فصل چهاردهم.

مقیاس‌افزایی بیت‌کوین

بر اساس «گزارش جهانی پرداخت ۲۰۲۰» که توسط شرکت‌های کپجیمینای[۱] و بی ان پی پاریبا[۲] تهیه شده ۷۰۸/۵ میلیارد تراکنش غیرنقدی در سال ۲۰۱۹ انجام گرفته است که معادل روزانه حدود ۱/۹٤ میلیارد تراکنش خواهد بود[۳]. در گزارش آمده است که پیش‌بینی می‌شود تا سال ۲۰۲۳ میزان تراکنش‌های غیرنقدی به سالانه حدود ۱/۱ تریلیون (معادل ۳ میلیارد روزانه) برسد. برای مقایسه بهتر بد نیست بدانیم بالاترین حجم تراکنش‌های روزانه بیت‌کوینی که از آغاز تا امروز شاهد بوده‌ایم ٤۹۰،٤۵۹ تراکنش است که در ۱٤ دسامبر ۲۰۱۷ اتفاق افتاد. در سه سال منتهی به می ۲۰۲۱ تعداد تراکنش‌های روزانه به طور متوسط ۲۹۷،٤۷۷ با انحراف معیار ۵۰،٦۸۲ بوده است. اگر فرض کنیم بیت‌کوین می‌تواند تا روزانه نیم‌میلیون تراکنش را پردازش کند می‌توان نتیجه گرفت که این ارز جدید از پس رفع‌ورجوع ۰/۰۱٦۷ درصد از کل تراکنش‌های مورد انتظار در ۲۰۲۳ برآید! به زبان دیگر اگر بنا باشد همه پرداخت‌های دیجیتال جهان با بیت‌کوین صورت گیرند باید ظرفیت تراکنش‌های درون-زنجیره‌ای طی دو سال آینده حدود ٦۰۰۰ برابر افزایش یابد!

ظرفیت تراکنش فعلی بیت‌کوین با اندازه بلاک[٤] در حدود یک مگابایت حاصل شده است. یک رویکرد دم‌دستی و البته خام برای بهبود مقیاس‌افزایی این است که اندازه بلاک‌ها افزایش یابد تا بتوان کل تراکنش‌های جهان را با بیت‌کوین پوشش داد. این رویکرد مورد علاقه هواداران هاردفورک[۵]های نه چندان خوش‌فرجامی نظیر «بیت‌کوین ایکس‌تی[٦]»، «بیت‌کوین کلاسیک[۷]»، «بیت‌کوین آن‌لیمیتد[۸]» و «سِگویت توایکس[۹]» بود. همین ایده همچنین محرک هاردفورک نافرجام «بی‌گَش[۱۰]» (و البته هاردفورک نافرجام‌تر «بی‌گَش‌اِس‌وی[۱۱]») نیز به حساب می‌آمد. برای شناخت بهتر بیت‌کوین بد نیست داستان‌های تأسف‌بار و غم‌انگیز این تلاش‌های نسنجیده و البته ناموفق را مطالعه کرد[۱۲][۱۳]. نتیجه مهمی

---

۱. Capgemini
۲. BNP Paribas
۳. “The World Payment Report ۲۰۲۰.” Capgemini, Web. ۳ Oct. ۲۰۲۱.
٤. block size
۵. hard fork: اشاره به ایجاد تغییرات اساسی در شبکه بلاک‌چین است که پس از اعمال آن یک رمزارز دیگر افزون بر قبلی هم متولد می‌شود.
٦. Bitcoin XT
۷. Bitcoin Classic
۸. Bitcoin Unlimited
۹. Segwit۲X
۱۰. Bcash
۱۱. BcashSV
۱۲. Torpey, Kyle. “The Failure of SegWit۲x Shows Bitcoin is Digital Gold, Not Just a Better PayPal.” Forbes, ۲۰۱۸, Web.
۱۳. Bier, Jonathan. *The Blocksize War: The Battle Over Who Controls Bitcoin’s Protocol Rules*. Self published, ۲۰۲۱.

که از همه این ماجراها می‌توان گرفت این است که افزایش اندازه بلاک نمی‌تواند مسئله مقیاس‌افزایی را به شکل مطلوبی حل کند زیرا حتی افزایش مختصر اندازه بلاک هم باعث می‌شود هزینه‌های عملیاتی نُودهای کامل بیت‌کوین به‌شدت بالا بروند. این هم به احتمال زیاد کاهش تعداد نُودهای کامل را به همراه دارد؛ می‌دانیم که در نهایت آن عاملی که غیرمتمرکز ماندن بیت‌کوین و حفظ ثبات[۱] آن را تضمین می‌کند همین تعداد زیاد نُودهاست. در واقع با افزایش اندازه بلاک شاهد کاهش تعداد نُودهای کامل یا به عبارتی متمرکزتر شدن شبکه بیت‌کوین خواهیم بود.

ارزش پیشنهادی اصلی بیت‌کوین (ثبات و تغییرناپذیری آن) با اعمال قواعد اجماع سفت‌وسختی محقق می‌شود که تنها از طریق نُودهای کامل صورت می‌پذیرد. اعمال این قواعد تضمینی برای سانسورناپذیری ذاتی و سیاست پولی سخت («سخت بودن») بیت‌کوین به‌شمار می‌آید. افزایش اندازه بلاک برای بهبود مقیاس‌افزایی برای اهالی بیت‌کوین بسیار ناخوشایند بوده است زیرا شبکه را متمرکزتر می‌کند و هزینه اجرای یک نُود کامل را برای افراد معمولی بالا می‌برد. هرکسی هم قدمی در این مسیر برداشت عاقبتی بهتر از همین آلت‌کوین‌هایِ سرکاری نداشت که هزاران نوع آن در اینجا و آنجا به چشم‌تان می‌آید. وانگهی حتی اگر اهالی بیت‌کوین بی‌خیال عدم تمرکز هم بشوند و افزایش اندازه بلاک را بپذیرند باز مشکل حل نمی‌شود و ممکن نیست به مقیاسی برسیم که همه تراکنش‌های جهان پوشش داده شوند.

بیت‌کوین برای پوشش همه تراکنش‌های جهان باید اندازه هر بلاک را به ۵ گیگابایت افزایش دهد! این هم بدان معناست که هر رایانه‌ای در شبکه بیت‌کوین باید هر ده دقیقه این مقدار داده را دانلود کند. هر رایانه‌ای باید فضای کافی برای ذخیره این حجم عظیم از بلاک‌ها را داشته باشد که هر روز ۰٫۷ ترا بایت هم به آن‌ها افزوده می‌شود. این میزان افزوده کم‌وبیش معادل متوسط فضای ذخیره یک رایانه تجاری امروزی است؛ در واقع دارندگان رایانه‌های تجاری امکان دانلود بلاک‌چین بیت‌کوین را نخواهند داشت. فقط آن‌هایی که رایانه‌های بسیار پیشرفته در اختیار دارند می‌توانند از پس اداره یک نُود کامل برآیند. در چنین وضعیتی تنها عده محدودی امکان این را دارند که سراغ اجرای نُودهای کامل بروند و پیامد آن هم متمرکز شدن یا حتی مصادره کل زنجیره است. اگر فقط معدودی نُودهای کامل در سراسر جهان داشته باشیم کار تبانی برای آن‌ها ساده‌تر می‌شود و می‌توانند قواعد اجماع را به سود خود تغییر دهند چنانکه در مورد نُودهای دستوری در سال ۱۹۱٤ شاهد بودیم.

خوشبختانه راه‌حل‌های دیگری هم هستند که بدون افزایش اندازه بلاک می‌توان ظرفیت شبکه برای تراکنش‌های درون-زنجیره‌ای را بالا برد. در بسیاری از «طرح‌های بهبود بیت‌کوین[۲]» روش‌های کارسازتری برای پردازش تراکنش‌ها پیشنهاد شده است. اما حتی با وجود تمام این بهبودها، باز هم برای ثبت و ضبط تراکنش‌ها در دفتر کل بیت‌کوین با محدودیت‌های سفت‌وسختی روبه‌رو هستیم. هرچقدر هم بهینه‌سازی کنیم باز از ثبت حداقلی از داده‌ها (داده مربوط به خروجی تراکنش) گریزی نیست که در حال حاضر هنوز ۳۵

---

۱. immutability
۲. Bitcoin Improvement Proposals (BIPs)

بایت برای هر تراکنش است. یک بلاک ٤ مگابایتی را در نظر بگیرید حتی با بالاترین کارایی در استفاده از فضای آن، چیزی در حدود ۱۷ میلیون تراکنش روزانه را شامل می‌شود؛ اما این عدد از میزان مورد نیاز برای پردازش همه تراکنش‌های جهان خیلی فاصله دارد.

پول سخت در حاشیه[۱] نخواهد ماند.

از آنجا که عامل اصلی ارزشمند تلقی شدن بیت‌کوین عدم تمرکز آن است نمی‌توان برای ارتقای ظرفیت تراکنش آن سراغ کاهش تعداد نُودهای کامل رفت (چیزی که پیش‌تر گفتیم به متمرکز شدن آن می‌انجامد). پس آیا بیت‌کوین محکوم به این است که هرگز به مقیاس بالا نرسد؟ آیا یک شبکه گوشه‌ای و حاشیه‌ای می‌ماند و فقط چند صد میلیون تراکنش در روز را پردازش خواهد کرد؟ آیا بیت‌کوین هم در میان پول‌ها چیزی مشابه اسپرانتو در میان زبان‌ها خواهد بود؟ چیزی که گروهی محدود از علاقه‌مندان از آن استفاده خواهند کرد و بیشتر مردم درکی از آن نخواهند داشت؟

پول سخت بنا به ماهیت خود نوعی تکنولوژی همه‌گیر و پیشتاز به شمار می‌آید که نمی‌توان جلوی رشد آن را گرفت. در تاریخ پول بارها و بارها دیده‌ایم که پول‌های سخت‌تر توانسته‌اند پول‌های سهل‌تر را از بین ببرند و جای آن‌ها بنشینند. پول سخت نمی‌تواند با پول‌های سهل‌تر همزیستی مسالمت‌آمیز داشته باشد و هم‌باشی آن‌ها چیزی بیش از یک تعادل ناپایدار نیست. وقتی اروپایی‌ها دیدند که اهالی آفریقای غربی از مهره به عنوان پول استفاده می‌کنند از این قضیه کمال بهره‌برداری را کردند زیرا هزینه تولید مهره‌های گران‌قیمت آفریقایی در اروپا بسیار پایین بود. اروپایی‌ها تعداد زیادی از این مهره‌ها را همراه خود آوردند تا هرچیز باارزشی را در افریقای غربی خریداری کنند. دیگر ممکن نبود که مهره‌ها در افریقا نقش پول را بازی کنند و البته احساس دارندگان آن‌ها هم این وسط خیلی اهمیتی نداشت! هرکسی که همچنان مُصر بود که این مهره‌ها را به عنوان پول به کار بگیرد قدرت خریدش از دست می‌رفت لذا مهره‌ها دیگر نمی‌توانستند نقش پول را ایفا کنند.

قدرت انتخاب شما در مورد پول نامحدود نیست؛ شما نمی‌توانید با وجود یک پول سخت و افراد دیگری که همگی در راستای منافع شخصی خود عمل می‌کنند سراغ پول دیگری بروید. بدی کار هم فقط این نیست که کسی را پیدا کنیم که پول ما را قبول کند؛ پای مسئله مهم‌تری در میان است: دیگران پول شما را با هزینه پایین‌تر از قیمت بازاری آن تولید می‌کنند و ارزش پول‌تان کاهش پیدا می‌کند! هرچقدر پول سخت‌تر باشد در طی زمان ارزش آن (در مقایسه با پول‌های سهل‌تر) بهتر حفظ می‌شود؛ از پیش می‌دانیم که افزایش عرضه پول‌های سخت‌تر به طور نسبی دشوارتر است.

وقتی ارزش‌های نسبی دو نوع پول (پول سخت و پول سهل) در جهت مخالف یکدیگر تغییر می‌کنند می‌بینیم که استخر نقدینگی در دسترس پول سخت نسبت به پول سهل بزرگ‌تر می‌شود. به عبارت دیگر، احتمال این بالا می‌رود که افراد بخواهند با کسی مبادله کنند که تمایل به پرداخت یا پذیرش پول سخت دارد. افزایش ارزش یک پول باعث بهبود وضعیت

---

۱. niche

آن از نظر «فروش آسان» خواهد شد؛ «فروش آسان» هم احتمال به فروش رسیدن (مشتری پیدا شدن برای) پول است وقتی که می‌خواهیم خرجش کنیم.

«فروش آسان» چنانکه کارل منگر هم تأکید می‌کند خصلت اصلی پول به حساب می‌آید. سختی پول برای «فروش آسان» اهمیتی حیاتی دارد زیرا باعث افزایش ارزش نسبی استخر نقدینگی در دسترس آن (برای مبادله) می‌شود. طبیعی است که وقتی افراد به این فرایند پی می‌برند و آگاهانه سخت‌ترین پول را برمی‌گزینند شتاب کار بیشتر هم می‌شود. طی زمان ثروت بیشتری به سوی پول سخت‌تر می‌رود و افراد بیشتری هم خواهان استفاده از آن می‌شوند و ازاین‌رو تقاضا برای آن هم افزایش پیدا می‌کند. از بین رفتن نقش پولی نقره که در «استاندارد بیت‌کوین» از آن گفتیم و شکست‌های پرشمار ارزهای ملی تورمی مثال‌هایی از این روند ناگزیر به شمار می‌آیند.

اینجا دوباره به بحث بیت‌کوین و آمارهای «گزارش جهانی پرداخت» برگردیم. ۷۰۸/۶ میلیارد تراکنش که پیش‌تر اشاره شد را به یک دلیل مشخص «تراکنش‌های غیرنقدی» می‌نامند: در این پرداخت‌ها واسطه‌هایی دست‌اندرکارند که کار پردازش پرداخت را انجام می‌دهند. با آنکه امروزه چنین تراکنش‌هایی به‌طور عمده به شکل دیجیتالی انجام می‌گیرند از منظر اقتصادی نمی‌توان آن‌ها را به طور کامل با تراکنش‌های بیت‌کوینی یکی دانست. تراکنش‌های بیت‌کوین نیز دیجیتالی هستند ولی با این حال باز نوعی پرداخت نقدی به حساب می‌آیند زیرا آن‌ها را نمی‌توان تعهد کسی تلقی کرد. بیت‌کوین شکلی از پول نقد است زیرا دارنده‌اش می‌تواند آن را خرج کند و این بدون کسب رضایت یا اجازه فلان واسطه شخص ثالث هم شدنی است. پرداخت‌های بیت‌کوین به عنوان یک پول نقد دیجیتالی بیشتر باید با انتقال فیزیکی پول‌های فیزیکی مقایسه شوند نظیر پرداخت‌های نقد بین افراد، تسویه قطعی تراکنش‌ها و جابه‌جایی فیزیکی طلا بین بانک‌های درگیر تسویه طلا یا بانک‌های مرکزی. بیت‌کوین را در واقع نمی‌توان با پرداخت‌های غیرنقدی مقایسه کرد حتی اگر هردو به دلیل دیجیتالی بودن مشابه به نظر برسند. در مورد بیت‌کوین مسئله مهم دیجیتالی بودن آن نیست بلکه این است که در تراکنش‌های بیت‌کوین خبری از ریسک طرف معامله[۱] نیست.

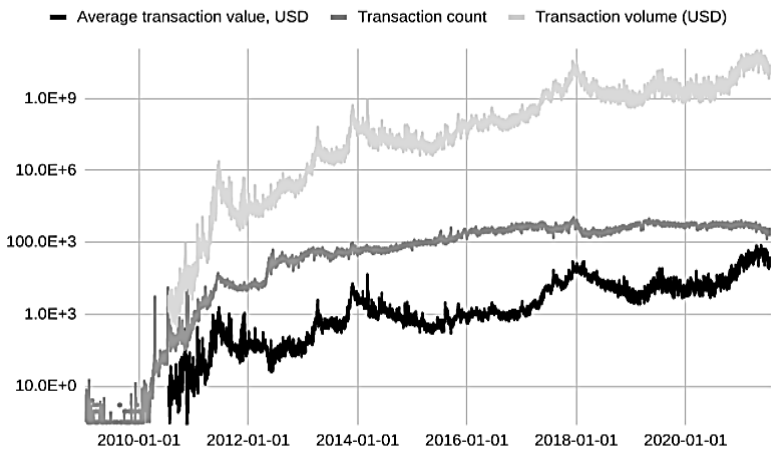
آن‌ها که منتظرند بیت‌کوین جایگزین پرداخت‌های غیرنقدی (با نقش‌آفرینی واسطه‌ها) شود و رشد کند ماهیت آن را خوب در نیافته‌اند. اگر بیت‌کوین بناست رشد کند این به‌طور عمده از مسیر پرداخت‌های نقد یا تسویه‌های قطعی رخ خواهد داد. نباید انتظار داشت که بیت‌کوین از طریق بالا رفتن تعداد تراکنش‌ها بزرگ شود و رشد کند. راهکارهای پرداخت روی بیت‌کوین با استفاده از لایه‌های فرعی ساخته می‌شوند و بار افزایش تعداد تراکنش‌ها هم روی همان لایه‌های فرعی خواهد بود. در مورد لایه نخست (زنجیره اصلی) روند حرکت به سوی تراکنش‌های کلان (با ارزش بالاتر) را شاهد هستیم؛ روندی که پیش از این‌ها آغاز شده است و وقتی کاربران برای تراکنش‌های خُرد سراغ تکنولوژی‌های لایه دوم بروند شتاب بیشتری هم خواهد گرفت. نباید از یاد برد که استفاده از راهکارهای لایه دوم نوعی بده‌بستان است که در ازای سرعت باعث قربانی کردن درجاتی از امنیت و ضد سانسور بودن می‌شود.

---

۱. counterparty risk

عرضه فضای بلاک بیت‌کوین

مرور دوازده سالی که از عمر بیت‌کوین می‌گذرد به‌روشنی نشان می‌دهد که روند حرکت آن به سوی تراکنش‌های کلان (با ارزش بالاتر) است. چنانکه در نمودار زیر هم می‌توان دید با آنکه تعداد تراکنش‌های روزانه افزایش یافته است ولی افزایش بسیار بیشتری را در ارزش این تراکنش‌ها شاهد هستیم. با مقایسه سال‌های اخیر (می ۲۰۲۱ و می ۲۰۲۰) با سال‌های پیشین می‌توان دریافت که متوسط ارزش یک تراکنش بیت‌کوینی تا ۱۵۰ برابر افزایش نشان می‌دهد. تعداد تراکنش‌های روزانه در پنج سال اخیر در عمل رشد چندانی نکرده است و از میانه‌های ۲۰۱۶ تا ۲۰۲۱ در دامنه ۲۰۰ هزار تا ٤۰۰ هزار باقی مانده‌اند اما ارزش تراکنش‌ها در همین دوره ۱۵ برابر شده است.



شکل ۱۷- ارزش متوسط تراکنش‌ها، تعداد تراکنش‌ها و حجم تراکنش‌های بیت‌کوین (Coinmetrics.io)

با وجود افزایش تقاضای بیت‌کوین طی این دوران می‌بینیم که مسیر رشد و مقیاس‌افزایی آن بالا رفتن تعداد تراکنش‌های درون-زنجیره‌ای نبوده بلکه ارزش تراکنش‌ها (چه برحسب بیت‌کوین و چه دلار امریکا) جهش داشته است. علی‌الاصول همین روند با افزایش تقاضا هم ادامه پیدا می‌کند. با توجه به ثابت بودن اندازه بلاک افزایش تعداد تراکنش‌های درون-زنجیره‌ای با محدودیت سفت‌وسختی روبه‌روست.

حتی اگر فرض کنیم با فورک‌های مناسب بتوانیم اندازه بلاک را افزایش دهیم، اگر این کار باعث شود کاربران معمولی در اجرای نُودهای خود دچار مشکل شوند پذیرش تغییرات جدید بسیار دشوار خواهد بود. این هم بدان معناست که باید اندازه بلاک را به صورت تدریجی و آهسته‌آهسته افزایش داد. از سوی دیگر تقاضای نگهداری بیت‌کوین می‌تواند بدون محدودیت جدی رشد کند و بالا رود. اگر بیت‌کوین بخواهد به ارزش پیشنهادی اصلی خود (یعنی پول سختی که عرضه آن مشخص و پیش‌بینی‌پذیر است) پایبند بماند این رشد تقاضا

مشکل‌ساز می‌شود؛ تقاضا از ظرفیت پردازش تراکنش‌های درون-زنجیره‌ای فراتر خواهد رفت.

اگر از منظر اقتصادی به بررسی فضای بلاک در بیت‌کوین بپردازیم می‌توانیم به‌خوبی پویایی بازار آن را درک کنیم. کمیابی ذاتی فضای بلاک بدان معناست که در یک رقابت قیمتی[۱] می‌توان اطمینان داشت آن‌هایی که فضای بلاک را ارزشمندتر می‌دانند به آن دست می‌یابند. طی زمان همین فشار رقابتی باعث شده است هزینه انجام برخی از انواع تراکنش بسیار بالا رود و بیشتر آن‌ها به صورت برون-زنجیره‌ای[۲] (از طریق راهکارهای لایه دوم یا دفاتر کل داخلی امانی[۳]) تسویه شوند. امروزه بسیاری از کسب‌وکارهای بیت‌کوینی، اغلبِ تراکنش‌های خود را در پایگاه‌های داده داخلی خودشان انجام می‌دهند. آن‌ها تنها بلاک‌چین بیت‌کوین را برای تسویه قطعی تراکنش‌های ورودی و خروجی به بنگاه استفاده می‌کنند. برای مثال وبگاه‌های قمار همه شرطبندی‌ها و بردها را در دفتر کل داخلی خود ثبت می‌کنند و تنها وقتی که کاربری بخواهد از وبگاه واریز یا برداشت کند از بلاک‌چین بیت‌کوین استفاده می‌شود. همین کار را صرافی‌ها هم انجام می‌دهند که کارشان پردازش سفته‌بازی‌های معامله‌گران بیت‌کوین و دیگر ارزهای دیجیتال است. در مقابل چندهزار تراکنش بیت‌کوینی که در دفتر کل داخلی (و البته خصوصی) انجام می‌گیرد فقط یک تراکنش درون-زنجیره‌ای خواهیم داشت. کار با روزهای آغاز بیت‌کوین خیلی متفاوت شده است؛ زمانی که این قبیل خدمات شرطبندی باید روزانه هزاران تراکنش را در بلاک‌چین بیت‌کوین ثبت می‌کردند. با توجه به افزایش کارمزد تراکنش‌های روی شبکه این مدل‌ها دیگر به کار نمی‌آیند و باید تغییر کنند و تنها برای تسویه قطعی از بلاک‌چین بیت‌کوین استفاده نمایند.

اگر افزایش تقاضا برای بیت‌کوین چشمگیر باشد بسیاری از تراکنش‌های کم‌ارزش بسیار گران تمام خواهند شد. از آنجا که محدودیت و سقفی برای افزایش تقاضا وجود ندارد ارزش کل تراکنش‌های روزانه بیت‌کوین در آینده شاید تا چند برابر مقدار فعلی افزایش یابد. اگر چنین شد شاهد بزرگ‌تر شدن استخر نقدینگی برای تراکنش‌های بیت‌کوین خواهیم بود و خریدها و فروش‌های بزرگ‌تری (با ارزش بالاتر) هم با بیت‌کوین انجام خواهند گرفت. پیامد ناگزیر این روند این است که تراکنش‌های کم‌ارزش‌تر بسیار گران تمام خواهند شد زیرا در مقایسه با تراکنش‌های بزرگ‌تر کارمزد آن‌ها به طور نسبی بسیار بیشتر است.

وقتی در مورد تراکنش‌های آینده بیت‌کوین صحبت می‌کنیم بجاست به بررسی دیگر بدیل‌های در دسترس هم بپردازیم. با مشخص شدن هزینه فرصت استفاده نکردن از تراکنش‌های درون-زنجیره‌ای بیت‌کوین در کاربردهای مختلف می‌توانیم ببینیم کدام یک بالاترین پیشنهاد را برای فضای بلاک خواهند داشت. اگر فرض کنیم فعالان بازار به دنبال امنیت بیشتر هستند و سیاست پولی سخت‌تر را می‌پسندند بیت‌کوین (درون-زنجیره‌ای) را انتخاب خواهند کرد؛ با آنکه شاید کارمزد آن بسیار بالاتر از دیگر راهکارهای پرداختی باشد که از طریق شخص ثالث و با امنیت کمتری کار را انجام می‌دهند. اگر هم کاربران

---

۱. bidding war
۲. off-chain
۳. custodial internal ledgers
اشاره به مواردی است که کلید خصوصی کاربران به صورت «امانی» در اختیار بنگاه‌هاست و مانده‌حساب‌ها و تراکنش‌ها در دفاتر کل داخلی ثبت می‌شود.

برای برخی کاربردهای خاص (نظیر تراکنش‌های با ارزش پایین) چندان دغدغه امنیت و سیاست پولی سخت را نداشته باشند هزینه فرصت استفاده نکردن از بیت‌کوین پایین خواهد بود.

در حال حاضر کارمزد پرداخت‌های مصرفی افراد به پردازشگران پرداخت[۱] از ۰ تا ۳ درصد متغیر است. ارزش پیشنهادی بیت‌کوین در حوزه پرداخت‌های خُرد چندان پررنگ نیست و فعالان بازار تنها وقتی سراغ تراکنش‌های بیت‌کوینی (درون-زنجیره‌ای) برای چنین پرداخت‌هایی می‌روند که کارمزدشان در حد چند سنت و حداکثر چند دلار باشد. همین طور برای حواله‌های بین‌المللی کارمزد تراکنش تا چند ده دلار می‌رسد که می‌توان آن را یک سقف قیمتی بالقوه برای بیت‌کوین در مورد حواله‌جات بین‌المللی به حساب آورد. اگر برای چنین کاربردهایی افراد سراغ بیت‌کوین بروند کارمزد تراکنش افزایش خواهد یافت و سقف قیمتی را رد خواهد کرد و دیگر برای کاربران اقتصادی نخواهد بود که تراکنش‌های خود را به صورت درون- زنجیره‌ای انجام دهند. این سازوکار بازخور ادامه خواهد یافت تا دوغ و دوشاب جدا شوند؛ به این معنا که مواردی که استفاده از بلاک‌چین اقتصادی نیست انجام نمی‌گیرند و فضای بلاک تنها برای آن‌هایی می‌ماند که بیت‌کوین بیشترین ارزش را برای آن‌ها فراهم می‌آورد. در شرایط فعلی تراکنش‌های درون- زنجیره‌ای بیت‌کوین تنها کسر کوچکی از کل تراکنش‌های بیت‌کوینی به حساب می‌آیند؛ حجم و تعداد تراکنش‌های انجام گرفته در صرافی‌های بیت‌کوینی و باشگاه‌های تفریحی[۲] بسیار زیاد است و همچنین نباید تراکنش‌های لایه دوم را در شرکت‌هایی که با بیت‌کوین تأمین مالی می‌شوند هم از یاد برد.

یکی از مواردی که متقاضیان حتی با افزایش کارمزد تراکنش‌های بیت‌کوین، به احتمال زیاد همچنان با میل برای آن پول خرج می‌کنند پرداخت‌های بین‌المللی مربوط به تسویه قطعی بین مؤسسات بزرگ مالی است. ماهیت این قبیل تراکنش‌ها به گونه‌ای است که پرارزش‌ترین و حساس‌ترین (از نظر امنیتی) تراکنش‌ها به حساب می‌آیند و از نظر قطعیت هم بیشترین شباهت را به تراکنش‌های بیت‌کوین دارند. امروزه انجام تمام‌وکمال پرداخت‌های بین‌المللی روزها (و شاید هفته‌ها) زمان می‌برد. بیت‌کوین تازه در آغاز راه است و به تدریج با افزایش اندازه و نقدشوندگی می‌توان آن را برای انجام امن و مطمئن چنین پرداخت‌هایی هم به کار گرفت. می‌توان حدس زد که با رشد بیت‌کوین، پرداخت‌های بزرگ (کلان) بیشتری هم با آن انجام خواهند گرفت که در نتیجه آن بسیاری از پرداخت‌های کوچک (خُرد) غیراقتصادی خواهند شد؛ چنین پرداخت‌هایی اغلب بدون استفاده از بلاک‌چین (برون-زنجیره‌ای) انجام خواهند گرفت. برای آن دسته پرداخت‌هایی که در این بازار غیراقتصادی می‌شوند «راهکارهای لایه دوم» به وجود آمده‌اند. این قبیل راهکارها با بهره‌گیری از برخی پروتکل‌ها برای انجام تراکنش‌های بیت‌کوینی طراحی شده‌اند؛ راهکارهای لایه دوم به ما وعده برخورداری از مزایای بیت‌کوین را (البته به درجاتی) می‌دهند بدون آنکه نیازی باشد کارمزد بالای استفاده از بلاک‌چین (تراکنش‌های درون-زنجیره‌ای) را پرداخت کنیم.

---

۱. payment processors
۲. Casinos

مقیاس‌افزایی لایه دوم

زمانی سکه‌های نقره همزمان با طلا برای معاملات (تراکنش‌های) خُرد مورد استفاده قرار می‌گرفتند؛ وقتی پرداخت با طلا به هر دلیل ممکن نبود مردم از نقره استفاده می‌کردند. اما با به وجود آمدن ابزارهای مالی مبتنی بر طلا این بساط هم برچیده شد. به همین ترتیب می‌توان حدس زد که تراکنش‌های لایه دوم بیت‌کوین هم جایگزین تراکنش‌هایی می‌شوند که با پول‌های سهل‌تر انجام می‌گیرند و این روند با اقبال بیشتر به بیت‌کوین و افزایش نقدشوندگی آن شدت می‌گیرد. هواداران دوآتشه بیت‌کوین شاید بگویند که این تراکنش‌های لایه دوم هرگز از نظر امنیت و اطمینان به پای تراکنش‌های اصلی (درون-زنجیره‌ای) نمی‌رسند. حرفشان حساب است ولی نکته‌ای مهم را نادیده می‌گیرند: تراکنش‌های لایه دوم رقیب تراکنش‌های لایه نخست (اصلی) به حساب نمی‌آیند بلکه این تراکنش‌ها در واقع با دیگر پول‌های نازل‌تر (سهل‌تر) رقابت می‌کنند.

با آنکه این هواداران دوآتشه گِله خواهند کرد که تراکنش‌های لایه دوم هرگز به درجه امنیت تراکنش‌های اصلی نمی‌رسند ولی محدودیت‌های مقیاس‌افزایی که پیش‌تر گفتیم یک چیز را نشان می‌دهند: بیت‌کوین نمی‌تواند آنقدر بزرگ شود (یا به زبانی دیگر، «مقیاس آن افزایش یابد») که از پس پردازش همه پرداخت‌های مصرفی روزمره افراد بربیاید.

تراکنش‌های بیت‌کوینی هر ۱۰ دقیقه یک بار در شبکه تأیید می‌شوند و برای پرداخت‌های مصرفی روزمره افراد مناسب نیستند؛ مشتریان انتظار دارند خیلی زودتر از این‌ها کارشان راه بیفتد. سطح امنیت و اطمینان بیت‌کوین برای تراکنش‌های خُرد «زیادی» و اتلاف وقت است؛ برای چنین تراکنش‌هایی گرفتن چند تأیید اولیه هم کافی است. آن هواداران پرجوش‌وخروش هم در مقابل این واقعیت اقتصادی تسلیم خواهند شد: افرادی که ترجیح می‌دهند از سازوکارهای پرداخت‌های لایه دوم یک پول سخت استفاده کنند تا اینکه سراغ سازوکارهای پرداخت لایه دوم پول‌های سهل‌تر بروند. محدودیت‌هایی که برشمردیم در راهکارهای پرداخت لایه دوم دیگر انواع پول هم وجود دارند. تفاوت اصلی این است که راهکارهای پرداخت پول سخت این امکان را به افراد می‌دهند که در آینده بهتر بتوانند ارزش پول‌شان را حفظ کنند. به بیانی دیگر، حالا که حرف از انتخاب بین دو گزینه (راهکارهای پرداخت پول سخت و پول سهل) است، عامل «فروش آسان در زمان‌های مختلف» تعیین‌کننده خواهد بود و پول سخت بی‌بروبرگرد برنده می‌شود.

اشتباه معمولِ بسیاری از اهالی بیت‌کوین در ارزیابی راهکارهای لایه دوم بیت‌کوین این است که آن‌ها را با تراکنش‌های بیت‌کوین مقایسه می‌کنند؛ اما درست‌تر آنست که آن‌ها را با تکنولوژی‌های پرداخت پول دستوری مقایسه کنیم. از نگاه نظری صِرف و روی کاغذ، حتی هفته آینده هم می‌توان همه تراکنش‌های جهان را با بیت‌کوین انجام داد مشروط بر اینکه در هفته جاری همه بانک‌های مرکزی جهان ذخایرشان را به بیت‌کوین تبدیل کنند! فرض کنید همه بانک‌های مرکزی جهان ارزهایی را منتشر کنند که پشتوانه آن‌ها بیت‌کوین است؛ اگر بلاک‌چین بیت‌کوین فقط برای تسویه تراکنش‌های بزرگ بین بانک‌های مرکزی استفاده شود در عمل می‌توان همه تراکنش‌های انجام شده در جهان را تراکنش‌های لایه دوم بیت‌کوین

تلقی کرد. در این سناریو پول‌های کاغذی دولتی، حساب جاری، کارت اعتباری و حتی حساب پی‌پل[۱] شما همه و همه راهکارهای پرداخت لایه دوم بیت‌کوین به حساب می‌آیند.

با افزایش تعداد دارندگان بیت‌کوین و تقاضا برای راهکارهای پرداخت، انگیزه برآوردن این نیاز هم به وجود خواهد آمد. اهل فن راهکارهای پرداخت فعلی را چنان بازطراحی (سفارشی‌سازی و بهینه‌سازی) خواهند کرد که بتوانند به خوبی با بیت‌کوین هم کار کنند. پیامد آن هم شاید ابداع دوباره بسیاری از سازوکارهای پرداختی باشد که امروز از آن‌ها بهره می‌گیریم. تراکنش‌های لایه فرعی البته امنیت تراکنش‌های اصلی را ندارند ولی برای تراکنش‌های خُرد مصرفی روزمره خیلی هم نیاز به آن سطح از امنیت نداریم! آن مشتری که حسابی در یک صرافی یا باشگاه تفریحی آنلاین افتتاح کرده از همان آغاز به طرف دیگر اعتماد کرده و به او اختیار انجام خیلی کارها را داده است؛ طرف می‌تواند تراکنش‌ها را بعد از دریافت وجوه واریزی مشتری در دفتر کل خودش ثبت کند که البته این ریسکی ندارد. اما اگر او بخواهد پول مشتری را بالا بکشد دستش باز است و می‌تواند چنین کند؛ فارغ از آنکه تراکنش‌های «داخلی» میان آن‌ها روی بلاک‌چین ثبت شده باشد یا خیر. کاربر فقط زمانی این وجوه را تحت کنترل واقعی خود خواهد گرفت که آن را از طرف (صرافی، باشگاه تفریحی، شرکت‌های خدمات پرداخت و مانند آن) تحویل گرفته باشد.

با افزایش تقاضای بیت‌کوین شاهد تکثیر این راهکارهای لایه دوم خواهیم بود. در نتیجه برای کاربردهای مختلف راهکارهای متنوع با درجات مختلف ریسک و امنیت هم طراحی خواهند شد. یک مثال خوب اُپن‌دایم‌ها[۲] (نوعی کیف پول سخت‌افزاری) هستند. این فلش‌مموری‌ها به شکلی طراحی شده‌اند که امکان دستکاری آن‌ها وجود ندارد و می‌توان مانده بیت‌کوین داخل آن‌ها را خیلی سریع تأیید و راست‌آزمایی کرد. اُپن‌دایم برای تراکنش‌های خُرد (با مبالغ پایین) بین افراد آشنا با یکدیگر که به هم اعتماد دارند سازوکار مناسبی به شمار می‌آید؛ این تراکنش‌های شخصی را می‌توان بدون نیاز به ثبت در بلاک‌چین بیت‌کوین انجام داد. اُپن‌دایم‌ها ضعف‌هایی هم دارند؛ برای مثال به دلیل نداشتن عبارت بازیابی[۳] برای نگهداری مبالغ بزرگ چندان امن و مناسب نیستند. با این حال این قبیل تکنولوژی‌ها پردازش تعداد زیادی از تراکنش‌های کوچک را امکان‌پذیر می‌سازند و همین امر نقدشوندگی تراکنش‌های بیت‌کوین را بهبود می‌بخشد. در واقع باید آن‌ها را نوعی سند در وجه حامل[۴] به حساب آورد.

راهکارهای امانی چندامضایی[۵] هم شاید بتوانند به ارزان‌تر شدن پرداخت‌های لایه دوم کمک کنند. اگر افراد کوین‌های خود را در حساب‌های چندامضایی سپرده‌گذاری کنند انتقال کوین‌ها روی بلاک‌چین تنها از طریق دسترسی به کلیدهای خصوصی صاحبان آن‌ها و بانک (هر دو با هم) ممکن می‌شود. بانک هم می‌تواند یک شبکه پرداخت برای صاحبان چنین حساب‌هایی روی پایگاه داده داخلی خودش ایجاد کند و افراد بین خودشان امکان انتقال

---

۱. PayPal
۲. Opendimes
۳. backup seed phrase
۴. bearer instrument
۵. multi-signature custody solutions

مالکیت کوین‌ها را خواهند داشت؛ تسویه این تراکنش‌های داخلی هم تنها به صورت دسته‌ای[۱] روی بلاک‌چین و در انتهای روز، هفته یا ماه انجام خواهد شد.

شبکه لایتنینگ (آذرخش)

شاید شبکه لایتنینگ (آذرخش) در حال حاضر جالب‌ترین و امیدوارکننده‌ترین طرح مقیاس‌افزایی لایه دوم باشد؛ اکوسیستمی نوظهور از نُودهایی که امکان اجرای خودکار، ارزان و سریع یک شبکه پرداخت را فراهم می‌سازد. شبکه لایتنینگ با ایجاد (باز کردن) کانال بین نودهای مختلف و به صورت چندامضایی عمل می‌کند: نُودها با ارسال وجوه (از طریق یک تراکنش درون-زنجیره‌ای) به یک نشانی چندامضایی یک کانال ارتباطی بین یکدیگر باز می‌کنند. هر طرف مانده خود را در آن حساب چندامضایی نگه می‌دارد و طرفین می‌تواند به یکدیگر پول انتقال دهند (پرداخت کنند) که این هم از طریق امضای تراکنش‌های لایتنینگ (بدون استفاده از بلاک‌چین) صورت می‌گیرد و مانده‌های طرفین به‌روز می‌شود. وقتی هریک از طرفین خواست که کانال را ببندد یک تراکنش روی بلاک‌چین (که برآیند همه تراکنش‌های قبلی است) از نشانی کانال چندامضایی برای دو طرف با مانده‌های مربوط به آن‌ها ارسال می‌شود.

اما کاربران لایتنینگ لازم نیست برای هر کسی و هر تراکنشی یک کانال مجزا باز کنند؛ پرداخت‌ها می‌توانند از مسیر نُودها و کانال‌های مختلف بگذرند و حتی دو طرفی که کانال مستقیمی با هم ندارند را به هم وصل کنند. وقتی تعداد کانال‌ها و البته نقدینگی آن‌ها افزایش پیدا کند مسیریابی[۲] میان کاربران هم ساده‌تر انجام می‌شود. نودهایی که در مسیر پرداخت بین دو نُود دیگر قرار می‌گیرند برای جبران هزینه‌های ناشی از تأمین نقدینگی (برای انتقال به نُودهای بعدی) می‌توانند کارمزد مسیریابی دریافت نمایند.

نقطه قوت این نوع مقیاس‌افزایی این است که باز کردن و بستن یک کانال در کل فقط به دو تراکنش درون-زنجیره‌ای نیاز دارد. از این طریق هر دو طرف می‌توانند بی‌شمار تراکنش برون-زنجیره‌ای بدون هیچ هزینه اضافی انجام دهند. از طرفی برای زمان‌بندی این تراکنش‌های درون-زنجیره‌ای هم انعطاف زیادی داریم؛ باز کردن و بستن کانال می‌تواند وقتی انجام شود که تقاضا برای تراکنش‌های درون-زنجیره‌ای پایین‌تر است (کارمزدها کمتر است). کاربران هم می‌توانند اطلاعات «مِم‌پول[۳]» را که در دسترس عموم است ببینند و بررسی کنند که آیا رقابت برای فضای بلاک کارمزدها را افزایش داده است یا خیر. آن‌هایی که تراکنش‌های تکراری زیادی دارند هم کارشان خیلی ساده‌تر می‌شود: آن‌ها می‌توانند در کانال‌های خودشان یا دیگران کار تسویه را انجام دهند بدون آنکه نیاز باشد هر تراکنشی روی دفتر کل بیت‌کوین ثبت شود. با وجود همه این مزایا باید به خاطر داشت که تراکنش‌های برون-زنجیره‌ای روی لایتنینگ به اندازه درون-زنجیره‌ای‌ها امن نیستند. اما مهم‌ترین اختلاف بین این دو نقدینگی است.

---

۱. batch
۲. routing
۳. Mempool

محدودیت واقعی شبکه لایتنینگ، امنیت یا تعداد تراکنش‌های آن نیست بلکه به عمق استخر نقدینگی آن برمی‌گردد. هرچقدر تعداد افراد در این شبکه و پول‌هایی که در کانال‌ها رد وبدل می‌شود بیشتر باشد احتمال اینکه افراد با شخص دیگری در شبکه تعامل داشته باشند بالا می‌رود. اما عکس ماجرا نیز صادق است؛ یعنی نقدینگی اندک، کارمزد بیشتر و زمان انتظار بالاتر را به همراه دارد. تأمین نقدینگی برای شبکه هم ساده نیست؛ با کلافی تودرتو و بسیار پیچیده از تصمیم‌های اقتصادی افراد روبه‌رو هستیم؛ تصمیم‌هایی که وابستگی همه‌جانبه به ارزش‌گذاری آن‌ها از زمان و عدم قطعیت ناگزیر آینده دارند.

لودویگ فون میزس نشان می‌دهد که عدم‌قطعیت‌های آتی را باید محرک اصلی تقاضا برای نگهداری پول به حساب آورد[۱]. اگر هیچ عدم قطعیتی نسبت به آینده وجود نداشته باشد، انسان‌ها پیشاپیش از همه هزینه‌ها و درآمدهای خود آگاه خواهند بود و به شکلی برنامه‌ریزی خواهند کرد که نیازی به نگهداری پول نقد نباشد. اما عدم قطعیت بخشی جدایی‌ناپذیر از زندگی انسان‌هاست پس آن‌ها نیز مجبورند برای مخارج آتی پول نگهداری کنند.

نباید فراموش کرد که مانده بیت‌کوین در یک کانال لایتنینگ هم‌ارز با پول نقد نیست. علت هم این است که پول در آن کانال تنها می‌تواند برای پرداخت به طرف‌های دیگر کانال یا دیگرانی که در شبکه لایتنینگ به آن‌ها وصل شده‌اند مورد استفاده قرار گیرد. نقدشوندگی این پول به اندازه کوین‌ها نیست که می‌توانند بلافاصله در شبکه بیت‌کوین مورد استفاده قرار بگیرند. همچنین باید به یاد داشت که ایجاد یک کانال نیازمند صرف برخی هزینه‌ها برای کارمزد، زمان و هماهنگی است (هرچند چشمگیر نباشند) و همچنین نقدشوندگی (نقدینگی) پول کاربر یک کانال به درجه نقدشوندگی (نقدینگی) طرف‌های دیگر آن کانال بستگی دارد. از آنجا که نقدینگی یک کانال می‌تواند بازده‌ای در قالب کارمزد مسیریابی هم به همراه داشته باشد شاید بهتر باشد مانده کانال را نوعی سرمایه‌گذاری در ازای دریافت هزینه‌های مسیریابی و البته نوعی قرارداد اختیار معامله[۲] در نظر بگیریم: حق (نه الزام و تعهد) ارسال آنی فلان مقدار ارزش اقتصادی از طریق آن کانال در صورت باز بودن.

با توجه به اینکه تأمین نقدینگی کانال‌ها می‌تواند سودی هم عاید افراد کند پس باید یک نکته را در نظر داشت: تصمیم‌گیری در مورد میزان نقدینگی یک نُود خاص تنها بر اساس میزان تقاضای مانده نقدی فرد نیست بلکه یک تصمیم سرمایه‌گذاری با توجه به بازده مورد انتظار کارمزدهای مسیریابی هم به شمار می‌آید. اگر افراد مانده‌های لایتنینگ خود را تنها بر اساس نیاز شخصی به مانده نقدی، مدیریت می‌کردند البته بعید بود نقدینگی کافی برای مسیریابی پرداخت‌های دیگران در دسترس باشد. اما از آنجا که تقاضای زیادی برای نقدینگی کانال‌ها به منظور انجام تراکنش‌های ارزان وجود دارد می‌توان قضیه را نوعی سرمایه‌گذاری هم تلقی کرد؛ با برآوردن این تقاضا می‌توان سود خوبی (در قالب کارمزدهای مسیریابی) به دست آورد که البته نیازمند تخصص است. به بیان دیگر، پویایی‌شناسی شبکه

---

۱. Mises, Ludwig von. *Human Action: The Scholar's Edition. Auburn*, AL, Ludwig von Mises Institute, ۱۹۹۸.

۲. option contract

لایتنینگ بر این دلالت دارد که اپراتورهای نُود[۱] تخصصی پا به میدان خواهند گذاشت تا بتوانند در ازای تأمین نقدینگی سود کسب کنند. امروز هم کار بانک‌ها در حوزه پردازش پرداخت‌ها چیزی جز تأمین نقدینگی نیست و در مالیه سنتی کار فراهم کردن پول نقد با بانک‌هاست. به شکلی مشابه می‌توان گفت رشد شبکه لایتنینگ هم در گرو مدیریت حرفه‌ای و تأمین نقدینگی است.

مدیریت نقدینگی در کانال‌ها برای حداکثر کردن سود (کارمزدها) بیشتر شبیه به کار یک بنگاه تجاری تخصصی است تا افرادی که در پی مدیریت هزینه‌های خود در بین حساب‌های بانکی، کارت‌های اعتباری و پول نقد هستند. بعید به نظر می‌رسد که نقدینگی فراوان مورد نیاز برای شبکه و همچنین مسیریابی آن تنها با نقش‌آفرینی افرادی فراهم آید که برای تعامل با یکدیگر وارد کانال‌ها می‌شوند. علت اصلی هم این است که یک گلوگاه این وسط وجود دارد و هرکس با نقدینگی کانال‌های طرف‌های مقابل محدود می‌شود. وقتی فردی کانال‌های بیشتری در شبکه لایتنینگ ایجاد می‌کند نقدینگی بیشتری برای آن فراهم می‌آورد ولی هزینه‌های بالاتری برای باز کردن و بستن کانال‌های متعدد متحمل خواهد شد. اما باز کردن کانالی با یک نُود تخصصی برای تأمین نقدینگی (البته همراه با کانال‌های متعدد که رو به نُودهای دیگر باز شده‌اند) می‌تواند نقدشوندگی و دسترسی بسیار بهتر برای شخص فراهم آورد. اپراتورهای نُود تخصصی این امکان را برای کاربران تازه‌وارد شبکه بیت‌کوین فراهم می‌آورند که وارد شبکه شوند و از مزایایی تراکنش‌های بیت‌کوینی سریع و ارزان بهره‌مند شوند.

فرصت کسب سود از تأمین نقدینگی و مسیریابی برای کاربران حاکی از این است که با ادامه رشد شبکه لایتنینگ یحتمل تأمین نقدینگی به کسب‌وکاری پرسود و البته بسیار پیچیده تبدیل شود. از منظر کارایی اقتصادی هم اگر تأمین نقدینگی به یک خدمت حرفه‌ای بدل شود و کسب‌وکارهای حرفه‌ای آن را بر عهده بگیرند شبکه هم پابرجاتر خواهد بود. در این سناریو انتظار می‌رود به تدریج شاهد ظهور الگوی قطب- اقمار[۲] باشیم؛ یک شبکه جهانی از نُودهای تخصصی با نقدینگی چشمگیر که همگی با هم از طریق کانال‌ها ارتباط دارند و یک کاربر معمولی هم تنها با چند کانال باز می‌تواند با این نُودهای نقدینگی بزرگ مرتبط شود. یک شبکه پابرجا متشکل از نودهایی با نقدینگی فراوان، مسیریابی سریع‌تر و ارزان‌تر را ممکن می‌سازد.

وانگهی با فرض درستی آنچه بالاتر درباره امانت‌گذاری[۳] گفتیم، بسیاری از مردم ترجیح خواهند داد خودشان از کانال‌های پرشمار برای رفع و رجوع امورشان استفاده نکنند. افراد به‌جای این کار پولشان (بیت‌کوین‌ها) را نزد اپراتورهای نُود لایتنینگ امانت می‌گذارند که آن‌ها می‌توانند به صورت درون-زنجیره‌ای به تسویه پرداخت‌ها بپردازند.

بده‌بستان‌ها و ریسک‌ها

---

۱. node operators
۲. hub-and-spoke
۳. custody

رفتن به سوی مقیاس‌افزایی لایه دوم نه تنها ریسک‌هایی برای افراد به همراه دارد بلکه یک ریسک سیستمی هم برای خود شبکه نیز ایجاد می‌کند. نخستین و آشکارترین پیامد آن بحث مقاومت در برابر سانسور در شبکه است. بیت‌کوین تنها تکنولوژی مطمئن برای انتقال ارزش اقتصادی بدون نیاز به واسطه‌هاست ولی فقط امکان انجام چند صدهزار تراکنش در روز از طریق آن وجود دارد. با افزایش تقاضا برای تراکنش‌های بیت‌کوین و رو آوردن افراد به راهکارهای لایه دوم (که برای تصفیه حساب از اشخاص ثالث استفاده می‌کنند) کار سخت می‌شود: این اشخاص ثالث می‌توانند تراکنش‌ها را سانسور و حتی کوین‌ها را مصادره کنند. ازاین‌رو یکی از مزیت‌های اصلی شبکه بیت‌کوین با این مقیاس‌افزایی‌های لایه دوم از دست می‌رود.

دومین ریسک بسیار جدی‌تر و اساسی‌تر است زیرا پروتکل‌ها و پارامترهای اجماع کل شبکه را تهدید می‌کند. اگر تراکنش‌های بیت‌کوین به راهکارهای لایه دوم منتقل شوند که بسیاری از افراد ناگزیر باید به اشخاص ثالث برای راست‌آزمایی تراکنش‌ها و اِعمال قواعد اجماع شبکه اعتماد کنند دیگر به‌سختی بتوان بیت‌کوین را سیستمی همتابه‌همتا دانست. در نتیجه ریسک تبانی بین نودهای مسئول پردازش تراکنش‌ها بالا می‌رود. بد نیست آن «بهبود» نافرجام «سِگویت توایکس» را به یاد آوریم و دنیایی را تصور کنیم که کاربران بسیار کمتری می‌توانستند نُودهای کامل خود را اجرا کنند. اگر کاربران به کسب‌وکارهای بیت‌کوینی برای اعمال قواعد اجماع متکی باشند این کسب‌وکارها می‌توانند پارامترهای اجماع بیت‌کوین را تغییر بدهند. با کاهش تعداد نُودها، اثرگذاری و نقش آن‌ها بیشتر می‌شود و به لقمه آماده‌تری برای دولت‌ها و «مهاجمان[۱]» بدل خواهند شد. شبکه بیت‌کوین با چندصد نُود پابرجایی و امنیت بسیاری کمتری از یک شبکه ده‌ها هزار نُودی خواهد داشت.

فرد در ارزیابی خود از گزینه‌های پرداخت لایه دوم در کنار سهولت و هزینه‌های پایین آن‌ها باید به یک ریسک مهم توجه داشته باشد: از دست رفتن مقاومت در برابر سانسور. این ریسک البته پیامد مستقیم خود فرایند پردازش لایه دوم به حساب نمی‌آید بلکه دلیل آن کاهش تعداد نُودهاست که خطری وجودی برای ماهیت غیرمتمرکز بیت‌کوین تلقی می‌شود. با این حال باید به یاد داشت در نقطه شلینگ[۲] (کانونی) نُودهای بیت‌کوین (با فرض آنکه روی پارامترهای اصلی اجماع توافق دارند) نیازی نیست هر کاربر یک نُود کامل را اجرا کند. برای جلوگیری از اینکه یک گروه کوچک پارامترها را به نفع خود تغییر ندهد فقط باید تعداد کافی نُود کامل مستقل وجود داشته باشند.

برای مقیاس‌افزایی بیت‌کوین یک چالش اساسی این خواهد بود که راهکارهای لایه دومی را معرفی کنیم که نیاز به اعتماد به شخص ثالث و احتمال سانسور تراکنش‌ها از سوی آن‌ها را به حداقل برساند. برای بقای بیت‌کوین باید پارامترهای اصلی اجماع به ویژه پارامترهای اقتصادی بدون تغییر باقی بمانند. برای تحقق این امر بیت‌کوین نیازمند تعداد زیادی نُود مستقل است که امکان هماهنگی (بخوانید تبانی) نداشته باشند. هرچه تعداد این نُودها زیادتر

---

۱. attackers

۲. Schelling point

مفهومی در نظریه بازی‌ها به معنای استراتژی یا راهکاری است که افراد در غیاب ارتباط با یکدیگر به صورت پیش‌فرض سراغ آن می‌روند.

باشد احتمال تبانی زیرگروه‌ها کاهش می‌یابد. آیه نازل نشده که همه باید بتوانند تراکنش‌های بیت‌کوینی خود را روی بلاک‌چین (درون-زنجیره‌ای) راست‌آزمایی و تأیید کنند. اگر با رشد راهکارهای لایه دوم شاهد گسترش استخر نقدینگی باشیم و ارائه خدمات بانکداری توسط نُودهای کامل بیت‌کوین سود خوبی داشته باشد می‌توان به یک چیز امیدوار بود: مشوق‌های مالی مناسبی برای رشد نُودهای مستقل وجود خواهند داشت و تغییر پروتکل‌های بیت‌کوین بسیار دشوارتر خواهد بود. هماهنگی بین نُودها با افزایش تعداد آن‌ها دشوارتر می‌شود و البته مشوق‌های سود هم باعث می‌شوند که نُودها با احتیاط و محافظه‌کاری بیشتری عمل کنند.

خبر خوب این است که برای مقیاس‌افزایی بیت‌کوین در سطح جهان نیازی نیست فقط به گزینه‌های درون-زنجیره‌ای فکر کنیم. نکته این است که بیت‌کوین خدمات تصفیه پرداختی در سطح جهانی ارائه می‌دهد که مطمئن (بدون نیاز به شناخت و اعتماد به طرف مقابل)، خودکار و مقاوم در برابر سانسور است و در حال حاضر رقیبی هم ندارد. تنها دارایی نزدیک به آن طلا است که جابه‌جایی و انتقال آن بسیار گران است و البته همواره ترس از مصادره آن وجود دارد. بیت‌کوین باید به حد کافی امن و نامتمرکز بماند تا رِندان نتوانند دست به کنترل و مصادره آن بزنند. همچنین اجماعی روشن، همه‌جانبه و پابرجا روی قواعد شبکه و همچنین روی ملاحظات عرضه پول ضروری به نظر می‌رسد. فکر کنم برای همه روشن است که لازم نیست برای مثال تراکنش خرید قهوه شما به صورت درون-زنجیره‌ای انجام گیرد!