که آمادگی این شرایط را ندارند فشارهایی را وارد کند. ممکن است برخی از ماینرها در شرایط مناسبی برای ارتقاء نباشند، یا اصلاً ترجیح دهند که در فرآیند اجرای سافت فورک شرکت نکنند؛ و این حق آن‌ها است. ولی رأی مخالف این ماینر [در روش سیگنال اکثریت هش‌ریت] موجب اجرا نشدن

سافت فورک برای دیگران خواهد شد، در حالی که سافت فورک‌ها اساساً اختیاری هستند! به نظر می‌رسد این وضعیت برخلاف طبیعت داوطلبانه سیستم بیت کوین است که در آن مشارکت در تمام سطوح به صورت اختیاری انجام می‌پذیرد و صداقت در آن از طریق معرفی انگیزه‌های متوازن حفظ می‌شود.

...

گزینه دیگری که در اینجا مطرح می‌شود، «فعال‌سازی در روز مشخص شده»^۱ است که در آن نودها در یک روز از پیش تعیین شده به اعمال [قوانین جدید] می‌پردازند. این روش نسبت به روش فعال‌سازی از راه سیگنال اکثریت هش‌ریت به تخصیص زمان تدارکات^۲ بیشتری نیاز دارد ولی مزایای زیادی دارد و چه بسا ممکن است موازنه بهتری میان شرایط مختلف برقرار کند.

در روز ۱۲ مارس سال ۲۰۱۷ شاولین فرای پیشنهاد خود را به صورت رسمی ارائه کرد که با نام BIP148 شناخته می‌شود. هدف وادار کردن ماینرها برای اعلام پشتیبانی از اجرای سگویت بر اساس یکی از قوانین اجماع، و در نتیجه فعال کردن آن بود. به نوعی می‌توان گفت که این پیشنهاد خود یک سافت فورک بود که یک سافت فورک دیگر را فعال می‌کرد. ماینرها می‌بایست از تاریخ ۱ اوت سال ۲۰۱۷، یعنی حدوداً ۴ ماه و نیم دیگر برای اجرای سافت فورک سیگنال آمادگی می‌دادند. سپس این مسأله می‌توانست موجب فعال شدن سگویت، قبل از انقضاء پنجره فعال‌سازی^۳ آن شود. متن پیشنهاد BIP148 به شرح زیر است:

1 Flag day activation
2 Lead time
3 Activation window

انگیزه اجرا

سگویت سایز بلاک را افزایش می‌دهد، مشکل تغییرپذیری تراکنش‌ها^۱ را برطرف می‌کند، موجب آسانتر شدن فرآیند ارتقاء اسکریپت^۲ بیت کوین می‌شود، و فواید زیاد دیگری را با خود به همراه می‌آورد.

امیدواریم که ماینرها با فعال‌سازی زود هنگام سگویت و قبل از مؤثر واقع شدن BIP148 نسبت به آن واکنش مثبت نشان دهند. در غیر این صورت BIP148 موجب فعال‌سازی اجباری نسخه فعلی فعال‌سازی سگویت، قبل از پایان نیمه شب ۱۵ نوامبر ۲۰۱۷ خواهد شد.

مشخصات

همه زمان‌ها بر اساس میانگین زمان سپری شده^۳ مشخص شده‌اند.

اگر روش فعلی فعال‌سازی سگویت تا دوره زمانی^۴ ۱۵۰۱۵۴۵۶۰۰ بر روی شبکه قفل^۵ یا فعال نشده باشد، این BIP در فاصله زمانی بین نیمه شب ۱ اوت ۲۰۱۷ (دوره زمانی ۱۵۰۱۵۴۵۶۰۰) و نیمه شب ۱۵ نوامبر ۲۰۱۷ (دوره زمانی ۱۵۱۰۷۰۴۰۰۰) فعال خواهد بود. در صورت قفل شدن سگویت این BIP غیرفعال خواهد شد.

در زمان فعال بودن این BIP، سه بیت اول متغیر nVersion و متغیر bit در سربرگ همه بلاک‌ها باید (بر اساس روش فعال‌سازی فعلی سگویت) ۰۰۱ باشد (۱<<۱). بلاک‌هایی که این اصول را رعایت نکنند پذیرفته نخواهند شد (نودهای

1 Transaction malleability
2 Script
3 Median past time
4 Epoch time
5 locked-in

اعمال کننده قوانین BIP148 این بلاک را به شبکه نظیر-به-نظیر بیت کوین رله نخواهند کرد. - م).

این ایده از نظر طرفداران بلاک‌های کوچک بسیار بحث‌برانگیز و یک حرکت بسیار پرخطر بود. اول اینکه شعار طرفداران بلاک‌های کوچک تا این مرحله دعوت به صبر و آرامش و تغییر قوانین اجماع در نهایت آرامش و ایمنی بود. این روش ارتقاء بسیار خطرناک بود، ماینرها می‌بایست سیگنال حمایت از اجرای سگویت را به شبکه ارسال می‌کردند و تخطی از آن می‌توانست موجب ایجاد شکاف در زنجیره بلاک بیت کوین شود. دومین مسأله‌ای که موجب خطرناک بودن روش BIP148 UASF می‌شد این بود که اگر شکست می‌خورد - که بسیار هم محتمل به نظر می‌رسید - می‌توانست موجب آن شود که ابتکار عمل در دستان طرفداران بلاک‌های بزرگ قرار گیرد. در این مرحله از مناقشه طرفداران بلاک‌های بزرگ به چندین جناح تقسیم شده بودند: به عنوان مثال، گروهی از آن‌ها معتقد بودند که کریگ رایت، ساتوشی است و برخی دیگر فکر می‌کردند که او یک کلاهبردار است. گروهی بودند که معتقد بودند Bitcoin Unlimited ایده قرص و محکمی است و در مقابل گروهی بودند که فکر می‌کردند BU معایبی دارد. و در نهایت افرادی بودند که بیت کوین را ترک کرده بودند تا ICO¹ پروژه‌های خود را راه‌اندازی کنند، و در مقابل کسانی بودند که همچنان بر روی بیت کوین تمرکز داشتند. با این حال انصافاً باید بگوییم که طرفداران بلاک‌های کوچک تا این مرحله همچنان با یکدیگر متحد بودند. این یک نقطه قوت مهم برای آن‌ها محسوب می‌شد و موجب شد بتوانند مقبولیت زیادی در این مناقشه کسب کنند. این حرکت بحث‌برانگیز طرفداران بلاک‌های کوچک در انتخاب روش UASF خطرناک بود، چون ممکن بود آن‌ها را به دو گروه تقسیم کند و از رسیدن به اهدافشان باز دارد.

1 Initial coin offering

به عنوان مثال گرگوری مکسول، یکی از تاثیرگذارترین نظریه پردازان گروه طرفداران بلاک‌های کوچک با UASF مخالفت، و دیدگاه خود را در تاریخ ۱۴ آوریل سال ۲۰۱۷ به روشنی در یک ایمیل بیان کرد:

دلایل من برای مخالفت با روش UASF BIP148 دقیقاً همان دلایلی است که به موجب آن‌ها از سگویت پشتیبانی می‌کنم؛ بخشی از ارزشمند بودن بیت کوین به دلیل امنیت و ثبات بالای آن است و سگویت طوری با دقت طراحی شده تا بتواند از یکپارچگی مهندسی بیت کوین پشتیبانی و آن را تقویت کند، به گونه‌ای که افراد بتوانند هم امروز و هم در آینده روی آن حساب کنند.

من فکر نمی‌کنم رویکرد پیشنهاد شده در BIP148 با استانداردهای تعیین شده توسط سگویت، یا روش‌های پیشنهاد شده از جانب جامعه توسعه‌دهندگان برای توسعه پروتکل بیت کوین مطابقت داشته باشد.

اشکال اصلی BIP148 این است که نودهایی که در حال حاضر برای پشتیبانی از سگویت اعلام آمادگی کرده‌اند ولی UASF نیستند را مجبور به فعال‌سازی می‌کند و یک اختلال جزئی حتمی را پدید خواهد آورد.

سگویت با دقت و به گونه‌ای طراحی و مهندسی شده بود تا ماینرهای قدیمی که تغییری نکرده بودند بتوانند بدون هیچگونه وقفه‌ای پس از اعمال شدن سگویت بر روی شبکه به کار خود ادامه دهند.

نودهای قدیمی تراکنش‌های سگویتی را به بلاک‌ها اضافه نمی‌کنند، بنابراین بلاک‌های آن‌ها حتی با وجود اینکه از سگویت پشتیبانی نمی‌کنند، معتبر است. آن‌ها می‌توانند طبق برنامه زمان‌بندی خود نرم‌افزارشان را به‌روزرسانی کنند. تنها خطری که این ماینرها را تهدید می‌کند این است که ممکن است بر روی یک

بلاک نامعتبر کار کنند و این ریسکی است که بسیاری از ماینرها اغلب با بکار بستن روش مخفی ماین کردن^۱ پذیرفته‌اند.

از نظر من این روشِ بدی نیست و مهندسی آن از خیلی از روش‌های دیگری که بسیاری از آلت کوین‌ها بکار می‌بندند بهتر است، ولی مطابق با استانداردهای معمول ما نیست. من به انگیزه‌های نویسندگان BIP148 احترام می‌گذارم. اگر هدف ما این باشد که سگویت را در سریع‌ترین زمان ممکن فعال کنیم، در این صورت استفاده از بیشتر از ۸۰ درصد نودهای موجود که از سگویت پشتیبانی می‌کنند بسیار مفید است.

اما هدف ما نباید فعال‌سازی سگویت در سریع‌ترین زمان ممکن باشد - همیشه یک آلت کوین متمرکز یا توسعه‌دهندگان بی‌پروا وجود دارند که می‌توانند سریع‌تر از ما از یک قابلیت پشتیبانی کنند - ولی اگر ما این هدف را انتخاب کنیم وجه تمایز ما در مهندسی پروژه و همچنین پایداری شبکه تضعیف خواهد شد.

«هدف اول باید این باشد که ضرری به سیستم وارد نشود». ما تا جایی که می‌توانیم باید مکانیزم‌هایی را بکار ببندیم که کمترین ضرر را به سیستم می‌رسانند، و پیشنهاد BIP148 برای این کار مناسب نیست. مشاهده می‌شود برخی از افراد که توسعه‌دهنده نیستند در سایت ردیت و مشابه آن حتی قابلیت سرگردان کردن اجباری^۲ بلاک‌ها در BIP148 را یک مزیت می‌دانند و معتقدند می‌تواند برای تنبیه ماینرهایی که رفتار درستی ندارند به کار گرفته شود. من با این دیدگاه به شدت مخالف هستم.

البته من با مفهوم کلی UASF مخالفتی ندارم ولی به‌طور کلی یک سافت فورک (از هر نوع که باشد) لزوماً نباید در کار ماینینگ بیت کوین اختلالی بوجود آورد، همانطور که سگویت نمی‌آورد. در گذشته UASF روش اصلی اجرای سافت فورک

1 Spy-mining

2 Forced orphaning blocks

بوده و ساتوشی فقط از این روش استفاده می کرده است. سافت فورک P2SH بر اساس رسیدن به یک روز خاص فعال شده، و همه سافت فورک های قبل از آن هم بر پایه رسیدن به یک زمان خاص و یا شماره بلاک خاص فعال شده اند. ما روش فعال سازی مبتنی بر آمادگی ماینرها را به عنوان بخشی از روند ایجاد ثبات و هماهنگی بیشتر میان جامعه فعالان بیت کوین معرفی کردیم. اینکه UASF به عنوان یک پدیده جدید معرفی شود موضوع عجیبی است.

مهم این است تا جایی که امکان دارد سعی کنیم تصمیمات هیكچدام از فعالان اکوسیستم مانند توسعه دهندگان، صرافی ها، اتاق های گفتگو، یا تولید کنندگان دستگاه های استخراج تأثیری بر روی کاربران نداشته باشد. در نهایت اثربخشی قوانین شبکه بیت کوین به این دلیل است که جمیع کاربران آنها را بر روی شبکه اعمال می کنند. این چیزی است که به بیت کوین معنا می دهد و چیزی است که باعث می شود مردم بتوانند به آن اعتماد کنند: اینکه قوانین به سادگی قابل تغییر نیستند.

پیشنهاد های UASF دیگری هم وجود دارند که ایجاد اختلال اجباری در آنها مطرح نیست. روش آنها به گونه ای طراحی شده است که همچنان به ماینر هایی که به نسخه UASF به روزرسانی نکرده اند اجازه می دهد که به کار خود ادامه دهند. من فکر می کنم این روش بهتری است. ممکن است به زمان بیشتری برای اجرای آنها نیاز باشد ولی از نظر من این ایرادی ندارد.

ما باید صبور باشیم. بیت کوین سیستمی است که باید در طولانی مدت دوام بیاورد و به توانمند سازی بشر ادامه دهد. این اختلافات در ده سال آینده فراموش خواهند شد. اما چیزی که اهمیت دارد شهرتی است که ما برای حفظ ثبات و یکپارچگی بیت کوین به عنوان پولی که مردم می توانند روی آن حساب کنند، کسب می کنیم.

این بحث‌ها پیش می‌آید تا به افراد یادآوری شود بیت کوین به راحتی و بخاطر خوشایند افراد تغییر نمی‌کند، حتی اگر نیت این افراد خیر باشد. همچنین اینکه چگونه این امر باعث شده که روش مدیریت بیت کوین با همه پول‌های دیگری که در دنیا وجود دارند متفاوت باشد.

بنابراین صبر داشته باشید و به دنبال راه‌های میان‌بر نگردید. سگویت برای بیت کوین یک پیشرفت بسیار خوب است و ما باید قدر آن را با پرهیز از عجله بدانیم و از بهترین راه ممکن فعالش کنیم.

یکی از اولین توسعه‌دهندگان شناخته شده بیت کوین که از UASF پشتیبانی می‌کرد، لوک داش‌یر^۱ بود، او اولین کسی بود که روش اجرای سگویت به صورت سافت فورک را کشف کرد. لوک با پشتیبانی از یک روش اجماع فرعی که تقریباً مورد حمایت هیچ کس نبود، خود را در معرض خطر بزرگی قرار داد. با این حال با توجه به شخصیتی که داشت به نظر می‌رسید این مسأله او را آزار نمی‌دهد. یکی از برجسته‌ترین توسعه‌دهندگان در گروه طرفداران بلاک‌های کوچک پیتر والای^۲ که بیشتر کدهای نرم‌افزاری سافت فورک سگویت را او نوشته بود نیز با پیشنهاد BIP-148 مخالف بود. او در ماه مه سال ۲۰۱۷ در گفتگوی اینترنتی که با لوک داشت، اینگونه نظر خود را اظهار کرد:

پیش‌بینی می‌کنم که نودهای اقتصادی مطرح چند ساعت پس از اینکه ببینند BIP148 مورد حمایت هش‌ریت قابل توجهی قرار نگرفته است، از آن رویگردان شوند.

...

لوک داش‌یر من فکر می‌کنم تو دیوانه‌ای

1 Luke Dashjr
2 Pieter Wuille

لازم به ذکر است که پیتر بلافاصله از اینکه او را دیوانه خطاب کرده بود، عذرخواهی کرد. با توجه به نظرات توسعه‌دهندگانمانند پیتر و گرگوری، اکنون بسیار بعید به نظر می‌رسید که Bitcoin Core نرم‌افزاری که BIP 148 در آن پیاده‌سازی شده باشد را منتشر کند. اگر اجرای طرح UASF به نتیجه می‌رسید، طرفداران بلاک‌های کوچک از قضا می‌بایست یک نرم‌افزار فرعی با قوانین اجماع متفاوت را اجرا کنند، شبیه به کاری که طرفداران بلاک‌های بزرگ می‌خواستند با اجرای Bitcoin Classic، Bitcoin XT و Bitcoin Unlimited انجام دهند.

دقیقاً همین اتفاق افتاد و سرانجام لوک نرم‌افزاری که BIP 148 در آن پیاده‌سازی شده بود را با نشانگر ' /Satoshi:0.14.2/UASF-Segwit:0.3(BIP148) ' منتشر کرد. همچنان کاربران ترغیب شدند تا [نسخه اصلی] Bitcoin Core را اجرا و نشانگر آن را به گونه‌ای تغییر دهند تا از این روش بتوانند حمایت خود از BIP148 را اعلام کنند، روشی که به نظر می‌رسد در آن زمان متداول بوده است. برخی استدلال می‌کردند که این روش مناسبی نیست چون نسخه اصلی Bitcoin Core قوانین BIP148 را واقعاً پیاده‌سازی نکرده است، اما برخی دیگر پاسخ می‌دادند که با این کار می‌خواهیم قصد خود را بیان و نشان دهیم که کاربران قبل از روز اول اوت نرم‌افزار خود را ارتقاء خواهند داد. برخی اشاره می‌کردند که این کار ریاکاری است چون این دقیقاً همان رفتاری است که طرفداران بلاک‌های کوچک برای آن، گروه مقابل را مورد تمسخر و انتقاد قرار می‌دادند.

در اوایل ماه مه سال ۲۰۱۷ من با یکی از برجسته‌ترین طرفداران پشت صحنه UASF در هنگ کنگ گفتگو کردم. او توسعه‌دهنده‌ای بود که کُد نرم‌افزاری UASF را نوشته بود و از چندین وب‌سایت که در حمایت از UASF کمپین‌های تبلیغاتی برگزار می‌کردند، نگهداری می‌کرد. من برای او توضیح دادم که UASF خطرناک است و اهمیت صبر در مواجهه با قوانین اجماع پروتکل بیت‌کوین را برای او شرح دادم. او جوابی طولانی و محکم به من داد. گفت: «در مواقع عادی حرف شما درست است» و تأکید کرد «ولی

1 User agent Id/tag

اکنون شرایط عادی نیست و ما در جنگ هستیم». او اینچنین ادامه داد: «بیت کوین در شرایط بحرانی قرار دارد. شرکت Bitmain از آسیب پذیری ASICBoost سوءاستفاده می کند، سگویت این مشکل را برطرف می کند و ما باید به سرعت این مسأله را حل کنیم. این یک وضعیت اضطراری است، بنابراین ما وقت کافی برای بکار بستن روش عادی و صبر پیشه کردن نداریم». وی در ادامه توضیح داد که شرایط جنگی به ما امکان انتخاب زمان مناسب را نمی دهد. او از اینکه تنها چند ماه دیگر به فعال سازی UASF باقی مانده است خوشحال بود، اما توضیح داد که طرفداران بلاک های کوچک در حال حاضر دست بالا را در جنگ دارند و هیچ تضمینی برای ادامه یافتن این برتری وجود ندارد. او اظهار کرد: «اکنون که قدرتمند هستیم، زمان بیرون کشیدن سلاح های بزرگ است». وی ادامه داد: «ما چاره دیگری نداریم و باید هرچه زودتر برای حفظ بیت کوین اقدام کنیم. باید محکم ترین ضربه را به آن ها بزنیم و قاطعانه در این جنگ پیروز شویم. اگر این کار را نکنیم، ممکن است شکست بخوریم و در این صورت بیت کوین از بین خواهد رفت». به نظر می رسد این توسعه دهنده همه سناریوهای محتمل را مورد بررسی قرار داده و در نهایت متقاعد شده است که BIP148 مؤثر خواهد بود. از نظر او این واقعیت که BIP148 یک سافت فورک و بخشی از قوانین اجماع فعلی بود، یک مزیت قابل توجه به حساب می آمد و می توانست برای مجبور کردن ماینرها در پذیرفتن زنجیره BIP148 کارآمد باشد. دیدگاه او این بود که BIP148 یک تهدید به حساب می آمد و ماینرها به قصد کم کردن فشارها سگویت را فعال خواهند کرد، به گونه ای که سافت فورک BIP148 هرگز در اوت ۲۰۱۷ فعال نخواهد شد. «BIP 148 طوری پیاده سازی شده است که اگر سگویت بر روی زنجیره اعمال شده باشد، فعال نخواهد شد.»

در حالی که اوایل کار این ایده در گروه طرفداران بلاک های کوچک بحث برانگیز بود، اما تا ماه مه سال ۲۰۱۷ این روش جذابیت قابل توجهی پیدا کرده بود. حالا کانال اژدهایان پر بود از کمپین های تبلیغاتی که از BIP148 و UASF پشتیبانی می کردند. تا جایی که سمسون ما^۱ کلاه نقاب داری را تولید کرده بود و می فروخت که عبارت UASF در مقابل

1 Samson Mow

آن گلدوزی شده بود. این کلاه معمولاً شبیه به کلاه‌های نظامی بود و طرفداران بلاک‌های کوچک آن را در کنفرانس‌ها و رویدادهای بیت کوین بر سر می گذاشتند تا حمایت خود را از این کارزار خودجوش نشان دهند. در این مرحله بحث درباره UASF فقط در جامعه بلاک‌های کوچک در جریان بود و طرفداران بلاک‌های بزرگ و فعالان بزرگ صنعت ارزهای دیجیتال به آن توجهی نمی کردند. تا اینکه بالاخره در اواخر ماه مه سال ۲۰۱۷ این ایده به صورت گسترده‌تری در خارج از اردوگاه طرفداران بلاک‌های کوچک مورد بررسی قرار گرفت.

با بررسی موضوع از نگاه تاکتیکی می توان گفت طرفداران بلاک‌های بزرگ در درک UASF و واکنش نشان دادن به آن کند عمل کردند. طرفداران بلاک‌های بزرگ باید این شکاف بالقوه که در اردوگاه بلاک‌های کوچک پدید آمده بود را هرچه زودتر رصد، توجهات را به آن جلب، و از آن بهره‌برداری می کردند. دقیقاً به همان صورت که طرفداران بلاک‌های کوچک از شکاف‌های پدید آمده در اردوگاه طرفداران بلاک‌های بزرگ بهره‌برداری می کردند. ولی در عوض آن‌ها UASF را نادیده گرفتند. در اواخر ماه مه من با یکی از برجسته‌ترین طرفداران بلاک‌های بزرگ درباره UASF گفتگو کردم. او به من گفت باور نمی کند گروگوری مکسول واقعاً با UASF مخالف باشد و این رفتارها ناشی از «دروغ‌ها و بازی‌های همیشگی» او است. به نظر می‌رسید که در این مرحله، سطح بی‌اعتمادی بسیار زیاد به علاوه درک متفاوتی که طرفداران بلاک‌های بزرگ از نحوه کار بیت کوین داشتند در نهایت منجر به این شد که آن‌ها نتوانند حرکت بعدی طرفداران بلاک‌های کوچک را پیش‌بینی کنند. به نظر می‌رسید که سرانجام طرفداران بلاک‌های کوچک حرکتی انجام دادند و یک راه نفوذ برای گروه مقابل باز گذاشته‌اند. طرفداران بلاک‌های بزرگ برای ادامه این جنگ باید از این راه نفوذ حداکثر استفاده را می کردند ولی به نظر می‌رسید آن‌ها نمی‌دانند چه باید بکنند.

به نظر می‌رسید طرفداران بلاک‌های بزرگ واقعاً نگران UASF بودند. در آغاز این جنگ آن‌ها اندازه و قدرت نفوذ اردوگاه طرفداران بلاک‌های کوچک را بسیار دست پایین گرفته بودند و انتظار داشتند به آسانی در این جنگ پیروز شوند. طرفداران بلاک‌های بزرگ اغلب گروه مقابل را بی‌اهمیت و ساده‌لوح قلمداد می‌کردند. در این مرحله و پس از تجربه سه تلاش ناموفق برای هارد فورک و شکست‌هایی که آن‌ها را غافلگیر کرد، اکنون به نظر می‌رسید اغلب طرفداران بلاک‌های بزرگ قدرت و نفوذ طرفداران بلاک‌های کوچک را دست بالا می‌گرفتند. در حقیقت، طرفداران بلاک‌های کوچک ضعیف‌تر از چیزی بودند که آن‌ها فکر می‌کردند. دلیل اصلی موفقیت آن‌ها در شکست طرفداران بلاک‌های بزرگ تا آن زمان درک بهتر آن‌ها از بیت کوین نسبت به گروه مقابل، اشتباهات تاکتیکی اردوگاه طرفداران بلاک‌های بزرگ، و تاب‌آوری ذاتی بیت کوین در مقابله با تغییر قوانین پروتکل بود. طرفداران بلاک‌های بزرگ به دلیل درک ناقصی که داشتند دلیل شکست خود را مانورهای زیرکانه طرفداران بلاک‌های کوچک که از نظر آن‌ها حيله‌گر و قدرتمند بودند می‌دیدند. بنابراین به نظر می‌رسید طرفداران بلاک‌های بزرگ به طرفداران بلاک‌های کوچک احترام می‌گذاشتند و بسیاری از آن‌ها از UASF که به نظر آن‌ها حرکت بزرگ بعدی طرفداران بلاک‌های کوچک بود، هراسان بودند. آن‌ها به فرصت تاکتیکی‌ای که UASF برای آن‌ها فراهم می‌کرد توجهی نمی‌کردند، فرصتی که نتوانستند از آن بهره‌ای ببرند.

در این مرحله، هیچ صرافی‌ای از UASF حمایت نمی‌کرد. اغلب مدیران عامل صرافی‌هایی که من در آن زمان با آن‌ها صحبت کردم یا انتظار داشتند UASF شکست بخورد، یا اصلاً نمی‌دانستند چیست. سطح حمایت بازیگران اقتصادی فعال در بیت کوین در خارج از اردوگاه طرفداران بلاک‌های کوچک بسیار ناچیز بود. این یک حرکت مخاطره‌آمیز از طرف طرفداران بلاک‌های کوچک بود و من فکر می‌کردم ممکن است آن‌ها روی زنجیره‌ای باقی بمانند که اثبات کار کمتری دارد و به‌عنوان بیت کوین پذیرفته نمی‌شود. آنچه طرفداران بلاک‌های بزرگ باید در نظر می‌گرفتند انتشار یک «سافت فورک در

تقابل^۱ با UASF به منظور ممنوع کردن سیگنال‌دهی برای BIP148 در بلاک‌ها بود. این زنجیره احتمالاً حمایت اکثریت فعالان اقتصادی و اکثریت هش‌ریت را دارا بود و این اطمینان را حاصل می‌کرد که یک شکاف کامل^۲ در زنجیره بوجود خواهد آمد و زنجیره‌ای که در مقابل UASF پدید می‌آمد از خطر حذف شدن^۳ مصون بود. با این حال طرفداران بلاک‌های بزرگ این‌گونه فکر نمی‌کردند. آن‌ها خواهان یک هارد فورک برای افزایش سایز بلاک بودند و تخصص یا تمایلی برای پیاده‌سازی یک سافت فورک در مقابل BIP148 نداشتند.

جهان‌وو از کمپین‌هایی که برای UASF برگزار می‌شد بسیار عصبانی به نظر می‌رسید. از نظر وی UASF روایت او را مبنی بر اینکه قوانین پروتکل بیت‌کوین بیشترین تأثیر را از ماینرها می‌پذیرند، زیر سؤال می‌برد. در تاریخ ۲۸ مه سال ۲۰۱۷ جهان تصویری از قربانیان قتل عام جونزتاون^۴ به همراه هشتگ #UASF را توثیق کرد. خشم و هراس او از UASF بسیار جدی به نظر می‌رسید. در اواسط ماه ژوئن، صرافی ViaBTC که مرتبط با جهان‌وو بود معاملات آتی BIP148 را روی صرافی خود لیست کرد. این ایده شبیه به کاری بود که صرافی Bitfinex چند ماه پیش با لیست کردن توکن Bitcoin Unlimited انجام داده بود. این تلاشی برای تضعیف BIP148 بود، درست مانند کاری که معاملات آتی شرکت Bitfinex با Bitcoin Unlimited کرده بود. اگرچه شرایط این قرارداد کاملاً عجیب و غریب بود و احتمال تقلب در آن وجود داشت. شرایط اینگونه تعریف شده بود که بازپرداخت سرمایه‌گذاری افراد روی توکن BIP148 فقط در صورتی انجام می‌شد که زنجیره BIP148 و زنجیره فعلی (غیر BIP148) در کنار هم ادامه پیدا می‌کردند. این مشخصاً چیزی نبود که طرفداران BIP148 می‌خواستند. آن‌ها معتقد بودند که زنجیره قوانین اصلی بیت‌کوین متوقف خواهد شد، خصوصاً به دلیل اینکه زنجیره اصلی نسبت به حذف شدن در مقابل زنجیره BIP148 آسیب‌پذیر بود. بنابراین سرمایه‌گذاری روی توکنی که به ادامه یافتن زنجیره اصلی (غیر BIP148) وابسته بود

1 Counter soft fork
2 Clean split
3 Wipeout
4 Jonestown

برای حامیان BIP148 چندان منطقی نبود. این قرارداد نتوانست به حجم معاملات قابل توجهی دست پیدا کند و به نظر می‌رسد که در خدشه‌دار کردن BIP148 هم موفق نبود.

در ۱۴ ژوئن سال ۲۰۱۷ شرکت Bitmain در یک پست در وبلاگ خود طرح واکنش احتمالی خود در پاسخ به UASF را تشریح کرد:

پیشنهاد BIP148 برای صرافی‌ها و سایر کسب و کارهای فعال در بیت کوین بسیار خطرناک است. هیچ نشانه‌ای از حمایت قابل توجه [بازیگران] اقتصادی از BIP148 مشاهده نمی‌شود و میزان حمایت از آن زمانی که بر روی بلاک چین فعال شود را تنها می‌توان از طریق حدس و گمان تخمین زد. فعالیت ماینرهایی که از BIP148 حمایت می‌کنند ممکن است هر لحظه و بدون اطلاع قبلی متوقف شود، و ممکن است سرمایه‌گذارانی که تصمیمات خود را براساس تبلیغاتی که حول BIP148 شکل گرفته می‌گیرند، تمام سرمایه خود را از دست بدهند. هر صرافی که بعد از اجرای فورک تصمیم به پشتیبانی از زنجیره UASF بگیرد، باید عواقب آن را هم بپذیرد.

...

زنجیره UASF خطر از بین رفتن زنجیره اصلی را با خود به همراه دارد. اگر برنامه‌ای نداشته باشیم، تمام فعالیت‌های اقتصادی که بعد از فورک UASF روی زنجیره اصلی ثبت شده‌اند با خطر از بین رفتن روبرو هستند. این عواقب فاجعه‌باری برای کل اکوسیستم بیت کوین به همراه دارد. UASF حمله به کاربران و شرکت‌هایی است که با فعال کردن سگویت بدون افزایش سائز بلاک مخالف هستند، [قید افزایش سائز بلاک] بند مهمی در پیمان‌نامه هنگ کنگ است که جامعه جهانی بیت کوین در فوریه سال ۲۰۱۶ روی آن به توافق رسیدند.

...

این طرحی برای فعال سازی هارد فورک از جانب کاربران^۱، یا UAHF است.

...

شرکت Bitmain درصد مشخصی از زیرساخت خود را به تأمین هشریت لازم اختصاص می‌دهد و حداقل ۷۲ ساعت بعد از اجرای فورک BIP148 به عملیات استخراج بر روی زنجیره [اصلی] (غیر BIP148) ادامه خواهد داد. شرکت Bitmain به احتمال زیاد بلاک‌های ماین شده را روی شبکه بیت کوین منتشر نخواهد کرد، مگر اینکه شرایط خاصی فراهم شود. این بدان معنی است که Bitmain ابتدا این زنجیره را به صورت خصوصی ماین می‌کند. ما قصد داریم در شرایط زیر بلاک‌های ماین شده را برای عموم منتشر کنیم (این لیست کامل نیست):

هنگامی که زنجیره BIP148 فعال شود و متعاقباً مورد حمایت قابل توجهی از جانب ماینرها قرار بگیرد. یعنی بعد از اینکه BIP148 با موفقیت زنجیره را فورک کند.

یا هنگامی که بازار برای اجرای هارد فورکی که سایز بلاک را افزایش دهد آماده باشد، و منطق اقتصادی ما را به استخراج چنین بلاک‌هایی سوق دهد، مثلاً اگر قیمت بلاک‌های بزرگ بالا رود.

یا اینکه مقدار قابل توجهی از ماینرها به طور عمومی یک زنجیره از بلاک‌های بزرگ را ماین کنند و ما تصمیم بگیریم که ادامه کار بر روی این زنجیره از نظر ما منطقی است. در چنین شرایطی ما پیوستن به آن زنجیره را نیز در نظر خواهیم

1 User activated hard fork

گرفت و از خیر زنجیره‌ای که [به صورت خصوصی] ماین کرده‌ایم خواهیم گذشت تا خطر تغییر آرایش^۲، این زنجیره UAHF عمومی را تهدید نکند.

وقتی شرکت Bitmain به صورت عمومی شروع به ماین زنجیره UAHF کند، آن را به طور مداوم استخراج خواهیم کرد و انگیزه‌های اقتصادی کوتاه مدت را نادیده خواهیم گرفت. ما معتقدیم نقشه راهی که شامل گزینه‌ای برای تنظیم سایز بلاک باشد در نهایت به نفع کاربران است و طبق پیش‌بینی ما در بلند مدت قیمت بالاتری پیدا خواهد کرد.

برنامه Bitmain این بود که تقریباً همزمان با فعال شدن UASF، هارد فورکی را به منظور افزایش سایز بلاک بر روی زنجیره بیت کوین اجرا کند. این طرح شامل برنامه‌ای برای افزایش سایز بلاک بود. محدودیت سایز بلاک در اوت سال ۲۰۱۷، ۲ مگابایت بود. سپس به تدریج و در مراحل که از پیش تعیین شده بود در اوت سال ۲۰۱۹ به ۱۶/۸ مگابایت می‌رسید. به نظر می‌رسید این طرح تهدیدی باشد که طرفداران UASF را نشانه گرفته است. طرفداران بلاک‌های بزرگ به هارد فورک خود می‌رسیدند در حالی که فکر می‌کردند گروه مقابل به شدت تلاش می‌کند تا مانع دستیابی به آن شود.

اگرچه به نظر می‌رسید جیهان و و این مسأله را درک نکرده است که این طرح در واقع بسیار مطلوب طرفداران UASF بود، این در واقع بدان معنی بود که به احتمال زیاد زنجیره UASF اثبات کار بیشتری نسبت به زنجیره اصلی (غیر BIP148) به خود اختصاص می‌داد چون برنامه Bitmain این بود که کار را بر روی یک زنجیره جایگزین جدید ادامه دهد. علاوه بر این Bitmain قصد داشت زنجیره جدید هارد فورک را به مدت ۷۲ ساعت به صورت خصوصی ماین کند. اگر آن‌ها قصد داشتند قدرت هش ریت را به سمت استخراج این زنجیره هارد فورک جدید سوق دهند، با توجه به اینکه هیچ کس قادر به دریافت این زنجیره [خصوصی] نبود، یا نرم‌افزاری وجود نداشت که از آن پشتیبانی کند، و صرافی‌ها

نیز قادر به پشتیبانی از آن نبودند، این حرکت بسیار حرکت بدی بود. مشخص نیست چه انگیزه‌ای باعث انتشار این پست در وبلاگ این شرکت شده بود. به نظر می‌رسد جیهان و و به شدت عصبانی شده و به سرعت طرحی را برای ناکام کردن مخالفانش تهیه کرده است، ولی از جهات مختلف آن را در نظر نگرفته است. جیهان و و برای رسیدن به این هدف باید اعلام می‌کرد که در صورت اجرای UASF او همچنان به استخراج بر روی زنجیره اصلی بیت کوین ادامه خواهد داد و همچنین طرحی را برای جلوگیری از موفق شدن UASF اجرا خواهد کرد. هرچند اگر او این روش را انتخاب می‌کرد چاره‌ای جز ادامه دادن زنجیره ۱ مگابایتی بیت کوین نداشت، و بنابراین احساس می‌کرده که گزینه‌ای جز این ندارد.

طرفداران بلاک‌های کوچک در کانال اژدهایان این پست وبلاگ شرکت Bitmain را با خوشحالی جشن گرفتند، چون تقریباً از پیروزی کامل خود اطمینان پیدا کرده بودند. با این حال برخی از آن‌ها رویکرد محتاط‌تری نسبت به آن داشتند و معتقد بودند «صرف اینکه جیهان بگوید کار احمقانه‌ای را انجام خواهد داد به این معنی نیست که او این کار را خواهد کرد». به نظر من انتخاب این مواضع محتاطانه‌تر، رویکرد مناسب‌تری بود. با نزدیک شدن به اول اوت، احتمالاً جیهان متوجه بی‌اثر بودن این روش می‌شد و روش مؤثرتر دیگری را برمی‌گزید.

با نزدیک شدن به ضرب‌العجل UASF طرفداران بلاک‌های بزرگ در موضع ضعف بودند، چون نمی‌دانستند چه واکنشی باید از خود نشان دهند. تقریباً هیچ گزینه مناسبی هم برای آن‌ها باقی نمانده بود. به نظر می‌رسد سرانجام طرفداران بلاک‌های بزرگ با شکست سختی روبرو خواهند شد و آن‌ها از این موضوع باخبر بودند. به همین خاطر باید برای حفظ ظاهر کاری از پیش می‌بردند.

فصل هجدهم

توافق نیویورک

در تاریخ ۲۲ مه سال ۲۰۱۷ میلادی، جلسه‌ای با هدف حل منازعات موجود توسط بری سیلبرت^۱ از گروه ارز دیجیتال (DCG) در شهر نیویورک برگزار شد. یکی از شرکت کنندگان در این نشست جیهان وو بود. حاصل این نشست توافق دیگری بود که با عنوان توافق نامه نیویورک (NYA) شناخته می‌شود و متن آن به شرح زیر است:

ما می‌پذیریم بدون فوت وقت از دو ارتقاء که قرار است بر اساس پیشنهاد اولیه Segwit2Mb به‌طور همزمان بر روی شبکه بیت کوین فعال شود حمایت کنیم:

سگویت روی آستانه ۸۰٪ و با سیگنال روی بیت شماره ۴ فعال شود

ظرف شش ماه یک هارد فورک ۲ مگابایتی بر روی شبکه اجرا شود

1 Barry Silbert

ما همچنین به تحقیق و توسعه مکانیزم‌های فنی برای بهبود فرآیند سیگنال‌دهی در جامعه بیت کوین و ایجاد ابزارهای ارتباطی به منظور ایجاد هماهنگی بیشتر میان فعالان این حوزه در امر طراحی، تلفیق، و استقرار راه‌حل‌های ایمن برای افزایش ظرفیت بیت کوین، متعهد می‌شویم.

ما از همه شرکت‌ها، استخراج‌کنندگان، توسعه‌دهندگان، و کاربران دعوت می‌کنیم برای آماده‌سازی بیت کوین برای آینده به ما ملحق شوند و در این راه به ما کمک کنند.

شرکت‌هایی که این توافق‌نامه را امضاء کرده‌اند نماینده حجم بزرگی از فعالان حوزه بیت کوین هستند. تا تاریخ ۲۵ مه، این گروه شامل:

۵۸ شرکت که در ۲۲ کشور قرار دارند

۸۳/۲۸ درصد هشریت شبکه

گردش مالی ماهانه ۵/۱ بیلیون دلار

۲۰/۵ میلیون کیف پول بیت کوین

گذشته از آن، تا روز ۲۴ ماه مه شرکت‌های زیر متعهد شده‌اند که خدمات فنی و مهندسی لازم برای تست و پشتیبانی نرم‌افزار را فراهم، و همچنین در انجام امور لازم برای ارتقاء نرم‌افزارها به شرکت‌ها کمک‌رسانی کنند:

Abra | BitClub Network | Bitcoin.com | BitFury | BitGo |
Bitmain | BitPay | Blockchain | Bloq | BTCC | Circle | Ledger |
RSK Labs | Xapo

اگر مایل به ارائه خدمات فنی مهندسی هستید لطفاً به ما اطلاع دهید تا نام تیم شما هم در لیست بالا قرار گیرد.

این توافق بر اساس پیشنهادی بود که قبلاً در مارس سال ۲۰۱۷ توسط یکی از توسعه‌دهندگان و محققان بیت کوین سرجیو لرنر^۱ ارائه شده بود. ایده اصلی این بود که هم سگویت بر روی شبکه فعال شود، هم بخش غیر سگویتی بلاک از طریق اجرای یک هارد فورک به ۲ مگابایت افزایش یابد. به گفته افراد نزدیک به بری سیلبرت، این پیشنهاد حکم یک مصالحه داشت؛ گروهی خواهان فعال شدن سگویت، و گروه دیگر خواهان اجرای یک هاردفورک بودند، با این روش هر دو گروه به خواسته‌شان دست پیدا می‌کردند. آن‌ها به من می‌گفتند که سیلبرت نگران به بن بست رسیدن اوضاع است و معتقد است باید برای ایجاد حرکت و پیشرفت کاری کرد. گویا نسخه اولیه این توافق‌نامه توسط ملت دمیرورس^۲، کارمند شرکت DCG تهیه شده است. این تفاهم‌نامه - شبیه به توافق‌نامه‌ای که یک ماه قبل برای لایت کوین منتشر شده بود - روشی برای مقابله با تهدیدهای بالقوه UASF بود و موجب جلوگیری از شرمساری هرچه بیشتر جهان و می‌شد.

تعداد و اهمیت امضاء کنندگان این توافق‌نامه بسیار چشمگیر بود. در مجموع ۵۸ امضاء کننده از جمله کوین اندریسن، Bitcoin.com (راجر ور)، شرکت Bitmain (جهان وو)، و صرافی کوین بیس (برایان آرمسترانگ) آن را امضاء کرده بودند. اگرچه بسیاری از این امضاء کنندگان (۳۳ نفر از آن‌ها) از اعضای پرتفوی شرکت DCG بودند، اما خارج از این گروه نیز صرافی‌ها و استخرهای استخراج زیادی وجود داشتند که از این توافق‌نامه اعلام حمایت کرده بودند. بدین ترتیب بسیاری از ناظران این فضا به این نتیجه رسیدند که مشکل سائز بلاک سرانجام برطرف، و اجرای موفقیت‌آمیز این توافق تقریباً اجتناب‌ناپذیر است. این توافق برای طرفداران بلاک‌های بزرگ - مخصوصاً در زمانی که در موضع ضعف بودند - یک دستاورد بسیار چشمگیر محسوب می‌شد و به نظر می‌رسید که

1 Sergio Lerner

2 Meltem Demirors

یک نقطه عطف بسیار مهم در این درگیری باشد. این حرکت موجب تغییر شرایط برای طرفداران بلاک‌های بزرگ شد و آن‌ها را از موضع ضعف بیرون آورد.

با این حال طرفداران بلاک‌های بزرگ کاملاً از این توافق رضایت نداشتند چون به هر حال سگویت -یعنی همان چیزی که علاقه‌ای به آن نداشتند- نیز در آن گنجانده شده بود. اما به نظر می‌رسید قادر است از عهده انجام یک کار برآید، و آن «اخراج Bitcoin Core» بود. در واقع راجر و به همین دلیل از آن حمایت می‌کرد. او مدعی بود اگرچه این توافق‌نامه را نمی‌پسندد، اما حداقل باعث خلاص شدن از شر Bitcoin Core می‌شود. برخی از طرفداران بلاک‌های بزرگ نسبت به این توافق مشکوک، و برخی دیگر از آن‌ها که افراطی‌تر می‌اندیشیدند با آن مخالف بودند. این توافق‌نامه متعهد می‌شد تا سگویت را قبل از هارد فورک بر روی شبکه فعال، و ظرف شش ماه هارد فورک را اجرا کند. در متن توافق آمده بود که هارد فورک و سافت فورک به‌طور همزمان بر روی شبکه استقرار پیدا می‌کنند، ولی ابتدا سافت فورک فعال می‌شود. برخی از طرفداران بلاک‌های بزرگ نگران بودند که ممکن است مرحله اول اتفاق بیفتد و امضاء کنندگان از اجرای مرحله دوم این توافق‌نامه سر باز بزنند.

طرفداران بلاک‌های کوچک در نشست نیویورک نماینده‌ای نداشتند و نظرات آن‌ها در این توافق‌نامه منعکس نشد. در این متن جملهٔ دوپهلوی عبارت متناقضی به چشم نمی‌خورد و به نظر می‌رسید کُل آن توسط طرفداران بلاک‌های بزرگ تهیه شده باشد. نکته قابل توجه اینکه در این توافق‌نامه هیچ اشاره‌ای به اینکه کنترل پروتکل بیت کوین در اختیار کاربران بیت کوین است و بدون پشتیبانی کاربران امکان تغییر قوانین شبکه وجود ندارد، نشده بود. حتی برای حفظ ظاهر هم حرفی از اهمیت نظرات کاربران در تغییر قوانین پروتکل بیت کوین در این توافق‌نامه به میان نیامده بود. شرایط به شکلی بود که گویی شرکت‌های بزرگ، قوانین را از بالا به پایین به کاربران بیت کوین تحمیل می‌کنند. اگر قرار بود بیت کوین به این روش کار کند، وجه تمایز اصلی آن زیر سؤال می‌رفت. به نظر

می‌رسید لابی و جلب رضایت کاربران قبل از فعال کردن فورک، برای امضاء کنندگان این توافق‌نامه اهمیتی نداشت. در عوض، بیشتر شبیه به یک تهدید یا اتمام حجت^۱ بود.

این روش علاوه بر تضعیف ارزش اصلی بیت‌کوین، تاکتیک بدی نیز بود. کاربران بیت‌کوین می‌خواستند کنترل بیت‌کوین در دست آن‌ها باشد و دوست نداشتند کسی به آن‌ها دستور دهد. بنابراین توافق نیویورک از نظر آن‌ها فرقی با Bitcoin XT و Bitcoin Classic و Bitcoin Unlimited نداشت. طرفداران بلاک‌های بزرگ دوباره همان اشتباه قدیمی را مرتکب شدند، منتهی این بار از حمایت بخش بزرگی از فعالان حوزه بیت‌کوین برخوردار بودند. با این حال نکته قابل توجه این است که در میان امضاء کنندگان این توافق‌نامه جای امضاء چند شرکت مهم و در حال رشد خالی بود. از همه مهم‌تر جای خالی شرکت Bitfinex - که شاید بتوان گفت در آن زمان مشهورترین شرکت اقتصادی فعال در حوزه بیت‌کوین بود - به چشم می‌آمد. دیگر شرکت‌های مهمی که در لیست امضاء کنندگان غایب بودند عبارتند از: Local Bitcoins (بزرگترین صرافی بدون واسطه بیت‌کوین در آن زمان)، Poloniex، شرکت BitMEX، و استخراج استخراج Slush.

قسمتی از متن این توافق‌نامه که روش فعال‌سازی سگویت را توضیح می‌داد از دید طرفداران بلاک‌های کوچک پنهان‌نماند و اشکالات آن به دقت مورد بررسی قرار گرفت. در این بخش آمده بود: «سگویت در آستانه ۸۰ درصدی و از طریق سیگنال‌دهی روی بیت ۴ فعال خواهد شد». این بی‌معنی بود چون سگویت از بیت شماره ۱، نه ۴ برای فعال شدن استفاده می‌کرد. ماینرها می‌توانستند از بیت شماره ۴ برای اعلام آمادگی برای فعال‌سازی سگویت استفاده کنند، ولی این کار منجر به فعال‌سازی سگویت نمی‌شد. ظاهراً و براساس گفتگویی که با یکی از شرکت‌کنندگان در جلسه داشتم، جیهان وو روی این مورد اصرار داشته است، شاید به این دلیل که ماه‌ها برای سیگنال دادن روی بیت ۱ تحت فشار بوده و

1 ultimatum

نمی‌خواسته به خواسته‌های طرفداران بلاک‌های کوچک تن دهد. با این حال فعال‌سازی سگویت با استفاده از بیت ۴ امکان‌پذیر نبود و دقیقاً مشخص نبود که چه اتفاقی خواهد افتاد.

تقریباً بلافاصله پس از انتشار توافق‌نامه نیویورک در ۲۲ مه سال ۲۰۱۷، جیمز هیلارد^۱ یکی از توسعه‌دهندگان بیت کوین و نرم‌افزارهای استخراج راه‌حلی برای حل مشکل بیت ۴ با عنوان BIP-91 پیشنهاد کرد:

من می‌خواهم روشی پیشنهاد دهم که قسمت اول پیشنهاد بری سیلبرت را به صورت مستقل از قسمت دوم انجام دهد:

«سگویت روی آستانه ۸۰٪ و با سیگنال روی بیت شماره ۴ فعال شود»

هدف در اینجا از یک طرف به حداقل رساندن مخاطرات فورک شدن زنجیره و ایجاد اختلال در شبکه، و از طرف دیگر به حداکثر رساندن سازگاری و همچنین فعال‌سازی سریع سگویت در آستانه ۸۰ درصد و با استفاده از بیت شماره ۴ است.

ما می‌توانیم با فعال‌سازی سگویت در اولین فرصت ممکن و پرهیز از هرگونه هارد فورک، از ایجاد مخاطرات و مشکلات گسترده‌ای که روش فعال‌سازی سگویت + یک هارد فورک عجولانه در شبکه به وجود خواهند آورد جلوگیری، و ظرفیت شبکه بیت کوین را افزایش دهیم.

جیمز پیشنهاد کرد که سگویت توسط دو سافت فورک و در دو مرحله فعال شود. اولین سافت فورک همانطور که در توافق‌نامه نیویورک قید شده بود، با استفاده از آستانه سیگنال دهی ۸۰ درصد ماینرها فعال، و ماینرها را ملزم به اعلام آمادگی برای فعال‌سازی

1 James Hillard

سگویت با استفاده از بیت شماره ۱ کند. این موجب فعال شدن سافت فورک دوم، یعنی خود سگویت خواهد شد. سافت فورک اول موجب سازگاری روش ارتقاء قوانین پروتکل با BIP-148 می‌شد، چون ماینرها را ملزم به اعلام آمادگی برای فعال‌سازی سگویت با استفاده از بیت شماره ۱ می‌کرد. در واقع BIP-91 توسط جیمز هیلارد و شاولین فرای، نویسنده BIP-148 نوشته شده بود. سرانجام نرم‌افزاری با نام Segsignal تهیه و منتشر شد. این نرم‌افزار در واقع نسخه‌ای از Bitcoin Core بود و تغییراتی در آن ایجاد شده بود تا از BIP-91 پشتیبانی کند. BIP-91 پیشنهاد ارتقاء بسیار عجولانه‌ای بود و اگر به آستانه ۸۰ درصدی پشتیبانی ماینرها می‌رسید؛ یعنی ۲۹۶ بلاک از ۳۳۶ بلاک در یک پنجره علامت‌دهی از آن پشتیبانی می‌کردند، فعال می‌شد.

به سرعت مشخص شد نرم‌افزاری که قرار است توافق‌نامه نیویورک را پیاده‌سازی کند BTC1 نامگذاری شده و توسعه‌دهنده اصلی آن نیز جف گارزیک، فردی است که در سال ۲۰۱۰، چند هفته پس از اعمال محدودیت سائز بلاک توسط ساتوشی پیشنهاد افزایش سائز بلاک را به او داد. از جف خواسته شده بود تا نرم‌افزار BTC1 را با BIP-91 سازگار کند، با این استدلال که سیگنال‌دهی روی بیت ۱ از نقطه نظر فنی بی‌معنی است. جف در ابتدا بدون ارائه دلیل مشخصی از این کار امتناع کرد.

در تاریخ ۲۹ مه، یک ایمیل از طرف مایک بلشه^۱ مدیرعامل شرکت BitGO به بیرون درز کرد که شامل یک برنامه و جدول زمان‌بندی برای اجرای توافق نیویورک بود. لازم به ذکر است که اگرچه نام شرکت BitGO به‌عنوان یکی از شرکت‌های ارائه‌دهنده پشتیبانی فنی ذکر شده بود، ولی آن‌ها توافق‌نامه را امضاء نکرده بودند. حتی در پایین متن توافق‌نامه آمده بود: «توجه: شرکت BitGO به اشتباه در لیست اولیه منتشر شده قرار گرفته است. این اشکال در حال حاضر رفع شده است.» از صحبت‌هایی که با برخی از کارمندان این شرکت داشتم، درک من این است که آن‌ها بعداً خواستار حذف نام این شرکت از این لیست شده‌اند چون فکر می‌کرده‌اند به عنوان متولی نگهداری از بیت‌کوین‌های مشتریان و

1 Mike Belshe

پرداخت‌ساز^۱ باید بی‌طرف بمانند و از هر دو فورک پشتیبانی کنند. در هر صورت، ایمیلی که لو رفته بود حاوی یک جدول زمانی برای انتشار نسخه اولیه نرم‌افزار، راه‌اندازی شبکه تست^۲، و سپس آغاز سیگنال‌دهی ماینرها از ۲۱ ژوئیه بود.

بسیاری از افراد در جامعه بیت کوین وقتی متوجه شدند توسعه و برنامه‌ریزی برای تهیه نرم‌افزار لازم برای اجرای توافق‌نامه نیویورک مخفیانه و در محافل خصوصی پیش می‌رود، بسیار خشمگین و عصبانی شدند. قرار بود بیت کوین یک سیستم باز باشد و هر کس بتواند آن را مورد بررسی و تجزیه و تحلیل قرار دهد. توسعه مخفیانه نرم‌افزاری که منجر به ایجاد تغییر در قوانین پروتکل خواهد شد، با بیت کوین مغایر است. با این حال دلیل پیش بردن آن در خفا روشن بود: اگر آن‌ها این کار را به صورت عمومی انجام می‌دادند بدون شک گروه طرفداران بلاک‌های کوچک اشکالاتی در آن پیدا می‌کردند و باعث می‌شدند پیشنهاد آن‌ها ضعیف به نظر برسد. سگویت بسیار پیچیده بود و گروهی که درک کاملی از آن نداشت تصمیم به پیاده‌سازی آن گرفته بود. با توجه به اتفاقاتی که در ادامه رخ داد می‌توانیم با اطمینان بگوییم انجام بسیاری از مراحل اجرای سگویت پشت درهای بسته یک اشتباه بود، چون به نظر می‌رسید فراهم نبودن امکان بررسی دقیق آن موجب به وجود آمدن اشکالات متعدد دیگری در ادامه کار شد.

در پایان ماه مه سال ۲۰۱۷، فشار وارد شده بر روی جف گارزیک به دلیل ناسازگاری روش فعال‌سازی BTC1 در به خدمت گرفتن بیت ۴، و روش سگویت بسیار زیاد بود. طرفداران بلاک‌های کوچک و اعضای کانال اژدهایان دریافتند که این یک نقص عمده در نرم‌افزار BTC1 است و اگر آن‌ها بتوانند جف را مجاب به ایجاد این تغییر و پذیرش BIP-91 کنند، ممکن است سرانجام سگویت روی بیت کوین فعال شود. اگر این اتفاق می‌افتاد طرفداران بلاک‌های کوچک می‌توانستند توجه خود را بر روی متوقف کردن قسمت دوم توافق‌نامه نیویورک، یعنی اجرای هارد فورک معطوف کنند. رسانه‌های

1 Payment processor

2 Testnet

اجتماعی پُر بود از اظهار نظر افرادی که فکر می کردند جف گارزیک با پذیرفتن BIP-91 موجب ایجاد اخلال در روند کار ارتقاء شده و با دیگران همکاری نمی کند. احتمالاً او ایمیل های زیادی هم از طرف طیف وسیعی از افراد فعال در حوزه فنی بیت کوین دریافت می کرده که درخواست های مشابهی از او داشته اند و اتهامات مشابهی به او زده اند.

سرانجام در تاریخ ۵ ژوئن سال ۲۰۱۷، جف گارزیک به دلیل فشاری که به او وارد می شد کوتاه آمد و BIP-91 را در نرم افزار خودی یعنی BTC1 قرار داد. طرفداران بلاک های کوچک به خواسته خود رسیدند چون نرم افزار توافق نامه نیویورک UASF را پیاده سازی کرده بود. در کانال اژدهایان جشن های هیجان انگیزی برگزار می شد.

برنامه اجرای هارد فورک نیز در این مرحله تغییر کرده بود؛ اکنون گفته می شد برنامه اجرای هارد فورک برخلاف برنامه ریزی گذشته که قرار بود شش ماه پس از فعال سازی سگویت روی شبکه اجرا شود تغییر کرده و به سه ماه کاهش پیدا کرده است. با این حال، من منطق پیاده سازی اجرای این هارد فورک در کُد نرم افزار را درک نمی کردم و زمان بندی آن نیز دارای ابهامات زیادی بود. این دوره سه ماهه در واقع نصف زمانی بود که در توافق نامه نیویورک تعیین، و در نسخه اولیه نرم افزار BTC1 پیاده سازی شده بود. من از گفتگو با برخی از افرادی که به اطلاعات پشت پرده BTC1 دسترسی داشتند متوجه شدم که ظاهراً هدف از تغییر زمان بندی اجرای هارد فورک این بوده است که فاصله زمانی میان فعال سازی سگویت و اجرای هارد فورک به قدری کوتاه باشد که کاربران از اجرای مرحله دوم توافق نامه پشیمان نشوند و هارد فورک حتماً اجرا شود. این رویکرد از نظر من اشتباه بود چون می توانست موجب دشوارتر شدن اجرای هارد فورک شود، چون بر اساس این برنامه زمان بندی، طرفداران اجرای هارد فورک زمان کمتری برای ترغیب کاربران به نصب نرم افزار جدید و اجرای هارد فورک داشتند. (سه ماه بجای شش ماه).

در مورد BTC1 باید بگوییم حتی پس از پیاده‌سازی BIP-91، این نرم‌افزار همچنان پر از اشکالات نرم‌افزاری بود. جف گارزیک احتمالاً درک درستی از سگویت نداشت و در پیاده‌سازی بخش شبکه نظیر-به-نظیر^۱ سگویت اشتباهاتی مرتکب شده بود که برای رفع آن‌ها باید از دیگران کمک می‌گرفت. نکته جالب دیگر موضوعی بود که یک نفر در تاریخ ۱۴ ژوئن در ایمیلی به آن اشاره کرد؛ اینکه هنوز بخش نرم‌افزاری هارد فورک برای افزایش سایز بلاک در BTC1 پیاده‌سازی نشده است. نرم‌افزار BTC1 تغییری در محدودیت سقف ۴ میلیون واحدی محاسبه وزن بلاک نداده بود و این امر از اجرای هارد فورک جلوگیری، و در نتیجه سایز بلاک هرگز افزایش پیدا نمی‌کرد. به نظر می‌رسید جف گارزیک اصلاً محدودیت جدیدی که توسط سگویت اعمال می‌شد را درک نکرده است؛ اگر خاطرتان باشد در فصول قبلی گفتیم که او فکر می‌کرده سگویت دو محدودیت جدا از هم دارد. بخش نرم‌افزاری هارد فورک پس از انتشار این ایمیل و جلب شدن توجه جامعه فعالان حوزه بیت کوین، به BTC1 اضافه شد. برای حامیان توافق‌نامه نیویورک دو برابر کردن چیزی که از آن سر در نمی‌آوردند، کار دشواری بود.

جف گارزیک همچنین برای اضافه کردن قابلیت محافظت در برابر خرج شدن دوباره^۲ در نرم‌افزار BTC1 تحت فشار بود، ولی با آن مخالفت می‌کرد. استدلال او این بود که BTC1 یک کوین جدید ایجاد نخواهد کرد، بلکه پس از به‌روزرسانی پروتکل و به دلیل حمایت گسترده‌ای که از زنجیره قوانین جدید خواهد شد، زنجیره قبلی از پیشرفت باز خواهد ایستاد. به نظر می‌رسید اغلب طرفداران بلاک‌های بزرگ رخداد فورک سال ۲۰۱۶ در زنجیره اتریوم را فراموش کرده بودند. بنابراین از نظر طرفداران توافق‌نامه نیویورک اضافه کردن این قابلیت ضروری نبود. با این حال، این تکرار استدلال‌هایی بود که در گذشته بارها و بارها تکرار شده بود؛ برخی معتقد بودند زنجیره اصلی بیت کوین از حرکت باز خواهد ایستاد و در مقابل افرادی بودند که می‌گفتند شاید زنجیره اصلی ادامه پیدا کند و بر همین اساس پیاده‌سازی این قابلیت را ضروری می‌دیدند. در تاریخ ۱۴ ژوئن سرجیو لرنر^۳،

1 peer-to-peer
2 Replay protection
3 Sergio Lerner

فردی که توافق نامه نیویورک بر پایه پیشنهاد وی بنا نهاده شده بود از پیاده سازی این قابلیت حمایت کرد. در این مرحله جف گارزیک از همه طرف تحت فشار شدیدی بود:

مردم به دو گروه تقسیم شده اند و هر کدام از این دو گروه دیدگاه متفاوتی نسبت به بیت کوین دارند. هیچکدام از این دیدگاه ها «اشتباه» نیست. یکی از آنها به چیزهایی مثل تمرکززدایی، کم کردن نقش دولت، مقاومت در برابر سانسور، و ناشناس بودن اهمیت زیادی می دهند. آنها معتقدند بیت کوین طی ۲۰ تا ۳۰ سال آینده دنیای ما را متحول خواهد کرد. برای رسیدن به این هدف، برای آنها بسیار مهم است که به این ارزش ها پایبند باشند و هیچ عجله ای هم ندارند. گروه مقابل به مسائل دیگری مانند رساندن کاربران بیت کوین به یک میلیارد تا ۵ سال آینده و ارائه خدمات مالی به افرادی که امروزه به خدمات بانکی دسترسی ندارند، اهمیت می دهند حتی اگر لازم باشد برای رسیدن به این اهداف نیازمند توافق سیاسی شوند. هر دو چشم انداز شایستگی های خود را دارند ولی با هم ناسازگارند. قابلیت محافظت در برابر خرج شدن دوباره به هر یک از این دو گروه «بیت کوینر» فرصت می دهد تا نهایت تلاش شان را برای رسیدن به دیدگاه مورد نظر خود به کار ببندند. این دو دیدگاه می توانند در کنار یکدیگر وجود داشته باشند.

در تاریخ ۱۶ ژوئن سال ۲۰۱۷، ماینرهای بیت کوین نشست دیگری برگزار کردند. تقریباً تمام استخراج های بزرگ استخراج در این نشست شرکت داشتند. در این جلسه ماینرها از توافق نامه نیویورک اعلام حمایت کردند.

اولین نسخه BTC1 قابلیت محافظت در برابر پاک شدن زنجیره^۱ را پیاده سازی نکرده بود، و همانطور که قبلاً در این کتاب توضیح دادیم اجرای یک هارد فورک جنجالی، بدون پیاده سازی این قابلیت مانند این است که شما به جنگ بروید و خودتان به عمد دستان

1 Wipeout protection

خود را از پشت ببندید. در ماه مه سال ۲۰۱۷، جیهان وو پس از تقریباً دو سال منازعه بر سر اجرای هارد فورک سرانجام این مسأله را درک، و برای پیاده‌سازی قابلیت محافظت در برابر پاک شدن زنجیره تلاش کرد. او در تاریخ ۱۲ مه سال ۲۰۱۷ از این قابلیت اعلام حمایت کرد:

از آنجا که این یک تغییر مهم در قوانین اجماع است و ۴ سال مورد بحث و بررسی قرار گرفته است، می‌توانیم قانون اجماع دیگری را فقط و فقط در نقطه انشعاب زنجیره به پروتکل اضافه کنیم، و سائز این بلاک باید از ۱,۰۰۰,۰۰۰ بایت بزرگ‌تر باشد. این یک روش بسیار ساده و سر راست برای جلوگیری از رخداد تنظیم مجدد بلاک‌ها^۱ روی زنجیره است.

با افزایش فشار بر روی جف گارزیک و روشن شدن این موضوع که هارد فورک برنامه‌ریزی شده در توافق‌نامه نیویورک ممکن است جنجالی‌تر از چیزی باشد که پیشنهادکنندگان آن در ابتدا تصور می‌کردند، او راضی شد تا قابلیت محافظت در برابر پاک شدن زنجیره را اضافه کند. جیهان وو او را به اضافه کردن این قابلیت به BTC1 ترغیب کرد و در نهایت جف گارزیک این کار را در ۲۰ ژوئن انجام داد. بر این اساس بجای اینکه صرفاً بلاک‌های بزرگ‌تر از ۱ مگابایت پس از اجرای هارد فورک در شبکه مجاز شمرده شوند، برای محافظت در برابر حذف شدن زنجیره هارد فورک، اولین بلاک ساخته شده بلافاصله پس از اجرای هارد فورک باید بزرگ‌تر از ۱ مگابایت می‌بود.

با توجه به درخواست شرکت Bitmain و BU مبنی بر اضافه شدن قابلیت محافظت در برابر حذف شدن زنجیره هارد فورک، من و دیگر اعضای تیم توسعه با ایده پیش‌بینی‌پذیرتر شدن روش ارتقاء قوانین شبکه موافق هستیم.

...

1 re-org

روش سنتی اجرای هارد فورک به این صورت است که شکاف در زنجیره «در لحظه یا بعد از» اجرای هارد فورک رخ می‌دهد؛ هر زمان که اولین بلاک بزرگ‌تر از ۱ مگابایت توسط یک ماینر ساخته شود. پیشنهاد شده که این قانون محدودتر شود، به گونه‌ای که بلاک ساخته شده بلافاصله پس از اجرای هارد فورک و تغییر قوانین، «باید» بزرگ‌تر از ۱ مگابایت باشد. این امر وقوع هارد فورک روی یک بلاک مورد نظر را تضمین می‌کند و موجب پیش‌بینی‌پذیرتر شدن این رویداد خواهد شد.

این قابلیت به درستی پیاده‌سازی نشده بود و در تاریخ ۱۱ جولای سال ۲۰۱۷، زنجیره شبکه تست ۱ BTC1 دو پاره شد. به نظر می‌رسید فردی توانسته زنجیره شبکه تست را ۵۰ بار سریع‌تر از دیگران ماین، و هارد فورک را زودتر از موعد فعال کند. سپس با توجه به اشکال موجود در پیاده‌سازی قانون تعیین شده برای بلاک اول که می‌بایست بیشتر از ۱ مگابایت می‌بود، زنجیره جدیدی در کنار زنجیره نسخه‌های قبلی نرم‌افزار BTC1 پدید آمد. دلیل این امر این بود که ساینز بلاک اول (پس از فعال شدن هارد فورک) بیش از ۱ مگابایت نبود، چون تعداد تراکنش‌های اضافه شده به این بلاک کم بود. این اشکال و دو پاره شدن زنجیره مجدداً توسط طرفداران بلاک‌های کوچک مورد سوءاستفاده قرار گرفت و آن‌ها ادعا می‌کردند که BTC1 ضعیف است و اشکال دارد. پاسخ تیم BTC1 این بود که شبکه تست در واقع برای شناسایی همین مشکلات راه‌اندازی شده است و با این استدلال از خود دفاع می‌کردند. با این حال این رخدادها نشان از این داشت که برنامه BTC1 برای تغییر قوانین اجماع بیت‌کوین سرسری و عجولانه است. آن‌ها در این مدت کوتاه چندین نسخه از نرم‌افزار را منتشر کردند که به دلیل اشکالات نرم‌افزاری و تغییراتی که در دقیقه ۹۰ اعمال شده بود، با یکدیگر سازگار نبودند.

در اوایل ژوئیه حدود ۸۰ تا ۹۵ درصد از ماینرها (از نظر هش‌ریت) حروف "NYA" را در سربرگ بلاک‌هایی که ماین می‌کردند قرار می‌دادند و به نظر می‌رسید توافق‌نامه نیویورک

در وضعیت برنده است. با این حال تقریباً هیچکدام از کاربران نرم افزار BTC1 یا حتی Segnet (که بخش اول توافق نامه نیویورک را فعال می کرد) را اجرا نمی کردند و می توان گفت این نرم افزارها مورد پذیرش کاربران قرار نگرفته بود. این در حالی بود که طبق صحبت هایی که با صرافی های بزرگ کردم، آنها هم از Segnet، BTC1 یا BIP148 استفاده نمی کردند، بلکه فقط Bitcoin Core را اجرا می کردند. چشم انداز آینده بسیار نامشخص به نظر می رسد.

در واقع، ماینرها و استخراج های استخراجی که من با آنها صحبت کردم هم علی رغم درج حروف NYA در بلاک های ماین شده، از نرم افزار BTC1 استفاده نمی کردند. در اواسط ژوئیه سال ۲۰۱۷ من با افراد مشغول در دو استخراج بیت کوین صحبت کردم. این استخراج های استخراج هر دو توافق نامه نیویورک و میزگرد ماینرها در ژوئن ۲۰۱۷ را امضاء کرده بودند. شرایط به این صورت بود که اگر یک ماینر نرم افزار BTC1 را اجرا می کرد، این نرم افزار به صورت پیش فرض روی بیت ۴ و بیت ۱ سیگنال آمادگی می داد. با فعال شدن اولین سافت فورک، سیگنال دهی روی بیت ۱ اجباری، و در نتیجه سگویت فعال می شد. این ماینرها به من گفتند که آنها به نرم افزار BTC1 اعتماد ندارند و بنابراین از Segnet یا Bitcoin Core استفاده می کنند. آنها که Bitcoin Core را اجرا می کردند حروف NYA و سیگنال دهی روی بیت ۱ یا ۴ را به صورت دستی انجام می دادند. آنها به من گفتند که این امر کاملاً محرمانه است و به عنوان یک راز خصوصی با من در میان گذاشته شده؛ ولی آنها در ملاء عام باید از BTC1 و NYA حمایت کنند و این بسیار حیاتی است.

در ۲۰ ژوئیه، جیهان وو در یک توثیت اعلام کرد که شرکت Bitmain نرم افزار BTC1 را اجرا می کند؛ تنها تفاوت ماجرا این بود که او همچنین اعلام کرد که این شرکت تغییری در نرم افزار ایجاد، و سیگنال دهی روی بیت ۱ را از آن حذف کرده است. به نظر

می‌رسید جی‌هان و و می‌خواهد تا جایی که امکان دارد فعال‌سازی سگویت را به تعویق بیندازد و تا لحظه‌ای که سیگنال‌دهی برای اجرای آن اجباری نشده، آن را فعال نکند.

شرکت Bitmain نرم‌افزار BTC1 را اجرا می‌کند ولی ما آن را به گونه‌ای تغییر داده‌ایم که در این مرحله فقط روی بیت ۴ سیگنال می‌دهد.

روند سیگنال‌دهی ماینرها بسیار آشفته بود و کاربران نمی‌دانستند ماینرها چه نرم‌افزاری را اجرا کرده‌اند. به عنوان مثال ماینرها بدون اینکه نرم‌افزار BTC1 را اجرا کنند، از توافق‌نامه نیویورک پشتیبانی می‌کردند. شرکت Bitmain هم یکی از مهم‌ترین بازیگران خاطی در زمینه سیگنال‌های دروغین بود. به عنوان نمونه استخراج Antpool (وابسته به شرکت Bitmain) قبل از انتشار نرم‌افزار BTC1 روی بیت ۴ شروع به سیگنال‌دهی کرده بود، این نشان دهنده این بود که آن‌ها از نرم‌افزاری استفاده می‌کردند که در آن زمان وجود خارجی نداشت. این شرکت حتی در جولای سال ۲۰۱۷ همچنان سیگنال پشتیبانی از Bitcoin Unlimited را به شبکه ارسال می‌کرد، در حالی که این نرم‌افزار BTC1 (یعنی هارد فورک) و سگویت را پیاده‌سازی نکرده بود، بنابراین این سیگنال‌ها با هم در تضاد بودند.

چند روز بعد، در اواخر ژوئیه ۲۰۱۷ و فقط چند روز قبل از پایان مهلت مقرر، شرکت Bitmain سرانجام سیگنال‌دهی روی بیت ۱ را شروع کرد. طرفداران بلاک‌های کوچک از این اتفاق به وجد آمده بودند. پس از یک کارزار طاقت‌فرسا، و پس از گذشت بیش از ۱۰ ماه از انتشار نرم‌افزار سگویت، سرانجام بزرگترین شرکت فعال در صنعت استخراج در فضای بیت‌کوین از آن حمایت کرد. اغلب طرفداران بلاک‌های کوچک معتقد بودند که این اتفاق هرگز رخ نخواهد داد. سرانجام فعال‌سازی سگویت محتمل به نظر می‌رسید.

سپس آستانه ۸۰ درصدی لازم برای فعال‌سازی BIP-91 تحقق یافت و سرانجام این سافت فورک در ۲۱ ژوئیه سال ۲۰۱۷ روی شبکه قفل شد. طبق قانون این سافت فورک موقت ماینرها ملزم بودند از ۲۶ جولای سال ۲۰۱۷، با ارسال سیگنال لازم از سگویت پشتیبانی کنند. با نزدیک شدن به این تاریخ، برخی از بیت کوینرها نگران مخاطرات اجرای سگویت بودند. اگر همه ماینرها سیگنال صحیحی به شبکه ارسال نمی‌کردند، ممکن بود اشکالاتی در شبکه بوجود آید. با این حال، روز موعود فرا رسید و ماینرها به‌درستی روی بیت ۱ سیگنال دادند. هیچ‌گونه شکافی در زنجیره بیت کوین رخ نداد و سگویت سرانجام روی شبکه بیت کوین قفل، و سپس فعال شد. با توجه به شلختگی و پیچیدگی ضرب‌العجل‌های درهم‌تنیده و مکانیزم‌های فعال‌سازی، پی‌گیری رخدادها تقریباً غیرممکن بود. به نظر می‌رسید هر چند روز یک روش فعال‌سازی و یک ضرب‌العجل جدید معرفی می‌شد. شما تا اینجای کتاب حتماً متوجه شده‌اید که مناقشه سائز بلاک برای من اهمیت زیادی داشته و ذهن من به کلی با این موضوع درگیر بوده، با این حال پی‌گیری رخدادها حتی برای من نیز چالش‌برانگیز بود.

BIP-91 فقط چند روز مانده به ضرب‌الاجل تعیین شده در BIP-148 (تاریخ ۱ اوت ۲۰۱۷) فعال شد، و بین فعال شدن BIP-91 که سیگنال‌دهی برای سگویت را الزامی می‌کرد تا فعال شدن BIP-141 که قوانین UASF را بر روی شبکه اعمال می‌کرد فقط ۵ روز فاصله بود. اینکه BIP-91 فقط کمی قبل از موعد مقرر فعال شده می‌تواند نشان‌دهنده این باشد که تهدیدهای UASF مؤثر بوده است. موفقیت UASF یک دستاورد معجزه‌آسا بود. UASF در هیچ‌کدام از نسخه‌های Bitcoin Core پیاده‌سازی نشد و برخی از تأثیرگذارترین توسعه‌دهندگان آن صریحاً با آن مخالف بودند.

UASF همراستا با روح واقعی بیت کوین و خالق ناشناس آن ساتوشی بود و از میزگردها و نشست‌هایی که پشت درهای بسته، و میان بازیگران مهم برگزار می‌شد بیرون نیامده بود. در عوض در یک فضای آزاد و با اطلاع عموم کاربران منتشر، و توسط یک توسعه‌دهنده

با نام مستعار شاولین فرای تبلیغ شد. به نوعی، یک فرد با نام مستعار، چند دنباله‌رو که به صورت خودجوش فعالیت می‌کردند و چند کلاه نقاب‌دار که توسط سمسون ما تهیه شده بود توانستند با شرکت چند میلیارد دلاری Bitmain و حامیان سرمایه‌دارش رو در رو شوند، و برنده این جنگ باشند. به یاد دارم که در آن زمان با خودم فکر می‌کردم همین چیزی فقط در بیت کوین امکان‌پذیر است. این میدان جنگ در فضای بیت کوین موضوع منحصر به فردی بود و نتیجه عجیبی هم داشت.

ارتقاء BIP-91 از نظر طرفداران بلاک‌های کوچک به هیچ‌وجه بی‌نقص نبود؛ با عجله تهیه شده بود، پنجره رأی‌گیری آن ۳۳۶ بلاک و بسیار کوتاه بود (فقط ۲/۳۳ روز طول می‌کشید)، الزام ماینرها به سیگنال‌دهی کار خطرناکی بود، و از همه مهم‌تر با توجه به اینکه قرار بود فقط ماینرها آن را اجرا کنند، بسیار پر مخاطره بود. ممکن بود منجر به جدا شدن زنجیره ماینرها و کاربران از یکدیگر شود. طرفداران بلاک‌های کوچک صرفنظر از شلخته و خطرناک بودن این روش به خواسته خود رسیدند: سگویت بر روی شبکه فعال شده بود و به نظر می‌رسید UASF توانسته بود جیهان وو را مجبور به پذیرش آن کند. در این مرحله آن‌ها می‌توانستند تلاش‌های خود را روی توقف مرحله دوم توافق‌نامه نیویورک متمرکز، و از اجرای هارد فورک جلوگیری کنند.

طرفداران بلاک‌های بزرگ از این تحولات بسیار عصبانی بودند. یکی از طرفداران برجسته بلاک‌های بزرگ شخصاً به من گفت که «این کلاه‌های احمقانه UASF کارساز شدند» و ماینرها را مجبور به فعال‌سازی سگویت کردند. او مخصوصاً از این موضوع عصبانی بود که همه این اتفاقات قبل از ۱ اوت ۲۰۱۷ رخ داده است. از نظر او اگر سگویت بعد از این تاریخ فعال می‌شد، روایت طرفداران بلاک‌های بزرگ مبنی بر اینکه سگویت بر اساس توافق نیویورک فعال شده، نه UASF باورپذیرتر به نظر می‌رسید. طرفداران بلاک‌های بزرگ احساس می‌کردند افراطی‌ترین بخش گروه طرفداران بلاک‌های کوچک کنترل

بیت کوین را به دست گرفته‌اند و موجب فعال‌سازی چیزی بر روی شبکه شده‌اند که آن‌ها به شدت با آن مخالف بوده‌اند. به نظر می‌رسید آن‌ها از بیت کوین سرخورده شده بودند و اهمیتی به اجرای فاز دوم توافق‌نامه نیویورک نمی‌دادند.

به نظر من جیهان وو می‌توانست ترفندی بزند و منتظر سپری شدن مهلت روز ۱ اوت ۲۰۱۷ شود، و سپس سگویت را روی شبکه بیت کوین فعال کند. این امر کار طرفداران بلاک‌های کوچک در حمایت از زنجیره BIP-148 را دشوارتر می‌کرد، چون سگویت به هر حال روی زنجیره دیگری فعال شده بود. در این صورت جیهان می‌توانست ادعا کند که UASF را شکست داده است. با این حال، جیهان وو ترجیح داد این کار را انجام ندهد چون به نظر می‌رسد UASF مؤثر بوده است. جیهان وو از فورک شدن زنجیره بیت کوین می‌ترسید، و احتمالاً قدرت مخالفان خود را هم دست‌بالا گرفته بود و در نهایت تسلیم این فشارها شد.

پس از فعال شدن سگویت، طرفداران بلاک‌های کوچک قادر بودند روی زنجیره خود -یعنی بیت کوین- به کار خود ادامه دهند. با این حال همچنان یک مشکل به قوت خود باقی بود؛ بسیاری از شرکت‌های مهم در این فضا، به‌ویژه شرکت‌های مستقر در ایالات متحده و شرکت‌های استارت‌آپ متعهد به افزایش ساینز بلاک از طریق اجرای هارد فورک شده بودند. آن‌ها نمی‌خواستند کوین جدیدی خلق شود و این زنجیره باید به‌عنوان بیت کوین شناخته می‌شد. منصرف کردن این شرکت‌ها کار بسیار دشواری به نظر می‌رسید، بنابراین مناقشه ساینز بلاک همچنان ادامه داشت. هارد فورک مورد نظر قرار بود در عرض سه ماه آینده اجرا شود و هر روز به تنش موجود در میدان این جنگ افزوده می‌شد.

فصل نوزدهم

بیت کوین گش Bitcoin Cash

در تاریخ ۳۰ ژوئن سال ۲۰۱۷، در شهر آرنهم^۱ هلند یک کنفرانس از جانب طرفداران بلاک‌های بزرگ به عنوان «کنفرانس آینده بیت کوین ۲۰۱۷» برگزار شد. سخنرانان این کنفرانس عبارت بودند از جیهان وو، اندرو استون^۲ از Bitcoin Unlimited، کریگ رایت (که یک سخنرانی طولانی و بی سر و ته کرد) و یک توسعه‌دهنده کمتر شناخته شده به نام آموری ساچه^۳. عنوان سخنرانی آموری «بازگشت به اصول اولیه» بود، و در این سخنرانی او از پروژه کوچکی رونمایی کرد که به گفته او مدتی بود مشغول آن بوده است. او برنامه اجرای این هارد فورک جدید را تشریح کرد که شامل افزایش محدودیت ساینز بلاک و محافظت اختیاری از پخش مجدد^۴ بود و بنابراین به افرادی که علاقه‌ای به افزایش ساینز بلاک نداشتند اجازه می‌داد زنجیره قدیمی خود را دنبال کنند. آموری یک نرم‌افزار جدید را با نام Bitcoin ABC معرفی و اظهار کرد که در واقع این همان برنامه UAHF است که چند هفته پیش توسط جیهان وو اعلام شده بود.

1 Arnhem
2 Andrew Stone
3 Amaury Sachet
4 Replay protection

این نرم‌افزار جدید با نام Bitcoin ABC حوالی ۱۲ جولای سال ۲۰۱۷، یعنی تنها چند هفته مانده تا مهلت مقرر UASF (یعنی ۱ اوت سال ۲۰۱۷) منتشر شد. برخلاف نرم‌افزارهای قبلی مثل Bitcoin Classic، Bitcoin Unlimited، Bitcoin XT و آخرین آن‌ها یعنی BTC1، روز ۱ اوت سال ۲۰۱۷ به‌عنوان یک روز ثابت در نرم‌افزار Bitcoin ABC برای اجرای هارد فورک تعریف شده بود و این فعال‌سازی نیازی به سیگنال‌دهی ماینرها نداشت. آن را عمده‌اً طوری تنظیم کرده بودند که مصادف با ضرب‌الاجل UASF باشد. زنجیره جدید شامل قابلیت حفاظت در برابر حذف شدن^۱ بود، در نتیجه این هارد فورک می‌توانست با موفقیت منجر به اجرای افزایش محدودیت ساینز بلاک شود. سگویت که از نظر طرفداران بلاک‌های بزرگ منفور بود در این کوین جدید حذف شده بود، هرچند در واقعیت اگر نرم‌افزار ABC با دقت بیشتری مورد بررسی قرار می‌گرفت، مشخص می‌شد که این نرم‌افزار شامل اغلب قسمت‌های سگویت از جمله الگوریتم جدید تجزیه و تحلیل تراکنش‌ها است که برخی از مشکلات مربوط به تراکنش‌ها را برطرف می‌کرد. با این حال به نظر می‌رسید همچنان به کارگیری روش ASICBoost مخفیانه در این زنجیره امکان‌پذیر است. سرانجام، طرفداران بلاک‌های بزرگ به خواسته خود می‌رسیدند: یک زنجیره با بلاک‌های بزرگ، بدون استفاده از نرم‌افزاری که توسط توسعه‌دهندگان Bitcoin Core منتشر شده، و از همه مهم‌تر به دور از اتخاذ رویکرد انعطاف‌ناپذیر و بسیار محتاطانه برای تغییر قوانین اجماع؛ چیزی که طرفداران بلاک‌های بزرگ بیش از هر چیز از آن متنفر بودند. در تاریخ ۱۷ ژوئیه سال ۲۰۱۷، ViaBTC که در آن زمان دیگر به‌عنوان نماینده جیهان وو در نظر گرفته می‌شد و معمولاً فضا را قبل از اعلام سیاست‌های شرکت Bitmain مورد سنجش قرار می‌داد اعلام کرد که آن‌ها استخراج جدیدی برای استخراج کوین جدید راه‌اندازی خواهند کرد. آن‌ها نام این کوین را Bitcoin Cash گذاشتند و نماد BCC را برای آن انتخاب کردند. این نماد در نهایت به BCH تغییر پیدا کرد.

ما توکن «بیت کوین کش» (BCC) را به کوین احتمالی که پس از اجرای UAHF پدید خواهد آمد اختصاص خواهیم داد.

1 Wipeout protection

در حالی که بسیاری از اعضای گروه بلاک‌های بزرگ از بیت کوین کش پشتیبانی می‌کردند، ولی اغلب آن‌ها فکر می‌کردند که این یک برنامه پشتیبان^۱ است که قرار است در صورت شکست مرحله دوم توافق‌نامه نیویورک به کار گرفته شود. در تاریخ ۲۵ ژوئیه سال ۲۰۱۷ راجر وور، مدیر عامل سایت Bitcoin.com نوشت:

اگر بخش 2x از Segwit2x اجرا نشود، Bitcoin.com بلافاصله تمام منابع شرکت را به پشتیبانی انحصاری از بیت کوین کش اختصاص خواهد داد.

در تاریخ ۲۳ ژوئیه سال ۲۰۱۷، تنها یک هفته مانده به راه‌اندازی بیت کوین کش، Ben DeLo یکی از مؤسسان یکی از بزرگترین صرافی‌های ارزهای دیجیتال در آن زمان، موضوعی را در صفحه گیت‌هاب پروژه Bitcoin ABC مطرح کرد. او درخواست کرد که نرم‌افزار ABC به جای پیاده‌سازی اختیاری قابلیت محافظت در برابر انتشار مجدد^۲، آن را به صورت اجباری پیاده‌سازی کند. او به‌عنوان امانت‌دار دارایی مشتریان خود نگران بود و می‌ترسید یا بیت کوین کش‌های آن‌ها را از دست دهد یا مجبور باشد برای محافظت از حملات انتشار مجدد، مبلغ قابل توجهی هزینه کند. اگرچه برخی شک داشتند که این قابلیت در راستای برنامه اصلی جیهان و و باشد، و با توجه به اینکه پیاده‌سازی این قابلیت همواره خواسته مورد علاقه طرفداران بلاک‌های کوچک بود، ولی آموری با هدف کسب حمایت صرافی‌ها در پشتیبانی از این توکن جدید، به درخواست بن عمل کرد. تنها شش روز قبل از خلق کوین جدید، قابلیت محافظت در برابر انتشار مجدد به صورت دوطرفه و الزامی به نرم‌افزار Bitcoin ABC اضافه شد. بنابراین بالاخره اجرای یک فورک کامل امکان‌پذیر می‌شد و دو طرف درگیر این جنگ می‌توانستند با صلح و صفا راه خود را از یکدیگر جدا کنند.

1 Backup plan
2 Replay protection

از آنجایی که انتظار می‌رفت بیت کوین کش زنجیره‌ای با هشریت اقلیت باشد، یکی از نگرانی‌ها این بود که روند تولید بلاک‌ها در ابتدای کار به اندازه‌ای کند باشد که زمان رسیدن به دوره‌ی بازتنظیم دو هفته‌ای سختی شبکه بسیار طولانی شود. بنابراین سختی موردنیاز برای تولید بلاک‌های بیت کوین کش کاهش یافت، که ویژگی ناخواسته ولی مطلوبی با خود به همراه داشت: سربرگ بلاک‌های بیت کوین کش با سربرگ بلاک‌های بیت کوین ناسازگار بود و این باعث می‌شد کیف پول‌های سبک^۱ و کیف پول‌های نصب شده روی موبایل زنجیره‌ی بیت کوین کش را دنبال نکنند. این یکی دیگر از قابلیت‌های ایمنی بود که طرفداران بلاک‌های کوچک از پیاده شدن آن استقبال می‌کردند. با این حال، بعداً مشخص شد که الگوریتم بازتنظیم سختی شبکه در بیت کوین کش دارای اشکال اساسی است، زیرا ماینرها را ترغیب می‌کرد تا شبکه را ترک کنند و دوباره پس از بازتنظیم سختی و افزایش سود دهی، به شبکه بازگردند. این مشکل باعث می‌شد که هشریت شبکه بیت کوین کش بسیار پرنوسان باشد، و این ضعف بزرگ روی قابلیت اطمینان بیت کوین کش به عنوان یک شبکه پرداخت اثر منفی داشت. این اشکال همچنین باعث شد تا بلاک‌ها با سرعت بیشتری ماین شوند، که در نهایت باعث شد بیت کوین کش حدود ۱۰,۰۰۰ بلاک از بیت کوین جلوتر باشد و کوین‌های پاداش تولید بلاک زودتر از موعد استخراج شوند. این اشتباه بزرگی از جانب آموری بود. او می‌بایست بجای ایجاد یک الگوریتم کاملاً جدید، سختی شبکه را فقط برای یک دوره، آن هم فقط در زمان آغاز بیت کوین کش پایین می‌آورد. در نهایت این الگوریتم به طور قابل توجهی بهبود پیدا کرد، با این حال در زمان نوشتن این کتاب همچنان کاملاً برطرف نشده است.

با نزدیک شدن به روز سه‌شنبه ۱ اوت سال ۲۰۱۷، هیجان در هر دو طرف این مناقشه افزایش یافت، این روز می‌رفت تا به یک روز تاریخی در فضای بلاک‌چین تبدیل شود. شماره‌ی آخرین بلاک مشترک بین بیت کوین و بیت کوین کش ۴۷۸,۵۵۹ بود که در ساعت ۱:۱۶ عصر روز ۱ اوت سال ۲۰۱۷ توسط استخراج BTC.com ماین شد. بلاک بعدی بیت کوین هفت دقیقه بعد توسط ViaBTC استخراج شد. استخراج اولین بلاک

1 Light clients

بیت کوین گش حدود ۵ ساعت طول کشید و آن هم توسط ViaBTC ماین شد. پیام زیر در تراکنش کوین بیس این بلاک قرار داده شده بود: «به دنیا خوش آمدی، شویا یانگ!» و سائز آن ۱/۹ مگابایت بود.

این دو کوین بالاخره از یکدیگر جدا شدند و طرفداران آنها می توانستند دیدگاه های خود را دنبال کنند. بلاک بعدی بیت کوین گش هم توسط ViaBTC ماین شد. سومین بلاک بیت کوین گش در اواخر شب به وقت هنگ کنگ استخراج شد و توسط یک ماینر ناشناس تولید شده بود و این پیام در تراکنش کوین بیس این بلاک قرار داده شده بود: «بلاک سفر پیدایش ۲۳-۲۶۹ خیابان هِنسی، ون چای هنگ کنگ!»

من وقتی فردا صبح زود سر کار رفتم، متوجه شدم که اکثریت قریب به اتفاق بلاک های بیت کوین گش حاوی این پیام مرموز هستند. من این آدرس را روی نقشه های سایت گوگل جستجو کردم و متوجه شدم فاصله زیادی با جایی که هستم ندارد و همان کاری را کردم که هر طرفدار دو آتشه ارزهای دیجیتال می کرد، بلافاصله میز کارم را ترک کردم و راهی آنجا شدم. حدوداً ۱۵ دقیقه بعد به آنجا رسیدم و پس از ۵ دقیقه پرسه زدن در آنجا متوجه حضور بن دلو -صاحب صرافی که اصرار به پیاده سازی قابلیت انتشار مجدد در نرم افزار ABC داشت- شدم. به نظر می رسید او در حال بررسی موقعیت است و خیابان را بالا و پایین می کند. با او صحبت کردم و به نظر می رسید که او نیز در موقعیت مشابهی مثل من قرار دارد و عمیقاً گیج شده است. سرانجام ما متوجه دری شدیم که باز بود و به یک پلکان می رسید. ما در زدیم و با صدای بلند «سلام» کردیم، ولی جوابی نشنیدیم. ما تصور می کردیم که این یک بازی رازآلود بیت کوینی است و از پله ها بالا رفتیم تا در نهایت به یک ساختمان نیمه کاره رسیدیم. پس از حدود ۵ دقیقه واکاوی سرانجام شخصی را پیدا کردیم که وضعیت را برای ما توضیح دهد. قرار بود این ساختمان فضای جدیدی برای برگزاری جلسات افراد فعال در بیت کوین و شرکت های نوپا در هنگ کنگ باشد. پیامی که در بلاک های بیت کوین گش قرار داشت در واقع یک روش برای بازاریابی بود،

1 Genesis Block 269-273 Hennessy Road Wan Chai Hong Kong

و پیتر نج^۱ صاحب این مجموعه، یک مزرعه استخراج داشت که به استخراج بیت کوین گش اختصاص داده بود تا به بازاریابی این مکان جدید کمک کند. با این حال، آنجا هنوز آماده نشده بود و ما از اینکه گنجی در یک بازی رمزآلود و جادویی بیت کوین گش پیدا نکرده بودیم، بسیار ناامید شدیم و هر دو به آرامی آنجا را ترک کردیم و به سمت محل کار خود برگشتیم.

در این مرحله حال و هوای جامعه طرفداران بلاک‌های بزرگ خوشنودی مطلق بود. آن‌ها سال‌ها حس می‌کردند که طرفداران بلاک‌های کوچک دست و پای آن‌ها را بسته‌اند و آن‌ها را مورد آزار و اذیت قرار داده‌اند، ولی اکنون آن‌ها بالاخره آزادی خود را به دست آورده بودند. آن‌ها سرانجام به یک کوین دست پیدا کرده بودند که می‌توانستند آن را به فروشندگان معرفی، از آن آزادانه استفاده کنند، و از شر کارمزد تراکنش فلج‌کننده‌ای که بر آن‌ها تحمیل شده بود نجات پیدا کرده بودند. این کوین متعلق به آن‌ها و تحت کنترل خودشان بود، درست شبیه به حسی که سال‌ها پیش نسبت به بیت کوین داشتند. همچنین یک حس انتقام‌جویی هم در این مورد وجود داشت. این فرصتی بود تا به طرفداران بلاک‌های کوچک نشان دهند که چه کارهایی می‌توانند با کوین خود انجام دهند و به آن‌ها ثابت کنند که در اشتباه بوده‌اند.

به نظر می‌رسید استراتژی طرفداران بلاک‌های کوچک این بود که کوین جدید را مسخره کنند و از آن به‌عنوان یک ایده‌احمقانه نام ببرند. برخی از آن‌ها به قصد توهین عبارت «بی‌گش» (Bcash) را به جای بیت کوین گش به کار می‌بردند، و با حذف کلمه بیت کوین از نام این کوین، آن را هرچه بیشتر از بیت کوین جدا می‌کردند. به نظر می‌رسید این اسم موجب رنجش برخی از طرفداران بلاک‌های بزرگ، مخصوصاً راجر ورسه بود و همین باعث استفاده هرچه بیشتر از آن می‌شد. این فورک جنبه مالی هم داشت: هر کس قبل از اجرای این فورک بیت کوین داشت، اکنون صاحب همان مقدار بیت کوین گش می‌شد. طرف‌های مقابل می‌توانستند کوینی که مورد قبول آن‌ها نیست را بفروشند و

1 Peter Ng

به کوینی که طرفدارش هستند تبدیل کنند. از نظر گروه طرفداران بلاک‌های کوچک بیت کوین گش با توجه به نقص‌های اساسی که در چشم‌انداز گروه طرفداران بلاک‌های بزرگ است و عدم تقاضای سرمایه‌گذاران و اشتباهات فنی که آن‌ها حتماً مرتکب خواهند شد، قطعاً در قیمت پایینی احتمالاً حدود ۲ درصد قیمت بیت کوین معامله می‌شد. برخی از طرفداران بلاک‌های کوچک اعلام کردند که دارایی بیت کوین گش خود را خواهند فروخت و قیمت را تا ۲ درصد بیت کوین کاهش خواهند داد.

رویکرد گروه طرفداران بلاک‌های کوچک نسبت به بیت کوین گش در حلقه‌های خصوصی با استراتژی عمومی آن‌ها یعنی به سخره گرفتن این کوین جدید، کاملاً متفاوت بود. آن‌ها دیدگاه ظریف و تاکتیک خود را داشتند. به یاد دارم در آن زمان با یکی از برجسته‌ترین افراد گروه طرفداران بلاک‌های کوچک که مقدار زیادی هم بیت کوین داشت صحبت کردم. به‌طور خصوصی او به من گفت عجله‌ای برای فروش بیت کوین گش‌هایش ندارد. او توضیح داد «اطمینان از موفق بودن بیت کوین گش، حیاتی است»، و افزود اگر بیت کوین گش‌ها بیش از حد سریع فروخته شوند، قیمت به قدری پایین می‌آید که طرفداران بلاک‌های بزرگ خوشبینی خود را نسبت به این کوین جدید از دست می‌دهند. اکثر طرفداران بلاک‌های کوچک می‌خواستند گروه طرفداران بلاک‌های بزرگ بیت کوین را رها کنند و با معرفی هارد فورک‌های خطرناک، پیشنهاد افزایش محدودیت‌های بلاک به‌صورت تهاجمی، و جلوگیری از انجام به‌روزرسانی‌های مهم مانند سگویت موجب مزاحمت نشوند. بنابراین باید اطمینان حاصل می‌شد که بیت کوین گش به یک «سرعت خروج» مناسبی رسیده و برخی از این طرفداران بلاک‌های بزرگ برای همیشه فضا را ترک کرده‌اند. به نظر می‌رسید طرفداران بلاک‌های بزرگ فکر می‌کنند که طرفداران بلاک‌های کوچک از بیت کوین گش متنفر هستند و ترجیح می‌دهند آن‌ها را برای همیشه در بیت کوین به دام بیندازند. با این حال این یک تصور اشتباه بوده است، زیرا تقریباً همه طرفداران بلاک‌های کوچک که من با آن‌ها صحبت کردم از رفتن این گروه خوشحال بودند.

بیت کوین گش پس از گذشت فقط یک ماه از مطرح شدن این ایده و آنقدر سریع راه اندازی شد که صرافی Bitfinex فرصت نکرد بازار آتی برای آن ایجاد کند. معامله این توکن تقریباً بلافاصله در چندین صرافی مثل Kraken آغاز شد و بیت کوین گش در حدود ۱۰ تا ۱۲ درصد قیمت بیت کوین معامله می شد. با این حال امکان واریز بیت کوین گش در صرافی ها وجود نداشت، چون همچنان مشخص نبود که شبکه این کوین جدید برای سپرده پذیری صرافی ها تا چه اندازه امنیت دارد. بنابراین، معامله گران فقط می توانستند بیت کوین گش هایی که در نتیجه فورک در حساب شان بود، را معامله کنند. به عنوان مثال، اگر یک کاربر قبل از اجرای فورک یک بیت کوین در صرافی Kraken نگهداری می کرد، یک بیت کوین و یک بیت کوین گش به او اختصاص می یافت. راه اندازی بیت کوین گش برای بسیاری از صرافی هایی که نمی توانستند پاسخگوی تقاضای مشتریانی باشند که مایل به معامله بیت کوین گش بودند، مشکلات عظیمی بوجود آورد. وبسایت های این صرافی ها از دسترس خارج شدند و فاصله بین ارسال سفارش ها و اجرای آن ها بسیار طولانی شد. به ویژه صرافی Kraken شرایط را بسیار نامطلوب اداره کرد، به طوری که برخی از کاربران آن گزارش می دادند که سفارشات آن ها با تاخیرهای چند روزه تکمیل می شود.

در این مرحله شرایط کمی پیچیده شد. صرافی ها علاوه بر مبادلات آتی^۱، از معاملات اهرمی و بازارهای بدهی استفاده می کردند که انتخاب های صرافی ها را دشوار می کرد. در طول اجرای فورک بیت کوین گش، پلتفرم های مالی مختلف سیاست های متفاوتی داشتند. به عنوان مثال، پلتفرم مشتقات^۲ BitMEX اساساً بیت کوین گش را نادیده گرفت و قیمت معاملات آتی آن در واقع قیمت بیت کوین بود. با این حال به عنوان مثال، Kraken از بیت کوین گش پشتیبانی می کرد، اینگونه که به افرادی که وجه تضمین بلند مدت روی بیت کوین داشتند، بیت کوین گش هم پرداخت می شد. بنابراین اگر شما یک بیت کوین به حساب خود در این صرافی واریز می کردید و یک وجه تضمین بلند مدت^۳ برابر روی آن باز می کردید می توانستید بعد از فورک ۴ بیت کوین گش خود را برداشت کنید. نکته مهم

1 Spot exchanges

2 Derivatives platform

این است که در صرافی Kraken، اگر شما بیت کوین خود را می‌فروختید، به صورت خودکار بیت کوین گش شما هم به فروش می‌رفت.

این سیاست‌های مختلف بین صرافی‌ها می‌توانست مورد سوءاستفاده قرار بگیرد: آن‌ها نامتقارن بودند و از نظر تئوری می‌شد آن‌ها را برای کسب بیت کوین گش رایگان به کار بست. به عنوان مثال می‌شد قبل از اجرای هاردفورک با فروش بیت کوینی که روی BitMEX بود و خرید بلندمدت آن روی صرافی Kraken، بیت کوین گش رایگان بدست آورد. Bitfinex بزرگترین صرافی این فضا در آن زمان، حتی در سیاست‌های خود ناهماهنگی‌هایی داشت. اگر در زمان اجرای فورک شما روی Bitfinex به کسی بیت کوین وام داده بودید، پس از اجرای فورک بیت کوین گش نیز به طلب شما اضافه می‌شد. با این حال اگر شما در زمان اجرای هارد فورک بیت کوین قرض گرفته بودید، پس از اجرای هارد فورک تعهدی به بازپرداخت بیت کوین گش نداشتید. این امر منجر به کمبود بیت کوین گش و پدید آمدن ضریب توزیع ۰/۸۵ برای آن شد. اگر شما در زمان فورک یک بیت کوین در Bitfinex داشتید، در قبال آن فقط ۰/۸۵ بیت کوین گش به شما اختصاص پیدا می‌کرد. در همین حال، کسانی که از این ناسازگاری در سیاست‌های Bitfinex سوءاستفاده کردند، سود خوبی به جیب زدند. ممکن است کسی تصور کند که این سیاست نامناسب بوده است، با این حال باید در نظر گرفت که همه چیز در آن زمان جدید بود و مجسم کردن شرایط و تدوین سیاست‌های درست، کار بسیار دشواری بود. دلیل این سیاست این بود که خرید بیت کوین گش برای افرادی که وام گرفته بودند کار سختی بود، مخصوصاً اگر نقدینگی بیت کوین گش کم می‌بود.

پس از گذشت حدود یک هفته از معاملات پر نوسان، سرانجام صرافی‌ها در تاریخ ۶ اوت سال ۲۰۱۷، به کاربران خود اجازه واریز بیت کوین گش را دادند. اولین صرافی، صرافی Bittrex بود. تا این لحظه، طرفداران بلاک‌های کوچک هیچ راهی برای فروش بیت کوین گش‌هایشان نداشتند، مگر برای آن دسته که قبل از اجرای فورک

بیت کوین‌شان را در صرافی نگه می‌داشتند. البته بسیاری از بیت کوینرها این روش را نمی‌پسندیدند؛ آن‌ها ترجیح می‌دادند از خطر سپردن کلیدهای خصوصی خود به دیگران اجتناب کنند و کنترل آن‌ها را شخصاً بر عهده بگیرند. در این مرحله، طرفداران بلاک‌های کوچک بالاخره می‌توانستند بیت کوین‌کش‌های خود را به صرافی ارسال کرده و آن‌ها را بفروشند. بسیاری از طرفداران بلاک‌های کوچک می‌خواستند بیت کوین‌کش‌های خود را در اسرع وقت بفروشند، زیرا فکر می‌کردند در حال حاضر ارزش آن بیشتر از چیزی است که باید باشد و زمانی که دیگران امکان فروش پیدا کنند، قیمت آن کاهش پیدا خواهد کرد. قدم اول این بود که بیت کوین‌ها را به یک کیف پول جدید منتقل، و بعد کلیدهای خصوصی خود را در یک کیف پول بیت کوین‌کش وارد کنید. به این ترتیب، بیت کوین‌های شما هرگز در معرض خطرات و آسیب‌پذیری‌های نرم‌افزارها و کیف پول‌های بیت کوین‌کش قرار نمی‌گرفت. طرفداران بلاک‌های کوچک می‌توانستند با استفاده از این روش بیت کوین‌کش‌های خود را به صرافی Bittrex ارسال و آن را بفروشند. با این حال آن‌ها باید زمان طولانی منتظر می‌ماندند. با توجه به اینکه هش‌ریت شبکه بیت کوین‌کش به دلیل الگوریتم جدید بازتنظیم سختی بسیار پرنوسان بود، صرافی‌ها بلاک‌های بیشتری را به عنوان تاییدیه درخواست می‌کردند، و عملیات واریز چندین ساعت به طول می‌انجامید. فروشندگان بیت کوین‌کش در صف انتظار برای تأیید تراکنش واریز خود بودند تا بتوانند به فروش کوین‌های خود اقدام کنند.

سرانجام، با ماین شدن اولین بلاک‌هایی که کاربران را قادر به معامله می‌کرد، قیمت بیت کوین‌کش بلافاصله تقریباً ۲۰ درصد کاهش یافت. معامله‌گران آنقدر مشتاق فروش بیت کوین‌کش بودند که بلافاصله پس از واریز شدن کوین‌ها به حساب‌شان، آن‌ها را به بالاترین قیمت پیشنهادی به فروش می‌رساندند. این امر ساعت‌ها ادامه پیدا کرد و قیمت بیت کوین‌کش با استخراج هر بلاک بیشتر سقوط می‌کرد و گروه طرفداران بلاک‌های کوچک هم در رسانه‌های اجتماعی از این موضوع بهره می‌برد و با آن شوخی می‌کرد. برخی از صندوق‌های تجاری فعال در این فضا این الگو را مشاهده کردند: از نظر آن‌ها طرفداران بلاک‌های کوچک به دلایل ایدئولوژیک بیت کوین‌کش‌های خود را می‌فروختند

و این فرصتی بود که آنها می‌توانستند از آن استفاده کنند. این صندوق‌ها بیت‌کوین‌گش‌هایی که توسط طرفداران بلاک‌های کوچک فروخته می‌شد را خریداری می‌کردند و در موقعیت‌های مناسب بعدی به فروش می‌رساندند. مسائل عجیبی در نتیجه این فورک در بازار پدید آمد.

پس از گذشت هیجان اولیه و اوج گرفتن چندباره قیمت، به نظر می‌رسید قیمت بیت‌کوین‌گش در محدوده ۱۵ درصد قیمت بیت‌کوین تثبیت شده باشد. دیدگاه‌های اعضای کانال اژدهایان و برخی از کانال‌های تلگرامی طرفداران بلاک‌های کوچک خیلی پیچیده و محتاطانه بود. پیام‌هایی منتشر می‌شد و از مردم می‌خواست که بیت‌کوین‌گش‌های خود را به کمتر از هفت درصد قیمت بیت‌کوین بفروشند. به نظر می‌رسید منطق آنها این است که با این روش باعث شوند طرفداران بلاک‌های بزرگ بهای اعمالشان را پرداخت کنند. برای مثال، اگر قیمت بیت‌کوین‌گش یک درصد بیت‌کوین بود، این بدان معنا است که اگر طرفداران بلاک‌های بزرگ قبل از فورک ۲۱۰,۰۰۰ بیت‌کوین داشته باشند، از نظر تئوری می‌توانند کل ۲۱ میلیون بیت‌کوین‌گش موجود در بازار را خریداری کنند. سپس آنها می‌توانند قیمت بیت‌کوین‌گش را بالا ببرند و سود خوبی به جیب بزنند، ثروتمند شوند و از موضع قدرت به مقابله با بیت‌کوین پردازند. در مقابل، اگر نسبت تبدیل ۱۰ درصد باشد، در این صورت طرفداران بلاک‌های بزرگ باید برای بدست آوردن همان مقدار بیت‌کوین‌گش، ۱۰ برابر بیت‌کوین بیشتری هزینه کنند. برخی از طرفداران بلاک‌های کوچک از این موضوع آگاه بودند و به همین دلیل افراد دیگر را ترغیب می‌کردند که بیت‌کوین‌گش‌های خود را زیر نرخ تبدیل ۷ درصد بفروشند. «کاری کنید بهای آن را پردازند» در آن زمان عبارت مشهوری بود که در گروه‌ها و جمع‌های خصوصی گروه طرفداران بلاک‌های کوچک پخش می‌شد. این رخدادها به نظر من بسیار جذاب بود. جنگ سردی که اساساً نبردی در زمینه ارتباطات میان گروه‌های مختلف و سیاست بود، اکنون به یک جنگ تمام‌عیار مالی در زمینه سرمایه‌گذاری، بازار، معامله، و سود و زیان تبدیل شده بود.

در اوایل سپتامبر سال ۲۰۱۷، من با گروهی از برجسته‌ترین افراد گروه طرفداران بلاک‌های بزرگ ملاقات کردم. آنان روی این مسأله با یکدیگر اجماع داشتند که ایده اصلی بیت کوین گش تهدید بزرگی بوده است، و قشر وسیع‌تری از کاربران بیت کوین را مجبور به اجرای مرحله دوم توافق‌نامه نیویورک خواهد کرد. با وجود بیت کوین گش مردم خواهند دید که طرفداران بلاک‌های بزرگ دیگر «با کسی شوخی ندارند». آن‌ها به من اطمینان دادند که این روش جواب خواهد داد، چون بیت کوین گش یک تهدید واقعی است. من به یاد دارم که در آن زمان به خودم می‌گفتم آن‌ها خیلی در اشتباه هستند. بیت کوین گش در وهله اول یک هارد فورک بود و به ماینرها یادآوری می‌کرد که در صورت به وقوع پیوستن مرحله دوم توافق‌نامه نیویورک، چاره‌ای جز اجرای یک هارد فورک بر روی شبکه نیست. از فورک زنجیره اتریوم در ژوئیه سال ۲۰۱۶ بیشتر از یک سال می‌گذشت و داشت کم کم از خاطره‌ها محو می‌شد، و اکنون فورک بیت کوین گش بود که عواقب اجرای هارد فورک را به همه یادآوری می‌کرد. همچنین بیت کوین گش مسئولیت‌های اداری زیادی را به صرافی‌ها تحمیل، و طیف وسیعی از پیچیدگی‌ها مانند نحوه مدیریت موجودی وجه ضمان و مدیریت بازارهای بدهی را به مجموعه آن‌ها اضافه کرد. صرافی‌ها به هیچ‌وجه حاضر نمی‌شدند که این مسائل حدود چند ماه دیگر دوباره تکرار شود. از سوی دیگر طرفداران بلاک‌های کوچک استدلال می‌کردند که طرفداران بلاک‌های بزرگ با حمایت از یک کوین متفرقه، از توافق‌نامه نیویورک تخطی کرده‌اند و این توافق‌نامه باطل است. حقیقتاً اگر قرار بود پس از امضای این توافق‌نامه از فورک‌های مختلف یک زنجیره پشتیبانی کنند، اصلاً چه نیازی به این توافق‌نامه بود؟ طرفداران بلاک‌های بزرگ با این ادعا که بیت کوین گش فعالان فضای بیت کوین را وادار به اجرای مرحله دوم توافق‌نامه نیویورک می‌کند، نشان دادند که آن‌ها وضعیت را کاملاً اشتباه درک کرده‌اند و شیپور را از سر گشاد آن می‌زنند. به نظر می‌رسید طرفداران بلاک‌های بزرگ دوباره گل به خودی زده‌اند و اشتباه تاکتیکی بزرگ دیگری را مرتکب شده‌اند.

فصل بیستم

توافق نامه نیویورک - SegWit2x

اکثر طرفداران بلاک‌های کوچک در ابتدا مخالفت شدیدی با فاز دوم توافق نامه نیویورک نشان نمی‌دادند، آن‌ها امیدوار بودند که ابتدا مرحله اول این توافق نامه قبل از شروع درگیری‌های جدی با موفقیت انجام پذیرد. در اوت سال ۲۰۱۷، وقتی سگویت روی شبکه قفل شد، زمان افزایش مبارزات علیه مرحله دوم این توافق نامه فرا رسید. در این مرحله از درگیری، برخلاف روزهای آغازین آن، گروه طرفداران بلاک‌های کوچک از حمایت اکثریت کاربران بیت کوین برخوردار بودند. طرفداران بلاک‌های کوچک از راه استدلال منطقی و همچنین به دلیل موفقیت‌هایی که به دست آورده بودند، توانستند پشتیبانی بخش بزرگی از جامعه معامله‌گران را نیز بدست آورند. اکثر افراد ترجیح می‌دادند از طرف برنده حمایت کنند.

با پیشرفت جنگ، شخصیت‌های اصلی گروه طرفداران بلاک‌های بزرگ هم تغییر می‌کردند. گروه طرفداران بلاک‌های کوچک در دور اول کوین اندریسن و مایک هرن، و در دور دوم راجر وور و جیهان وو را شکست دادند. سرانجام نوبت به دور سوم و شکست دادن جف گارزیک و مایک بلشه رسید. جف گارزیک توسعه‌دهنده اصلی

نرم افزار SegWit2x و مایک بلشه مدیرعامل شرکت BitGo به نمایندگی از گروه طرفداران بلاک های بزرگ در خط مقدم این جنگ حاضر بودند. راجر وور و جیهان وو در این مرحله از جنگ عقب نشینی کرده، و در عوض تلاش های خود را بر روی تبلیغ بیت کوین گش متمرکز کرده بودند.

در ۳ اوت سال ۲۰۱۷، تغییری در نرم افزار Bitcoin Core بوجود آمد که به موجب آن نودهای نرم افزار BTC1 از ارتباط با نودهای Bitcoin Core منع می شدند. استدلال آن ها این بود که چون به هر صورت قرار است این دو شبکه از یکدیگر جدا شوند، این کار به نفع هر دو کوین است و به آن ها اجازه می دهد تا ارتباط قوی تری با نودهای شبکه خود برقرار کنند. با این حال جف گارزیک از این موضوع راضی نبود و اظهار داشت:

با وجودی که در حال حاضر نرم افزار Bitcoin Core و SegWit2x کاملاً بر اساس قوانین ۱۰۰٪ یکسانی به اعتبارسنجی بلاک ها می پردازند، این تغییر موجب ایجاد شکاف در زنجیره خواهد شد؛ به دلیل انحراف های احتمالی که ممکن است در آینده میان قوانین پروتکل های این دو کوین پدید آید، امروز شاهد ایجاد شکاف در شبکه خواهیم بود. ناگزیر جزایر پیش بینی ناپذیری پدید خواهند آمد. این یک تغییر بسیار خصمانه و ناامن قبل از اجرای فورک segwit2x است.

اگرچه این تغییر در Bitcoin Core از نظر فنی برای هر دو کوین در زمان فورک یک مزیت محسوب می شد، ولی پیام سیاسی آن روشن بود. Bitcoin Core روی زنجیره فعلی بیت کوین به کار خود ادامه خواهد داد و SegWit2x را پیاده سازی نخواهد کرد.

یکی دیگر از تاکتیک های طرفداران بلاک های کوچک به منظور تلاش برای منصرف کردن جامعه فعالان بیت کوین از اجرای نرم افزار BTC1 برجسته کردن دورویی جف گارزیک بود. به نظر می رسید جف گارزیک در سال ۲۰۱۲ مطلبی را بیان کرده بود که دقیقاً شبیه به نکاتی است که طرفداران بلاک های کوچک مطرح می کردند:

در صورتی که [نرم‌افزار] کاربران به صورت دسته‌جمعی از پذیرش و رله^۱ کردن بلاک‌های شما سر باز بزنند، ۵۱ درصد توان هَش یا حتی ۹۰ درصد آن هیچ فایده‌ای نخواهد داشت.

حتی در فوریه سال ۲۰۱۳، گارزیک در مورد اهمیت اقتصادی یک هارد فورک، و مشکلات مربوط به پیاده‌سازی نشدن قابلیت حفاظت اجباری در برابر انتشار مجدد^۲ صحبت کرده بود. این مسائل با توجه به اینکه من برای اولین بار در معرض آن‌ها قرار می‌گرفتم، بسیار تکان دهنده بود. و حالا از قضا او در حال توسعه نرم‌افزاری بود که دقیقاً همان کارهایی را انجام می‌داد که حدود چهار سال قبل علیه آن‌ها بحث کرده بود. البته عقاید هر شخصی می‌تواند با گذر زمان تغییر کند و این به معنی این نیست که جف گارزیک بدخواه یا دورو است. با این حال این موضوع موجب شد طرفداران بلاک‌های کوچک او را بخاطر کوتاه آمدن از اصول خود برای خوشایند شرکت‌های بزرگ، سرزنش کنند. گارزیک در فوریه سال ۲۰۱۳ نوشت:

باید قبل از وارد شدن به مقوله تغییر محدودیت سائز بلاک، مفهوم هارد فورک و اثرات اقتصادی آن را درک کنیم. هارد فورک رویداد مهمی است که در خلال آن دست کاربران موجه بیت کوین را از شبکه کوتاه، کوین‌ها را غیرقابل استفاده، و بسته به وضعیت نرم‌افزار نودی که به آن متصل شده‌اید (اینکه به روزرسانی شده یا نه)، امکان خرج کردن یک کوین روی دو شبکه مجزا را فراهم می‌کند. اگر بخواهیم کمی آن را دراماتیک کنیم، هارد فورک رویدادی ویرانگر است. اگر هارد فورک به درستی اجرا نشود ممکن است موجب بروز شبهه در [اصالت] بیت کوین دریافت شده توسط پذیرندگان شود، و این با پایه و اساس ارزش اقتصادی آن‌ها در تضاد است. علاوه بر این، هارد فورک شبیه به مجمع تغییر قانون اساسی است چون امکان بازنویسی قوانین اساسی بیت کوین را میسر می‌کند؛ خواه این بازنویسی تغییر محدودیت سائز بلاک، تغییر سقف ۲۱ میلیون، تغییر الگوریتم

1 Relay

2 Mandatory replay protection

هش SHA256، یا تغییر هر کدام از قوانین اجماع دیگر باشد. بنابراین، همیشه این خطر وجود دارد که ماینرها، کاربران، و توسعه‌دهندگان وجود داشته باشند که بخواهند علاوه بر تغییر محدودیت سائز بلاک، نسبت به تغییر دیگر قوانین اجماع اقدام کنند؛ با این استدلال که از نظر فنی و مهندسی بهترین زمان برای تغییر این قوانین در زمان اجرای هارد فورک‌ها است. هارد فورک‌ها شبیه به گزینه بمب اتم هستند و پیامدهای اقتصادی گسترده‌ای برای همه کاربران بیت کوین دارند.

تاکتیک دیگر گروه طرفداران بلاک‌های کوچک تهیه لیست رسمی حامیان SegWit2x بر اساس سند توافق‌نامه نیویورک بود. آن‌ها قصد داشتند نقایص این توافق‌نامه را از راه برگزاری نشست‌های حضوری و همچنین برقراری تماس با این شرکت‌ها به آن‌ها توضیح دهند. مخصوصاً اینکه اجرای آن موجب بروز یک شکاف در زنجیره بیت کوین خواهد شد، و با توجه به پیاده‌سازی نشدن قابلیت جلوگیری از انتشار مجدد - برخلاف بیت کوین کش - احتمالاً برخی از کاربران سرمایه خود را از دست خواهند داد. تعداد این شرکت‌ها زیاد بود و به احتمال زیاد برخی از آن‌ها نقاط ضعف NYA را درک نکرده بودند. انفصال هریک از این شرکت‌ها می‌توانست به این توافق‌نامه صدمات قابل توجهی وارد کند و می‌توانست نشانه‌ای باشد از مخالفت با این طرح و نبود اجماع در بین امضاءکنندگان اصلی آن، چه برسد به اجماع طیف وسیع‌تری از کاربران بیت کوین.

اولین عقب‌نشینی در ۲۲ اوت سال ۲۰۱۷ رخ داد. Bitwala اعلام کرد که از این توافق پیروی نخواهد کرد:

ما سؤالات زیادی در مورد حمایت Bitwala از توافق‌نامه نیویورک (مخفف NYA) دریافت کرده‌ایم.

...

این توافق‌نامه موجب رشد سیگنال آمادگی برای اجرای سگویت به میزان بالاتر از آستانه لازم، و در نهایت منجر به فعال‌سازی این سافت فورک بدون هیچ مشکلی بر روی شبکه بیت کوین شد. تقریباً همزمان با این رخداد، گروهی از ماینرها تصمیم گرفتند تا زنجیره جدیدی بر پایه زنجیره دربردارنده اولین بلاک بیت کوین پدید آورند و نام آن را نیز «بیت کوین کش» (BCH) گذاشتند. سگویت از زنجیره بیت کوین کش حذف، و تغییراتی در آن اعمال شد که بتواند از بلاک‌های ۸ مگابایتی پشتیبانی کند.

...

Bitwala از توسعه‌دهندگان بیت کوین حمایت مالی نمی‌کند، و هیچکدام از آن‌ها را استخدام نکرده است، بنابراین ما تأثیری روی فعالیت‌های تیم توسعه پروتکل بیت کوین نداریم. ما می‌خواهیم نسبت به قراردادی که بر روی آن توافق کرده‌ایم (به‌عنوان یکی از اولین شرکت‌هایی که به آن پیوستیم و این واقعیت را نمی‌دانستیم که اکثر توسعه‌دهندگان به آن نخواهند پیوست) متعهد بمانیم. با وجود این ما یک شرکت خدماتی هستیم و همواره از آنچه مشتریان ما استفاده می‌کنند و می‌خواهند استفاده کنند پیروی خواهیم کرد.

...

ما از زنجیره‌ای که به‌عنوان «بیت کوین» شناخته، و توسط تیم فعلی توسعه‌دهندگان پروتکل بیت کوین پشتیبانی می‌شود، جدا نخواهیم شد.

این لحظه مهمی در تاریخ مقابله با مرحله دوم توافق‌نامه نیویورک، و اولین جدایی از آن بود. با این حال یک پیروزی کامل نبود. به نظر می‌رسید Bitwala قصد دارد زنجیره‌ای که مورد حمایت «تیم فعلی توسعه‌دهندگان پروتکل» است را دنبال کند، و این لزوماً به معنی پشتیبانی از زنجیره فعلی قوانین نبود؛ مگر اینکه پشتیبانی گسترده‌ای برای تغییر

قوانین وجود داشت. این باعث به وجود آمدن این تصور غلط شد که این یک نبرد میان توسعه‌دهندگان و ماینرها است، و Bitwala طرف توسعه‌دهندگان را گرفته است. علیرغم چهارچوب جدیدی که طرفداران بلاک‌های بزرگ برای تفسیر تصمیم Bitwala تعریف کردند، گروه طرفداران بلاک‌های کوچک این رخداد را به‌عنوان یک پیروزی تلقی کردند و جشن گرفتند.

با وجود عقب‌نشینی Bitwala، مایک بلشه مشتاق بود که همچنان پروژه و کارها را در مسیر خود پیش ببرد. در ۲۳ آوت سال ۲۰۱۷، او در لیست گروه ایمیلی Segwit2x نوشت:

با توجه به فعال شدن سگویت، اکنون زمان مناسبی برای اطلاع‌رسانی در مورد پروژه است. شاید شما هم متوجه شده باشید که این اواخر تیم Segwit2x خیلی ساکت بوده است. این نشانه خوبی است چون نشان می‌دهد که کُد نرم‌افزار مطابق انتظار کار می‌کند. هدف Segwit2x ایجاد یک نرم‌افزار ساده، پایدار، و «حوصله سر بر»^۱ است. نشانه خوبی است اگر در هفته‌های آینده هم خبرهای زیادی از توسعه Segwit2x نشنوید.

در ۳۱ اوت، F2Pool یکی از استخرهای استخراج بیت کوین که این توافق‌نامه را امضاء کرده بود، اعلام کرد که قصد پشتیبانی از Segwit2x را ندارد. اگرچه در آن زمان این استخر همچنان علامت "NYA" را در سربرگ بلاک‌های خود قرار می‌داد، ولی وانگ چان^۲، متصدی این استخر اظهار کرد که قصد دارد بعد از راه‌اندازی مجدد سرورهای خود این علامت را حذف کند. این یکی دیگر از شکست‌های مهم این توافق‌نامه به شمار می‌آید. با در اختیار داشتن یک استخر استخراج بزرگ، زنجیره بیت کوین به پیش می‌رفت و تا زمانی که سرمایه‌گذاران زنجیره حاوی قوانین اصلی بیت کوین را ترجیح می‌دادند (که در این مرحله به نظر می‌رسید اینگونه باشد)، احتمالاً ماینرهای بیشتری دست از حمایت از این

1 boring
2 Wang Chan

توافق نامه می کشیدند و برای کسب سود بیشتر روی زنجیره اصلی بیت کوین به استخراج مشغول می شدند.

در تاریخ ۱ اوت، مدیرعامل و بنیانگذار شرکت Wayniloans، یکی دیگر از شرکت‌هایی که این توافق نامه را امضاء کرده بود در توثیقی نوشت که آن‌ها هیچوقت با همه متن توافق نامه NYA موافق نبوده‌اند و این توافق پس از امضاء این شرکت تغییر کرده است. این موضوع چند هفته بعد از طریق یک ایمیل تأیید شد، که بری سیلبرت به آن پاسخی داد که نشان‌دهنده میزان ناامیدی او بود:

مطمئناً شما در لغو پشتیبانی خود از Segwit2x مختار هستید، ولی بیانیه شما دقیق نیست. من در تاریخ ۲۱ مه، ساعت ۸:۴۰ عصر، ایمیلی مبنی بر تأیید حمایت شما از بیانیه نهایی این توافق نامه دریافت کردم و این ایمیل در ۲۳ مه منتشر شد. همچنین، لازم به یادآوری است که از طرف شرکت Wayniloans برای اضافه شدن به لیست حامیان این توافق نامه با من تماس گرفته شد و ما تماسی با ایشان نداشتیم، بنابراین من از چیزهایی که به شما گفته‌اند اطلاعی ندارم.

در این مرحله تعداد لغو حمایت‌ها از توافق نامه نیویورک افزایش یافت. در تاریخ ۲۶ سپتامبر ۲۰۱۷، شرکت Vaultero پشتیبانی خود را از این توافق نامه لغو کرد:

ما این توافق نامه را خیلی قبل تر از وقوع رخداد فورک بی گش امضاء کردیم. هدف ما از امضاء این توافق نامه رفع بن‌بست‌های موجود بین طرف‌های درگیر بود. اکنون به هدف خود رسیدیم و اکنون سگویت بر روی شبکه فعال شده است. من مثل هر تاجر خوشنام دیگری به حرف و امضاء خود پایبندم و دوست داشتم از 2x حمایت کنم، ولی بدون قابلیت محافظت از انتشار مجدد تراکنش قادر به انجام این کار نیستم.

صرافی آمریکای جنوبی surBTC نیز حمایت خود را از NYA پس گرفت:

ما نمی‌توانیم وانمود کنیم که در حوزه مقیاس‌پذیری بیت‌کوین متخصص هستیم. ما معتقدیم تلاش برای ایجاد تغییر در قوانینی که از نظر توسعه‌دهندگان پروتکل بیت‌کوین ایمن نیست، کار اشتباهی است. سطح سابقه فنی تیمی که در حال حاضر روی هسته پروژه بیت‌کوین با یکدیگر همکاری می‌کنند، بی‌نظیر است. ما معتقدیم آن‌ها حداقل به‌عنوان یک گروه، متخصصان بی‌طرفی هستند و نظر آن‌ها شایسته شنیده شدن است. با اینکه ما از وجود بلاک‌های بزرگ برای پاسخ‌گویی به تقاضای روزافزون کاربران بسیار خوشحال می‌شویم، ولی احساس می‌کنیم برای اجرای مسئولانه این امر حداقل به حمایت حداکثری توسعه‌دهندگان پروتکل بیت‌کوین نیاز خواهیم داشت. ما این پشتیبانی را ندیده‌ایم و شرایط مخزن کُد btc1 را از نظر ملاحظات فنی و همکاری در توسعه این پروژه اپن-سورس نمی‌پسندیم.

سپس صرافی Crypto Facilities از این توافق خارج شد. مدیرعامل Kraken، شرکتی که سرانجام Crypto Facilities را خریداری کرد هم یکی دیگر از افرادی بود که به دلیل پیاده‌سازی نشدن قابلیت جلوگیری از انتشار مجدد با SegWit2x مخالفت کرد. Bitfury هم یکی دیگر از امضاءکنندگانی بود که اعلام کرد به‌طور بالقوه تمایلی برای اجرای مرحله دوم توافق‌نامه نیویورک ندارد. حساب شرکت‌هایی که از این توافق خارج می‌شدند - به دلیل تعداد زیادشان - دیگر از دست خارج شده بود و به نظر می‌رسید این توافق‌نامه در حال فروپاشی است.

برخی از امضاءکنندگانی که از این توافق خارج می‌شدند، متعلق به اردوگاه گروه طرفداران بلاک‌های بزرگ بودند. یکی از آن‌ها شرکت Yours بود که اعلام کرد قصد دارد همه توان خود را بر روی زنجیره بیت‌کوین گش منتقل کند. Antpool، استخراج استخراج متعلق به شرکت Bitmain هم به استخراج بر روی زنجیره بیت‌کوین گش مشغول شده بود. البته می‌توان ادعا کرد که پشتیبانی و استخراج بیت‌کوین گش به معنی

خروج از توافق نیست. ممکن است یک نفر بگوید یک کسب و کار حق دارد به منظور کسب درآمد یا پشتیبانی از کوین‌های مختلف بر روی زنجیره‌های گوناگون، به استخراج چند کوین متفاوت مشغول باشد. این روش برای کسب و کارها عادی است و از آن‌ها پذیرفته می‌شود. با این حال، اگر وضعیت به این گونه باشد که امضاءکنندگان بتوانند پس از اجرای فورک به حمایت از دو کوین به وجود آمده ادامه دهند و ماینرها بتوانند به استخراج بر روی هر دو زنجیره ادامه دهند، می‌توان استدلال کرد که در این صورت توافق نامه نیویورک تا حد زیادی بی‌معنی است و هر دوی این زنجیره‌ها ادامه پیدا خواهند کرد. طرفداران بلاک‌های کوچک معتقد بودند قابلیت جلوگیری از انتشار مجدد به همین دلیل ضروری است، و SegWit2x بدون پیاده‌سازی این قابلیت به‌طور بالقوه یک حرکت خصمانه است، بنابراین نباید مورد حمایت کسب و کارهایی قرار گیرد که رفتاری مسئولانه دارند.

مایک بلشه در تاریخ ۱۸ اکتبر سال ۲۰۱۷، علی‌رغم چشم‌انداز رو به افول SegWit2x و تقاضای جدی برای پیاده‌سازی قابلیت جلوگیری از انتشار مجدد، کار را همچنان پیش می‌برد:

به قول شما «قابلیت محافظت از انتشار مجدد»^۱، موجب ایجاد شکاف در زنجیره می‌شود. از کار انداختن ناگهانی بیش از ۱۰ میلیون نرم‌افزار کیف پول SPV^۲ بی‌معنی است. هدف SegWit2x جلوگیری از رخ دادن این اتفاقات است. امروز ما با همکاری اکثریت قریب به اتفاق ماینرهایی که از SegWit2x پشتیبانی می‌کنند، در مسیر اجرای آن هستیم. علاوه بر آن ۹۹/۹۴ درصد نودها و SPVها به‌طور خودکار از طولانی‌ترین زنجیره یعنی زنجیره segwit2x پیروی می‌کنند. من می‌دانم افرادی هستند که نمی‌خواهند بیت کوین به این صورت کار کند، ولی به‌روزرسانی‌های بیت کوین از این روش پیاده‌سازی می‌شوند.

1 Replay protection
2 Simple Payment Verification

سپس برخی از حامیان SegWit2x استدلال کردند که قابلیت محافظت اجباری از انتشار مجدد باید توسط زنجیره اصلی بیت کوین پیاده‌سازی شود، چون قرار بود این زنجیره هشریت پایین‌تری [نسبت به زنجیره SegWit2x] داشته باشد. ولی این موضوع واقعاً عملی نبود چون قابلیت محافظت اجباری از انتشار مجدد یک تغییر ناسازگار بود و منجر به پدید آمدن یک کوین جدید و شکاف در زنجیره می‌شد، بنابراین به جای ۲ کوین، ۳ کوین متفاوت به وجود می‌آمد. پاسخ گروه طرفداران بلاک‌های کوچک این بود که پیاده‌سازی این قابلیت فقط در نرم‌افزار ناسازگار [با قوانین فعلی شبکه] امکان‌پذیر است.

صرافی Bitfinex در ۶ اوت سال ۲۰۱۷، توکن‌های پدید آمده از به‌روزرسانی SegWit2x را شبیه به کاری که اوایل سال برای کوین Bitcoin Unlimited کرده بود، در صرافی خود لیست کرد. این کوین بین ۴ تا ۲۰ درصد قیمت بیت کوین معامله می‌شد. این نشان‌دهنده این بود که اغلب فعالان اقتصادی، یعنی دست‌کم سرمایه‌گذاران و معامله‌گران از زنجیره اصلی بیت کوین، نه SegWit2x حمایت می‌کردند.

این شرکت همچنین موضع خود را در ارتباط با فورک زنجیره روشن کرد و اظهار داشت که در وهله اول زنجیره «پیاده‌سازی فعلی» را به عنوان بیت کوین می‌شناسد و زنجیره جدید را به عنوان یک کوین جایگزین و با نام «B2X» در نظر خواهد گرفت. این سیاست به گفته Bitfinex، حتی تحت شرایطی که زنجیره B2X از هشریت بالاتری برخوردار می‌شد، به قوت خود باقی بود. با این حال، این شرکت همه درها را بر روی حمایت از NYA نبست و اظهار کرد که «فعالان بازار می‌توانند طرح‌های جایگزینی را برای نام‌گذاری [این کوین‌ها] پیشنهاد دهند». اساساً منظور این شرکت این بود که در نهایت اینکه کدام یک از این کوین‌ها به عنوان بیت کوین شناخته می‌شود بر عهده سرمایه‌گذاران و معامله‌گران است و بستگی به این دارد که کدام یک از آن‌ها قیمت بیشتری در بازار داشته باشد.

با توجه به اینکه به نظر می‌رسد پروتکل اجماع Segwit2x فعال شود، ما فعلاً نماد B2X را برای فورک Segwit2x در نظر گرفته‌ایم. پیاده‌سازی فعلی (بر اساس پروتکل اجماع فعلی بیت کوین) همچنان با نماد BTC معامله خواهد شد، حتی اگر زنجیره B2X توان هش بیشتری داشته باشد. ما این کار را به دلایل اجرایی و عملیاتی انجام می‌دهیم و ملاحظات سیاسی در اینجا موضوعیتی ندارد. ما قادر به تغییر یا تخصیص دوباره نمادها نیستیم، ولی می‌توانیم برچسب نام یا توضیحات این نمادها را تغییر دهیم. فعلاً، BTC به عنوان «Bitcoin»، و B2X به عنوان «B2X» برچسب گذاری خواهد شد. این امر تا زمانی که نیروهای فعال بازار طرح نام گذاری جایگزین و مناسب‌تری را برای یک یا هر دو زنجیره پیشنهاد دهند، ادامه خواهد یافت.

حدود یک هفته بعد یعنی در تاریخ ۱۳ اکتبر سال ۲۰۱۷، شرکت BitMEX بیانیه‌ای منتشر کرد که حتی از بیانیه Bitfinex هم محکم‌تر بود و در آن خاطر نشان کرد که زنجیره B2X را به عنوان کوین متفرقه در نظر می‌گیرد، حتی اگر از توان هش بالاتری برخوردار باشد:

هدف پیشنهاد Segwit2x (B2X) افزایش سایز بلاک است و قرار است در نوامبر سال ۲۰۱۷ اجرا شود. این تغییر با مجموعه قوانین فعلی پروتکل بیت کوین ناسازگار است و بنابراین ممکن است یک کوین جدید ایجاد شود. طرفداران آن امیدوارند که این کوین جدید به عنوان بیت کوین شناخته شود، ولی اینکه کدام کوین به عنوان بیت کوین شناخته می‌شود را طرفداران کوین جدید تعیین نمی‌کنند و این سرمایه‌گذاران و معامله‌گران هستند که تصمیم می‌گیرند کدام کوین ارزش بیشتری دارد. برای اجرای هرچه بهتر این فرآیند، پیاده‌سازی قابلیت جلوگیری از انتشار مجدد تراکنش‌ها (به صورت دوطرفه) الزامی است. تا جایی که ما اطلاع داریم پیشنهاد Segwit2x به طور پیش فرض، قابلیت جلوگیری از انتشار مجدد تراکنش‌ها را فعال نکرده است. بنابراین BitMEX قادر به پشتیبانی از Segwit2x نخواهد بود. به این ترتیب، BitMEX از توزیع B2X پشتیبانی نمی‌کند و همچنین مسئولیتی هم

در قبال B2Xهایی که به این صرافی ارسال می‌شود، بر عهده نخواهد گرفت. این سیاست حتی در صورتی که زنجیره Segwit2x دارای اکثریت هش‌ریت باشد، اعمال خواهد شد.

آرتور هیز^۱ مدیرعامل BitMEX در تاریخ ۲۳ اکتبر مطلبی با عنوان «معامله‌شست کوین x2» منتشر کرد. این مِم^۲ مورد استقبال طرفداران بلاک‌های کوچک قرار گرفت و وضعیت را برای آخرین حامیان NYA سخت‌تر کرد. به نظر می‌رسید اگر آن‌ها این کوین را روانه بازار کنند در نهایت تبدیل به آلت کوین دیگری خواهد شد که زیر ۱۰ درصد قیمت بیت کوین معامله می‌شود.

روز بعد، جف گارزیک اعلام کرد که در حال راه‌اندازی کوین جدیدی به نام Metronome است. این برای گروه طرفداران بلاک‌های کوچک فرصت جدیدی به وجود آورد تا زبان به انتقاد از پروژه Segwit2x بکشایند و اظهار کنند که توسعه‌دهنده اصلی این پروژه تمرکز خود را از دست داده و مشغول کار بر روی پروژه‌های دیگر شده است. گزارش بلومبرگ^۳ از این رویداد به شرح زیر است:

جف گارزیک، یکی از معدود توسعه‌دهندگان کلیدی بیت کوین که در ایجاد زیرساخت‌های بیت کوین (که به بلاک‌چین معروف است) مشارکت داشته، نواقص این سیستم را از نزدیک مشاهده کرده است. بنابراین تصمیم به ساخت یک ارز دیجیتال بهتر گرفته است. او نام آن را مترونوم گذاشته است و می‌گوید این اولین موردی است که می‌تواند روی بلاک‌چین‌های مختلف کار کند. این قابلیت جابجایی به این معناست که اگر یک بلاک‌چین در نتیجه درگیری بین توسعه‌دهندگان یا به دلیل کاهش استفاده از بین برود، صاحبان مترونوم می‌توانند دارایی خود را به جای دیگری منتقل کنند. گارزیک، یکی از بنیان‌گذاران

1 Arthur Hayes
2 Meme
3 Bloomberg

استارتاپ Bloq که مترونوم را ایجاد کرده است در یک مصاحبه تلفنی اظهار کرد که این امر به حفظ ارزش کوین‌ها و همچنین طول عمر آنها کمک می‌کند.

شرکت کوین بیس^۱ در تاریخ ۲۳ اکتبر سال ۲۰۱۷ سیاست خود را در رابطه با SegWit2x اعلام کرد. کوین بیس یکی از امضاءکنندگان توافق‌نامه نیویورک بود و تا اینجای کار از آن خارج نشده بود. همچنین با توجه به سابقه پشتیبانی این شرکت از هارد فورک‌های سایر پروژه‌ها، همگان در انتظار اعلام سیاست‌های این شرکت بودند. این شرکت هم دقیقاً به مانند Bitfinex و BitMEX اعلام کرد که به توافق‌نامه نیویورک متعهد نخواهد بود و کوین SegWit2x را به عنوان یک کوین متفرقه در نظر می‌گیرد:

پیش‌بینی می‌شود که فورک SegWit2x در تاریخ ۱۶ نوامبر اجرا، و به طور موقت موجب ایجاد دو زنجیره مجزا در شبکه بیت کوین شود. کوین بیس پس از اجرای فورک همچنان زنجیره فعلی بیت کوین را به عنوان بیت کوین (BTC) می‌شناسد، و عنوان Bitcoin2x (B2x) را به زنجیره فورک شده اختصاص می‌دهد.

گروه طرفداران بلاک‌های کوچک از این اتفاقات خوشحال بودند. به نظر می‌رسید سرانجام کوین بیس نیز به اردوگاه آنها پیوسته، و این آخرین میخ بر تابوت SegWit2x بود. گروه طرفداران بلاک‌های کوچک ایمیل‌ها و پیام‌های زیادی به مدیرعامل کوین بیس، برایان آرمسترانگ ارسال کردند و پیش گرفتن این سیاست را به او تبریک گفتند. کوین بیس در قبال دارایی‌های مشتریان خود مسئولیت داشت و در هر صورت باید از هر دو زنجیره این فورک پشتیبانی می‌کرد، بنابراین برخی معتقد بودند امضاء توافقی که فقط از یکی از طرفین این فورک احتمالی پشتیبانی می‌کند برای شرکتی که باید از دارایی مشتریان خود به صورت امانی نگهداری کند کار درستی نیست. شاید این شرکت اکنون متوجه شده است که امضاء توافق‌نامه نیویورک کار نادرستی بوده است.

1 Coinbase

با این حال، کوین بیس دو روز بعد و در یک اقدام بسیار عجیب مطلبی در تضاد با تصمیم قبلی این شرکت در وبلاگ خود منتشر کرد. این شرکت در این بیانیه جدید اعلام کرد که زنجیره دارای بیشترین اثبات کار از نظر آن‌ها بیت کوین است:

در مطلب قبلی منتشر شده در وبلاگ اعلام شد که ما در زمان اجرای هارد فورک، زنجیره فعلی را بیت کوین، و زنجیره Segwit2x را Bitcoin2x می‌نامیم. با این حال برخی از مشتریان از ما درباره وضعیت [نام‌گذاری زنجیره‌ها] پس از اجرای هارد فورک پرسیده‌اند. ما به زنجیره‌ای که دارای بیشترین اثبات کار باشد بیت کوین می‌گوییم.

البته، حتی این بیانیه را نیز می‌توان به عنوان بی‌اعتنایی شرکت کوین بیس به NYA تلقی کرد. هدف از توافق نیویورک این بود که امضاءکنندگان آن کوین جدیدی که پدید می‌آید را به عنوان بیت کوین بپذیرند و از آن حمایت کنند، نه اینکه میان کوین اصلی و جدید موضعی خنثی اتخاذ کنند. این سیاست جدید شرکت کوین بیس که توسط چندین صرافی دیگر (مثل Gemini) که در ایالات متحده مستقر بودند نیز اتخاذ شده بود، طرفداران بلاک‌های کوچک را گیج و سردرگم کرد.

وقتی فرآیند کارها با دقت مورد بررسی قرار می‌گرفت، سیاست جدید کوین بیس بی‌معنی به نظر می‌رسید. در مورد لیست سفارشات خرید و فروش^۱ و نماد نیز، این شرکت باید وارث کوین اصلی را انتخاب می‌کرد. در غیر این صورت این شرکت باید [معاملات این کوین] را در صرافی تعطیل می‌کرد. به نظر می‌رسید این تصمیم از نظر تجاری تصمیم بدی است و منجر به از دست رفتن درآمد این شرکت - درست در زمانی که تقاضای معاملاتی افزایش می‌یافت - می‌شد. نکته دیگر اینکه، کوین بیس پس از گذشت چه زمانی تعیین می‌کرد که کدام زنجیره دارای بیشترین هش‌ریت است: پس از گذشت یک ساعت [از اجرای هارد فورک]، یک روز، یک هفته، یک ماه، یا یک سال؟ کوین بیس هیچ‌وقت این

1 Order book

موضوع را روشن نکرد. البته امکان این وجود داشت که اکثریت هش‌ریت بین این دو زنجیره رقیب در فواصل زمانی جابجا شود. ماینرها به احتمال زیاد بازارها را برای تعیین کوین با ارزش‌تر مورد بررسی قرار می‌دادند و این بازارها در انتخاب کوینی که مایل به ماین آن هستند کمک می‌کردند. اگر صرافی‌ها تعطیل می‌شدند، ماینرها این اطلاعات را از کجا بدست می‌آوردند؟ هر دو گروه یعنی صرافی‌ها و ماینرها اساساً معطل یکدیگر می‌شدند. به نظر می‌رسید کوین‌بیس در صدد شانه خالی کردن از مسئولیت خود که همانا کمک به برقراری نظم در بازارها - در فضایی پر از شک و تردید - و کمک به تسهیل فرآیند اقتصادی که در آن سرمایه‌گذاران می‌توانند نظر خود را بیان، و به ماینرها منتقل کنند، بود. به نظر من روشی که Bitfinex و BitMEX در پیش گرفته بودند، از روش نابسامان و گیج‌کننده Coinbase مسئولیت‌پذیرتر و شفاف‌تر بود.

با رسیدن به پایان ماه اکتبر، مخالفت در برابر اجرای SegWit2x در جامعه فعالان بیت کوین مهارشدنی نبود. بیانیه‌هایی در اعتراض به اجرای SegWit2x در نشست‌های محلی ارائه و تأکید می‌شد که آن‌ها زنجیره اصلی را به عنوان بیت کوین می‌شناسند. این بیانیه‌ها توسط جوامع محلی واقع در کره، هنگ کنگ، ایتالیا، آلمان، اسرائیل، برزیل، و آرژانتین منتشر شد. بیانیه اسرائیل به شرح زیر است:

ما معتقدیم برای تغییر قوانین پروتکل پولی که نام «بیت کوین» را به یدک می‌کشد (منحوصاً از راه هارد فورک)، نیاز به یک اجماع همگانی داریم. هارد فورک SegWit2x قادر به فراهم کردن این اجماع لازم نیست و تا زمانی که شرایط به این صورت باشد ما نمی‌توانیم پولی که در نتیجه اجرای این فورک پدید می‌آید را «بیت کوین» بنامیم.

جامعه فعالان هنگ کنگ لحن تندتری به کار برده بود:

قابلیت جلوگیری از انتشار مجدد تراکنش‌ها در SegWit2x پیاده‌سازی نشده است و اجماع همگانی برای اجرای آن میان فعالان بیت کوین وجود ندارد. با توجه به فقدان این قابلیت و نبود توافق میان فعالان، از نظر ما SegWit2x تلاشی بی‌پروا است که باعث بروز اختلال در اکوسیستم خواهد شد و به آن آسیب خواهد زد. بنابراین ما به شدت با SegWit2x مخالف هستیم، حتی اگر زنجیره SegWit2x از هشریت اکثریت برخوردار، یا قیمت بالاتری داشته باشد.

آخرین کنفرانس مقیاس‌پذیری بیت کوین با عنوان Scaling IV در خلال مناقشه سائز بلاک، در روزهای آخر هفته ۴-۵ نوامبر سال ۲۰۱۷ در دانشگاه استنفورد واقع در ایالات متحده آمریکا برگزار شد. درست مانند اولین نشست مقیاس‌پذیری که در مونترال کانادا برگزار شد (Scaling I)، مرخصی سالانه نداشتم و تصمیم گرفتم آخر هفته برای شرکت در این نشست از هنگ کنگ به ایالات متحده پرواز کنم. این رویداد بسیار آرام و بی سروصدا بود و مشخص بود که این مناقشه در حال پایان یافتن است. تقریباً هیچ‌کس در این نشست از SegWit2x پشتیبانی نمی‌کرد. با این حال یک استثناء قابل توجه در این مورد وجود داشت؛ بابی لی که در پایان روز اول در مورد «بیت کوین در چین» سخنرانی کرد. بابی یکی از معدود حامیان مشتاق SegWit2x بود، زیرا معتقد بود مصالحه‌ای است که می‌تواند دو طرف درگیر را با هم آشتی دهد. در این مرحله، بابی یکی از آخرین حامیان باقی‌مانده SegWit2x بود که هنوز تصور می‌کرد این پیشنهاد به‌طور بالقوه قابل اجرا است. این در حالی است که صرافی بابی BTCC (از امضاءکنندگان توافق‌نامه نیویورک)، توکن‌های پدید آمده پس از هارد فورک زنجیره را لیست کرده بود و کوین SegWit2x در حدود ۱۰ درصد قیمت بیت کوین در این صرافی معامله می‌شد. بابی سرسختانه از توافق‌نامه نیویورک حمایت نمی‌کرد. در پایان سخنرانی او نوبت به بخش پرسش و پاسخ رسید. با این حال بابی درست قبل از آن گفت:

من قصد صحبت کردن درباره SegWit2x و NYA را ندارم، بحث ما روی بازار چین و موارد دیگر متمرکز است.

به نظر می‌رسید بابتی می‌داند SegWit2x محبوبیت چندانی ندارد و حتماً با سؤالات منفی در مورد این پیشنهاد روبرو خواهد شد. او شجاعت این را نداشت که با این موضوع روبرو شود و در مورد آن بحث کند. در این مرحله طرفداران SegWit2x از حمایت و ترغیب جامعه فعالان بیت کوین دست کشیدند و از بررسی دقیق و بحث در مورد آن خودداری کردند.

با رسیدن به ماه نوامبر، مهلت اجرای این پیشنهاد هم نزدیک می‌شد. قرار بود SegWit2x در شماره بلاک ۴۹۴,۷۸۴ در روز ۱۵ نوامبر سال ۲۰۱۷ فعال شود. شایعه‌ای در برخی از کانال‌های طرفداران بلاک‌های بزرگ در حال پخش شدن بود. ظاهراً جیهان وو گفته بود SegWit2x را فقط دو روز با ضرر ماین خواهد کرد. در این صورت اگر ادامه استخراج SegWit2x مقرون به صرفه نباشد، دوباره به استخراج روی بیت کوین و بیت کوین کش باز خواهد گشت. شرکت Bitmain قبلاً به دلیل استخراج بیت کوین کش ضرر زیادی کرده بود و ظاهراً تمایل نداشت پول بیشتری هدر دهد. طرفداران بلاک‌های بزرگ هیچ‌وقت واقعاً از SegWit2x حمایت نمی‌کردند، قلب آن‌ها پیش بیت کوین کش بود. SegWit2x از جانب کاربران نیز حمایت نمی‌شد. این پیشنهاد با توجه به اینکه تقریباً همه از نرم‌افزار Bitcoin Core استفاده می‌کردند، هیچ شبکه فول نودی نداشت. صرافی‌ها یا SegWit2x را رد کرده بودند یا در مقابل آن موضعی خنثی داشتند. در حال حاضر فقط یک استخراج‌کننده از آن پشتیبانی می‌کرد و به نظر می‌رسید ماینرهای آن در حال محو شدن هستند. کار SegWit2x تمام بود. طرفداران بلاک‌های کوچک در انتظار یک پیروزی پر شور بودند. پیروزی قطعی بود و فقط باید زمان آن فرا می‌رسید.

فصل بیست و یکم

پیروزی

در روز چهارشنبه، ۸ نوامبر سال ۲۰۱۷ ساعت ۴:۵۸ عصر (به وقت UTC)، تنها یک هفته مانده به فعال شدن هارد فورک SegWit2x، ایمیلی از طرف مایک بلشه به گروه ایمیلی SegWit2x ارسال شد که توسط دیگر طرفداران برجسته SegWit2x نیز امضاء شده بود. این ایمیل اساساً اعلام تسلیم بی قید و شرط، و لغو رسمی مرحله دوم توافق نامه نیویورک بود. طرفداران SegWit2x حق انتخاب دیگری نداشتند: پیشروی طبق برنامه و اجرای هارد فورک، فقط به خلق کوین متفرقه جدیدی منجر می شد که از محبوبیت کمتری نسبت به بیت کوین گش برخوردار است. در این مرحله و پس از گذشت ۸۱۶ روز از شروع جنگ، خصومت ها به پایان رسید.

SegWit2x در ماه مه با یک هدف ساده شروع شد: افزایش سایز بلاک و بهبود مقیاس پذیری بیت کوین. جامعه فعالان بیت کوین در آن زمان با وجود گذشت ۳ سال از بحث و درگیری، در شرایطی بحرانی قرار داشت و توافق بر روی اجرای سگویت - که تنها از پشتیبانی ۳۰ درصد ماینرها برخوردار بود - همچون سرابی در دوردست به نظر می رسید. SegWit2x اولین موفقیت خود را در ماه اوت به دست آورد، زیرا طلسم سگویت را شکست و در نهایت موجب فعال سازی موفقیت آمیز

آن شد. از آن به بعد تیم اجرایی Segwit2x تلاش‌های خود را بر روی مرحله دوم پروژه، یعنی افزایش سایز بلاک به ۲ مگابایت متمرکز کرد.

به روزرسانی بیت کوین به دور از هرگونه مشاجره و بحث و جدل همواره هدف اصلی ما بوده است. اگرچه ما به نیاز به بلاک‌های بزرگ‌تر عمیقاً اعتقاد داریم، ولی از نظر ما حفظ اتحاد میان جامعه فعالان از رسیدن به آن هدف مهم‌تر است. متأسفانه، روشن است که ما در حال حاضر به اجماع کافی برای افزایش بی‌دردسر سایز بلاک دست پیدا نکرده‌ایم. ادامه مسیر فعلی می‌تواند موجب ایجاد تفرقه میان جامعه فعالان، و در نهایت مانعی برای رشد بیت کوین باشد. هدف Segwit2x هرگز چنین چیزی نبوده است. ما معتقدیم با افزایش کارمزد تراکنش، بالاخره مشخص می‌شود که افزایش ظرفیت زنجیره بیت کوین ضروری است. ما امیدواریم در آن زمان جامعه فعالان بیت کوین دور هم جمع شوند و احتمالاً با بکارگیری روش افزایش سایز بلاک، برای این مشکل چاره‌ای بیندیشند. تا آن زمان ما برنامه‌های خود را برای افزایش سایز بلاک به ۲ مگابایت تعلیق می‌کنیم.

ما از همه موافقین و مخالفین پروژه Segwit2x که مشارکت سازنده‌ای در آن داشته‌اند تشکر می‌کنیم. تلاش‌های شما دقیقاً همان چیزی است که موجب خارق‌العاده بودن بیت کوین می‌شود. بیت کوین بهترین پولی است که بشر تا به امروز دیده است، و ما همچنان به محافظت و پیشرفت آن متعهد هستیم.

Mike Belshe, Wences Casares, Jihan Wu, Jeff Garzik,
Peter Smith and Erik Voorhees

با سقوط Bitcoin Classic، Bitcoin XT و Bitcoin Unlimited و اکنون لغو رسمی BTC1 توسط طرفداران آن، جنگ به پایان رسیده بود. طرفداران بلاک‌های بزرگ خسته شده بودند، آن‌ها می‌دیدند که روش‌های آن‌ها کارآمد نبوده است و از طرف دیگر به هیچ‌وجه نمی‌توانستند پیشنهاد مشاجره‌انگیز دیگری را مطرح کنند. این یک پیروزی

هیجان‌انگیز برای طرفداران بلاک‌های کوچک پس از دو سال جنگ پر تنش بود. آن‌ها سرانجام به هدف خود نه تنها در موضوع محدودیت سائز بلاک، بلکه در مورد نحوه تغییر قوانین پروتکل بیت کوین نیز رسیده بودند. اکنون سرانجام همه این واقعیت را پذیرفته بودند که برگزاری جلسات با شرکت‌های بزرگ فعال در این فضا و تصمیم‌گیری در مورد تغییرات پروتکل بیت کوین، کارساز نیست. اکثریت ماینرها نیز قادر به تغییر قوانین پروتکل بیت کوین نخواهند بود. اگر کسی قصد دارد قوانین پروتکل بیت کوین را تغییر دهد، نیاز به کسب حمایت کاربران بیت کوین و متقاعد کردن سرمایه‌گذاران آن دارد، چون این قوانین باید از جانب آن‌ها پذیرفته شود. این کاربران عادی بودند که قدرت تصمیم‌گیری نهایی را داشتند و این حاکمیت مالی دقیقاً چیزی بود که بیت کوین را منحصر به فرد، و برای افراد جذابیت ایجاد می‌کرد. پس از یک پیروزی حیرت‌انگیز، سرانجام روایت طرفداران بلاک‌های کوچک مبنی بر اینکه کاربران نهایی باید با تغییرات قوانین پروتکل موافقت کنند، قانع‌کننده به نظر می‌رسید.

با این حال همه با این موضوع موافق نبودند. بعضی از افراد، به‌ویژه تعدادی از طرفداران بلاک‌های بزرگ، این جنگ را به‌عنوان نبرد بین توسعه‌دهندگان نرم‌افزار Bitcoin Core و ماینرها تفسیر می‌کردند. از نظر آنها، Bitcoin Core برنده شده بود و ماینرها شکست خورده بودند، بنابراین اکنون کنترل بیت کوین در دست توسعه‌دهندگان Bitcoin Core است. این ذهنیت علی‌رغم این واقعیت که Bitcoin Core هرگز پیشنهاد UASF را پیاده‌سازی نکرد، همچنان پابرجا بود. در ذهن برخی از افراد، درک سیستمی که تحت کنترل کاربران آن باشد بسیار دشوار است. در عوض آن‌ها به دنبال کسی یا موجودیتی می‌گردند که سیستم را کنترل می‌کند. برخی از مردم نمی‌توانند ایده سیستمی را که بدون وجود رهبر، دارای یک اجماع جهانی است درک کنند. در ذهن آن‌ها، در سال ۲۰۱۵ کوین اندریسن رهبر پروژه بود، سپس جیهان وو، و اکنون توسعه‌دهندگان Bitcoin core. قضاوت در مورد اینکه آیا بیت کوین آنطور که ادعا می‌شود واقعاً سیستمی بدون رهبر است و اینکه آیا همیشه اینطور باقی خواهد ماند، هنوز زود است. با این حال رویدادهای هیجانی و حقه‌بازی‌هایی که در خلال مناقشه سائز بلاک

روی داد یک چیز را روش کرد: همچنان می‌توانیم به حقیقت داشتن این ادعا امیدوار باشیم.

انتشار خبر لغو اجرای SegWit2x موجب افزایش فوق‌العاده‌ای در ارزش Bitcoin Cash، تنها کوین مورد توجه طرفداران بلاک‌های بزرگ شد. در روز یک‌شنبه ۱۲ نوامبر سال ۲۰۱۷، در حالی که حساب ارزهای دیجیتال در حال نوسان بود، بیت کوین گش یک افزایش قیمت تاریخی را تجربه کرد. چند روز قبل از انتشار ایمیل مایک بلشه، بیت کوین گش در حدود ۸ درصد قیمت بیت کوین معامله می‌شد. با این حال چند روز بعد و قبل از اینکه ارزش آن دوباره سقوط کند، به اوج قیمتی خود یعنی حدود ۴۸ درصد قیمت بیت کوین رسید. وقتی بیت کوین گش به اوج قیمت خود رسید، اکثر طرفداران بلاک‌های کوچک همچنان از پیروزی اخیر خوشحال بودند. با این حال باور اینکه آن‌ها از احتمال از دست دادن عنوان پرارزش‌ترین کوین بازار هراسان نبوده‌اند، سخت است. گفته می‌شود این افزایش قیمت به دلیل هجوم سرمایه‌گذاران خرد کره جنوبی در این دوره به بازار ارزهای دیجیتال بوده است. با این حال این رشد ناگهانی قیمت به سرعت کند، و در نهایت از بین رفت.

طرفداران بلاک‌های بزرگ در طول دوره افزایش قیمت بیت کوین گش در نوامبر سال ۲۰۱۷، از دستاوردهای بزرگ خود فوق‌العاده هیجان‌زده بودند. برخی از اعضای این گروه که من با آن‌ها صحبت کردم، به امید اینکه این کوین از بیت کوین پیشی می‌گیرد، مقادیر زیادی بیت کوین گش را در قله قیمتی آن خریداری کرده بودند. در آن زمان یک گروه تلگرامی بزرگ به نام «مرگ زنجیره» وجود داشت که نام این گروه به مرگ احتمالی زنجیره بیت کوین و چیره شدن بیت کوین گش اشاره داشت. من به این گروه دسترسی نداشتم، با این حال یکی از اعضای این گروه برخی از چت‌های آن را روی صفحه کامپیوترش به من نشان داد. افراد برجسته گروه طرفداران بلاک‌های بزرگ در آن عضو

بودند و در دوره افزایش قیمت بازار ارزهای دیجیتال در سال ۲۰۱۷ بسیار فعال، و از شرایط خوشنود بودند.

ایده «مرگ زنجیره» این بود که بالاخره قیمت بیت کوین گش به دلیل برتری آن به عنوان ابزار پرداخت^۱، افزایش خواهد یافت. این امر در نهایت باعث می شود که استخراج بیت کوین گش برای ماینرها منفعت بیشتری داشته باشد و ماینرها به همین دلیل از استخراج بیت کوین رویگردان شده و به سمت بیت کوین گش بروند. در این صورت زنجیره بیت کوین از پیشرفت باز می ماند و متوقف می شود. سپس بیت کوین از بین می رود و بیت کوین گش جای آن را می گیرد. البته بیت کوین برای حل این مشکل از یک ساز و کار برای بازتنظیم سختی شبکه برخوردار بود، با این حال اجرای این بازتنظیم حدود دو هفته زمان می برد. طرفداران بلاک های بزرگ فکر می کردند از بین بردن زنجیره بیت کوین قبل از وقوع این بازتنظیم، امکان پذیر است. در مقابل طرفداران بلاک های کوچک فکر می کردند این امیدواری گروه طرفداران بلاک های بزرگ احمقانه است. به هر حال طرفداران بلاک های کوچک طرف صبور ماجرا بودند و برای آنها مهم نبود دوره بازتنظیم سختی شبکه چقدر طول می کشد. همچنین مسأله دوره بازتنظیم سختی شبکه بیت کوین گش که بسیار کوتاه تر از دو هفته بود نیز مطرح بود. افزایش قیمت بیت کوین گش باعث می شد تا ماینرهای بیشتری به استخراج آن مشغول شوند و این مسأله موجب افزایش سختی شبکه زنجیره بیت کوین گش و بازگشت ماینرها به زنجیره بیت کوین -قبل از سررسید دوره بازتنظیم سختی شبکه- می شد. به نظر می رسید طرفداران بلاک های بزرگ -حداقل در این دوره- هرگز از این زاویه به امر بازتنظیم سختی شبکه توجه نکرده بودند.

سرانجام وقتی در تاریخ ۱۵ نوامبر سال ۲۰۱۷ موعد فعال سازی Segwit2x فرا رسید، معلوم شد که نرم افزار آن پر از اشکالات مهم بوده است. قرار بود هارد فورک در شماره بلاک ۴۹۴,۷۸۴ اجرا شود اما به دلایلی، نرم افزار BTC1 دو بلاک زودتر روی بلاک ۴۹۴,۷۸۴ گیر کرده بود. به دلیل اشتباهاتی که در پیاده سازی رخ داده بود، این نرم افزار برخی از

1 Medium of exchange

جنبه‌های هارد فورک را دو بلاک زودتر اجرا کرده بود. این امر می‌توانست برای صرافی‌ها یک فاجعه باشد، زیرا قصد داشتند موجودی کاربران را در زمان اجرای هارد فورک ثبت کنند. علاوه بر این، اشکالات مهم دیگری نیز در BTC1 وجود داشت که استخراج روی زنجیره Segwit2x را غیرممکن می‌کرد. جف گارزیک ابتدا وجود مشکل را تکذیب کرد و سپس چند روز بعد مشکل را برطرف کرد. به دلیل این اشکالات فاجعه‌بار، زنجیره Segwit2x هرگز وجود خارجی پیدا نکرد و هیچ بلاکی بر روی زنجیره آن تولید نشد. با این حال این واقعیت که این پیشنهاد نیز به موجب عوامل سیاسی و اقتصادی شکست خورد، حتی مهم‌تر از اشکالات فنی Segwit2x است. این رخداد از هر جنبه‌ای مورد بررسی قرار گیرد، یک شکست قاطع است.

در روز ۲۰ دسامبر ۲۰۱۷، اتفاقات شبه‌ناک بیشتری در بازار معاملات بیت کوین گش رخ داد. صرافی کوین بیس بیت کوین گش را لیست کرد و این کوین با هیجانی که پدید آمد تا رقم ۸,۵۰۰ دلار آمریکا در بازار معامله می‌شد. این رقم از نظر ارزش برابری با دلار آمریکا - نه نسبت به قیمت بیت کوین - یک رکورد محسوب می‌شد. به محض لیست شدن کوین، صرافی کوین بیس نتوانست از پس تقاضای خرید خریداران بر بیاید و تأخیرهای زیادی در سیستم پدید آمد. روش کار آن‌ها بسیار آشفته بود و برخی از طرفداران بلاک‌های کوچک با توجه به سابقه صرافی کوین بیس در پشتیبانی از Bitcoin Classic، Bitcoin XT و حتی Bitcoin Unlimited با دیده شک و تردید به اقدام اخیر این شرکت نگاه می‌کردند. آن‌ها صرافی کوین بیس را به جرم نشت اطلاعات سری بازار معاملات^۱ به گروه طرفداران بلاک‌های بزرگ، قبل از لیست شدن بیت کوین گش متهم می‌کردند.

راجر ورن نیز که از مدافعان سرسخت بلاک‌های بزرگ و اجرای هارد فورک بود، اکنون به همراه شرکت Bitmain به یکی از مبلغان اصلی بیت کوین گش تبدیل شده بود. آن‌ها کنفرانس‌ها، رویدادها، و مهمانی‌هایی برای ترغیب فروشندگان برای پذیرش بیت کوین

1 Insider trading

گش ترتیب می‌دادند، کالاها و کوین‌های رایگان به آنها اهداء می‌کردند، و همه این کارها به قصد تبلیغ برای بیت کوین گش بود. آنها احتمالاً در خلال این چند سال ده‌ها میلیون دلار برای تبلیغ این کوین هزینه کرده‌اند.

با وجود این تلاش‌ها این کوین هرگز در مقایسه با بیت کوین مورد توجه قرار نگرفت. در طول سال‌های بعد نیز بیت کوین گش از نظر قیمت عملکرد ضعیفی نسبت به بیت کوین داشته است. از این گذشته، در حالی که ادعا می‌شد عامل اصلی افزایش سائز بلاک به منظور بالا بردن توان پردازش تراکنش‌ها در شبکه است، بیت کوین گش از حجم تراکنش کمتری نسبت به بیت کوین برخوردار بود. شرایط برای بیت کوین گش در مارس سال ۲۰۱۸، در شرایطی که حجم تراکنش‌ها بر روی زنجیره بیت کوین گش حتی از تراکنش‌های سگویی بیت کوین کمتر بود، وخیم‌تر به نظر می‌رسید. سگویت بیشتر از بیت کوین گش موجب افزایش تراکنش‌ها بر روی زنجیره بیت کوین شده بود. روایت اصلی که بیت کوین گش و بلاک‌های بزرگ روی آن بنا شده بود، در این مرحله تقریباً ناپود شده بود. با این حال حجم معاملات، نکته کلیدی مورد توجه طرفداران بلاک‌های بزرگ نبود، بلکه آنها به فلسفه ظرفیت مازاد در بلاک‌ها معتقد بودند؛ یعنی تقاضای احتمالی در آینده، موجب پر شدن بلاک‌ها نشود.

در آگوست سال ۲۰۱۸ و در حالی که زمان زیادی از پایان این جنگ گذشته بود، شرکت Bitmain اقدام به عرضه اولیه سهام^۱ خود در بورس هنگ کنگ کرد. اسناد این عرضه اولیه نشان می‌داد که این شرکت بیش از ۸۸۸ میلیون دلار روی بیت کوین گش سرمایه‌گذاری کرده است. این پول تقریباً به اندازه سودی بود که این شرکت از رشد قیمت ارزهای دیجیتال در سال ۲۰۱۷ به دست آورده بود. در این مرحله، بیت کوین گش از نظر قیمت عملکرد خوبی نداشت و این شرکت ضررهای سنگینی را در بازار تجربه می‌کرد. جیهان وو از مدافعان سرسخت بلاک‌های بزرگ بود و بی‌امان در نبردی که بیشتر از ۲ سال به طول انجامید، به جنگیدن ادامه داد. با این حال، این اعتقادات بر قضاوت‌های او

1 IPO

اثرات منفی داشت و موجب شد تصمیمات ضعیفی در زمینه سرمایه گذاری بگیرد. شرکت Bitmain به دلیل سرمایه گذاری روی بیت کوین گش متحمل ضررهای سنگینی شده بود.

تا حدودی به دلیل مشکلات اجرای هارد فورک در فضای بیت کوین، جامعه فعالان بیت کوین گش رویکرد دیگری را برگزیدند. آنها هر شش ماه یکبار در ماه مه و نوامبر هر سال، برای اجرای هارد فورک برنامه ریزی کرده بودند. در نوامبر سال ۲۰۱۸، در حالی که فقط کمی بیشتر از یک سال از راه اندازی بیت کوین گش گذشته بود، تنش هایی در جامعه فعالان بیت کوین گش رخ داد. دوباره سر و کله کریگ رایت (ساتوشی تقلبی)، کسی که در گذشته از جانب بسیاری از طرفداران بلاک های بزرگ حمایت می شد، پیدا شد. کریگ رایت قصد داشت برنامه افزایش محدودیت سائز بلاک ها را حتی افراطی تر از آن چیزی که افراد فعال در جامعه بیت کوین گش می خواستند، اجرا کند. او بسیاری از روایت هایی که گروه طرفداران بلاک های بزرگ چند سال قبل و در اوایل مناقشه سائز بلاک عنوان می کردند را تکرار می کرد. با به کار بستن هاردفورکی که از قبل در تاریخ ۱۵ نوامبر سال ۲۰۱۸ برنامه ریزی شده بود، بیت کوین گش به دو کوین تقسیم شد: یکی از آنها عنوان Bitcoin ABC، و دیگری که مورد حمایت کریگ رایت بود با عنوان Bitcoin Satoshi's Vision زنجیره خود را ادامه دادند. طرف Bitcoin ABC نام بیت کوین گش را حفظ کرد، در حالی که Bitcoin Satoshi's Vision به BSV معروف شد. در نتیجه فورک و عدم قطعیت ناشی از آن، ارزش بیت کوین گش نسبت به بیت کوین همچنان رو به کاهش بود. درست همانطور که گروه طرفداران بلاک های کوچک انتظار داشتند، برخی از طرفداران بلاک های بزرگ به آرامی متوجه این مسأله می شدند که در صورت بروز اختلاف بر سر قوانین، مجموعه قوانین اصلی به عنوان نقطه شلینگ^۱ (یا نقطه کانونی، اصطلاحی در نظریه بازی است که وقتی افراد امکان برقراری با یکدیگر را ندارند، از آن استفاده می کنند. - م) عمل خواهد کرد. اگر این نگرش نادیده گرفته شود، این خطر وجود دارد که کوین در آینده به گروه های کوچک تری تجزیه شود و طرفداران بلاک های بزرگ در حال تجربه بدون واسطه این واقعیت دردناک بودند.

1 Schelling point

در تاریخ ۸ نوامبر سال ۲۰۱۸ و در اوج نبرد بین Bitcoin ABC و BSV، راجر وور از برجسته‌ترین طرفداران بلاک‌های بزرگ در یک ویدئوی افشاگرانه چنین گفت:

فکر می‌کنم چیزی که از این رویدادها آموختم این است که توسعه‌دهندگان Bitcoin Core با اجرای یک هارد فورک پر حاشیه بسیار بسیار مخالف بودند و من [اکنون] فکر می‌کنم هراس از این موضوع کاملاً درست است، زیرا ما در حال حاضر شاهد هستیم که یک هارد فورک پر حاشیه قادر است چه خساراتی به بار آورد.

با این حال، پیروزی قاطع طرفداران بلاک‌های کوچک لزوماً به این معنی نیست که قضاوت آن‌ها در مورد سائز بلاک حتماً درست بوده است. در ظاهر اینطور به نظر می‌رسید که بیت کوین موفق شده است. قیمت بیت کوین در گذر سال‌ها به‌طور قابل توجهی افزایش یافته، و نظریه طلای دیجیتال با گذشت زمان موضوعیت بیشتری پیدا می‌کند. به نظر می‌رسد روش طرفداران بلاک‌های کوچک مبنی بر پیشه کردن صبر، کارآمد بوده است. با این حال شاید بهتر بود از روش متعادل‌تری برای افزایش سائز بلاک و تأمین ظرفیت مورد نظر برای چند سال آینده استفاده می‌کردیم. شاید بیت کوین با انتخاب این روش موفق‌تر می‌شد و فروشندگان بیشتری آن را [به عنوان ابزار پرداخت] می‌پذیرفتند. این موضوع همواره برای ما یک معما باقی خواهد ماند.

برخلاف موضوع سائز بلاک که قاطعانه نمی‌توان گفت حق با کدام گروه بوده است، در مورد مسأله انعطاف‌پذیری قوانین پروتکل بیت کوین و روش تغییر آن‌ها جای هیچ شک و شبهه‌ای نیست که حق کاملاً با طرفداران بلاک‌های کوچک بوده است. ممکن است برخی از طرفداران بلاک‌های کوچک تردیدی نداشته باشند که کنترل بیت کوین قطعاً در دستان کاربران بیت کوین است و طرفداران بلاک‌های بزرگ هرگز شانس برای پیروز شدن در این جنگ نداشته‌اند. با این حال ممکن است شما با خواندن این کتاب به نتیجه متفاوتی برسید. گروه طرفداران بلاک‌های بزرگ می‌توانستند پیروز این میدان باشند و خیلی به آن

نزدیک شده بودند. در آغاز درگیری، طرفداران بلاک‌های بزرگ از پشتیبانی قابل توجهی برخوردار بودند. تنها دلیلی که باعث پیروزی برجسته طرفداران بلاک‌های کوچک شد، مجموعه‌ی غریبی از رویدادها و اشتباهات تاکتیکی اردوگاه طرفداران بلاک‌های بزرگ بود که در نهایت موجب موفقیت طرفداران بلاک‌های کوچک در تغییر دادن نظر جامعه‌ی فعالان بیت کوین شد.

در اصل، موضوع از این قرار است که طرفداران بلاک‌های کوچک روایت جذاب‌تر و باورپذیرتری نسبت به روایت طرفداران بلاک‌های بزرگ ساخته بودند. روایت شکل جدیدی از پول که قوانین آن توسط کاربران تعیین می‌شود، از داستان ظرفیت پردازش بالا، کارمزد پایین، و سیستم پرداخت جهانی، (صرف‌نظر از اینکه هر کدام از این روایت‌ها تا چه اندازه حقیقت داشتند) مقبول‌تر افتاد. پول در نهایت یک بازی اعتماد جمعی است، و طرفداران بلاک‌های کوچک در این زمین بازی خوبی از خود ارائه دادند و پاداش آن‌ها نیز پیروزی در این جنگ بود.

طرفداران بلاک‌های کوچک در طول این نبرد دو ساله موفق شدند بر ماینرها و دیگر کسب‌وکارهای بزرگ فعال در این فضا غلبه کنند و با وجودی که رقبای آن‌ها در گروه طرفداران بلاک‌های بزرگ برای این جنگ صدها میلیون دلار هزینه کرده بودند، توانستند به یک پیروزی باورنکردنی و چشمگیر دست پیدا کنند. این موضوع بر این ادعا که کنترل بیت کوین در دست کاربران آن است صحنه گذاشت.

با این حال هیچ تضمینی وجود ندارد که شرایط همواره برای بیت کوین به این شکل باقی بماند. مناقشه سائز بلاک فقط توانست چند سال برای بیت کوین زمان بخرد. این جنگ ممکن است نسبت به چالش‌هایی که در آینده ممکن است برای بیت کوین رخ دهد، یعنی زمانی که ذینفعان اصلی سیستم‌های پولی متمرکز به پتانسیل‌های یک پول کاربر محور پی ببرند، فقط شبیه به یک دست گرمی باشد. نبردهای آینده ممکن است به جای مقیاس‌پذیری

و محدودیت سائز بلاک، بر سر ویژگی مقاومت در برابر سانسورپذیری^۱ بیت کوین در بگیرند. این بار احتمالاً تشکیلات مالی و سیاسی آغازگر درگیری خواهند بود. آنها به احتمال زیاد منابع قابل توجهی را صرف این موضوع خواهند کرد، و بار دیگر فشار بسیار زیادی روی سیستم وارد خواهد شد. بدون تردید تاریخ تکرار خواهد شد، و احتمالاً [همانطور که در مناقشه سائز بلاک شاهد بودیم]، آنها برخی از ظرایف موجود در مشوقها را درک نمی کنند و اشتباهاتی در طول مسیر مرتکب می شوند، و موقعیت های تاکتیکی بالقوه ای را در اختیار کاربران قرار خواهند داد. نتیجه این جنگ به هیچ وجه قابل پیش بینی نیست.

با این حال حداقل فعلاً، رؤیای دنیایی که در آن کنترل نهایی و مستقیم قوانین حاکم بر پول در دست مردمان عادی است، همچنان ادامه دارد.

1 Censorship resistance

THE BLOCKSIZE WAR

JONATHAN
BIER

THE BATTLE
FOR CONTROL
OVER BITCOIN'S
PROTOCOL RULES

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»^۱ معروف بود. یکی از رویدادهای مهمی که به باور برخی از کارشناسان به دلیل وجود این مشکل به وقوع پیوست، رخداد هک صرافی «مت.گاکس»^۲ 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»^۳ 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^۱ 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^۲ این تراکنش می‌تواند توسط نودهایی که تراکنش را به نودهای ماینرهای بیت کوین 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 بیت کوین‌ها را بین ارسال و دریافت کننده جابه‌جا می‌کنند. هرچند یک مشکل دیگر پدید خواهد آمد؛ اینکه دیگر نمی‌توان تراکنش‌های جدیدی را برپایه تراکنش‌هایی که هنوز تأیید نشده‌اند^۳ 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^۴ مثل لایتینگ^۵ 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»^۶، «مت کورالو»^۷، «لوک داش‌یر»^۸، و «گرگوری مکسول»^۹ و «تی‌مس»^{۱۰} 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

«بیت کوین تاک^۱» در کانال «آی آر سی^۲» توسعه بیت کوین 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^۳» و گرگوری مکسول برنامه‌نویسان بیت کوین، مجدداً درباره روش حل این مشکل در کانال آی آر سی بیت کوین 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^۴» دوباره درباره این مشکل در کانال آی آر سی بیت کوین 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^۵» اساسی نیاز دارد و اجرای آن بسیار مشکل است.»

در ماه آگوست سال ۲۰۱۴ میلادی شرکت بلاک‌استریم^۶ توسط آدام بک و گرگوری مکسول، همچنین با همراهی «آستین هیل^۷» و چند تن از برنامه‌نویسان پروتکل بیت کوین مثل دکتر «پیتر والا^۸» تاسیس شد. این شرکت می‌خواست روی «زنجیره‌های جانبی^۹» تمرکز کند. زنجیره‌های جانبی که می‌توانستند به شبکه بیت کوین وصل^{۱۰} 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 بلاک استریم تصمیم گرفتند ویژگی جدیدی را در نمونه اولیه زنجیره جانبی خود که «المنت»^۱ 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»^۲ بود.

هارد فورک‌ها^۳ و سافت فورک‌ها^۴

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

تا اینجا متوجه شدیم که نرم‌افزار بیت کوین 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 در هنگام 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. در نهایت، می‌دانیم که نرم‌افزار بیت کوین طولانی‌ترین زنجیره‌ای که بیشترین حجم انباشته اثبات کار را در خود جای داده باشد به عنوان زنجیره معتبر می‌پذیرد، و می‌دانیم که چند شاخه شدن زنجیره‌ها (یا به اصطلاح فورک‌ها) به دلایلی که در فصل ۶ کتاب «اختراع بیت کوین» به تفصیل توضیح داده شده اتفاق می‌افتند.

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

حالا بیا بید به فورک‌هایی که به عمد ایجاد می‌شوند پردازیم. فورک عمدی زمانی است که تعدادی از ماینرها و/یا کاربران با قوانین جاری بیت کوین موافق نباشند و تصمیم بگیرند آن را تغییر دهند. به طور کلی دو نوع فورک برای تغییر قوانین وجود دارد: سافت فورک، که با قوانین قبل سازگاری دارد^۱ و هارد فورک که با قوانین قبل سازگار نیست^۲. ببینیم این فورک‌ها چگونه اتفاق می‌افتند و مثال‌هایی از آنها را مطرح کنیم.

سافت فورک‌ها

یک سافت فورک ایجاد تغییر در قوانین اجماع بیت کوین 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 به روزرسانی نشده باشد، بلاک‌هایی که با قوانین جدید ساخته شده‌اند همچنان برای نود شما معتبر هستند. برای یک نود که با فورک جدید به روزرسانی شده است تمام بلاک‌هایی که قبلاً 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 بیت کوین معرفی شد: سائز بلاک‌ها حداکثر می‌تواند ۱ مگابایت باشد. این قانون برای مقابله با اسپم‌ها در بلاک‌چین اعمال شد. قبل از این قانون، بلاک‌ها با هر سائزی 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 به روزرسانی 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 به روزرسانی 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 به روز کنند تا بلاک‌های تولیدشده از قوانین جدید پیروی کنند. وقتی یک ماینر قانون محدودیت ۱ مگابایت را در فورک جدید به روزرسانی می‌کرد، سائز 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 به روزرسانی نشده‌اند دیگر نمی‌توانند بلاک‌هایی را که تحت قوانین جدید ایجاد شده‌اند بررسی کنند. به همین دلیل تا نرم‌افزار خود را به روزرسانی نکنند در زنجیره قبلی باقی خواهند ماند. یکی از نمونه‌های هارد فورک افزایش سائز بلاک‌ها از ۱ مگابایت به سائز 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 به روزرسانی 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 از کار افتاده است و وادار به ارتقاء نرم‌افزار خود خواهد شد.

هارد فورک‌ها در عمل 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 بیت کوین در زمینه پرداخت‌های ارزان (با کارمزد کم) ناراضی بودند،

تصمیم گرفتند برای ایجاد زنجیره‌ای با بلاک‌های بزرگ‌تر یک فورک ایجاد کنند. چون قانون بیت کوین 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 بیت کوین 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 بیت کوین جدا شده است، کوین‌هایی که در آن تولید می‌شوند دیگر بیت کوین نیستند و بنابراین توسط هیچ نودی در شبکه بیت کوین پذیرفته نخواهند شد.

اینکه چه چیزی بیت کوین «است» و چه چیزی بیت کوین «نیست» در طی یک سال بعد از فورک Bitcoin Cash بحث داغی بود. بعضی از افرادی که طرفدار Bitcoin Cash بودند، اعتقاد داشتند که بیت کوین 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 مشاخره‌هایی که در شبکه‌های اجتماعی شکل می‌گیرند کار نمی‌کند، بلکه براساس انتخاب افراد در اجرای نرم‌افزاری خاص، برای اجرای قوانین مشخصی عمل می‌کند.

در مورد این فورک، اکثریت افرادی که نودهای مهمی از نظر اقتصادی اجرا می‌کردند (مثل کیف پول‌ها، صرافی‌ها و پذیرندگان بیت کوین) 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 هش 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 به وجود بیاید، دو کوین متفاوت ایجاد

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

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

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 بیت کوین و به سرپرستی الف.آزاد در بهار سال ۱۴۰۰ آغاز و در تابستان همان سال به پایان رسید.

منابع فارسی بیت کوین

ویراست اول

تابستان ۱۴۰۰

bitcoind.me

منابع فارسی بیت کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی‌زبان بیت‌کوین تألیف یا ترجمه شده‌اند