



برشی از تاریخچه بیت کوین؛  
مروری بر مناقشه افزایش سائز بلاک بیت کوین

«آنان که تاریخ نمی‌دانند، محکوم به تکرار آن هستند.»

- ادموند بورک

تقدیم به فعالان جامعه فارسی زبان بیت کوین

## پیش‌گفتار

تلاش برای ارتقاء پروتکل بیت‌کوین از طریق اعمال سگویت<sup>۱</sup>، یک نقطه عطف بسیار آموزنده در تاریخ بیت‌کوین است. این ارتقاء، اشکال «تغییرپذیری تراکنش<sup>۲</sup>» را برطرف، و امکان ایجاد لایه‌های بیرونی (مثل شبکه لایت‌نینگ<sup>۳</sup>) را بر روی زنجیره بیت‌کوین فراهم می‌کرد.

با این وجود، در حین اجرای این به‌روزرسانی، میان طرفین دعوا که انگیزه‌های متفاوتی داشتند یک بن‌بست به وجود آمد. ولی درنهایت این درگیری به همه طرف‌های درگیر آموخت که شبکه بیت‌کوین چگونه کار می‌کند. سؤال اصلی این بود: آیا ماینرها کنترل بیت‌کوین را در دست دارند یا کاربران و نودها آن را کنترل می‌کنند. توسعه‌دهندگان بیت‌کوین چه نقشی دارند؟

برای پاسخ به این سؤال‌ها و درک نحوه کار شبکه بیت‌کوین مقاله زیر را که در دو بخش به توضیح مسائل مربوط می‌پردازد بخوانید.

---

1 Segregated Witness  
2 Transaction Malleability  
3 Lightning Network

خواندن این مطلب پیش‌نیازی ندارد ولی دانش کلی از طرز کار شبکه بیت‌کوین کمک بزرگی به درک هرچه بهتر آن می‌کند. در پیوست، بخش‌هایی از کتاب «اختراع بیت‌کوین» که در سایت منابع فارسی قابل دریافت است، به همین منظور آورده شده است.

[bitcoind.me](http://bitcoind.me)

سایت منابع فارسی بیت‌کوین

زمستان ۱۳۹۹

## 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»<sup>۱</sup> 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»<sup>۲</sup> 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

---

1 Transaction malleability

2 Mt.Gox

منتقل می‌شوند و اطلاعاتی از این قبیل. بخش دوم به «گواهی»<sup>۱</sup> 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.

این امضای دیجیتالی مشکلی دارد که به اشکال تغییرپذیری<sup>۲</sup> 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<sup>۳</sup> 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<sup>۴</sup> 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<sup>۵</sup> مثل لایتینگ<sup>۶</sup> بسیار دشوار خواهد بود.

---

1 Witness  
2 Malleability bug  
3 TxId  
4 Unconfirmed Transactions  
5 Second layer  
6 Lightning

## راه حل برطرف کردن این مشکل

یک راه حل 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»<sup>۱</sup>، «مت کورالو»<sup>۲</sup>، «لوک داش‌یر»<sup>۳</sup>، و «گرگوری مکسول»<sup>۴</sup> و «تایموس»<sup>۵</sup> مدیر سایت «بیت کوین تاک»<sup>۶</sup> در کانال «آی آر سی»<sup>۷</sup> 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»<sup>۸</sup> 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»<sup>۹</sup> 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»<sup>۱۰</sup> اساسی نیاز دارد و اجرای آن بسیار مشکل است.»

---

1 Russell O'Connor  
2 Matt Corallo  
3 Luke Dashjr  
4 Gregory Maxwell  
5 Theymos  
6 Bitcointalk.org  
7 IRC  
8 Peter Todd  
9 Adam Back  
10 Hard fork



در ماه آگوست سال ۲۰۱۴ میلادی شرکت بلاک‌استریم<sup>۱</sup> توسط آدام بک و گرگوری مکسول، همچنین با همراهی «آستین هیل<sup>۲</sup>» و چند تن از برنامه‌نویسان پروتکل بیت‌کوین مثل دکتر «پیتر والا<sup>۳</sup>» تاسیس شد. این شرکت می‌خواست روی «زنجیره‌های جانبی<sup>۴</sup>» تمرکز کند. زنجیره‌های جانبی که می‌توانستند به شبکه بیت‌کوین وصل<sup>۵</sup> شوند.

در اوایل سال ۲۰۱۵ میلادی مهندسان شرکت بلاک‌استریم تصمیم گرفتند ویژگی جدیدی را در نمونه اولیه زنجیره جانبی خود که «المنت<sup>۶</sup>» 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<sup>۷</sup>» بود.

در بخش بعد تاریخچه دعوی معروف سائز بلاک را مرور و در انتها روشی را که در نهایت برای حل مشکل تغییرپذیری تراکنش‌ها به کار گرفته شد توضیح می‌دهیم.

---

1 Blockstream  
2 Austin Hill  
3 Pieter Wuille  
4 Sidechains  
5 Pegged  
6 Element  
7 SegWit (Segregated Witness)

## دعوا بر سر سائز بلاک

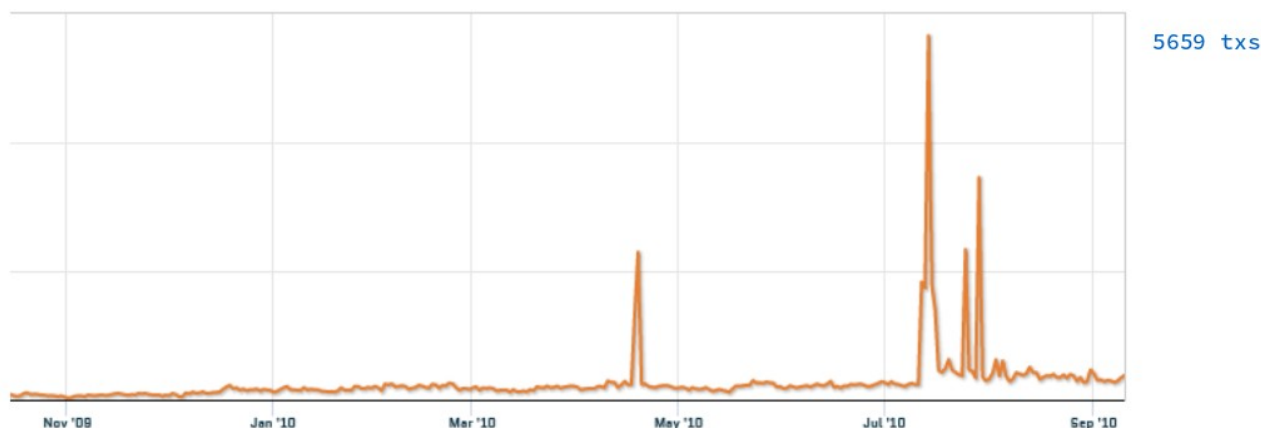
ممکن است از خود پرسیده باشید این محدودیت سائز بلاک از کجا و از چه زمانی به قوانین شبکه بیت کوین اضافه شده است.

برای پاسخ به این سؤال باید به عقب برگردیم. جایی که محدودیت فضای بلاک در شبکه بیت کوین توسط شخص ساتوشی ناکاموتو اعمال شد. او اسط سال ۲۰۱۰ میلادی شبکه بیت کوین با یک مشکل پیش‌بینی نشده روبرو شد. فردی با سوءاستفاده از رایگان بودن کارمزد تراکنش‌ها و با به‌کارگیری از یک نرم‌افزار اقدام به تولید و ارسال تراکنش‌های اسپم به شبکه کرد و باعث پر شدن فضای مم‌پول<sup>۱</sup> (تراکنش‌هایی که در صف ثبت شدن در بلاک قرار دارند) شد. این اتفاق به «واقعه سیل پول خرد<sup>۲</sup>» معروف است.

---

1 mempool

2 Penny Flooding Incident



تعداد تراکنش‌های روزانه شبکه

عکس‌العمل ساتوشی در مقابل این واقعه این بود که یک سقف ۱ مگابایتی برای سایز بلاک‌ها تعیین کرد. این تغییر در تاریخ ۱۵ جولای ۲۰۱۰ در کد بیت کوین وارد شد ولی در عمل در تاریخ ۲۰ سپتامبر ۲۰۱۰ فعال و در شبکه اعمال شد تا فضای بلاک هم مثل خود بیت کوین کمیاب باشد.

ساتوشی فقط در یک مورد و حدود ۲ ماه قبل از ترک پروژه، در اکتبر سال ۲۰۱۰ و در جواب به «جف گارزیک»<sup>۱</sup> که یک افزونه نرم‌افزاری<sup>۲</sup> برای افزایش فضای بلاک پیشنهاد کرده بود و افرادی که در تالارهای گفتگوی سایت بیت کوین تاک درخواست افزایش فضای بلاک را داشتند، اینگونه ابراز نظر کرد:

از این افزونه استفاده نکنید چون در این صورت نرم‌افزار شما دیگر با قوانین پروتکل سازگار نخواهد بود و این موضوع به ضرر شما تمام خواهد شد. ممکن است در آینده و در زمانی که نیاز باشد آن را تغییر دهیم.<sup>۳</sup>

- ساتوشی ناکاموتو

1 Jeff Garzik

2 patch

3 [bitcointalk.org/index.php?topic=1347.0](http://bitcointalk.org/index.php?topic=1347.0)

زمان سپری شد و این موضوع مجدداً در فوریه سال ۲۰۱۳ میلادی به بحث داغ<sup>۱</sup> بین برنامه‌نویسان و فعالان تبدیل شد و «گوین اندریسن»<sup>۲</sup> مطلبی<sup>۳</sup> در این مورد در سایت خود منتشر کرد. ولی فعالان و برنامه‌نویسان همچنان به نتیجه مشترکی نرسیدند تا اینکه بالاخره موضوع افزایش ساینز بلاک در بهار سال ۲۰۱۵ تبدیل به یک مناقشه<sup>۴</sup> تمام‌عیار شد.

به‌طور خاص گوین اندریسن، برنامه‌نویس بازنشسته پروتکل بیت کوین و «مایک هرن»<sup>۵</sup> برنامه‌نویس اصلی پروژه «بیت کوین جی»<sup>۶</sup> معتقد بودند ساینز بلاک باید با یک هارد فورک افزایش یابد. هارد فورک‌ها تغییراتی هستند که ناقض قوانین فعلی شبکه هستند و برای به‌روزرسانی موفق‌آمیز، همه شبکه باید نرم‌افزار بیت کوین خود را به آخرین نسخه تغییر دهند. گذشته از دشواری، اجماع گسترده‌ای هم در جامعه فعالان بیت کوین روی آن وجود نداشت. (در پیوست کتاب، هارد فورک و سافت فورک‌ها را توضیح داده‌ایم.)

در تابستان سال ۲۰۱۵ اندریسن و هرن اعلام کردند که علیرغم اختلاف نظر فعالان و برنامه‌نویسان بر روی روش افزایش ساینز بلاک با استفاده از مکانیزم هارد فورک، تصمیم دارند برنامه‌های خود را پیش ببرند و برای این منظور نسخه‌ای از نرم‌افزار بیت کوین<sup>۷</sup> به نام «بیت کوین ایکس‌تی»<sup>۸</sup> را پیاده‌سازی کردند. این کار آن‌ها بسیار بحث‌برانگیز شد و جامعه توسعه‌دهندگان<sup>۹</sup> و فعالان صنعت بیت کوین را در شرایطی تقریباً بحرانی قرار داد.

در نیمه دوم سال ۲۰۱۵ و در تلاش برای حل شکاف بوجود آمده بین این دو گروه و رسیدن به یک راهکار مشترک برای پایان دادن به مناقشه ساینز بلاک، دو کنفرانس

1 [bitcointalk.org/index.php?topic=144895.0](http://bitcointalk.org/index.php?topic=144895.0)

2 Gavin Andresen

3 [gavinandresen.ninja/time-to-roll-out-bigger-blocks](http://gavinandresen.ninja/time-to-roll-out-bigger-blocks)

4 [lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007869.html](http://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-May/007869.html)

5 Mike Hearn

6 Bitcoinj (<https://bitcoinj.github.io>)

7 Software client

8 Bitcoin XT

9 Core developers

برگزار شد. «افزایش ظرفیت شبکه بیت کوین در مونترال»<sup>۱</sup> و «افزایش ظرفیت شبکه بیت کوین در هنگ کنگ».

یکی از راهکارهایی که در کنفرانس مونترال معرفی<sup>۳</sup> شد و از بقیه روش‌ها امیدوار کننده‌تر به نظر می‌رسید، شبکه لایتینگ<sup>۴</sup> بود. یک شبکه پیچیده روی شبکه بیت کوین (لایه دوم) که مقاله علمی<sup>۵</sup> آن چند ماه قبل از آن توسط «جوزف پون»<sup>۶</sup> و «تاج درایا»<sup>۷</sup> منتشر شده بود. فقط یک مشکل وجود داشت؛ ابتدا باید مشکل «تغییرپذیری تراکنش»<sup>۸</sup> در لایه اول شبکه بیت کوین حل می‌شد.

## اعمال تغییرات به روش سافت فورک

در این برهه از زمان، برنامه‌نویسان پروتکل بیت کوین هنوز مطمئن نبودند از چه روشی مشکل تغییرپذیری تراکنش‌ها را حل کنند. تقریباً همه اطمینان داشتند که اعمال سگویت<sup>۹</sup> روی شبکه بیت کوین فقط از راه هارد فورک امکان‌پذیر است.

همه بجز لوک دش‌یر، برنامه‌نویس پروتکل بیت کوین و مسئول پروژه «بیت کوین ناتس»<sup>۱۰</sup>.

- 
- 1 Scaling Bitcoin Montreal (<https://scalingbitcoin.org/event/montreal2015>)
  - 2 Scaling Bitcoin Hong kong (<https://scalingbitcoin.org/event/hongkong2015>)
  - 3 [youtube.com/watch?v=TgjrS-BPWDQ&feature=youtu.be&t=41m54s](https://youtube.com/watch?v=TgjrS-BPWDQ&feature=youtu.be&t=41m54s)
  - 4 Lightning Network
  - 5 White paper ([lightning.network/lightning-network-paper.pdf](https://lightning.network/lightning-network-paper.pdf))
  - 6 Joseph Poon
  - 7 Thaddeus Dryja
  - 8 Transaction malleability
  - 9 Segregated Witness
  - 10 Bitcoin Knots

در اکتبر سال ۲۰۱۵ میلادی، و درست بین کنفرانس‌های افزایش ظرفیت شبکه بیت کوین، برنامه‌نویسان پروتکل بیت کوین اریک لامبروزو<sup>۱</sup>، پیتر والا<sup>۲</sup>، ولادمیر ون در لان<sup>۳</sup>، و لوک دش‌یر درباره مدل جدید بالقوه‌ای برای اعمال سگویت به صورت سافت فورک بر روی شبکه در آی آر سی بیت کوین با هم بحث و گفتگو می‌کردند. در خلال بحث لوک دش‌یر اظهار داشت که ساز و کار پیشنهادی او فقط برای نوع خاصی از سافت فورک‌ها کارآمد است.

جالب اینجاست که دیگران گزینه اعمال سگویت بر روی شبکه از راه سافت فورک را اصلاً در نظر نگرفته بودند درحالی‌که این امر برای لوک دش‌یر بدیهی بود.

برای اعمال سگویت بر روی شبکه به صورت یک سافت فورک، اطلاعات مربوط به امضای دیجیتال<sup>۳</sup> تراکنش باید به مکان جدیدی در بلاک منتقل می‌شد. و همچنین ریشه درخت مرکل<sup>۴</sup> همه این داده‌ها هم باید به یک بخش نامتعارف در بلاک بیت کوین، یعنی تراکنش کوین‌بیس<sup>۵</sup> که تراکنش پاداش ساختن بلاک برای ماینرها است انتقال می‌یافت.

طی روزها و هفته‌های بعد برنامه‌نویسان پروتکل بیت کوین متوجه شدند که این روش امکان جالب توجهی را بوجود می‌آورد، مزیتی که نامتعارف به نظر می‌رسید. با ایجاد یک بخش جدید در بلاک بیت کوین و انتقال اطلاعات مربوط به امضای دیجیتال تراکنش به این بخش، می‌توان ساینز بلاک را به گونه‌ای افزایش داد که اخلاقی در کار نودهایی که نرم‌افزار بیت کوین خود را به روزرسانی نکرده‌اند بوجود نیاید. با استفاده از این روش می‌توان ساینز بلاک را بدون تغییر محدودیت ساینز بلاک (که توسط ساتوشی روی ۱ مگابایت تنظیم شده بود) افزایش داد.

---

1 Eric Lombrozo  
2 Wladimir van der Laan  
3 Witness  
4 Merkle root  
5 Coinbase

تنها چند هفته قبل از برگزاری دومین کارگاه افزایش ظرفیت شبکه بیت کوین، چند نفر از برنامه‌نویسان پروتکل بیت کوین فکر می‌کردند که بالاخره توانسته‌اند حداقل یک راه‌حل موقت برای فیصله دادن به مناقشه سائز بلاک پیدا کنند. سگویت می‌توانست به‌طور موثری سائز بلاک را با استفاده از روش سافت فورک و سازگار با نودهای فعلی شبکه افزایش دهد و در عین حال اشکال تغییرپذیر بودن تراکنش را که از قبل در شبکه وجود داشت برطرف کند و در نتیجه به کارگیری از روش‌های پیشرفته‌تری برای افزایش ظرفیت شبکه بیت کوین، مثل شبکه لایت‌نینگ را امکان‌پذیر کند.

این یک راه‌حل بُرد-بُرد-بُرد بود یا حداقل آن‌ها این‌طور فکر می‌کردند.

## معرفی سگویت در هنگ کنگ

راهکار اعمال سگویت بر روی شبکه بیت کوین از راه سافت فورک برای اولین بار در دسامبر سال ۲۰۱۵ میلادی<sup>۱</sup> و توسط پیتر والا در دومین کنفرانس افزایش ظرفیت شبکه بیت کوین که در هنگ کنگ برگزار می‌شد ارائه شد. بیشتر افراد برای اولین بار در این کنفرانس با این روش آشنا شدند و به نظر می‌رسید استقبال گرمی از آن شود.

اندکی پس از پایان این کنفرانس گرگوری مکسول یک نقشه راه<sup>۲</sup> برای افزایش ظرفیت شبکه بیت کوین معرفی کرد که یکی از بخش‌های اصلی آن سگویت بود. این نقشه راه به سرعت مورد تأیید<sup>۳</sup> توسعه‌دهندگان بیت کوین و همچنین دیگر برنامه‌نویسان و کاربران اکوسیستم قرار گرفت.

1 [youtube.com/watch?v=fst1IK\\_mrng&feature=youtu.be&t=36m](https://youtube.com/watch?v=fst1IK_mrng&feature=youtu.be&t=36m)

2 [lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011865.html](https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011865.html)

3 [bitcoincore.org/en/2015/12/21/capacity-increase](https://bitcoincore.org/en/2015/12/21/capacity-increase)

ولی علی‌رغم هیجان اولیه این روش منتقدان خودش را هم داشت.

نگرانی‌ها در مورد روش پیشنهادی برای ارتقاء پروتکل بیت کوین (سگویت) متفاوت بود. جف گارزیک که در گذشته توسعه‌دهنده کُد بیت کوین بود و به تازگی شرکتی به نام «بلاک<sup>۱</sup>» تاسیس کرده بود، معتقد بود سگویت تنها یک راه حل کوتاه مدت برای حل مشکل افزایش ظرفیت بیت کوین است. در همین حال مایک هرن برنامه‌نویس اصلی نرم‌افزار بیت کوین ایکس‌تی به هیچ وجه با این پیشنهاد قانع نشده بود. او معتقد بود که این یک کلک حسابداری بیش نیست و اندکی بعد فضای توسعه و برنامه‌نویسی بیت کوین را کنار گذاشت و این پروژه را ترک کرد.

«جاناتان تومیم<sup>۲</sup>» که برنامه‌نویس یکی از نسخه‌های دیگر نرم‌افزار بیت کوین به نام «بیت کوین کلاسیک<sup>۳</sup>» بود هم اعتقاد داشت که این یک طرح «زشت و ناجور» است و پیشنهاد می‌کرد این تغییر بهتر است از راه یک هارد فورک انجام شود. حتی پیترو تاد هم که یک توسعه‌دهنده بیت کوین بود نگرانی‌هایی مخصوصاً در ارتباط با اثر آن روی استخراج بیت کوین داشت.

با این حال توسعه‌دهندگان سگویت معتقد بودند بخشی از این نگرانی‌ها قابل حل و بخشی دیگر از آن‌ها غیرقابل قبول (غیر مرتبط) هستند. همچنین از نظر آنان سگویت با توجه به امتیازاتی که داشت در کل روش مناسبی بود و در هر صورت توسعه کُد سافت فورک را آغاز کردند.

---

1 bloq

2 Jonathan Toomim

3 Bitcoin Classic



## توسعه کُد سگویت

با وجود اینکه یک نسخه اولیه سگویت روی زنجیره جانبی المنت شرکت بلاک استریم پیاده‌سازی شده بود، کُد مربوط به زنجیره اصلی شبکه بیت کوین باید جداگانه تهیه می‌شد. این مسأله بخاطر این بود که آن‌ها قصد داشتند این تغییر را به صورت یک سافت فورک بر روی شبکه اعمال کنند و همچنین طیف وسیعی از ویژگی‌های جدیدی که در المنت وجود نداشت هم باید در نظر گرفته می‌شدند. از میان آن‌ها می‌توان به راهکار افزایش سائز بلاک<sup>۱</sup> و تغییراتی که باید در شبکه نظیر<sup>۲</sup>-به-نظیر<sup>۲</sup> بیت کوین به وجود می‌آمدند، اشاره کرد.

نسخه نهایی پیشنهاد بهبود بیت کوین<sup>۳</sup> برای اعمال سگویت که شماره BIP141 به آن اختصاص داده شده بود توسط پیتر والا، اریک لامبروزو مدیر شرکت سایفرکس<sup>۴</sup>، و یک برنامه‌نویس مستقل به نام دکتر «جانسون لو»<sup>۵</sup> نوشته شد. در اوایل ژانویه سال ۲۰۱۶ میلادی و در بحبوحه بحث بر سر سائز بلاک آن‌ها و دیگر افرادی که به کار توسعه و برنامه‌نویسی در پروژه بیت کوین فعال بودند یک شبکه آزمایشی اختصاصی برای ارتقاء پروتکل راه‌اندازی کردند و نام آن را «سگ‌نت»<sup>۶</sup> گذاشتند. دو هفته بعد این شبکه در دسترس عموم فعالان در امر توسعه بیت کوین قرار گرفت تا روی آن آزمایش کنند. و کمی بعد در ماه مارس این شبکه برای پیشتیبانی از نسخه آزمایشی شبکه لایتینگ مجدداً ارتقاء پیدا کرد.

توسعه سگویت در ماه‌های آینده ادامه پیدا کرد. به این صورت که فعالان در امر توسعه بیت کوین نظراتشان را به تیم توسعه سگویت می‌دادند و اشکالات را برطرف می‌کردند و کُد آن را بهبود می‌دادند و یک نسخه جدید سگ‌نت را راه‌اندازی می‌کردند.

1 Witness discount

2 peer-to-peer

3 Bitcoin Improvement Proposal (BIP)

4 Ciphrex

5 Dr. Johnson Lou

6 SegNet

در همین حال، توسعه‌دهندگان کُد بیت کوین تلاش کردند با طیف وسیعی از شرکت‌هایی که به نحوی در زمینه بیت کوین فعال هستند، در ارتباط باشند و این مسأله باعث شد در طول زمان شرکت‌های بیشتری از این پروژه حمایت کنند.

تا ماه ژوئن سال ۲۰۱۶ میلادی ۴,۷۴۳ خط کُد جدید (با احتساب بخش‌هایی که به تست نرم‌افزار مربوط می‌شد) برای پیاده‌سازی سگویت به پروژه بیت کوین اضافه و ۵۵۴ خط هم حذف شد یا تغییر پیدا کرد. بعد از بازبینی کُد سگویت توسط برنامه‌نویسان و توسعه‌دهندگان پروژه بیت کوین در اواخر همان ماه، در نهایت مسئول اصلی نگهداری کُد بیت کوین ولادمیر ون در لان این بخش از کُد را در مخزن اصلی<sup>۱</sup> پروژه ادغام کرد.

## همایش‌ها و جلسات

هم‌زمان با توسعه سگویت تنش‌های مربوط به ساینز بلاک دوباره در کامیونیتی بیت کوین بالا گرفت. این بار چند شرکت فعال در زمینه بیت کوین و استخراج و به رهبری بیت کوین کلاسیک مصمم شدند تا ساینز بلاک را به روش هارد فورک به ۲ مگابایت افزایش دهند.

چند تن از برنامه‌نویسان بیت کوین و نمایندگان چند استخراج‌کننده و دیگر شرکت‌های فعال در زمینه بیت کوین یک بار دیگر و دوباره در هنگ کنگ در یک جلسه اضطراری با یکدیگر دیدار کردند تا در مورد مشکل افزایش ظرفیت شبکه بیت کوین بحث و گفتگو کنند.

---

1 Master branch

این جلسه به توافقی منجر شد که به «توافق میزگرد بیت کوین<sup>۱</sup>» (یا توافق هنگ کنگ) معروف است. در این جلسه تیم برنامه‌نویسان بیت کوین موافقت کردند که بخش نرم‌افزاری افزایش سایز بلاک از راه هارد فورک را آماده و به جامعه فعالان بیت کوین معرفی و پیشنهاد کنند. در مقابل ماینرها پذیرفتند تا زمانی که هارد فورک آماده شود نسخه سگویت را اجرا کنند. به نظر می‌رسید با این توافق جلوی پیش آمدن یک بحران جدی گرفته شده است ولی دیری نپایید که مشخص شد طرفین از این توافق رضایت ندارند.

چند ماه بعد افراد بیشتری از توسعه‌دهندگان بیت کوین و افراد فعال در صنعت استخراج در کالیفرنیا واقع در ایالات متحده با هم دیدار کردند. در این جلسه توسعه‌دهندگان بیت کوین متقاعد شدند که ماینرها سگویت را خواهند پذیرفت و اجرا خواهند کرد.

## آماده‌سازی و انتشار گد سگویت

سگویت در حالی که قرار بود برای ماه آوریل سال ۲۰۱۶ آماده شود، در نهایت و با شش ماه تاخیر رسماً در اکتبر همان سال آماده و در نسخه 0.13.1 نرم‌افزار بیت کوین قرار گرفت. ارتقاء پروتکل بیت کوین همچنین در نسخه‌های دیگری از نرم‌افزار بیت کوین مثل «بیت کوین ناتس» و «بی کوین<sup>۲</sup>» هم انجام پذیرفت.

با توجه به اینکه قرار بود برای به حداقل رساندن اختلال در شبکه از روش فعال‌سازی BIP9 استفاده شود، برای فعال شدن سگویت بر روی شبکه بیت کوین باید ۹۵ درصد ماینرها (از نظر توان هش، نه تعداد) پشتیبانی خود را از آن (با استفاده از قرار دادن یک عدد بخصوص در سربرگ<sup>۳</sup> بلاک‌های ماین شده) اعلام می‌کردند. قرار بود این اعلام

---

1 Bitcoin Roundtable Consensus  
2 BCoin  
3 Block header

پشتیبانی از سوی ماینرها از ۱۵ نوامبر آغاز شود. در همین حال کاربران شبکه بیت کوین هم ترغیب شدند تا نرم افزارهای بیت کوین خود را به روزرسانی کنند. و با گذشت زمان بسیاری از آنها این کار را انجام دادند.

بسیاری از فعالان در زمینه بیت کوین معتقد بودند با توجه به جلساتی که با استخراجهای استخراج بیت کوین برگزار شده بود و همچنین اعتقاد عمومی مبنی بر اینکه سگویت برای بیت کوین یک مزیت محسوب می شود، فعال کردن آن روی شبکه به سرعت انجام خواهد شد.

## زد و بندهای سیاسی

اما این موضوع اتفاق نیفتاد چون بعداً مشخص شد چند شرکت کننده در توافق هنگ کنگ روی مواردی که پذیرفته بودند اختلاف نظر داشتند.

به طور خاص، «جیهان وو»<sup>۱</sup> مدیر عامل شرکت Bitmain اظهار داشت که تنها در صورتی مایل به فعال سازی سگویت در شبکه است که توسعه دهندگان بیت کوین بخش افزایش سایز بلاک با استفاده از هارد فورک را هم به کُد بیت کوین اضافه کرده باشند. سایر استخراجهای استخراج مثل F2Pool، HaoBTC و bitcoin.com هم از سافت فورک سگویت پشتیبانی نکردند.

علاوه بر این یک استخراج چینی با نام ViaBTC ظهور کرد که ارتباط نزدیکی با شرکت Bitmain داشت و با توجه به توان هش<sup>۲</sup> بالای خود توانست به تنهایی از فعال

---

1 Jihan Wu

2 Hash rate

شدن سگویت جلوگیری کند. «هایپو یانگ»<sup>۳</sup> مسئول این استخراج استخراج به عنوان منتقد سرسخت سگویت شناخته شد.

با این تفاسیر فعال شدن سگویت بسیار بعید به نظر می‌رسید.

### فعال سازی سافت فورک از جانب کاربران (UASF)

در ماه فوریه سال ۲۰۱۷ و در حالی که حدود سه ماه از انتشار رسمی سگویت گذشته بود یک فرصت جدید برای فعال کردن آن روی شبکه پدید آمد.

یکی از برنامه‌نویسان ناشناس با نام مستعار «شاو لین فرای»<sup>۱</sup> که قبلاً در توسعه پروژه «لایت کوین»<sup>۲</sup> مشارکت کرده بود روش جدیدی برای فعال کردن سگویت در خبرنامه توسعه‌دهندگان بیت کوین و سایت محبوب [bitcointalk.org](http://bitcointalk.org) معرفی کرد. روشی که در آن سافت فورک توسط کاربران (و نه ماینرها) روی شبکه فعال می‌شود.<sup>۳</sup>

او در ایمیل خود اینگونه توضیح داد که روش فعال سازی سافت فورک بر پایه توان هش شبکه (که تبدیل به یک استاندارد برای فعال کردن سافت فورک‌ها شده بود) به معنی رأی‌گیری از ماینرها نیست.

او همچنین اضافه کرد روش اعلام حمایت<sup>۴</sup> از فعال سازی یک سافت فورک (از جانب ماینرها)، به غلط تفسیر به رأی‌گیری از آنها شده است و به نظر می‌رسد اصلاح این سوء تفاهم در جامعه فعالان بیت کوین کار دشواری باشد.

---

3 Haipo Yang

1 Shaolin Fry

2 Litecoin

3 User Activated Soft Fork

4 Signaling methodology

او روش جدیدی پیشنهاد کرد که در آن کاربران (نه ماینرها) سافت فورک را در شبکه فعال می‌کنند. در این روش یک «روز مشخص»<sup>۱</sup> تعیین می‌شود و نودهای شبکه از آن روز به بعد قوانین جدید را در شبکه اعمال می‌کنند. مادامیکه یک UASF توسط اکثریت اقتصادی (یعنی نودهایی که پذیرنده بیت کوین هستند. مثل فروشگاه‌ها، صرافی‌ها، و شرکت‌های توسعه‌دهنده کیف پول‌های بیت کوین) در شبکه اعمال شود، اکثریت ماینرها هم مجبور به پیروی (یا به عبارت دیگر فعال سازی) سافت فورک خواهند شد.

این ایده بلافاصله در مجامع بیت کوین و رسانه‌های اجتماعی سر و صدا به پا کرد. و وقتی «سمسون ما»<sup>۲</sup> مدیر اجرایی سابق شرکت BTCC و یکی از طرفداران سرسخت سگویت صندوقی برای تأمین هزینه توسعه و پیاده‌سازی نرم‌افزار UASF تأسیس کرد، به نظر می‌رسید که این پیشنهاد می‌تواند به واقعیت تبدیل شود.

## افشای یک تکنولوژی ثبت اختراع شده

در هفته اول آوریل سال ۲۰۱۷ میلادی، گرگوری مکسول در خبرنامه بیت کوین یک افشاگری کرد که مثل بمب ترکید. او مدعی بود که یک تراشه ASIC را مهندسی معکوس کرده و دریافته است که از یک تکنولوژی ثبت اختراع شده به نام ASICBOOST استفاده می‌کند. علاوه بر این مکسول فاش کرد که استفاده پنهانی از این فناوری با سافت فورک سگویت سازگاری ندارد. او نوشت: «این مسأله به خوبی می‌تواند رفتارهای غیرقابل توجیه برخی از افراد فعال در صنعت استخراج را توضیح دهد.»

در حالی که نامی از هیچ تولیدکننده تراشه ASIC در ایمیل مکسول برده نشده بود، شرکت Bitmain تأیید کرد که این فناوری ثبت اختراع شده را در تراشه‌های استخراج خود

---

1 Flag day

2 Samson Mow

پیاده‌سازی کرده است ولی هرگونه استفاده از آن‌ها را در شبکه اصلی بیت کوین<sup>۱</sup> انکار کرد.

در هر صورت این افشاگری باعث شد برخی از کاربران بیت کوین تمایل بیشتری به فعال شدن سگویت به صورت سافت فورک از خود نشان دهند. و از آنجایی که فعال شدن سگویت از راه توان هش شبکه (یا همان BIP9) تقریباً ناممکن شده بود، اعمال سافت فورک از روش UASF تنها راه ممکن به نظر می‌رسید.

### پیشنهاد BIP148

شاولین فرای و یک دو جین از افراد فعال در کامیونیتی بیت کوین اندکی پس از پیشنهاد ایده UASF یک کانال در Slack بیت کوین ایجاد کردند.

این کانال به مرکز اصلی بحث و سازماندهی UASF تبدیل شد. در ابتدا روز اول اکتبر و در نهایت (و برای مدیریت احتمال پایین آمدن توان هش شبکه) روز اول آگوست همان سال به‌عنوان روز موعود<sup>۲</sup> انتخاب شد. شاولین فرای یک پیشنهاد بهبود بیت کوین (BIP) برای آن نوشت و شماره BIP148 به آن اختصاص یافت. «رودلفو نوواک<sup>۳</sup>» بنیانگذار کیف پول سخت‌افزاری Coldcard هم با ایجاد یک وب‌سایت به ترویج این ایده پرداخت.

برنامه اولیه این بود که صرافی‌های بیت کوین و دیگر کسب‌وکارهای مرتبط با بیت کوین را با UASF همراه کنند. اگر این شرکت‌ها از این پیشنهاد پشتیبانی و سافت فورک را اجرا می‌کردند، اکثریت اقتصادی مورد نظر تا حدود زیادی تحقق پیدا می‌کرد.

---

1 mainnet

2 Flag day

3 Rodolfo Novak

ولی UASF به اندازه‌ای که برخی از طرفداران آن امیدوار بودند مورد استقبال قرار نگرفت. صرف‌نظر از چند شرکت و چند نفر از توسعه‌دهندگان بیت‌کوین، هیچ کدام از صرافی‌ها یا کسب‌وکارهای بزرگ از آن حمایت نکردند و حتی با آن مخالف بودند.

حدود اواسط ماه آوریل گرگوری مکسول در خبرنامه توسعه‌دهندگان بیت‌کوین اظهار داشت که معتقد است BIP148 ایده خوبی نیست. او یکی از معتبرترین و بانفوذترین توسعه‌دهندگان بیت‌کوین بود و به همین خاطر ابراز نظر او باعث شد این نسخه از UASF محبوبیت خود را هرچه بیشتر از دست دهد.

در عوض افرادی کار را بر روی یک روش جایگزین شروع کردند. روش BIP149.

## اجرای سگویت روی زنجیره آلت‌کوین‌ها

بسیاری از آلت‌کوین‌ها<sup>۱</sup> براساس کد بیت‌کوین ساخته شده‌اند. این بدان معنی است که کد سگویت با وجودی که برای بیت‌کوین نوشته شده است ولی تا حدود زیادی با این آلت‌کوین‌ها سازگاری خواهد داشت. بنابراین جای تعجب نیست که چند آلت‌کوین تصمیم گرفتند تا سگویت را روی زنجیره خود پیاده‌سازی کنند. اولین پروژه‌ای که این کار را در اوایل ژانویه ۲۰۱۷ میلادی انجام داد Groestlcoin بود.

اما پروژه‌های دیگر مثل Litecoin و Viacoin و Vertcoin درگیر این بازی سیاسی و کشمکش‌های مربوط به آن شده بودند. آن‌ها تا حد زیادی به ماینرهای بیت‌کوین متکی بودند که قصد پشتیبانی از سگویت برای آلت‌کوین‌ها را نداشتند.

---

1 altcoin



دلیل پشتیبانی نکردن آنها مسائل فنی یا دلایل دیگر ذکر شده بود ولی به قول برنامه‌نویس ارشد پروژه Viacoin رومانو<sup>۱</sup>: «به نظر می‌رسد به احتمال زیاد آنها می‌خواهند از فعال شدن سگویت روی زنجیره آلت کوین‌ها جلوگیری کنند چون اگر این قابلیت بر روی این پروژه‌ها فعال شود مجبور خواهند شد آن را روی شبکه بیت کوین هم فعال کنند.»

این موضوع باعث شد در آوریل سال ۲۰۱۷ میلادی «چارلی لی<sup>۲</sup>» خالق پروژه Litecoin از فعال شدن سگویت به روش UASF بر روی کوین «خود» حمایت کند. این ابتکار عمل با استقبال خوبی در بین کاربران Litecoin مواجه شد و طولی نکشید که ماینرها، شخص او، و دیگر فعالان جامعه Litecoin یک جلسه آنلاین ترتیب دادند که نتیجه آن قطعنامه میزگرد جهانی لاین کوین<sup>۳</sup> بود.

ماینرها توافق کردند در ازای اجرای برخی از تعهدات از جانب لی سگویت را در شبکه فعال کنند. این تلاش‌ها باعث شد شاولین فرای و افراد فعال در UASF به موفقیت آن خوشبین شوند.

یک هفته پس از فعال شدن سگویت بر روی پروژه لایت کوین یک فرد ناشناس اقدام جسورانه‌ای انجام داد. او ۱ میلیون دلار لایت کوین را در یک آدرس از نوع سگویت قرار داد و همه را به چالش کشید تا آن را بدزدند. تا امروز این لایت کوین‌ها دست نخورده باقی مانده است و این باعث می‌شود بتوانیم به فناوری سگویت بیشتر اعتماد کنیم.

---

1 Romano

2 Charlie Lee

3 Litecoin Global Roundtable Resolution

## توافق‌نامه نیویورک (Segwit2x)

روزها می‌گذشت و دعوای افزایش سائز بلاک همچنان ادامه داشت. یک نسخه جدید از نرم‌افزار بیت‌کوین به نام Bitcoin Unlimited برای افزایش سائز بلاک به ازای هر هارد فورک توسعه یافت و مورد توجه جامعه فعالان صنعت استخراج خصوصاً جیهان وو از شرکت Bitmain قرار گرفت. با این تفاسیر به نظر می‌رسید که پروژه بیت‌کوین احتمالاً به سمت یک هارد فورک (بحث برانگیز) پیش می‌رود.

این تهدید گسترده و احتمال فورک شدن زنجیره بیت‌کوین، «بری سیلبرت»<sup>۱</sup> بنیانگذار و مدیرعامل شرکت DCG را بر آن داشت تا قبل از کنفرانس Consensus 2017 در نیویورک جلسه‌ای ترتیب دهد. این جلسه در ابتدا در یک خبرنامه خصوصی برای کارآفرینان و سایر اعضای فعال در زمینه بیت‌کوین ارسال شد و توانست بخش قابل توجهی از افراد فعال در صنعت بیت‌کوین از جمله ماینرها را گرد هم آورد. هر چند هیچکدام از توسعه‌دهندگان کُد بیت‌کوین در آن حضور نداشتند.

نتیجه این جلسه به «توافق‌نامه نیویورک» معروف است. برگزار کنندگان این کنفرانس قصد داشتند بین آن‌هایی که می‌خواهند اندازه بلاک را از طریق هارد فورک افزایش دهند با افرادی که می‌خواهند سگویت را بر روی شبکه فعال کنند سازش بوجود آورند. بر اساس این ایده که ابتدا توسط بنیانگذار RSK سرژیو دمیان لرنر<sup>۲</sup> مطرح شده بود، مقرر شد هم سگویت تحت شرایط خاصی فعال شود، هم هارد فورکی برای دوبرابر کردن محدودیت سائز بلاک در شبکه اعمال شود.

حالا گذشته از این مسأله که جامعه فعالان بیت‌کوین از این توافق‌نامه حمایت نکرد، یک مشکل خاص در آن برجسته بود. مشکل این بود که شرایط فعال‌سازی سگویت در آن با

---

1 Barry Silbert

2 Sergio Demian Lerner

روشی که توسط تیم توسعه بیت کوین پیشنهاد و پیاده‌سازی و توسط کاربران اجرا می‌شد، ناسازگار بود.

## اقلیت نامنعطف<sup>۱</sup>

به نظر می‌رسید اقبال عمومی نسبت به BIP148 کم و به سمت BIP149 رویگردان شده است ولی در واقعیت این‌طور نبود و همچنان کسانی بودند که از اولین پیشنهاد UASF منصرف نشده بودند.

شاولین فرای این روش را با این فرض که اکثریت اقتصادی فعال در زمینه بیت کوین از آن پشتیبانی می‌کند و چند روز قبل از روز موعود متوقف می‌شود، معرفی کرد. اما برخی از کاربران فعال در کانال UASF Slack نظر متفاوتی داشتند. برخی از آنها از جمله لوک دشر معتقد بودند این سافت فورک باید بدون توجه به تصمیم بقیه فعالان در زمینه بیت کوین روی شبکه فعال شود حتی اگر موافقان این روش در اقلیت باشند و نتیجه این اقدام باعث بوجود آمدن یک آلت کوین جدید شود.

حدوداً اواسط ماه مه بود که آلفونس پیس<sup>۲</sup> این تصمیم را به مفهوم «اقلیت نامنعطف» در نظریه بازی<sup>۳</sup> پیوند داد که توسط آمارشناس و نویسنده نسیم نیکلاس طالب<sup>۴</sup> مطرح شده بود. به‌طور خلاصه این ایده فرض می‌کند که حتی یک اقلیت اقتصادی می‌تواند ماینرها را مجبور به فعال کردن سافت فورک سگویت کند. وگرنه آنها بخش بزرگی از کاربران خود را از دست خواهند داد.

---

1 The Intolerant Minority  
2 Alphonse Pace  
3 Game Theory  
4 Nassim Nicholas Taleb

با توجه به رسوایی که بر سر ASICBoost رخ داده بود، فعال شدن سگویت روی پروژه لایت کوین، عدم اجماع بر روی توافق نامه نیویورک، و پشتوانه تئوری بازی، BIP148 دوباره جان گرفت و بر سر زبانها افتاد.

چندین مقاله دیگر به موضوع ظرفیت بالقوه UASF پرداختند و بحث‌های زیادی در رسانه‌های اجتماعی و کانال‌های یوتوب در گرفت. اریک لامبروزو هم از این پروژه پشتیبانی کرد و کلاه‌های سمسون ما هم خیلی سر و صدا به پا کرده بود. روز یکم آگوست با الهام از نامی که کیف پول الکترام برای نسخه بعدی خود انتخاب کرده بود، «روز استقلال بیت کوین<sup>۱</sup>» نام گرفت.

تنها مشکل این بود که توافق نامه نیویورک (که مورد توافق حدود ۸۵٪ توان هش شبکه بود) با روش فعال سازی BIP141 (مربوط به توسعه دهندگان پروتکل بیت کوین) و BIP148 همخوانی نداشت.

## تغییر موضع و یک راه حل ابتکاری

بالاخره مهندس شرکت Bitmain Warranty «جیمز هیلارد<sup>۲</sup>» بود که برای حل تداخل بین روش‌های فعال سازی سگویت روی شبکه بیت کوین راه حل کمی پیچیده ولی هوشمندانه‌ای ارائه داد. او یک پیشنهاد بهبود بیت کوین جدید با شماره BIP91 نوشت و اگر اکثر ماینرها قبل از روز اول آگوست آن را روی شبکه فعال می کردند، هیچگونه فورکی در شبکه بیت کوین پدید نمی آمد.

1 Bitcoin Independence Day

2 James Hilliard

فرصت زیادی باقی نمانده بود چون این پیشنهاد اواخر ماه مه مطرح شد، ولی توسعه‌دهنده اصلی توافق‌نامه نیویورک، جف گارزیک این پیشنهاد را پذیرفت و قرار شد نرم‌افزار مربوطه را تا قبل از اول آگوست آماده کند.

## فعال شدن سگویت

ماه جولای به نیمه رسیده بود و ماینرهای بیت کوین فرصت فعال‌سازی سگویت را از روش BIP141 (که در انتظار فعال شدن بود) از دست دادند و بالتبع با BIP148 هم سازگار نبودند. بازار از فورک شدن شبکه به دو زنجیره متفاوت وحشت‌زده بود. تنها در یک هفته ارزش بیت کوین از ۲۵۰۰ دلار به ۱۹۰۰ دلار سقوط کرد. این مقدار کمترین میزان آن در طی یک ماه گذشته بود.

جامعه ماینرهای بیت کوین با دیدن این تغییرات در بازار متحیر شده بودند و با عجله هرچه بیشتر برای فعال شدن BIP91 روی شبکه بیت کوین تلاش کردند. BIP91 در نهایت در ۲۰ جولای یعنی فقط ۱۰ روز قبل از روز اول آگوست (روز تعیین شده در BIP148) روی شبکه بیت کوین آماده و حدود دو روز بعد فعال شد.

بعد از فعال شدن BIP91 باید منتظر فعال شدن سگویت می‌شدیم و این اتفاق در نهایت در تاریخ ۲۴ آگوست سال ۲۰۱۷ افتاد و سگویت روی شبکه بیت کوین فعال شد.

## سرنوشت توافق نامه نیویورک و فورک بیت کوین کش

بند دوم توافق نیویورک که حاصل اجماع بین ۸۵٪ توان هش شبکه بود، به یک هارد فورک برنامه ریزی شده اشاره می کرد که باید تا شش ماه آینده انجام می شد. ولی در تاریخ ۸ نوامبر سال ۲۰۱۷ «مایک بلشه»<sup>۱</sup> رئیس شرکت «بیت گو»<sup>۲</sup> در قالب یک نامه عمومی اعلام کرد که شرکت های امضا کننده این توافق نامه از اجرای هارد فورک افزایش سائز بلاک به ۲ مگابایت منصرف شده اند.

در گیر و دار فعال شدن سگویت روی پروتکل شبکه بیت کوین و در تاریخ اول آگوست سال ۲۰۱۷ زنجیره بیت کوین دوشاخه شد و یک آلت کوین جدید به نام Bitcoin Cash بوجود آمد که سائز بلاک آن ۸ مگابایت بود. در زمان نگارش این مطلب (در زمستان ۱۳۹۹) یک واحد بیت کوین کش تقریباً ۱۲ هزارم یک واحد بیت کوین ارزش دارد.

## مطرح شدن ایده کاهش سائز بلاک از جانب لوک دشیر

در اوایل سال ۲۰۱۹ لوک دشیر، یکی از افرادی که در اجرای سافت فورک سگویت نقش تاثیر گذاری داشت اعلام کرد سائز بلاک های بیت کوین باید کاهش پیدا کند تا افراد بیشتری قادر به اجرای نرم افزار بیت کوین (فول نود) باشند. او برای تحقق این هدف تلاش و برای تحقق آن یک نقشه راه<sup>۳</sup> پیشنهاد کرد ولی کامیونیتی بیت کوین دیگر تاب و تحمل یک مناقشه جدید بر روی تغییر سائز بلاک را نداشت و از ایده لوک استقبال نکرد.

1 Mike Belshe

2 BitGo

3 [luke.dashjr.org/education/bitcoin/2018/bitcoin-changes/](http://luke.dashjr.org/education/bitcoin/2018/bitcoin-changes/)

## سافت فورک تپروت

در زمان نگارش این مطلب، کامیونیتی و توسعه‌دهندگان بیت کوین برای اعمال یک تغییر جدید به نام «تپروت»<sup>۱</sup> به صورت سافت فورک روی شبکه تلاش می‌کنند.

تپروت برای اولین بار در اوایل سال ۲۰۱۸ از جانب گرگوری مکسول در گروه ایمیل توسعه‌دهندگان بیت کوین مطرح<sup>۲</sup> شد و توسعه<sup>۳</sup> کُد و تست‌های مربوط به آن انجام شد تا اینکه بالاخره در ژانویه سال ۲۰۲۱ در نسخه ۰.۲۱.۵ نرم‌افزار بیت کوین قرار گرفت و برای فعال شدن بر روی شبکه آماده شد.

به نظر می‌رسد این سافت فورک به اندازه سگویت جنجال برانگیز نباشد و پیش‌بینی می‌شود تا آگوست سال ۲۰۲۲ روی شبکه بیت کوین فعال شود. هرچند فرآیند تغییر پروتکل بیت کوین در ذات خود بحث برانگیز<sup>۳</sup> است و باید ببینیم در گذر زمان تاریخ چگونه برای سافت فورک تپروت رقم خواهد خورد.

---

1 Taproot

2 [lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html](https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html)

3 [bitcoinmagazine.com/articles/lottrue-or-lotfalse-this-is-the-last-hurdle-before-taproot-activation](https://bitcoinmagazine.com/articles/lottrue-or-lotfalse-this-is-the-last-hurdle-before-taproot-activation)

## پیوست

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

اگر دونفر همزمان با هم یک بلاک را پیدا کنند چه اتفاقی می‌افتد و سائز بلاک چه تأثیری روی آن دارد؟

تصور کنید که شبکه بیت کوین در سراسر جهان در حال اجرا است. افراد در تمام دنیا از آمریکا تا چین به این شبکه سراسری متصل شده‌اند و عملیات اثبات کار و قرعه‌کشی برای ساختن بلاک‌های جدید را انجام می‌دهند.

یک نفر در شیکاگو یک بلاک معتبر را پیدا و آن را در شبکه منتشر (اعلام) می‌کند و تمام کامپیوترهای واقع در ایالات متحده آمریکا این خبر را دریافت می‌کنند. در همین زمان یک نفر در شانگهای چین همان بلاک را چند ثانیه بعد از بلاکی که در شیکاگو پیدا شده بود، پیدا می‌کند. کامپیوترهای نزدیک به شبکه چین هنوز از بلاکی که در آمریکا پیدا شده است خبر ندارند و اول بلاکی که در کشور چین ساخته شده است را دریافت خواهند کرد.

با انتشار این دو بلاک توسط نودهای شبکه بیت کوین به یکدیگر دو نسخه از بلاک چین پدید می‌آید که با یکدیگر در رقابت‌اند. آمریکایی‌ها بلاک چینی دارند که بلاک آمریکایی در انتهای آن است و بلاک پیدا شده در چین هم به انتهای بلاک چین چینی‌ها



وصل شده است. چون هر دو بلاک چین مقدار اثبات کار یکسانی دارند و هر دو حاوی تراکنش‌های معتبر هستند، شبکه به دو شاخه تقسیم می‌شود.

تعیین بلاک برنده در اختیار هیچ مرجعیت متمرکزی نیست. پس چه باید کرد؟ برای حل این مشکل، بیت کوین یک راه حل ساده دارد: باید صبر کنیم تا ببینیم چه پیش می‌آید. حالا دو نسخه از بلاک چین وجود دارد که در رقابت با هم هستند. حدوداً ۱۰ دقیقه بعد بلاک بعدی ساخته خواهد شد. امریکایی‌ها براساس بلاک چین خود و چینی‌ها نیز براساس بلاک چین خود عملیات استخراج را انجام می‌دهند.

هر کدام که بتواند بلاک بعدی را پیدا کند برنده خواهد شد. چگونه؟ قانونی در گد بیت کوین وجود دارد که می‌گوید در شرایطی که بلاک چین دوشاخه شود، زنجیره‌ای که طولانی‌تر است برنده خواهد بود. هر کس انرژی بیشتری را صرف کند برنده است؛ قانونی که ناهمخوانی بین زنجیره‌ها را براساس اثبات کار انباشته<sup>۱</sup> آنها حل می‌کند و به افتخار ساتوشی ناکاموتو، اجماع ناکاموتو<sup>۲</sup> نام‌گذاری شده است.

فرض می‌کنیم بلاک بعدی را چینی‌ها پیدا می‌کنند. حالا زنجیره آنها یک بلاک طولانی‌تر از زنجیره امریکایی‌ها است. وقتی آن را در شبکه منتشر کنند نودهای بیت کوین امریکایی متوجه می‌شوند که نودهای چینی زنجیره طولانی‌تری را تولید کرده‌اند و بلاک چین خود را اصلاح<sup>۳</sup> می‌کنند، یعنی بلاک خود را با دو بلاکی که چینی‌ها ساخته‌اند عوض می‌کنند. حالا به بلاکی که امریکایی‌ها ایجاد کرده‌اند بلاک یتیم<sup>۴</sup> می‌گویند؛ چرا که از طرف شبکه رد شده و استخراج‌کننده آن جایزه‌ای بابت آن نگرفته است.

اگرچه من از لفظ امریکایی و چینی برای اشاره به نودها استفاده کرده‌ام، اما در واقعیت آنها از هویت و موقعیت جغرافیایی یکدیگر بی‌خبرند. تنها چیزی که باید بدانند این است

1 Cumulative Proof of Work

2 Nakamoto Consensus

3 Reorg (Reorganization)

4 Orphan Block

که چه کسی طولانی‌ترین زنجیره از بلاک‌ها را دارد و تراکنش‌های موجود در زنجیره همگی معتبر هستند (هیچ کوین‌ای دوبار خرج نشده باشد و باقی قوانین).

احتمال دو شاخه شدن زنجیره بلاک چین بسیار کم است. در گذشته یک مورد در ماه و یا کمتر بود اما اخیراً به دلیل ارتقاء تکنولوژی انتشار بلاک‌ها و ارتباط بین استخراج‌کنندگان در شبکه این اتفاق تقریباً نادر است.

یکی از دلایلی که بیت‌کوین هر ۱۰ دقیقه بلاک‌های نسبتاً کوچکی (کمتر از ۲ مگابایت) تولید می‌کند برای این است که این بلاک‌های به اصطلاح یتیم تا جایی که ممکن است کمتر ایجاد شوند. دلیل دیگر، کاهش نیازهای سخت‌افزاری برای اجرای یک نود است تا افراد بیشتری تشویق به اجرای آن در سیستم شوند.

اگر در هر ثانیه یک بلاک ساخته می‌شد یا اندازه بلاک‌ها خیلی بزرگ بود، مغایرت در زنجیره بلاک‌های چینی و آمریکایی با احتمال بیشتری رخ می‌داد، چون به لحاظ جغرافیایی فاصله زیادی با هم دارند و مدت زمان بیشتری طول می‌کشد تا اطلاعات بین آن‌ها منتقل شود. اگر ایجاد بلاک‌های به اصطلاح یتیم در شبکه زیاد باشد بلاک‌چین از بین خواهد رفت چون این بلاک‌های یتیم پشت‌سرهم تولید خواهند شد و نودهای شبکه دیگر نمی‌توانند روی تاریخچه یکپارچه تراکنش‌ها با هم به توافق برسند.

یک نود بیت‌کوین برای جلوگیری از حمله هک‌رهایی که ممکن است اطلاعات نادرستی به آن بدهند، فقط کافیست به یک نود معتبر که آخرین نسخه صحیح بلاک‌چین را در اختیار دارد، دسترسی داشته باشد. نودهای شبکه مدام با یکدیگر در ارتباط هستند و بلاک‌های تولید شده را با یکدیگر به اشتراک می‌گذارند. نود شما برای پیدا کردن صحیح‌ترین نسخه بلاک‌چین فقط کافیست بلاک‌چین‌ای که بیشترین اثبات کار انباشته را در خود دارد، در شبکه پیدا کند. چون دیگران هم از این قانون که در کد نرم‌افزار نوشته

شده است پیروی می کنند، این اطمینان حاصل می شود که همه نودهای شبکه روی صحیح ترین نسخه دفتر کل با یکدیگر به توافق می رسند. بنابراین ارسال یک نسخه ناصحیح از بلاک چین به یک نود برای هکرها کار دشواری است، چون برای رسیدن به هدف خود باید ارتباط آن نود به همه نودهای معتبر دیگر را قطع کنند و او را تنها به نودهای نامعتبر وصل کنند.

اگرچه انشعاب‌های (چند شاخه شدن) زنجیره بلاک چین در شبکه بیت کوین عمدتاً تصادفی و به دلیل تأخیر در انتشار بلاک‌ها ایجاد می شوند، اما این احتمال نیز وجود دارد که یک عنصر مخرب بخواهد کنترل بلاک بعدی و محتوای تراکنش‌های آن را در دست بگیرد و از اجماع ناکام تو سوء استفاده کند. این کار در صورتی ممکن است که فرد خرابکار کنترل بیش از ۵۰٪ توان هش شبکه را در اختیار بگیرد و طولانی‌ترین زنجیره را بر اساس بیشترین اثبات کار انباشته ایجاد کند. این مشکل به «حمله ۵۱٪»<sup>۱</sup> معروف است که در فصل ۹ به طور مفصل درباره آن صحبت شده است.

## هارد فورک‌ها<sup>۲</sup> و سافت فورک‌ها<sup>۳</sup>

تا اینجا متوجه شدیم که نرم‌افزار بیت کوین چگونه قوانینی را که افراد روی آن‌ها توافق دارند در شبکه اعمال می کند و فهمیدیم که افراد چگونه قوانینی را که موافق آن هستند با استفاده از انتخاب نسخه نرم‌افزار اجرا می کنند.

همچنین توضیح دادیم که چطور ماینرها در هنگام تولید بلاک قوانین شبکه را رعایت می کنند 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.

---

1 51% attack  
2 Hard Fork  
3 Soft Fork

درنهایت، 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 به تفصیل توضیح داده شده اتفاق می‌افتند.

حالا بیایید 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<sup>۱</sup> و هارد فورک که با قوانین قبل سازگار نیست<sup>۲</sup>. 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

1 Backwards compatible

2 Backwards incompatible

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 نود خود را به‌روزرسانی کنند. اگر این کار را هم انجام ندهند، می‌توانند همچنان مثل گذشته به فعالیت خود ادامه دهند. فقط ماینرها که بلاک‌ها را تولید می‌کنند باید نرم‌افزار نود خود را به‌روز کنند تا بلاک‌های تولیدشده از قوانین جدید پیروی کنند. وقتی یک ماینر قانون محدودیت ۱ مگابایت را در فورک جدید به‌روزرسانی 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 به‌روزرسانی نشده‌اند دیگر نمی‌توانند بلاک‌هایی را که تحت قوانین جدید ایجاد شده‌اند بررسی کنند. به همین دلیل تا نرم‌افزار خود را به‌روزرسانی نکنند در زنجیره قبلی باقی خواهند ماند. یکی از نمونه‌های هارد فورک افزایش 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 به‌روزرسانی کنند. اگر کسی در جریان نباشد و از ایجاد تغییرات در قوانین اطلاع نداشته

باشد، دیگر بلاک‌های جدید را دریافت نخواهد کرد و اگر خوش‌شانس باشد متوجه می‌شود که نرم‌افزار 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 بیت‌کوین در زمینه پرداخت‌های ارزان (با کارمزد کم) ناراضی بودند، تصمیم گرفتند برای ایجاد زنجیره‌ای با بلاک‌های بزرگ‌تر یک فورک ایجاد کنند. چون قانون بیت‌کوین تولید بلاک‌هایی کمتر از ۱ مگابایت بود (با توجه به سافت فورک سال ۲۰۱۰)، این افراد تصمیم گرفتند زنجیره جدیدی ایجاد کنند که در آن اندازه بلاک‌ها بزرگتر باشد. این فورک با نام Bitcoin Cash شناخته می‌شود.

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

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

درمورد این فورک، اکثریت افرادی که نودهای مهمی از نظر اقتصادی اجرا می‌کردند (مثل کیف پول‌ها، صرافی‌ها و پذیرندگان 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.

برای نگارش این مطلب از مقاله زیر نوشته «آرون ون ویردوم» استفاده شده است. تمامی حقوق مادی و معنوی این اثر متعلق به مجله بیت کوین و نویسنده آن است.

[The Long Road To SegWit: How Bitcoin's Biggest Protocol Upgrade Became Reality - AARON VAN WIRDUM](#)

سایت منابع فارسی بیت کوین  
ویراست اول  
زمستان ۱۳۹۹

**bitcoind.me**

منابع فارسی بیت کوین

معرفی کتابها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی زبان بیت کوین تالیف یا ترجمه شده‌اند