۲۱ درس بیت کوین

نویسنده: Gigi

مترجم: نیما ملک پور

۲۱ درس بیت کوین

درس‌هایی که از سقوط در لانه خرگوش بیت کوین یاد گرفتم

نویسنده: Gigi

مترجم: نیما ملک پور

فهرست

سرآغاز

سقوط در لانه خرگوشِ بیت کوین [همانند آنچه برای آلیس در سرزمین عجایب رخ داد] تجربه‌ی شگفت‌انگیزی است. مانند بسیاری دیگر، احساس می‌کنم در چند سال گذشته که درباره بیت کوین مطالعه کردم، نسبت به تحصیلات دو دهه اخیر خودم چیزهای بیشتری یاد گرفته‌ام.

درس‌های پیش رو جوهره‌ی هر آن چیزی است که درباره بیت کوین یاد گرفتم. ابتدا آن‌ها را در قالب مقاله‌ای با عنوان «هر آنچه درباره بیت کوین آموختم» منتشر کردم و آنچه در ادامه خواهید دید، ویرایش دوم نسخه اصلی به حساب می‌آید.

این درس‌ها نیز مانند بیت کوین، ساکن نیستند. در نظر دارم که به صورت دوره‌ای بر روی آن‌ها کار کنم و نسخه‌های به‌روز شده و حتی چند درس اضافه‌تر از آن را در آینده منتشر کنم. اما برخلاف بیت کوین نسخه‌های بعدی این مجموعه، ممکن است با نسخه‌های قبلی سازگار نباشد. بر روی تعدادی از آن‌ها شاید بیشتر کار کنم، یا برخی را جایگزین کرده یا اینکه دوباره از ابتدا بنویسم. امیدوارم که نسخه‌های بعدی نیز برای شما مفید باشند، اما نمی‌خواهم در این باره به شما قولی بدهم.

بیت کوین یک معلم خستگی‌ناپذیر است، برای همین هم قصد ندارم بگویم که این درس‌ها جامع هستند و هر چیز مربوط به بیت کوین را در برمی‌گیرند؛ بلکه آن‌ها سفر من به درون لانه خرگوشِ بیت کوین را بازگو می‌کنند. درس‌های زیادی هستند که باید بیاموزیم و هر کسی که وارد دنیای بیت کوین می‌شود، احتمالا چیزهای متفاوتی از آنچه گفته خواهد شد، یاد می‌گیرد. امیدوارم که این درس‌ها به دردتان بخورد و فرایند یادگیری آن‌ها از طریق بازخوانی کلمات سخت نباشد.

مقدمه

در اکتبر ۲۰۱۸، آرجون بالاجی سوال مهم و در نگاه اول ساده‌ای را در توییتر مطرح کرد: چه چیزی از بیت کوین یاد گرفته‌اید؟ پس از تلاش برای پاسخ دادن به این سوال در قالب یک توییت کوتاه و شکست خفت‌بار در این کار فهمیدم که آموخته‌هایم از بیت کوین بسیار بیشتر از آن است که خیلی سریع بتوانم به سوال پاسخ دهم.

قطعا آموخته‌های من به طور مستقیم یا غیرمستقیم با بیت کوین در ارتباط است. با اینکه نحوه عملکرد داخلی آن را به اختصار در چند درس توضیح داده‌ام اما درس‌های پیش‌رو شرح چگونگی کارکرد بیت کوین یا چه بودن آن نیست. با این حال این درس‌ها می‌تواند به کشف بیشتر بیت کوین از جنبه‌های فلسفی گرفته تا واقعیت‌های اقتصادی و نوآوری‌های فناورانه‌اش کمک کند.

۲۱ درس بیت کوین در ۳ بخش هفت تایی تهیه شده است. هر بخش تلاش می‌کند تا بیت کوین را از یک زاویه خاص نگاه کند تا درس‌هایی که از این شبکه عجیب قابل یادگیری است گردآوری شود.

بخش اول جنبه‌های فلسفی بیت کوین را مورد اکتشاف قرار می‌دهد. بر هم کنش تغییر و تغییرناپذیری، مفهوم واقعی کمیابی، مفهوم عاری از اشتباه بودن، مسئله هویتی، قدرت آزادی بیان و محدویدت‌های دانش در این بخش بررسی شده‌اند.

بخش دوم یافته‌های اقتصادی از بیت کوین را مورد پژوهش قرار می‌دهد. درس‌هایی درباره جهل اقتصادی، تورم، ارزش، پول و تاریخچه پول در کنار بانکداری ذخیره کسری و معرفی دوباره پول سالم به طریق زیرکانه توسط بیت کوین در این بخش مورد بررسی قرار گرفته‌اند.

بخش سوم جنبه‌های فناوری بیت کوین را بررسی کرده است. قدرت اعداد، بازتاب‌هایی از اعتماد، چرایی نیاز به کار جهت اعلام زمان، معرفی حرکت آهسته و پیوسته به عنوان یک ویژگی نه یک ایراد، آنچه از بیت کوین می‌توان درباره حریم خصوصی یاد گرفت، چرا سایفرپانک‌ها کد را می‌نویسند و نه قانون را و تشابهاتی که از آینده بیت کوین می‌توان داشت، در این بخش به آن‌ها پرداخته شده است.

هر درس شامل نقل قول‌ها و لینک‌های مرتبط است. اگر ایده‌ای را به طور خاص بیشتر بررسی کرده باشم می‌توانید آن را در بخش انتهایی منبع اصلی پیدا کنید. همچنین اگر می‌خواهید عمق مطالعات خود را درباره یک موضوع خاص بیشتر کنید، از لینک‌های بخش «مسیری به عمق لانه خرگوش» منبع اصلی استفاده کنید.

اگرچه داشتن دانش قبلی درباره بیت کوین می‌تواند برای آغاز این مجموعه مفید باشد، اما امیدوارم که این درس‌ها توسط هر خواننده کنجکاوی قابل هضم باشند. در حالی که برخی درس‌ها به یکدیگر مرتبط هستند، اما می‌توان آن‌ها را جداگانه نیز مطالعه کرد. با اینکه تمام تلاشم را برای عدم استفاده از اصطلاحات پیچیده در این مجموعه به کار بردم، اما این امکان برای تعدادی از کلمات وجود نداشت.

امیدوارم نوشته‌هایم انگیزه کاوش‌های عمیق‌تر و مطرح ساختن پرسش‌های اساسی‌تری را درباره بیت کوین برای دیگران فراهم سازد. انگیزه من برای نوشتن این مجموعه به خاطر وجود تعدادی نویسنده و تولیدکننده محتواست که با تمام وجودم از آن‌ها سپاس‌گذارم.

آخرین حرفم پیش از شروع مطالعه مجموعه هم این است که تلاش من برای متقاعد ساختن شما انجام نشده است. هدف من وادار کردن شما به فکر کردن و نشان دادن این واقعیت است که بیش از یک مسیر برای آشنایی با بیت کوین وجود دارد. پس فکر اینکه من به شما بگویم «بیت کوین چیست» یا «چه چیزی به شما یاد می‌دهد» را از سرتان بیرون کنید. شما باید خودتان این مسیر را طی کنید.

> *بعد از این دیگر راه برگشتی وجود ندارد. اگر قرص آبی را بخوری، داستان همینجا تمام می‌شود و در حالی که هر چه را می‌خواهی می‌توانی باور کنی صبح در رختخوابت بیدار می‌شوی. اما اگر قرص قرمز را بخوری، در سرزمین عجایب باقی خواهی ماند و من به تو نشان می‌دهم که این لانه خرگوش تا کجاها که نمی‌رود! – مورفیوس از فیلم ماتریکس*

درس اول – تغییر و تغییرناپذیری

توصیف بیت کوین ذاتا کار سختی است. بیت کوین چیز جدیدی است که در صورت انجام هرگونه تلاشی برای مقایسه آن با مفاهیم قبلی، چه با خواندن آن به عنوان طلای دیجیتال یا پولِ اینترنت، قطعا پاره‌ای از موارد اصلی را جا خواهید گذاشت. با این حال مهم نیست که چه دیدگاهی نسبت به بیت کوین دارید، چرا که اعتقاد به دو جنبه بیت کوین همیشه ضروری خواهد بود: غیرمتمرکز و تغییرناپذیر بودن آن.

می‌توان بیت کوین را به عنوان یک قرارداد اجتماعی خودکار در نظر گرفت. نرم‌افزار آن تنها یک قطعه از پازل است که امید به تغییر دادن آن، تنها تلاشی بیهوده به حساب می‌آید. البته که برای این کار باید بقیه شبکه را به پذیرفتن تغییراتتان قانع کنید که بیشتر یک تلاش روانی است تا یک مسئله مهندسی نرم‌افزار.

عبارتی که می‌خواهم در ادامه به شما بگویم، شاید در نگاه اول پوچ و تهی به نظر برسد اما من به صحیح بودن آن عمیقا ایمان دارم:

شما بیت کوین را تغییر نمی‌دهید، بلکه بیت کوین شما را تغییر می‌دهد.

بیت کوین ما را بیشتر از آنچه در آن دست می‌بریم، تغییر خواهد داد. – مارتی بِنت

برای من مدتی طول کشید تا به این حقیقت برسم. شاید فکر کنید که بیت کوین تنها یک نرم‌افزار منبع‌باز است که می‌توانید آن را به راحتی تغییر دهید، مگر نه؟ اما این اشتباه است. یک اشتباه تمام عیار. تعجیب نکنید اگر به شما بگویم که خالق بیت کوین نیز این را می‌دانست.

ماهیت بیت کوین به گونه‌ای است که با انتشار نسخه ۰٫۱ (اولین نسخه)، طراحی اصلی آن برای ادامه حیاتش بدون تغییر باقی خواهد ماند – ساتوشی ناکاموتو

بسیاری تلاش کردند تا ماهیت بیت کوین را تغییر دهند و در نهایت همگی شکست خوردند. در حالیکه در اقیانوسی بی‌انتها از فورک‌ها و آلت کوین‌ها غرق شده‌ایم، شبکه بیت کوین دقیقا مانند روز اول که

اولین نودش آنلاین شد، به کار خود ادامه می‌دهد. آلت کوین‌ها در آینده اهمیتی نخواهند داشت، فورک‌ها در نهایت زنده نخواهند ماند و این بیت کوین است که اهمیت دارد. تا زمانی که درک بنیادین ما از ریاضیات و حتی فیزیک تغییر نکند، بیت کوین بی‌اعتنا به همه چیز و همه کس مسیر خود را طی خواهد کرد.

> *بیت کوین اولین نمونه از نوع جدید زندگی است که در اینترنت نفس می‌کشد و زندگی می‌کند. او زنده است چرا که به آن‌هایی که زنده نگهش می‌دارند، پول می‌دهد. آن را نمی‌توان تغییر داد و نمی‌توان در برابرش ایستاد. نمی‌توان آن را فاسد کرد یا به او رشوه داد. اگر بمب هسته‌ای نصف سیاره ما را نابود کند، بیت کوین باز هم به زندگی خود ادامه خواهد داد. – رالف مِرکل*

بیت کوین بیشتر از همه ما عمر خواهد کرد. پی بردن به این حقیقت، چیزی را درون من برای همیشه تغییر داد. بیت کوین اولویت زمانی من را تغییر داد، درک من را از اقتصاد عوض کرد و دیدگاه‌های سیاسی من را دگرگون ساخت. جای تعجب ندارد که حتی توانسته رژیم غذایی عده‌ای را هم تغییر دهد! اگر همه این حرف‌ها به نظرتان دیوانه‌وار می‌رسد، بدانید که در مسیر درستی قرار دارید که در عین جنون‌آمیز بودن، همگی در حال اتفاق افتادن هستند!

بیت کوین به من یاد داد که تغییر نخواهد کرد، بلکه من تغییر می‌کنم.

درس دوم – نایاب بودن عنصر کمیابی

در کل به نظر می‌رسد که پیشرفت فناوری، هر چیز دیگری را به تکامل برساند. هر روز تعداد بیشتری از مردم از کالاهایی که در گذشته کالاهای لوکس خوانده می‌شدند، می‌توانند استفاده کنند. همان‌طور که پیتر دیاماندیس در کتاب «فراوانی» نوشته است: سازوکار فناوری، رها بخشیدن منابعی است که می‌تواند کمیاب‌های دیروز را امروزه سرشار و فراوان سازد.

بیت کوین به خودی خود یک فناوری پیشرفته است که این روند را شکسته و کالایی ساخته که به معنای حقیقی کلمه «کمیاب» است. حتی برخی عقیده دارند که بیت کوین جزو کمیاب‌ترین چیزها در جهان هستی است. نمی‌توان آن را بیش از حد تعیین شده عرضه کرد، مهم هم نیست که چقدر تلاش کنید.

تنها دو چیز واقعا کمیاب است: زمان و بیت کوین. – سیف‌الدین آموس

به طور عجیب و متناقضی بیت کوین این کار را با کپی کردن انجام می‌دهد. تراکنش‌ها مخابره می‌شوند، بلاک‌ها ساخته و منتشر می‌شوند و دفتر کل توزیع شده، همانطور که می‌توانید حدس بزنید، بین همه توزیع می‌شود! همه این سازوکارها و کلمات زیبا در واقع همان کپی کردن هستند. حتی بیت کوین تا جایی که می‌تواند خودش را در کامپیوترهای مختلف کپی می‌کند تا به افراد انگیزه اقتصادی اجرای فول نود و استخراج بلاک‌های جدید را بدهد.

این دو فرایند به طرز شگفت‌انگیزی در کنار هم کار می‌کنند تا نتیجه آن یک کمیابی حقیقی باشد.

بیت کوین در زمان فراوانی به من معنای واقعی کمیاب بودن را یاد داد.

درس سوم – موجودیت و موقعیت مکانی

مکانیک کوانتوم را اگر کنار بگذارید، موقعیت مکانی یک ماده در دنیای واقعی مسئله‌ای حل شده است. این سوال که «فلان چیز الان کجاست؟» را می‌توان به طرز صحیحی پاسخ داد، اهمیتی هم ندارد که یک شیء یا شخص باشد. در دنیای دیجیتالی این سوال شاید گمراه‌کننده به نظر برسد اما باز هم پاسخ دادن به آن غیرممکن نیست. ایمیل‌های شما واقعا کجا هستند؟ پاسخ نه چندان جالبی که می‌توانید به این پرسش بدهید، این است که در فضای ابری ذخیره شده‌اند که در واقع فضای ذخیره‌سازی یک شخص دیگر می‌تواند باشد. با این حال اگر تمامی دستگاه‌ها را برای رسیدن به محل ذخیره شدن ایمیل‌هایتان دنبال کنید، می‌توانید مکان نگهداری آن‌ها را پیدا کنید.

اما وقتی به بیت کوین می‌رسیم، پرسش «الان کجاست؟» بسیار گمراه‌کننده می‌شود. بیت کوین‌هایتان واقعا کجاست؟

چشمانم را باز کردم، اطراف را نگاه کردم و سوالی که به طرز اسفناکی از ابتدای تاریخ، بشر را همراهی کرده از خود پرسیدم: من کجا هستم؟ – دنیل دِنِت

در واقع در پاسخ به این سوال با دو مشکل مواجهیم: اول اینکه دفترکل توزیع شده به صورت کامل تکثیر شده و در اختیار همه قرار دارد. دوم اینکه، واقعا بیت کوینی وجود ندارد! نه حتی به صورت فیزیکی، بلکه از نظر فنی و مجازی هم موجودیتی به نام بیت کوین نداریم!

نرم‌افزار بیت کوین مجموعه‌ای از خروجی‌های خرج نشده تراکنش را دنبال می‌کند و در واقع هیچگاه به یک عنصر مستقل به عنوان بیت کوین اشاره ندارد. وجود داشتن یا نداشتن بیت کوین از طریق نگاه کردن به مجموعه تراکنش‌های خرج نشده استنباط می‌شود که در ۸ رقم واحد اعشاری به نمایش درمی‌آید.

همین الان کجاست، آیا در حال انتقال است؟ اول از همه باید بدانید که بیت کوینی وجود ندارد. آن‌ها وجود ندارند. تنها سوابق دفترکل هستند که توزیع شده‌اند. آن‌ها در هیچ مکان فیزیکی قرار نگرفته‌اند و دفاترکل توزیع‌شده هستند که در هر مکان فیزیکی پخش شده‌اند. جغرافیا اینجا جواب نمی‌دهد و قرار هم نیست در پیدا کردن خط‌مشی‌تان کمکی کند. – پیتر ون والکنبورگ

پس وقتی که بیت کوینی وجود ندارد و می‌گویید که «من بیت کوین دارم»، واقعا مالک چه چیزی هستید؟ کلماتی که موقع ساختن کیف پول مجبور شدید آن‌ها را بنویسید را به یاد می‌آورید؟ به نظر می‌رسد این کلمات جادویی تنها چیزی هستند که شما دارید. جادویی که می‌توانید به وسیله آن در دفترکل چیزهایی اضافه کنید و کلیدی که با آن بیت کوین‌هایتان را انتقال دهید. برای همین هم بیت کوین شما، در واقع کلید خصوصی شماست.

اگر طور دیگری فکر می‌کنید، می‌توانید با فرستادن کلید خصوصی‌تان به من آن را امتحان کنید!

بیت کوین به من یاد داد که موقعیت مکانی یک مسئله گمراه‌کننده است.

درس چهارم – بحران هویتی

نیک کارتر، از نویسندگان شاخص این حوزه، در پاسخ به پرسشی که تامس نیگل، فیلسوف آمریکایی، در کتاب «خفاش بودن چه شکلی است؟» مطرح کرده، مقاله فوق‌العاده‌ای تحت عنوان «بحران وجودی بیت کوین» نوشته است. او در این مقاله به خوبی نشان داده که بلاک چین‌های عمومی و به خصوص بیت کوین، از پارادوکس کشتی تسئوس رنج می‌برند.

> *کافی است ببینید که دوام اجزای مختلف بیت کوین چقدر کم است. تمامی کدهای آن دست خوش تغییر شده‌اند، عوض شده‌اند، گسترش یافته‌اند و دیگر به سختی همان نسخه اولیه را می‌توان در آن یافت. اطلاعات ثبت شده‌ای که نشان می‌دهد چه کسی مالک چیست و دفترکل توزیع شده تنها چیزهای مجازی هستند که به عنوان خاصیت پایدار شبکه باقی مانده‌اند... برای اینکه [بیت کوین] کاملا بدون رهبر پیش برود، باید راه‌حل بدیهی را که یک نهاد می‌تواند زنجیره‌ای را مجاز بداند رها کنید. – نیک کارتر*

به نظر می‌رسد که پیشرفت فناوری ما را مجبور به پرسیدن سوالات فلسفی از خودمان می‌کند. دیر یا زود ماشین‌های بدون راننده با مشکلات دنیای واقعی مواجه خواهند شد و باید [در صورت مواجه شدن با خطر تصادف] درباره اینکه زندگی چه کسانی اهمیت دارد و چه کسانی اهمیت ندارد، تصمیمات اخلاقی بگیرند.ارزهای دیجیتال و به خصوص اولین هاردفورک‌های ادامه‌دار، ما را مجبور می‌کنند که درباره متافیزیک هویتی آن‌ها فکر کنیم و تصمیم بگیریم.

جالب است که دو نمونه مهم، به دو پاسخ متفاوت رسیده‌اند. در نخستین روز از آگوست ۲۰۱۷، بیت کوین به دو زنجیره تقسیم شد. بازار تصمیم گرفت که زنجیره بدون تغییر، همان بیت کوین اصلی باقی بماند. یک سال قبل از آن در ۲۵ اکتبر ۲۰۱۶ اتریوم به دو زنجیره تقسیم شد و بازار تقسیم گرفت که نام زنجیره‌ای که دچار تغییر شده بود، اتریوم باقی بماند. اگر تمرکززدایی به درستی اتفاق افتاده باشد، سوالاتی که توسط پارادوکس کشتی تسئوس به وجود می‌آیند، تا زمانی که این شبکه‌ها به فعالیت خود ادامه می‌دهند پاسخ داده خواهند شد.

بیت کوین به من آموخت که تمرکززدایی با هویت در تضاد است.

درس پنجم – یک مفهوم بی‌نقص

همه ما عاشق داستان‌های جذاب مربوط به پیدایش انسان هستیم. داستان پیدایش بیت کوین، قصه‌ای بی‌نظیر است که جزئیاتش مهمتر از چیزی است که در نگاه اول به نظر می‌رسد. ساتوشی ناکاموتو که بود؟ آیا یک شخص بود یا یک گروه؟ یا یک زن؟ یک هوش مصنوعی فوق پیشرفته و یا موجود فضایی که در زمان سفر می‌کند؟ جدا از فرضیه‌های علمی تخیلی در این باره، احتمالا هرگز به جواب این سوال نخواهیم رسید و این خیلی مهم است!

ساتوشی انتخاب کرد که ناشناس باقی بماند. او بذر بیت کوین را کاشت و برای مدت کافی در ابتدای راه در پروژه حضور داشت تا مطمئن شود که شبکه در همان آغاز، از بین نمی‌رود. تا اینکه ناگهان غیب شد.

گویا شاهکار ناشناس ماندن این نام مستعار، برای ایجاد یک سیستم حقیقتا غیرمتمرکز ضروری بود. هیچ کنترل مرکزی و هیچ نهاد متمرکزی در میان نیست. نه مخترعی، نه کسی که تحت تعقیب قرار گیرد، شکنجه شود، حق السکوت بگیرد یا تهدید شود. چیزی که داریم شاهکاری بی‌بدیل از مفهوم بی‌نقص فناوری است.

یکی از بزرگترین کارهایی که ساتوشی انجام داد، ناپدید شدنش بود – جیمی سانگ

از زمان تولید بیت کوین، هزاران ارز دیجیتال دیگر به وجود آمدند. اما هیچ یک از آن‌ها داستان ویژه پیدایش خود را ندارند. اگر می‌خواهید بیت کوین را پشت سر بگذارید، باید قصه‌ای بهتر از داستان پیدایش آن ارائه دهید. در جنگ ایده‌ها، قصه‌ها و داستان‌ها هستند که حکم زنده ماندن را امضا می‌کنند.

طلا ابتدا وارد جواهرسازی شد و برای بیش از ۷۰۰۰ سال در داد و ستد مورد استفاده قرار گرفت. درخشش فریبنده آن موجب شد تا هدیه‌ای از سوی خدایان در نظر گرفته شود. – کتابِ طلا: فلز خارق‌العاده

مانند طلا در دوران باستان، بیت کوین نیز شاید هدیه‌ای از سوی خدایان در نظر گرفته شود. بر خلاف طلا، داستان پیدایش بیت کوین تماما از انسان‌ها تشکیل شده است. اما این بار می‌دانیم که چه کسانی خدایان توسعه و نگهداری هستند: مردمانی از سرتاسر جهان که مهم نیست ناشناس باشند یا نه.

بیت کوین به من یاد داد که قصه‌ها و داستان‌ها مهم هستند.

درس ششم – قدرت ایده

بیت کوین یک ایده است. ایده‌ای که در قالب کنونی‌اش، تجلی ماشین‌آلات قدرت یافته از متون است. هر جنبه بیت کوین مجموعه‌ای از واژه‌ها است: وایت پیپر آن متن است. نرم‌افزارش که توسط نودها اجرا می‌شوند، خطوطی از کد است. دفتر کل آن متن سوابق است. تراکنش‌ها متشکل از متن هستند. کلیدخصوصی و عمومی کاراکترهای متنی است. به هر جنبه‌ای از آن نگاه کنید، با واژگانی طرف هستید که معادل یک سخنرانی است.

> *کنگره حق ندارد در ارتباط با تثبیت یک دین به عنوان دین رسمی، ممنوعیت پیروی آزادانه از ادیان، محدودسازی آزادی بیان، نقض آزادی مطبوعات، مداخله در حق تجمع صلح‌آمیز یا منع حق شکایت به منظور جبران خسارت‌ها از سوی دولت قانونی وضع کند. – متمم اول قانون اساسی ایالات متحده*

با اینکه جنگ نهایی ارزهای دیجیتال هنوز شروع نشده است، تبه‌کار جلوه دادن یک ایده کار بسیاری سختی است؛ مخصوصا ایده‌ای که تماما بر اساس پیام‌های متنی رد و بدل شده ایجاد شده باشد. هر بار که دولتی سعی می‌کند یک سخنرانی یا متن را از لحاظ قانونی نامعتبر سازد، یک قدم به سمت پوچی برمی‌دارد که در نهایت به اتفاقاتی مثل عدد اول ممنوع یا اعداد ممنوعه می‌انجامد.

تا زمانی که بتوان صحبت کرد و آزادی داشت، بیت کوین توقف‌ناپذیر خواهد بود.

هیچ دلیلی نمی‌توان یافت که متن بودن بیت کوین سبب مرگ آن شود، چرا که همواره یک متن بوده است. بیت کوین متن است. یک سخنرانی است. حتی نمی‌توان آن را در کشورهایی مثل ایالات متحده که حقوق انسان‌ها در آن تضمین شده و اولین کشوری است که حق انتشار را از زیر نظارت دولت‌ها بیرون کشیده، قانون‌گذاری کرد. – بیوتیون

بیت کوین به من آموخت که در یک جامعه آزاد، آزادی نرم‌افزارها و صحبت‌های آزادانه توقف‌ناپذیر است.

درس هفتم – محدودیت‌های دانایی

آشنایی با بیت کوین یک تجربه فروتنانه است. من فکر می‌کردم که چیزهای زیادی می‌دانم. فکر می‌کردم که یک آدم تحصیل‌کرده هستم. حداقل فکر می‌کردم که از علوم کامپیوتر سر درمی‌آورم. برای چندین سال با آن سروکله می‌زدم، پس حتما باید درباره امضای دیجیتال، هش‌ها، رمزگذاری، امنیت و شبکه همه چیز را می‌دانستم.

اما اشتباه می‌کردم.

یادگیری تمامی علوم پایه‌ای که بیت کوین به خاطر آن‌ها کار می‌کند، کار سختی است. اما درک عمیق تمامی آن‌ها تقریبا کار غیرممکنی است.

هیچکس تاکنون انتهای لانه خرگوش بیت کوین را پیدا نکرده است. – جیمسون لوپ

لیست کتاب‌هایی که باید آن‌ها را بخوانم سریعتر از آنکه قادر به انجام این کار باشم، در حال زیاد شدن است. فهرست مقاله‌هایی که باید بخوانم تقریبا بی‌انتهاست. تعداد پادکست‌های مربوط به این موضوع بسیار بیشتر از آن چیزی است که بتوانم به همه آن‌ها گوش دهم. این واقعا یک شکست نفسی است! علاوه بر این بیت کوین در حال تکامل است و همگام و بروز ماندن با شتاب نوآوری تقریبا ممکن نیست.

گرد و غبار لایه اول هنوز فرو ننشسته و مردم شروع به ساختن لایه دوم کرده‌اند و روی لایه سوم در حال کار کردن هستند.

بیت کوین به من آموخت که علم من تقریبا درباره همه‌چیز، خیلی اندک است. به من یاد داد که لانه خرگوش بیت کوین بی‌انتهاست.

درس هشتم – جهل اقتصادی

یکی از شگفت‌انگیزترین چیزها برای من، آن مقدار لازم از علم مالی، اقتصاد و روان‌شناسی بود تا بخشی از چیزی را که در نگاه اول به عنوان یک سیستم فنی خالص و شبکه‌ای از کامپیوترها می‌دیدم، درک کنم. مثل فیلم ارباب حلقه‌ها را دیده باشید، مانند کاراکتر سم که به فرودو می‌گوید: قدم گذاشتن به وادی بیت کوین کار خطرناکی است فرودو! تو وایت‌پیپر آن را خواندی، اگر حواست را جمع نکنی، نمی‌دانی که به چه چیزی دل خواهی بست!

برای درک یک سیستم پولی جدید، باید سیستم قبلی را خوب بشناسید. خیلی زود فهمیدم شناختی که از علم اقتصاد در سیستم آموزشی پیدا کرده‌ام، به شدت ناچیز است. همانند یک کودک پنج ساله شروع به سوال پرسیدن از خودم کردم. سیستم‌های بانکی چگونه کار می‌کنند؟ بازار سهام چگونه کار می‌کند؟ پول فیات چیست؟ پول معمولی چیست؟ چرا این همه بدهی در جهان انباشته شده است؟ چقدر پول تا الان چاپ شده است و چه کسی تصمیم چاپ کردن آن را می‌گیرد؟

پس از شوکه شدن از جهل خودم، خیلی زود فهمیدم که در سمت و سوی درستی قرار دارم.

> *آیا به نظرتان عجیب نیست که بیت کوین بیشتر از همه‌ی این سال‌هایی که در موسسات مالی کار می‌کردم، به من درباره پول یاد داد؟ که یکی از این شغل‌ها نیز آغاز حرفه کاری‌ام در یکی از بانک‌های مرکزی بود. – آرون تِی*

> *من در سه ماه گذشته‌ای که با ارزهای دیجیتال آشنا شدم درباره علم مالی، اقتصاد، فناوری، رمزنگاری، روانشناسی، سیاست، نظریه بازی‌ها، قانون و در نهایت خودم بیشتر از سه و نیم سال دانشگاه یاد گرفتم. – بیتکوین دانی*

این‌ها تنها تعدادی از اعترافات افراد در توییتر است. بیت کوین همانطور که در درس اول گفتیم، یک موجود زنده است. میزس، اقتصاددان آلمانی نیز گفته بود که اقتصاد یک موجود زنده است. همانطور که در تجارب شخصی خود فهمیدم، کشف و درک موجودات زنده یک فرایند پیچیده است.

> *یک سیستم علمی چیزی جز یک ایستگاه بی‌انتها و پیش‌رونده برای جستجوی علم نیست. این سیستم الزاما در تلاش‌های طبیعی و ناکافی هر انسانی نهفته است. اما آگاهی از این واقعیات به این معنی نیست که اقتصاد امروز با گذشته سازگار باشد. بلکه تنها بدان معنی است که اقتصاد یک موجود زنده است و برای زنده بودن باید ناقص و در حال تغییر باشد.*
> *– لودویگ فون میزس*

ما درباره بحران‌های مالی مختلف در اخبار چیزهایی شنیده‌ایم. اما هنوز جای تعجب دارد که چگونه چنین وقایع بزرگی اتفاق افتاده‌اند و این معما که کسی خسارات ناشی از آن را که تریلیون‌ها دلار بوده به عهده گرفته باشد، هنوز بی‌جواب مانده است. من هنوز سردرگمم، اما دست‌کم از اوضاع دنیای اقتصاد و چیزهایی که در آن می‌گذرد، چیزهایی فهمیده‌ام.

برخی افراد پا را فراتر گذاشته و جهالت عمومی در چنین موضوعاتی را به یک نادانی تعمدی و سیستماتیک تعمیم می‌دهند. در حالی که تاریخ، فیزیک، زیست، ریاضیات و زبان همگی بخشی از فرایند آموزشی را تشکیل می‌دهند، دنیای پول و اقتصاد به طور عجیبی تنها به صورت سطحی و گذرا آموزش داده می‌شود، که البته این آموزش جزئی هم معمولا ارائه نمی‌گردد. برای من جای سوال دارد که آیا مردم در صورت آموزش دیدن در حوزه‌های مالی و اقتصاد، باز هم به انباشتن بدهی تا جایی که می‌توانند، علاقه نشان می‌دهند؟ و سپس به این فکر می‌کنم که کلاه آلومینیومی‌ام باید چند لایه داشته باشد تا موثر واقع شود. و جواب احتمالا سه لایه است! (کلاه آلومینیومی نمادی است که القا می‌کند مغز انسان را از مداخلات خارجی حفظ می‌کند)

> *این سقوط‌ها، این ورشکستگی‌ها، هیچکدام تصادفی نیستند. و اگر هم از سر تصادف بوده باشند به خاطر نبود آموزش‌های مالی در مدارس است. درباره این موضوع از قبل مطالعه شده و تصمیماتی گرفته شده است. درست مثل دوران جنگ داخلی آمریکا که آموزش یک برده غیرقانونی بود، ما هم نباید درباره پول در مدارس چیزی یاد بگیریم. – رابرت کیوساکی*

مثل جادوگرِ شهر اُز، به ما گفته‌اند که به مرد پشت پرده توجه نکنیم. اما بر خلاف جادوگر شهر اُز، یک جادوگر واقعی وارد شهرمان شده است: شبکه‌ای باز، بدون‌مرز و مقاوم در برابر سانسور که قادر به انتقال ارزش است. پرده‌ای نیست و جادو برای همه عیان است.

بیت کوین به من آموخت که پشت پرده را ببینم و با جهالت خودم در اقتصاد روبرو شوم.

درس نهم – تورم

تلاش برای درک سیستم تورمی پول و چگونگی کارکرد سیستم‌های غیرتورمی مانند بیت کوین که شاید روش انجام کارها را تغییر دهد، نقطه ورود ماجراجویی من به دنیای اقتصاد بود. من می‌دانستم که تورم به معنی نرخ ایجاد پول جدید است، اما نمی‌دانستم که مفهومی فراتر از این هم داشته باشد.

شاید برخی اقتصاددانان استدلال کنند که تورم چیز خوبی است در حالی که به عقیده برخی دیگر پول‌های سخت (مانند طلا) که به ندرت دچار تورم می‌شوند، همانطور که در دوران استاندارد طلا شاهدش بودیم، برای یک اقتصاد سالم ضروری به نظر برسند. بیت کوین عرضه ثابت ۲۱ میلیون واحدی داشته و با عقیده گروه دوم همخوانی دارد.

معمولا اثرات تورم به صورت آنی قابل مشاهده نیست. بسته به نرخ تورم (به همراه سایر عوامل دیگر) ارتباط زمانی بین علت و معلول ممکن است حتی تا چندین سال پدیدار نشود. مشکل بدتر این است که تورم گروه‌های مختلفی از مردم را برای چندین سال درگیر خود می‌کند. همانطور که هنری هزلیت در کتاب «اقتصاد در یک درس» هم به آن اشاره کرده است:

> *هنر اقتصاد تنها شامل نگاه صرف به تغییرات آنی نیست بلکه نگاهی بلندمدت به اثرات هر اقدام یا سیاست‌گذاری است. اقتصاد از دنبال کردن عواقب این سیاست‌گذاری‌ها، نه تنها برای یک گروه بلکه برای تمامی گروه‌ها تشکیل شده است. – هنری هزلیت*

یکی از لحظات تکان‌دهنده فکری‌ام موقعی بود که فهمیدم ایجاد ارز جدید یا همان چاپ پول بیشتر، یک فعالیت اقتصادی کاملا متفاوت نسبت به بقیه فعالیت‌های اقتصادی‌ست. در حالی که کالاها و خدمات واقعی، برای مردم واقعی، ارزش واقعی خلق می‌کنند، چاپ بیشتر پول دقیقا برعکس عمل می‌کند.

این کار ارزش خلق شده را از همه کسانی که ارز تورم یافته را در اختیار دارند، می‌گیرد (یا به عبارت بهتر می‌دزدد!)

> *تورم در یک واژه صرفا به معنی چاپ هر چه بیشتر پول است که به دستمزدها و قیمت‌های بیشتر می‌انجامد. شاید شبیه به خلق یا ایجاد تقاضای بیشتر به نظر برسد اما در رابطه با تولید و مبادلات واقعی اصلا اینطور نیست. – هنری هزلیت*

تاثیرات نابودکننده تورم زمانی مشهود می‌شود که یک تورم کوچک، بزرگتر شود. در صورتی که پول دچار ابرتورم شود، در این صورت همه چیز بهم می‌ریزد. با فروپاشی ارز تورمی، قابلیت حفظ ارزش در طول زمان نیز از بین می‌رود و مردم سریعا سراغ کالاهایی می‌روند که می‌توانند این کار را به خوبی انجام دهند.

از دیگر نتایج ابرتورم‌ها این است که پولی که مردم در طول زندگی خود ذخیره کرده‌اند کاملا بی‌ارزش می‌شود. اسکناس‌های کاغذی که در کیف پول‌تان دارید سر جایش باقی می‌مانند اما دقیقا مثل یک کاغذ بی‌ارزش هستند.

ابر تورم در جمهوری وایمار (امپراتوری آلمان) – ۱۹۲۱ تا ۱۹۲۳

حتی پول با چیزی که از آن به عنوان تورم خزنده هم یاد می‌شود، ارزشش را از دست می‌دهد. این اتفاق به اندازه‌ای آرام رخ می‌دهد که بیشتر مردم متوجه از دست رفتن قدرت خریدشان نمی‌شوند. تا زمانی که دستگاه‌های چاپ پول کار می‌کنند، پول به راحتی در معرض تورم قرار می‌گیرد و حتی تورم خزنده نیز ممکن است با فشردن یک دکمه به موج خروشان تورم تبدیل شود.

همانطور که فردریش هایک در یکی از نظریه‌های خود به آن اشاره کرده است، تورم خزنده معمولا به یک تورم تمام عیارختم می‌شود.

تورم خزنده راه‌حل نیست، و تنها می‌تواند به تورم سرراست و تمام‌عیار تبدیل شود. – فردریش هایک

تورم معمولا تنها به نفع آن‌هایی است که به دستگاه‌های چاپ پول نزدیکتر از بقیه هستند. ورود پول جدید به اقتصاد و تاثیرگذاشتن آن بر روی قیمت‌ها معمولا زمان‌بر است. پس اگر شما قبل از اینکه کسی پولتان را بی‌ارزش سازد به پول‌های چاپ شده دسترسی داشته باشید، در منحنی تورم جلوتر از بقیه ایستاده‌اید. برای همین هم تورم را می‌توان به چشم مالیات پنهان دید که دولت‌ها از آن نفع می‌برند و بقیه بهای آن را می‌پردازند.

فکر نمی‌کنم اگر بگویم که تاریخ ما، تاریخ تورم‌ها بوده اغراق کرده باشم؛ تورم‌هایی که معماری آن‌ها توسط دولت‌ها چیده شده و به نفع دولت‌هاست. – فردریش هایک

تمامی ارزهای کنترل شده توسط دولت‌ها در نهایت یا جایگزین شده و یا دچار فروپاشی شده‌اند. مهم نیست نرخ تورم چقدر کم باشد؛ رشد پیوسته بیان دیگری از یک رشد نمایی است. در طبیعت نیز همانند اقتصاد، تمامی سیستم‌هایی که به صورت نمایی رشد می‌کنند، در نهایت به یک سطح نهایی می‌رسند یا دچار فروپاشی فاجعه‌باری می‌شوند.

شاید بگویید چنین چیزی در کشور من اتفاق نمی‌افتد! اگر یک ونزوئلایی باشید که ابر تورم را تجربه کرده، چنین دیدگاهی نخواهید داشت. با وجود نرخ تورمی که بیش از یک میلیون درصد است، پول اساسا به چیز بی‌ارزش تبدیل می‌شود.

شاید چند سال بعدی این اتفاق در کشورتان رخ ندهد یا شاید بر سر ارزی که هم‌اکنون در کشور شما رایج است، این بلا نیاید. اما یک نگاه گذرا به لیست پول‌های منسوخ‌شده، از اجتناب‌ناپذیر بودن آن در طول بازه‌های زمانی طولانی حکایت دارد. به یاد دارم که از ارزهای زیادی که در این لیست بودند استفاده کرده باشم: شیلینگ اتریش، مارک آلمان، لیر ایتالیا، فرانک فرانسه، پوند ایرلند، دینار کرواسی و غیره. مادربزرگ من حتی از کرون اتریش مجارستان هم استفاده کرده است. با گذشت زمان، ارزهایی که در

حال حاضر استفاده می‌شوند هم به آرامی اما به قطع یقین، وارد جایگاه ابدی خود یعنی گورستان‌ها خواهند شد. آن‌ها دچار ابرتورم خواهند شد یا جایگزین می‌شوند.

تاریخ به ما نشان داده که دولت‌ها به طور اجتناب‌ناپذیری تسلیم وسوسه اعمال تورم در عرضه‌های پولی می‌شوند – سیف‌الدین آموس

چرا بیت کوین متفاوت است؟ در مقابل پول‌هایی که توسط دولت‌ها اداره می‌شوند، پول کالاها وجود دارند که توسط دولت‌ها قانون‌گذاری نشده‌اند و اساس آن‌ها قوانین فیزیک است. آن‌ها به بقا و حفظ ارزش خود در طول زمان گرایش دارند. بهترین نمونه از چنین پول‌هایی طلا است که برای بیش از هزاران سال ارزش خود را حفظ کرده است. شاید به صورت ایده‌آل یک ارز پایدار نباشد، مفهومی که معنای آن در جایگاه نخست جای سوال دارد، اما ارزشی که طلا حفظ می‌کند در محدوده مشابهی قرار خواهد داشت.

در صورتی که یک پول کالا یا ارز قادر به حفظ ارزش خود در طول زمان باشد، از آن به عنوان پول سخت یاد می‌شود. در صورتی که نتواند ارزشش را به خاطر عواملی مثل تورم حفظ کند، پول نرم نامیده می‌شود. مفهوم سختی برای درک بیت کوین و بررسی‌های بیشتر ضروری است. برای همین هم در بخش‌های بعدی دوباره سراغ این مفهوم خواهیم رفت.

رفته رفته کشورهای بیشتری دچار ابرتورم می‌شوند و مردم بیشتری باید با واقعیت پول نرم و سخت مواجه شوند. حتی اگر خوش‌شانس باشیم، شاید مدیران بانک‌های مرکزی هم مجبور به بازنگری سیاست‌های پولی‌شان شوند. صرف نظر از هر اتفاقی که بیافتد، درکی که خاطر بیت کوین پیدا کرده‌ام قابل ارزش‌گذاری نیست.

بیت کوین به من مالیات پنهان تورم و اثرات فاجعه‌بار ابرتورم‌ها را یاد داد.

درس دهم – ارزش

ارزش یک مفهوم خود متناقض است. نظریه‌های متعددی وجود دارند که تلاش می‌کنند دلیل اینکه برخی چیزها را نسبت به برخی دیگر ارزشمند تلقی می‌کنیم، توضیح دهند. مردم برای هزاران سال از این پارادوکس باخبر بوده‌اند. افلاطون نیز در محاوراتش در «یوتیدیموس» به این موضوع اشاره کرده و گفته که ما برخی چیزها را به دلیل نایاب بودن آن‌ها ارزشمند تلقی می‌کنیم، و نه به خاطر اینکه برای بقای خود صرفا به آن‌ها نیاز داریم.

> *اگر انسان دوراندیشی باشید، این نصیحت را به شاگردان خود خواهید کرد که هرگز آن را جز از طریق مصاحبت با شما و یکدیگر به دست نمی‌آورند. همانطور که پیندار (شاعر یونان باستان) گفته، به خاطر نایاب بودن است که چیزی ارزشمند می‌شوند در حالی که آب یکی از ارزان‌ترین و در عین حال بهترین چیزهاست. – افلاطون*

توضیح مترجم: براساس پارادوکس ارزش‌ها، آب یکی از ارزان‌ترین و در عین حال ارزشمندترین چیزهاست، در حالی که برای نمونه الماس کاربرد بسیار کمتری نسبت به آب دارد اما قیمت آن در بازار نسبت به آب بسیار بیشتر است.

پارادوکس ارزش‌ها حقیقت جالبی را در رابطه با انسان‌ها نشان می‌دهد. به نظر می‌رسد که ما انسان‌ها، همه چیز را به طور ذهنی ارزش‌گذاری می‌کنیم و این کار را با معیارهای نامطلق (نسبی) مشخصی انجام می‌دهیم. شاید چیزی را به خاطر برخی دلایل ارزشمند بدانیم، اما چیزهای ارزشمند از نظر ما مشخصه‌های مشترکی هم دارند. اگر بتوانیم به آسانی آن‌ها را کپی کنیم یا به طور طبیعی فراوان باشد، ما آن‌ها را ارزشمند نخواهیم دانست.

به نظر می‌رسد ما چیزها را به خاطر کمیاب بودن آن‌ها ارزشمند می‌دانیم (مثل زمان، طلا و الماس)، یا اینکه تولید آن‌ها سخت و پرزحمت باشد و اینکه جایگزینی نداشته باشند (یک عکس قدیمی از کسی که دوستش داشته‌اید)، یا اینکه با وجود آن‌ها قابلیت‌هایی را به دست می‌آوریم که در غیابشان از داشتن آن‌ها محرومیم. می‌تواند ترکیبی از این موارد هم باشد، مثل آثار هنری.

بیت کوین همه این موارد را داراست! به شدت کمیاب است (تنها ۲۱ میلیون واحد)، تولید آن رفته رفته سخت‌تر می‌شود (به خاطر هاوینگ)، نمی‌توان جایگزینی برایش پیدا کرد (کلیدخصوصی گم شده بیت کوین‌ها را برای همیشه از دست می‌رود) و اینکه با وجود آن می‌توانیم برخی کارها را به صورت بهتری انجام دهیم. قطعا بیت کوین یکی از بهترین ابزارها برای انتقال ارزش در میان مرزهای جغرافیایی است، در مقابل سانسور مقاوم است و به افراد این اجازه را می‌دهد که ثروت خود را مستقل از بانک‌ها و دولت ذخیره کنند.

بیت کوین به من یاد داد که ارزش یک مفهوم نسبی و اختیاری است نه مطلق.

درس یازدهم – پول

پول چیست؟ ما هر روز از پول استفاده می‌کنیم اما پاسخ به این سوال به طرز عجیبی سخت است. ما در بیشتر فعالیت‌های روزمره خود به آن وابسته‌ایم و اگر مقدار کمی از آن داشته باشیم، احتمالا زندگی‌مان با مشکل روبرو می‌شود. با این حال ما خیلی کم درباره خود پول فکر کرده‌ایم؛ ابزاری که دنیا بر روی آن می‌چرخد. بیت کوین من را وادار به پرسش چندباره این سوال از خودم کرد که واقعا پول چیست؟

در دنیای مدرن، بیشتر مردم موقع فکر کردن به پول اجزای کاغذی آن را متصور می‌شوند، حتی با وجود این واقعیت که بیشتر پول‌های ما به صورت ارقام و اعداد دیجیتالی‌ست که در حساب‌های بانکی‌مان معنا می‌یابند. ما هنوز از صفر و یک‌ها برای پول‌مان استفاده می‌کنیم، پس چرا بیت کوین باید چیز متفاوتی باشد؟

بیت کوین متفاوت است زیرا ماهیت وجودی بیت کوین با پول‌هایی که تاکنون استفاده کرده‌ایم، بسیار فرق دارد. برای درک بهتر این موضوع نگاه دقیق‌تری به اینکه پول چیست، از کجا آمده و چرا نقره و طلا در تاریخ تجارت و بازرگانی تا حد زیادی مورد استفاده قرار می‌گرفتند، خواهیم داشت.

از یک نظر، بیشتر شبیه به فلزات گرانبهاست. به جای اینکه عرضه و مقدار آن تغییر کند تا ارزشش ثابت نگه داشته شود، مقدار کلی‌اش ثابت بوده و از قبل مشخص شده است و ارزش آن تغییر می‌کند. – ساتوشی ناکاموتو

صدف‌های دریایی، طلا، نقره، بیت کوین؛ پول هر چیزی است که مردم آن را به عنوان پول مورد استفاده قرار می‌دهند. اینکه شکل و قیافه آن چگونه باشد یا مقدارش چقدر است مهم نیست.

پول یک اختراع مبتکرانه است که دنیا در نبود آن به مکان پیچیده‌ای تبدیل می‌شد: چقدر ماهی باید بدهم تا یک کفش جدید برای خودم بگیرم؟ با دادن چند گاو می‌توانم یک خانه بخرم؟ الان هیچ چیزی نیاز ندارم اما برای خلاص شدن از سیب‌هایم که در حال گندیدن هستند باید چه کار کنم؟ برای رسیدن به این واقعیت که اقتصاد مبتنی بر مبادله کالا با کالا، بهره‌وری افتضاحی دارد به قوه تخیل قدرتمندی نیاز ندارید.

مهمترین خاصیت و ویژگی پول این است که می‌توانید آن را با هر چیز دیگری مبادله کنید. فکر کنم همین برای اینکه آن را یک اختراع بدانیم کافی باشد. نیک سابو در مقاله «ریشه‌های پول» به طور خلاصه و به طرز خارق العاده‌ای این مفهوم را رسانده است که ما انسان‌ها تاکنون همه چیز را به عنوان پول امتحان کرده‌ایم: از مهره‌های مواد نایاب مانند عاج فیل، صدف‌ها و استخوان‌های خاص گرفته تا جواهرات و فلزات گرانبهایی مانند طلا و نقره.

از طرفی باید بدانید که ما انسان‌ها موجودات تنبلی هستیم و درباره چیزهایی که می‌توانند مفیدتر باشند زیاد فکر نمی‌کنیم. پول در حالت فعلی‌اش کار ما را راه می‌اندازد، مثل ماشین‌هایی که داریم یا کامپیوترهایمان. بیشتر ما تنها زمانی درباره ساختار داخلی این چیزها وادار به فکر کردن می‌شویم که خراب می‌شوند. مردمی که سپرده‌هایشان را به خاطر ابر تورم از دست می‌دهند، قدر پول‌های سخت را می‌دانند. درست مانند مردمی که به خاطر لو رفتن اطلاعات، ناپدید شدن اعضای خانواده و دوستانشان را به دست نازی‌های آلمان یا شوروی دیده‌اند و ارزش محرمانگی را درک می‌کنند.

واقعیت مهم درباره پول فراگیر بودن آن است. پول جزء اساسی یک مبادله است؛ برای همین هم به نفع آن‌هایی است که قدرت خلق پول را دارند.

> *با توجه به اینکه پول نیمی از هر تراکنش مالی را در بر می‌گیرد و همه تمدن‌ها با توجه به کیفیت پولشان، افت و خیزهایی را تجربه می‌کنند، پس درباره قدرت فوق‌العاده‌ای صحبت می‌کنیم که زیر نقاب شب پرواز می‌کند. قدرتی که می‌تواند سراب‌هایی شکل دهد که تا زمان برقرار بودن واقعی به نظر برسند. این اساسی‌ترین قدرت فدرال رزرو است. – ران پاول*

بیت کوین به طور صلح‌آمیزی این قدرت را از میان برمی‌دارد و بدون متوسل شدن به زور، خلق پول را از قدرت خلع می‌سازد.

پول تاکنون چرخه‌های زیادی را طی کرده است. بسیاری از چرخه‌ها برای پول خوب بوده‌اند و قابلیت‌هایی را به آن اضافه کرده‌اند. اما اخیرا ساختار داخلی عملکرد پول دچار فساد شده است. امروزه تقریبا تمامی پول‌هایمان از روی باد هوا و قدرتی که پشت آن‌هاست ساخته می‌شوند. برای درک اینکه چطور به این نقطه رسیدیم، باید درباره تاریخ پول و افت‌وخیزهای آن مطالعه می‌کردم.

اینکه رفع فساد از پول نیازمند مجموعه‌ای از فجایع یا یک تلاش تاریخی برای آموزش جهت اصلاح است، هنوز مشخص نیست. البته من که دعا می‌کنم مورد دوم صحیح باشد!

بیت کوین به من یاد داد که پول واقعا چیست.

درس دوازدهم – تاریخچه و سقوط پول

بسیاری از مردم فکر می‌کنند که طلا پشتوانه پول است؛ طلایی که در گاو صندوق‌های بزرگ از آن نگهداری شده و توسط دیوارهای ضخیم محافظت می‌شود. بیش از چندین دهه از منسوخ شدن این واقعیت می‌گذرد. راستش را بخواهید قبلا هیچ درکی از طلا، پول‌های کاغذی و اینکه چرا اصلا باید حتما یک پشتوانه داشته باشند نداشتم.

بخشی از یادگیری درباره بیت کوین به شناختن پول‌های فیات (بدون پشتوانه) برمی‌گردد. پول فیات چه معنی دارد؟ از کجا سر و کله آن‌ها پیدا شد و چرا آن‌ها را نمی‌توان بهترین نوع پول در نظر گرفت؟ پس باید به این سوال پاسخ بدهیم که پول فیات چیست و چگونه استفاده از آن را شروع کردیم.

اگر به چیزی عبارت فیات را اضافه کنیم، به این معنی است که یک مقام (اتوریته) قانونی و رسمی، قدرت عرضه و کنترل آن را در اختیار دارد. پس پول‌های بدون پشتوانه یا فیات را به این دلیل پول می‌دانیم چون یک نفر گفته که این‌ها پول هستند. از آنجا که تمامی حکومت‌ها امروزه از ارزهای فیات استفاده می‌کنند، این مقام همان حکومت شماست. متاسفانه شما مجاز نیستید با ارزش تعریف شده در قالب

پول‌های فیات مخالفت کنید. خیلی زود احساس خواهید کرد که این ارزش‌گذاری شکل خشونت‌آمیزی هم دارد. اگر استفاده از ارزهای کاغذی را برای کسب‌وکار و پرداخت مالیات خود کنار بگذارید، بحث‌های اقتصادی‌تان را باید با هم‌سلولی خود ادامه دهید.

ارزش پول فیات از خصوصیات ذاتی آن سرچشمه نمی‌گیرد. اینکه یک پول فیات تا چه حد می‌تواند ارزشمند باشد، تنها به ثبات (یا بی‌ثباتی) سیاسی و اقتصادی مجموعه‌ی صاحب قدرت برمی‌گردد.

ریشه کلمه فیات در لاتین

تا چند دهه قبل استفاده از دو نوع پول رواج داشت: پول کالاها (Commodity Money) که همان اشیای ارزشمند و گرانبها هستند و پول نماینده‌ها (Representative Money) که نماینده‌ای از اشیای گرانبها هستند.

قبلا مختصری درباره پول کالاها توضیح دادیم. مردم در گذشته از استخوان‌ها، صدف‌های دریایی و فلزات گرانبها به عنوان پول استفاده می‌کردند. بعدها نیز سکه‌هایی از طلا و نقره به عنوان پول مورد استفاده قرار گرفتند. قدیمی‌ترین سکه یافت شده از ترکیب طلا و نقره ساخته شده و مربوط به ۲,۷۰۰ سال گذشته است. بنابراین مفهوم سکه بودن بیت کوین اصلا چیز جدیدی نیست.

سکه ای از جنس آلیاژ نقره و طلای لیدیایی

حتی به نظر می‌رسد که جمع‌آوری یا نگهداری سکه‌ها که از آن به عنوان هادل کردن هم یاد می‌شود، قدمتی به اندازه خود سکه‌ها دارد. اولین نگه‌دارنده سکه‌ها کسی بود که صد عدد از آن‌ها را در گلدانی زیر یک معبد دفن کرده بود که ۲۵۰۰ سال بعد کشف شد. اگر از من بپرسید کیف پول سرد بدی نبوده!

یکی از جنبه‌های منفی استفاده از فلزات گرانبها این بود که امکان تراشیدن آن‌ها موجب کوچکتر شدن سکه و کاهش بهای کلی آن‌ها می‌شد. سکه‌های جدید را می‌توان از طریق خرده‌های سکه‌های قبلی تولید و پول را طی زمان به تورم دچار کرد که در نهایت به کاهش ارزش هر یک از سکه‌های فلزات گرانبها منجر می‌شود. برای همین هم مردم تا می‌توانستند پشت و روی سکه‌های نقره را می‌تراشیدند.

از آنجا که حکومت‌ها حق خلق تورم را تنها برای خود قائل می‌شوند، برای توقف جنگ خاموش بی‌ارزش‌سازی پول تلاش‌های زیادی انجام دادند. مثل داستان‌های دزد و پلیس، تراشندگان سکه‌ها هر روز تکنیک‌های خلاقانه‌تری به کار می‌بستند و خدایان خلق سکه را وادار به اجرای اقدامات متقابل زیرکانه‌تری می‌کردند. آیزاک نیوتن، فیزیکدان مشهور جهان و نویسنده کتاب اصول ریاضی فلسفه طبیعی، یکی از همین افراد بود که کار تراش‌دهندگان را سخت کرد. افزودن شیارهای ریز در حاشیه سکه‌ها یکی از کارهای او بود که امروزه نیز در سکه‌ها وجود دارد. با این اقدامات کارهای تراش‌دهندگان سخت‌تر شده بود اما بی‌ارزش‌سازی سکه‌ها همچنان ادامه داشت.

تراشیدن سکه‌ها که موجب کاهش ارزش آن‌ها در گذشته می‌شد

از مشکلات دیگر سکه‌های فلزی سنگین بودن و سختی حمل‌ونقل مقادیر زیاد آن‌هاست. اگر برای هر بار خرید کردن نیاز به حمل کیسه سنگینی از سکه‌های نقره باشد، این شیوه جوابگو نخواهد بود.

اینکه «دلار آمریکا» چگونه دلار نامیده شد نیز داستان جالبی دارد. واژه دلار برگرفته از کلمه آلمانی تالر (Thaler)، کوتاه‌شده‌ی «یواخیمستالر» (Joachimsthaler) است. یک یواخیمستالر سکه‌ای بود که در شهر یاخیموو ضرب می‌شد. تالر در واقع به کسی یا چیزی گفته می‌شود که از دشت می‌آید و از آنجا که این شهر تولیدکننده‌ی سکه‌های نقره‌ای نیز در دشتی واقع شده بود، مردم به این سکه‌ها تالر می‌گفتند. این واژه ابتدا در هلندی به دالدرز (daalders) و سپس در انگلیسی به دلار تغییر یافت.

سکه دلار اولیه؛ تصویری از حضرت عمران با جامه و کلاه

ظهور پول نماینده‌ها (representative money) آغازی برای سقوط پول سخت بود. سروکله‌ی حواله‌های طلا در سال ۱۸۶۳ پیدا شد و حدود پانزده سال بعد نیز دلارهای نقره‌ای به تدریج با حواله‌های نقره جایگزین شدند. پس از ظهور حواله‌های نقره حدود ۵۰ سال زمان برد تا آن‌ها به چیزی که امروزه تحت عنوان اسکناس یک دلاری می‌شناسیم، تبدیل شوند.

یک دلار نقره در سال ۱۹۲۸ میلادی

باید یادآور شد که از اسکناس‌های دلار نیز تحت عنوان حواله‌های نقره استفاده می‌شد و سندی بود که مشخص می‌کرد دارنده آن‌ها مقدار مشخصی نقره طلبکار است. جالب است که متن مشخص‌کننده‌ی این موضوع روی اسکناس‌ها کوچکتر و کوچکتر شد تا اینکه پس از مدتی دیگر از واژه‌ی «حواله» بر روی اسکناس‌های دلار خبری نبود و این متن با اسکناس‌های فدرال رزرو جایگزین شده بود.

برای فلز زرد نیز ماجرای مشابهی رخ داد. بسیاری از کشورها از استاندارد دو فلزی استفاده می‌کردند؛ این بدین معنا بود که سکه‌ها از طلا یا نقره ضرب می‌شد. حواله‌های طلا که امکان بازخرید طلا با آن‌ها وجود داشت، قطعا یک پیشرفت فناورانه به حساب می‌آمد. سبکی کاغذ و حمل راحت‌تر آن در کنار امکان تقسیم به واحدهای کوچکتر با چاپ اعداد کوچکتر بر روی اسکناس، از جمله این ویژگی‌ها بود. دارندگان این حواله‌ها در واقع مالک طلا و نقره‌های حقیقی بودند که بر روی حواله‌ها نیز این موضوع ذکر شده بود.

برای یادآور شدن اینکه حواله مربوط به نقره یا طلاست، رنگ اسکناس‌ها با یکدیگر فرق داشت. به این اسکناس صد دلاری نگاهی بیندازید که این متن به وضوح روی آن دیده می‌شود:

این اسکناس گواهی می‌دهد که در خزانه‌ی ایالات متحده آمریکا، صد دلار به صورت سکه‌های طلای نگهداری می‌شود که در صورت تقاضای دارندگان حواله قابل پرداخت است.

اسکناس صد دلاری حواله طلا

در سال ۱۹۶۳ عبارت «در صورت تقاضای دارندگان حواله قابل پرداخت است» از روی تمامی اسکناس‌های جدید حذف شد و پنج سال بعد دیگر امکان باز خرید طلا و نقره با اسکناس‌های کاغذی وجود نداشت.

کلمات و عباراتی که ایده‌ی ایجاد پول‌های کاغذی را به وجود آورد، از روی آن‌ها پاک شده بود. رنگ طلایی از روی اسکناس‌ها برداشته شد و تنها خاصیتی که به همراه پول باقی ماند، قدرت حکومت‌ها در چاپ بی‌حد و اندازه‌ی پول بود.

با اعلام منسوخ شدن استاندارد طلا در سال ۱۹۷۱، تردستی قرن بیستم تکمیل شد. پول به سرابی بدل گشت تا همه ما خاطره مشترکی از بدون پشتوانه بودن آن داشته باشیم. یک ارزشمندی غیرواقعی، آن هم تنها به خاطر دستور مقامی که قدرت نظامی و کلید زندان‌ها در اختیار اوست. امروزه روی هر اسکناس دلاری می‌توانید این عبارت را ببینید:«این اسکناس یک پول قانونی است». به زبان ساده‌تر، ارزشمندی اسکناس به این خاطر است که خودش چنین می‌گوید!

اسکناس ۲۰ دلاری در سال ۲۰۰۴؛ «این یک پول قانونی است»!

درس مهم دیگری که در برابر دیدگان همه بر روی اسکناس‌های بانکی پنهان شده، عبارت دیگری است که می‌گوید استفاده از این پول قانونی «برای تمامی بدهی‌های عمومی و خصوصی است». واقعیتی که شاید برای اقتصاددان‌ها بدیهی به نظر برسد، برای من تعجب‌برانگیز بود: کل پول یک بدهی است. سر من هنوز به خاطر فهمیدن این واقعیت درد می‌کند. البته فهمیدن رابطه میان بدهی و پول را به عنوان یک تمرین به خواننده مطلب واگذار می‌کنم.

طلا و نقره برای بیش از هزار سال به عنوان پول مورد استفاده قرار گرفتند. طی زمان سکه‌هایی که از طلا و نقره ساخته می‌شدند با کاغذ جایگزین شدند و رفته رفته از آن‌ها به عنوان وجه پرداختی استفاده شد. این پذیرش سبب ایجاد توهمی شد که کاغذ به خودی خود ارزشمند قلمداد شود. قدم نهایی با منسوخ ساختن استاندارد طلا و متقاعد کردن همه به اینکه کاغذ ارزشمند است، جداسازی کامل میان پول نماینده‌ها و پول‌های واقعی بود.

بیت کوین به من تاریخ پول را یاد داد و بزرگترین تردستی تاریخ اقتصاد یعنی پول‌های بی‌پشتوانه را آموخت.

درس سیزدهم – جنون ذخیره کسری

مباحث ارزش و پول به خصوص در دنیای امروز، جزو موضوعات پیش پا افتاده نیستند. فرایند خلق پول در سیستم بانکداری فعلی نیز جزو مسائل مهمی است که من نمی‌توانم احساساتم را در رابطه با تعمدی بودن آن نادیده بگیرم. چیزی که پیشتر در حوزه آکادمیک و متون حقوقی با آن مواجه شدم، به نظرم در دنیای مالی نیز خود را نمایان ساخته است: هیچ چیزی به صورت ساده توضیح داده نمی‌شود، نه به خاطر اینکه واقعا پیچیده باشد، بلکه به این خاطر که حقیقت پشت چندین لایه از اصطلاحات عجیب با پیچیدگی غیرواقعی پنهان شده است.

سیاست پولی انبساطی، تسهیل کمی و تحریک مالی اقتصاد تنها تعدادی از این اصطلاحات هستند. مخاطبین سردرگم هم با این صحبت موافقند که توسط کلمات شیک هیپنوتیزم شده‌اند.

بانکداری ذخیره کسری و تسهیل کمی دو مورد از کلمات شیک اقتصاددان‌ها هستند که با پیچیده ساختن آنچه در حقیقت اتفاق می‌افتد، تلاش برای درک آن را دشوار می‌سازند. اگر این‌ها را بخواهید به یک کودک پنج ساله آموزش دهید، خیلی زود به نامعقول بودنشان پی خواهید برد.

گادفری بلوم، سیاستمدار بریتانیایی، در پارلمان اتحادیه اروپا به خوبی این مسئله را روشن می‌کند:

شما واقعا از مفهوم بانکداری چیزی سر در نمی‌آورید. تمامی آن‌ها ورشکست شده‌اند.
سانتاندر بانک، دویچه بانک، رویال بانک اسکاتلند، همه این‌ها ورشکست شده‌اند! چرا این

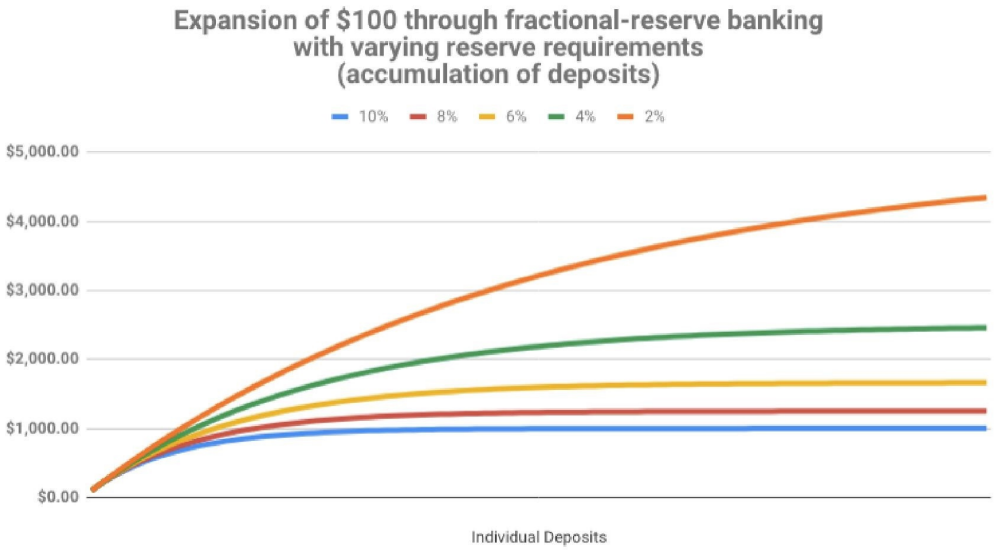
اتفاق افتاده است؟ آیا به خاطر نیروهای فرازمینی بوده یا یک سونامی موجب آن شده؟ آن‌ها همگی ورشکست شده‌اند زیرا ما سیستمی به نام بانکداری ذخیره کسری داریم. یعنی آن‌ها می‌توانند از پولی که واقعا ندارند، به مردم قرض دهند. این یک رسوایی جنایی است که برای دهه‌ها ادامه داشته است. ما در حال تقلب بودیم، که گاهی اسم آن را تسهیل کمی می‌گذارید، و این کار را با هر نامی انجام داده‌ایم. ماهیت چاپ پول به گونه‌ای است که اگر هر کسی آن را انجام دهد برای مدت طولانی راهی زندان خواهد شد و تا زمانی که بانکدارها و سیاستمداران را به خاطر این کارشان به زندان نیندازیم، این بی‌عدالتی ادامه خواهد داشت. - گادفری بلوم

بگذارید بخش مهم صحبت‌های این سیاستمدار را دوباره تکرار کنم: بانک‌ها می‌توانند از پولی که ندارند، به دیگران قرض دهند.

به لطف بانکداری ذخیره کسری، یک بانک تنها لازم است مقدار اندکی در حدود صفر تا ده درصد از پول‌هایی که دریافت می‌کند را نگهداری کند. این مقدار که به سمت عدد کمتر هم تمایل دارد، قضیه را وخیم‌تر هم می‌کند.

برای درک بهتر به این مثال توجه کنید. با در نظر گرفتن مقدار ۱۰ درصد که عدد رندی هم هست، محاسبات را انجام می‌دهیم. اگر بخواهید ۱۰۰ دلار در بانک سپرده داشته باشید، آن‌ها تنها ده درصد آن یعنی ۱۰ دلار را در بانک نگهداری خواهند کرد. پس با بقیه پول یعنی ۹۰ دلار چه می‌کنند؟

آن‌ها همان کاری را خواهند کرد که بقیه بانک‌ها می‌کنند .آن را به بقیه مردم به صورت وام قرض خواهند داد. نتیجه کار پدیده فزاینده پولی است که عرضه پول در اقتصاد را به طور چشمگیری افزایش می‌دهد. سپرده اولیه شما که ۱۰۰ دلار بود حالا به ۱۹۰ دلار تبدیل شده است. با قرض دادن ۹۰ درصد از سپرده ۱۹۰ دلاری جدید، خیلی زود این مقدار در اقتصاد به ۲۷۱ دلار و پس از آن به ۳۴۳.۹ دلار افزایش خواهد یافت. بانک‌ها با قرض دادن پولی که در واقع ندارند، عرضه پولی را به طور فزاینده‌ای افزایش می‌دهند و بدون هیچ جادویی و پس از چند دور وقوع این اتفاق، آن را به ۱۰ برابر مقدار اولیه تبدیل می‌کنند.



منحنی رشد سپرده اولیه با درصد بهره متفاوت

منظورم را اشتباه متوجه نشوید. هیچ مشکلی با قرض دادن یا نرخ بهره وجود ندارد. حتی اینکه بانک‌ها مثل دوران گذشته تنها به محافظت از سرمایه شما بپردازند یک اتفاق عالی است.

اما بانک‌های مرکزی غول‌های بدون شاخ و دمی هستند که قوانین مالی را به گند کشیده‌اند، نقش خدایی را بازی می‌کنند که تصمیماتش بر روی تمامی افراد کره زمین مشهود است، بدون هیچ وجدانی تنها به آینده نزدیک علاقه دارند و هیچ مسئولیت‌پذیری و حسابرسی برای آن‌ها وجود ندارد.

با اینکه بیت کوین هم تورمی است، اما عرضه آن بالاخره تمام خواهد شد. محدودیت ۲۱ میلیون واحدی آن سرانجام در نقطه‌ای تورم را کاملا کنار خواهد زد. ما هم‌اکنون دو جهان پولی داریم: در یکی از آن‌ها پول بسته به اختیار برخی افراد خیلی راحت چاپ می‌شود و جهان دیگری که بیت کوین را با محدودیت عرضه ثابت و امکان حسابرسی داریم. یکی از آن‌ها با خشونت و اجبار به ما تحمیل شده و دیگری با مشارکت داوطلبانه مردم رشد کرده است. هیچ مانعی برای ورود به چنین سیستمی وجود ندارد و لزومی هم به دریافت اجازه از کسی ندارید. مشارکت داوطلبانه زیبایی سیستم بیت کوین است.

البته به عقیده من مجادلات میان اقتصاددان‌های اتریشی و کینزی هم دیگر از حالت کاملا آکادمیک خارج شده است. ساتوشی موفق به ایجاد سیستمی برای انتقال ارزش شد که در نهایت به خلق سالم‌ترین

پول موجود انجامید. در نهایت افراد بیشتری درباره کلاهبرداری که بانکداری ذخیره کسری نام دارند، مطالعه خواهند کرد. اگر آن‌ها هم به همان نتیجه‌گیری یکسان اقتصاددان‌های اتریشی و بیت کوینرها برسند، احتمالا به شبکه در حال رشد اینترنت پول خواهند پیوست. هیچ کسی هم جلودار آن‌ها نخواهد بود.

بیت کوین به من آموخت که بانکداری ذخیره کسری یک دیوانگی محض است.

درس چهاردهم – پول سالم (Sound money)

مهمترین درسی که از بیت کوین گرفتم این بود که در بلندمدت، پول سخت نسبت به پول نرم برتری پیدا می‌کند. پول سخت که از آن به عنوان پول سالم (یا پول خوب) هم یاد می‌شود، به هر ارز مورد مبادله‌ای گفته می‌شود که یک ابزار ذخیره ارزش مطمئن است.

البته که بیت کوین هنوز کم سن‌وسال و پرنوسان است. منتقدین هم می‌گویند که نمی‌تواند ابزار ذخیره ارزش مطمئنی باشد. اما اشاره به نوسان بیت کوین از یک استدلال اساسی غافل می‌شود. نوسان چیزی است که باید اتفاقا انتظارش را داشته باشیم. بازار برای درک قیمت و ارزش پول جدید به زمان بیشتری نیاز دارد. همینطور که در برخی شوخی‌ها هم اشاره می‌کنند، نوسان بیت کوین به خاطر اشتباهی است که در اندازه‌گیری ارزش آن مرتکب می‌شویم. اگر همواره با این دید نگاه کنید که یک بیت کوین چند دلار ارزش دارد، نکته اصلی را که یک بیت کوین همواره به اندازه یک بیت کوین ارزشمند است متوجه نخواهید شد.

> *عرضه ثابت پول یا عرضه‌ای که تنها به خاطر معیارها و اهداف قابل برآورد تغییر یافته باشد، شرایط الزامی برای تحقق یک پول معنادار را فراهم می‌کند. – برنارد دمپسی*

با گذری کوتاه از گورستان ارزهای فراموش شده در تاریخ می‌توان فهمید پول‌هایی که قابلیت چاپ بیشتر را داشته باشند، بیشتر از حد نیز چاپ خواهند شد. چرا که هیچ انسانی در طول تاریخ در برابر این وسوسه نتوانسته مقاومت کند.

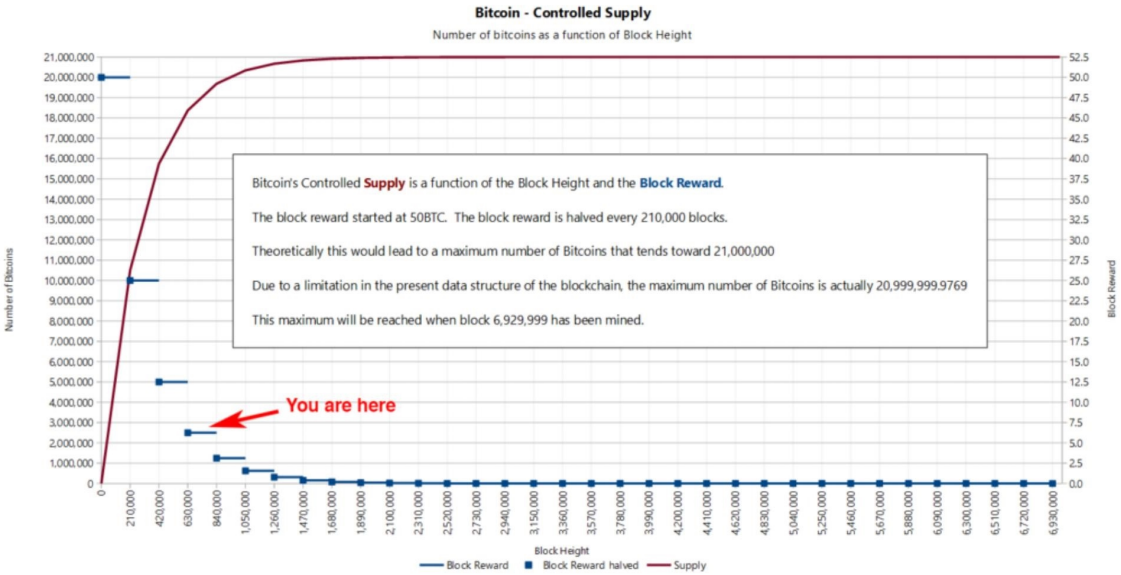
بیت کوین با از میان بردن وسوسه‌ی چاپ پول بیشتر، روشی خلاقانه معرفی کرده است. ساتوشی از طمع و خطاکار بودن انسان‌ها آگاه بود، برای همین نیز به چیزی مطمئن‌تر از خویشتن‌داری انسان‌ها یعنی ریاضیات متوسل شد.

$$\frac{\sum_{i=0}^{32} 210000 \left\lfloor \frac{50*10^8}{2^i} \right\rfloor}{10^8}$$

فرمول عرضه بیت کوین

در حالی که با استفاده از این فرمول می‌توان عرضه بیت کوین را محاسبه کرد، اما جالب است که نمی‌توانید آن را داخل کدهای بیت کوین پیدا کنید. عرضه‌ی بیت کوین‌های جدید به طور الگوریتمیک و با کاهش پاداش پرداختی به ماینرها طی هر چهار سال کنترل می‌شود.

از فرمول بالا به سرعت می‌توان آنچه درون سیستم بیت کوین جریان دارد را فهمید. شاید برای درک بهتر این مسئله لازم باشد که به پاداش پرداختی ماینرهایی که معمولا طی هر ده دقیقه موفق به یافتن بلاک معتبر می‌شوند، نگاهی بیندازید.



میزان بیت کوین‌های تعلق گرفته به ماینرها

درک شهودی فرمول‌ها، توابع لگاریتمی و نمایی شاید کار آسانی نباشد. مفهوم سالم بودن را اگر طور دیگری به نمودار نگاه کنیم درخواهیم یافت. اگر بدانیم چه مقدار از یک چیز وجود خواهد داشت و همینطور سختی تولید آن را نیز در آینده بدانیم، به سرعت می‌توانیم ارزش آن را درک کنیم. واقعیتی که در مورد نقاشی‌های پیکاسو، گیتارهای الویس پرسلی و ویولن‌های استرادیواریوس صحت دارد و می‌توان آن را به ارزهای فیات، طلا و بیت کوین نیز تعمیم داد.

سالم بودن ارزهای فیات به این عامل بستگی دارد که چه کسی مسئولیت چاپ آن را در اختیار داشته باشد. برخی حکومت‌ها طمع چاپ بیشتری نسبت به بقیه حکومت‌ها از خود نشان می‌دهند که به بی‌ارزش شدن ارز ملی آن کشور ختم می‌شود. برخی حکومت‌ها نیز برای چاپ بیشتر پول از خود مقاومت نشان می‌دهند که به سالم‌تر (سخت‌تر) ماندن ارز آن‌ها کمک می‌کند.

پیش از آنکه سراغ ارزهای فیات برویم، ویژگی‌های طبیعی اشیایی که از آن‌ها به عنوان پول استفاده می‌کردیم میزان سالم بودن آن را مشخص می‌کرد. میزان طلای موجود بر روی کره زمین توسط قوانین فیزیک محدود شده است. کمیاب بودن طلا به خاطر این است که سوپرنواها و انفجار ستاره‌های نوترونی زیاد اتفاق نمی‌افتند. جریان طلا نیز به خاطر زحمت استخراج آن محدود است؛ عنصر سنگینی که در اعماق زمین جا گرفته و بیرون کشیدن آن‌ها کار آسانی نیست.

منسوخ شدن استاندارد طلا راه را برای واقعیت جدیدی گشود: افزودن پول جدید تنها به چند قطره جوهر نیاز دارد. در دنیای مدرن این کار حتی ساده‌تر هم شده. اضافه کردن چند صفر به حساب‌های بانکی و بالا پایین کردن چند بیت در کامپیوترهای بانکی برای خلق پول کافی است.

> *یکی از جنبه‌های مهم واقعیت ساخته‌شده‌ی جدید این است که نهادهایی مثل فدرال رزرو هیچوقت ورشکست نمی‌شوند. آن‌ها هر چقدر پول نیاز داشته باشند، بدون اینکه هزینه‌ای پرداخت کنند، چاپ خواهند کرد. – گایدو هالسمن*

قاعده‌ای که از آن صحبت شد را می‌توان با نسبت انباشت به جریان (stock-to-flow ratio) معرفی کرد. به طور خلاصه، منظور از انباشت مقداری از چیزی است که در حال حاضر وجود دارد که در تعریف ما همان مقدار عرضه پول کنونی است. جریان نیز مقداری از همان چیز است که طی بازه زمانی

مشخصی، مثلا یک سال، تولید شده است. نکته کلیدی برای درک پول سالم در درک رابطه‌ی انباشت به جریان نهفته است.

محاسبه‌ی نسبت انباشت به جریان برای پول‌های فیات کار دشواری است، زیرا مقدار پول موجود وابسته به نوع نگاه شما به قضیه است. شما می‌توانید تنها اسکناس‌ها و سکه‌ها را بشمارید، چک‌های مسافرتی و سپرده‌های مربوط به آن را اضافه کنید، حساب‌های ذخیره و صندوق‌های سرمایه‌گذاری مشترک را حساب کنید، یا حتی گواهی سپرده‌های موجود را به مجموع آن اضافه کنید. همینطور نحوه تعریف و اندازه‌گیری هر یک از موارد در هر کشوری متفاوت است و از آنجا که فدرال رزرو انتشار آمار مربوط به ضمانت‌نامه‌ها را متوقف کرد، نمی‌توان آن را در محاسبات آورد. تایید این آمار هم کار دیگری است اما به هر حال به آمار منتشر شده فدرال رزرو اعتماد می‌کنیم.

طلا به عنوان یکی از کمیاب‌ترین فلزات بر روی زمین، بیشترین نسبت انباشت به جریان را در اختیار دارد. با استناد به پژوهش‌های زمین‌شناسی ایالات متحده، مقدار استخراج شده طلا اندکی بیش از ۱۹۰ هزار تن بوده و تا سال گذشته، هر ساله حدود ۳۱۰۰ تن از این فلز استخراج شده است.

با استفاده از این آمار به سادگی می‌توان نسبت انباشت به جریان طلا را حدود ۶۱ به دست آورد که از تقسیم ۱۹۰ هزار به ۳,۱۰۰ به دست می‌آید.

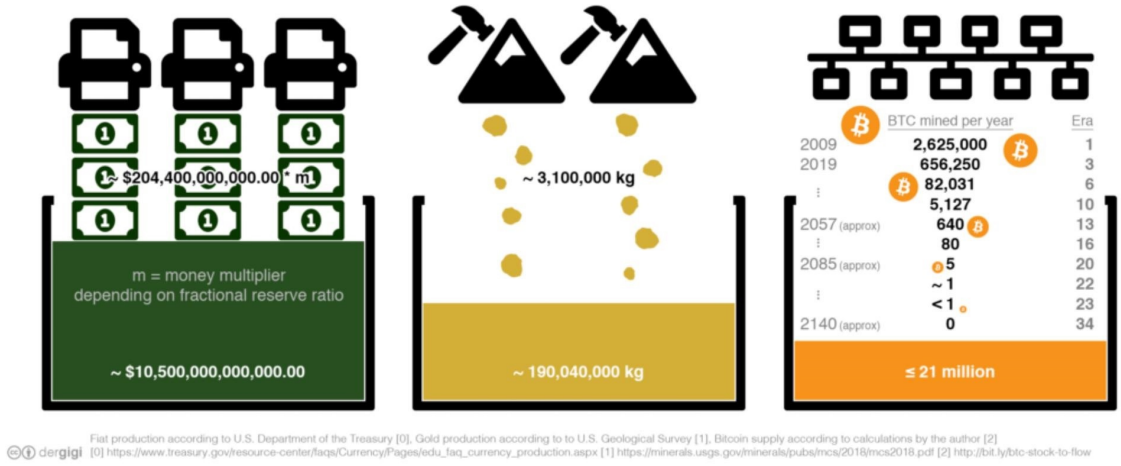
هیچ چیزی نسبت انباشت به جریان بیشتری نسبت به طلا ندارد، برای همین هم طلا سخت‌ترین و سالم‌ترین پول موجود حال حاضر است. گفته می‌شود کل طلاهای استخراج شده تاکنون را می‌توان در دو استخر المپیک جا داد که البته طبق محاسبات من این میزان ۴ عدد است. شاید این مقدار باید دوباره محاسبه شود یا اینکه استخرهای المپیک کوچکتر شده‌اند.

اما این نسبت برای بیت کوین چگونه است؟ همانطور که احتمالا می‌دانید، استخراج بیت کوین در سال‌های گذشته محبوبیت مضاعفی پیدا کرد. این به خاطر قرار داشتن در اوایل دوره‌ای است که از آن با نام عصر پاداش‌دهی یاد می‌شود و نودهای استخراج با تلاش‌های محاسباتی خود، بیت کوین قابل توجهی به دست می‌آورند. در حال حاضر ما در عصر پاداش‌دهی شماره سوم قرار داریم که در سال ۲۰۱۶ آغاز شد و در اوایل ۲۰۲۰ به پایان خواهد رسید. در حالی که عرضه بیت کوین از قبل مشخص شده است،

چگونگی کارکرد بیت کوین امکان پیش‌بینی زمان دقیق را فراهم می‌کند. با این حال می‌توانیم به صورت قطعی پیش‌بینی کنیم که نسبت انباشت به جریان بیت کوین چه مقدار خواهد شد.

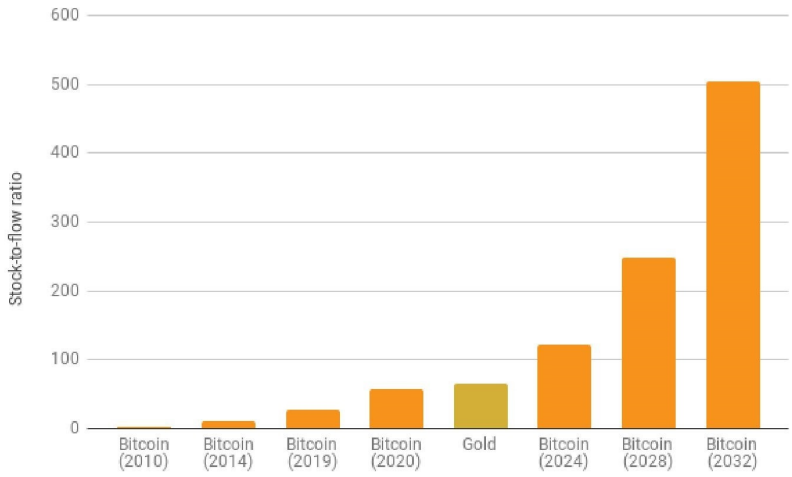
خطر اسپویل: بسیار زیاد!

اما چقدر زیاد؟ با نگاهی دقیق‌تر می‌توان دریافت که سختی بیت کوین یا به عبارتی سالم بودن آن در حال میل به سمت بی‌نهایت است.



نسبت انباشت به جریان برای دلار، طلا و بیت کوین

به دلیل کاهش نمایی پاداش استخراج، پارامتر جریان برای بیت کوین‌های جدید به شدت کاهش خواهد یافت که در نتیجه به افزایش شدید این نسبت خواهد انجامید. در سال ۲۰۲۰ این مقدار به نسبت طلا بسیار نزدیک می‌شود و چهار سال بعد از آن با افزایش دوبرابری بیشتر خواهد شد. این دو برابر شدن برای ۶۴ بار در طول تاریخ بیت کوین اتفاق خواهد افتاد و به لطف قدرت تابع نمایی، میزان استخراج سالانه بیت کوین طی ۵۰ سال به کمتر از ۱۰۰ بیت کوین و طی ۷۵ سال به کمتر از یک بیت کوین خواهد رسید. چشمه‌ی پاداش‌دهی سیستم بیت کوین رفته رفته خشک خواهد شد تا اینکه در سال ۲۱۴۰ به پایان می‌رسد و دیگر هیچ بیت کوینی تولید نخواهد شد. این یک بازی طولانی است و اگر این را می‌خوانید بدانید که هنوز ابتدای راه قرار دارید.



افزایش نسبت انباشت به جریان بیت کوین در برابر طلا

همانطور که بیت کوین به سمت نسبت انباشت به جریان بی‌نهایت حرکت می‌کند، به سالم‌ترین پول موجود در جهان تبدیل خواهد شد. رقابت با سالم بودن بی‌نهایت و شکست دادن آن قطعا کار سختی است.

اما اگر از دریچه‌ی دیگری هم به شبکه بیت کوین نگاه کنیم، تصحیح پارامتر سختی بیت کوین یکی از مهمترین عناصر سیستم است. سختی استخراج بیت کوین به سرعت استخراج بیت کوین‌های استخراج شده‌ی جدید بستگی دارد. تصحیح دینامیک سختی استخراج شبکه در واقع از ذخایر آن در آینده محافظت می‌کند.

سادگی الگوریتم تصحیح سختی شاید حواس شما را از عمق مفهوم آن پرت کند، اما این تصحیح حقیقتا انقلابی از جنس نسبیت انیشتین است. این پارامتر تضمین می‌کند که اندازه کار و تلاش در استخراج مهم نیست چقدر باشد، زیرا که به هر صورت در عرضه بیت کوین اختلالی ایجاد نخواهد کرد. یعنی دقیقا برعکس تمام منابع طبیعی دیگر، اصلا اهمیتی ندارد که افراد چه مقدار انرژی صرف استخراج بیت کوین کنند، به هر حال پاداش کلی آن افزایش نخواهد یافت.

همانطور که نظریه نسبیت خاص انیشتین ($E=mc^2$) از محدودیت سرعت در پهنه‌ی گیتی صحبت می‌کند، تصحیح سختی بیت کوین هم محدودیت کلی پول در بیت کوین را نشان می‌دهد.

اگر به خاطر این پارامتر نبود، تمامی بیت کوین‌ها تاکنون استخراج شده بود. اگر به خاطر تصحیح سختی نبود، بیت کوین احتمالا در ابتدایی‌ترین روزهای تولدش زنده نمی‌ماند. این پارامتری است که آن را در عصر پاداش‌دهی امن نگه داشته است. این دقیقا همان پارامتری است که توزیع عادلانه و پایدار بیت کوین‌های جدید را ممکن ساخته؛ ترموستاتی که سیاست‌های پولی بیت کوین را قاعده‌مند می‌کند.

انیشتین حقیقت جدیدی را به بشریت عرضه کرد: مهم نیست چقدر انرژی برای سرعت بخشیدن به یک شیء صرف کنید، در یک نقطه مشخص انتظار سرعت بیشتر از آن بیهوده خواهد بود. ساتوشی نیز واقعیت مبتکرانه‌ای را به ما نشان داد: مهم نیست چقدر برای استخراج طلای دیجیتال تلاش می‌کنید، در یک نقطه مشخص شما دیگر قادر به استخراج تعداد بیشتری از آن نخواهید بود. برای اولین بار در تاریخ بشریت یک سیستم پولی ابداع شده که به میزان کوشش شما توجهی نمی‌کند، زیرا در هر صورت قادر نخواهید بود مقدار بیشتری از آن تولید کنید.

بیت کوین به من آموخت که پول سالم یک الزام است.

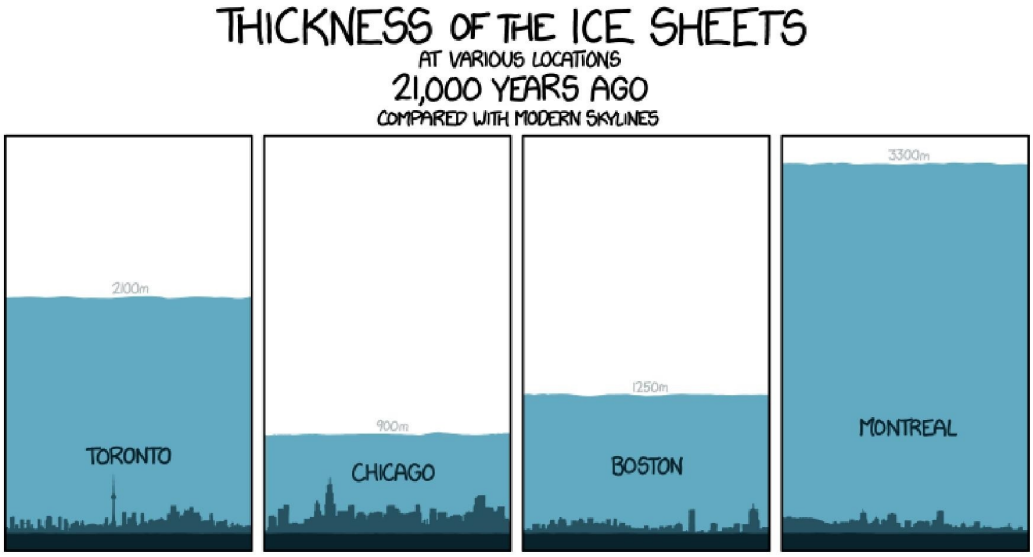
درس پانزدهم – قدرت اعداد

اعداد قسمت مهمی از زندگی روزمره ما را تشکیل می‌دهند. هرچند بسیاری از ما همچنان با اعداد بزرگ احساس نزدیکی نمی‌کنیم. اعداد بزرگی که احتمالا هر روز با آن‌ها برخورد داریم، در بازه‌ی چند میلیون، میلیارد و حتی تریلیون قرار دارند. احتمالا درباره میلیون‌ها نفری که در فقر به سر می‌برند، یا میلیاردها دلاری که صرف نجات ورشکستگی بانک‌ها شده یا بدهی‌های جهانی تریلیون دلاری اخباری شنیده باشیم. حتی با اینکه سردرآوردن از چنین تیترهای خبری دشوار است، می‌توان گفت که با اندازه و مقیاس این اعداد احساس راحتی می‌کنیم.

حتی اگر با میلیاردها و تریلیون‌ها هم احساس راحتی داشته باشیم، درک بزرگی آن‌ها برای ما تقریبا غیرممکن است. آیا واقعا می‌دانید برای سپری شدن یک میلیون/میلیارد/تریلیون ثانیه باید چقدر صبر کنید؟ اگر شما هم شبیه من باشید، احتمالا قبل از هضم این اعداد سردرگم شده‌اید.

بیایید نگاه نزدیکتری به این مثال داشته باشیم: تفاوت میان هر یک از اعداد بیان شده به سه مرتبه افزایش آن‌ها مربوط است. شاید مثال ثانیه جالب نباشد، برای همین بیایید این اعداد را در قالب دیگری بیان کنیم.

- ۱۰ به توان ۶ یا به عبارتی یک میلیون ثانیه قبل برابر است با حدود یک و نیم هفته پیش.
- ۱۰ به توان ۹ یا یک میلیارد ثانیه قبل مساوی است با حدود ۳۲ سال پیش.
- و در نهایت یک تریلیون ثانیه یا ۱۰ به توان ۱۲ ثانیه به زمانی برمی‌گردد که منهتن نیویورک زیر لایه ضخیمی از یخ پوشیده شده بود.



حدود یک تریلیون ثانیه قبل! ضخامت لایه یخی در شهرهای مختلف

به محض ورود به قلمروی نجومی رمزنگاری مدرن، درک شهودی ما از اعداد به یکباره نابود می‌شود. بیت کوین بر روی اعداد بزرگ و امکان‌ناپذیر بودن حدس آن‌ها ساخته شده است. این اعداد بسیار بسیار بزرگتر از آن چیزی است که حتی در زندگی روزمره بخواهیم با ذره‌ای ناچیز از آن‌ها روبرو شویم. در واقع فهمیدن بزرگی این اعداد یکی از لازمه‌های درک سیستم بیت کوین به عنوان یک مجموعه است.

برای نمونه به SHA-۲۵۶ که یکی از توابع هش مورد استفاده در بیت کوین است، نگاه کنید. شاید ۲۵۶ در نگاه اول عدد پیچیده‌ای به نظر نرسد و اصلا آن را بزرگ هم ندانید. هرچند عدد ۲۵۶ در SHA-۲۵۶ درباره بزرگی مرتبه آن صحبت می‌کند که مغز ما برای درک بزرگی آن قطعا ظرفیت کافی ندارد.

در حالی که طول بیت یک روش اندازه‌گیری مناسب است، اما معنای حقیقی امنیت ۲۵۶ بیتی، گمشده‌ای در برگردان میان زبان‌هاست. مشابه اعداد یک میلیون و میلیارد که همان ۱۰ به توان ۶ و ۹ هستند، مرتبه بزرگی SHA-۲۵٦ نیز ۲ به توان ۲۵۶ تعریف می‌شود.

پس با این حساب SHA-۲۵٦ واقعا تا چه حد قدرتمند است؟

> *الگوریتم SHA-۲۵٦ بسیار قدرتمند است. نمی‌توان آن را یک قدم تدریجی در جهت بهتر شدن مانند الگوریتم MD۵ به SHA۱ در نظر گرفت. در واقع این الگوریتم می‌تواند تا دهه‌ها بدون اینکه حمله قدرتمندی علیه آن انجام شود، دوام بیاورد. – ساتوشی ناکاموتو*

البته اگر علاقه‌مندید که بدانید ۲ به توان ۲۵۶ برابر با چه عددی می‌شود بهتر است به تصویر زیر نگاه کنید!

```
115 quattuorvigintillion 792 trevigintillion 89 duovigintillion 237
unvigintillion 316 vigintillion 195 novemdecillion 423 octodecillion
570 septendecillion 985 sexdecillion 8 quindecillion 687
quattuordecillion 907 tredecillion 853 duodecillion 269 undecillion
984 decillion 665 nonillion 640 octillion 564 septillion 39
sextillion 457 quintillion 584 quadrillion 7 trillion 913 billion
129 million 639 thousand 936.
```

عدد برابر با ۲ به توان ۲۵۶

تا جایی که چشم کار می‌کند در این عدد ایلیون‌ها و ایلیاردها دیده می‌شود! برای همین هم درک آن با مغز انسانی غیرممکن است. حتی در جهان هستی نیز نمی‌توان آن را با چیزی مقایسه کرد. این عدد حتی از تعداد کل اتم‌هایی که در پهنه گیتی قابل مشاهده وجود دارد هم بسیار بسیار بیشتر است. اصلا قرار نیست از بزرگی آن سردربیاوریم، پس زیاد به خود سخت نگیرید.

یکی از بهترین تجسم‌های بصری برای نمایش قدرت SHA-۲۵٦ در ویدیویی توسط گرنت سندرسون نشان داده شده است .این ویدیو که در یوتیوب با عنوان «امنیت ۲۵۶ بیتی چقدر قدرتمند است؟» به

زیبایی بزرگی فضای اشغالی آن را نشان می‌دهد. پس حتما با مشاهده این ویدیوی ۵ دقیقه‌ای عظمت این عدد را بهتر درک کنید.

بروس اشنایر از محدودیت‌های فیزیکی محاسبات کامپیوتری برای بررسی قدرت این عدد استفاده کرده است. به عقیده او حتی اگر قادر به ساخت کامپیوتر بهینه‌ای باشیم که تمامی انرژی تامین شده توسط کره دایسونِ پیرامون خورشید ما را برای محاسبه جذب کند و اجازه دهیم تا برای ۱۰۰ میلیارد میلیارد سال کار کند، تنها ۲۵ درصد شانس رسیدن به یک کلید خاص را در انبار کاه ۲۵۶ بیتی خواهیم داشت.

> *این اعداد هیچ ارتباطی با فناوری دستگاه‌های ما ندارند؛ آن‌ها بیشینه‌هایی هستند که ترمودینامیک اجازه حضور آن‌ها را داده است. آن‌ها تاکید دارند که حملات جستجوی فراگیر در برابر کلیدهای ۲۵۶ بیتی تا زمانی که کامپیوترها از چیزی جز ماده ساخته نشده باشند و فضایی جز مکان را اشغال نکرده باشند، غیرممکن خواهد بود. – بروس اشنایر*

قدرت این عدد به گونه‌ای است که حتی اجازه مبالغه را هم نمی‌دهد. رمزنگاری قوی تعادل قدرتی که دنیای فیزیکی وجود دارد و همه ما با آن آشنا هستیم را وارونه می‌سازد. چیزهای غیرقابل شکستنی در دنیای فیزیکی وجود خارجی ندارند. اگر به اندازه کافی نیرو اعمال کنید، بلاشک می‌توانید هر دری، جعبه‌ای یا گنجینه‌ای را باز کنید.

اما صندوق گنج بیت کوین کاملا فرق دارد. قفل این گنجینه با رمزنگاری قدرتمندی ساخته شده که در برابر قوی‌ترین نوع حملات بروت فورس هم آسیبی نمی‌بیند و تا زمانی که اصول ریاضیاتی بنیادین آن صحیح باشد، تنها امکان حملات بروت فورس (جستجوی فراگیر) وجود خواهد داشت.

البته حملات زورگیرانه با حمله فیزیکی به شخص دارنده بیت کوین هم گزینه دیگری است. اما شکنجه نیز درباره آدرس‌های بیت کوین و دیوارهای رمزنگاری آن که در برابر بروت فورس نیز ایستادگی می‌کنند، کاری از پیش نخواهد برد.

این واقعیت و پیامدهای آن در متن «فراخوانی برای ارتش رمزنگاران» از جولیان آسانژ به شکل زیر خلاصه شده است:

> *هیچ مقداری از نیروی مقتدارنه قادر به حل یک مسئله‌ی ریاضی نخواهد بود.*

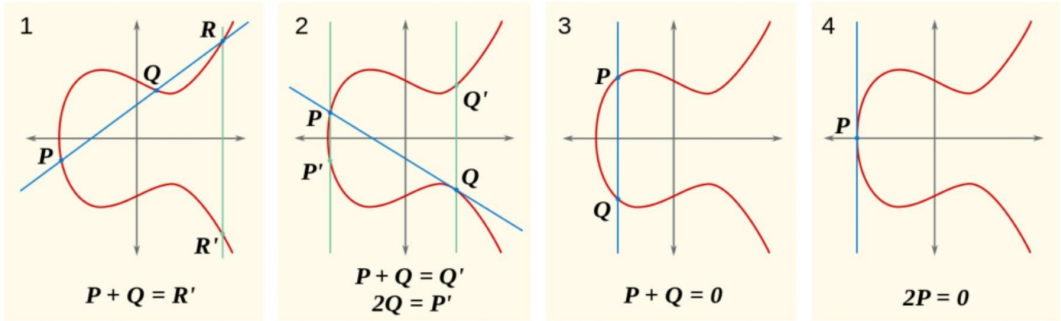
اینکه چرا جهان باید اینگونه می‌بود واضح نیست. اما به هر طریقی جهان به روی رمزنگاری لبخند زده است. – جولیان آسانژ

هنوز هیچکس نمی‌داند که خنده‌ی جهان واقعی است یا نه. احتمال دارد فرضیات ما از روابط نامتقارن ریاضی اشتباه باشد و یک روز بفهمیم که P واقعا با NP برابر است یا اینکه راه‌حل‌های بسیار سریعی برای مسائل خاصی پیدا کنیم که امروزه آن‌ها را دشوار می‌دانیم. اگر مسئله این باشد، رمزنگاری به صورتی که امروزه می‌شناسیم دیگر وجود نخواهد داشت و پیامدهای آن جهان را بیش از آنچه تصور می‌کنیم تغییر خواهد داد.

توضیح مترجم: اصل اساسی در مسائل رمزنگاری برابر نبودن پی و ان‌پی است که در صورت یافتن اثباتی برای برابر بودن پی و ان‌پی، شکل زندگی انسان‌ها دستخوش تغییرات گسترده‌ای خواهد شد.

عبارت لاتین «ویر این نومریس» (به معنی قدرت اعداد) تنها یک شعار جذاب میان بیت کوینرها نیست. فهم وجود قدرتی غیرقابل سنجش در اعداد ارزشمند است. درک این موضوع که امکان وارونه‌سازی تعادل‌های قدرت موجود را می‌دهد، به من امکان تغییر دیدگاهم نسبت به جهان و آینده پیش روی انسان‌ها را داد.

یکی از نتایج اصلی این واقعیت به عدم نیاز به اخذ اجازه از کسی برای مشارکت در شبکه بیت کوین برمی‌گردد. هیچ صفحه ثبت نامی، شرکتی که در راس امور باشد یا سازمان دولتی که برای گرفتن مجوز اقدام کنید، وجود ندارد. خیلی ساده اگر بگویم، یک عدد بسیار بزرگ تولید می‌کنید و کارتان در شبکه آغاز می‌شود. نهاد اصلی و ناظر بر ساخت حساب‌ها، همان ریاضیات است و تنها خداست که می‌داند چه کسی حاکم بر قوانین ریاضیات در جهان است.



نمونه هایی از منحنی بیضوی؛ جزء اصلی ساخت کلید خصوصی در بیت کوین

بیت کوین بر پایه‌ی بهترین نوع درک از واقعیت ساخته شده است. در حالی که هنوز مسائل حل‌نشده‌ی بسیاری در دنیای فیزیک، علوم کامپیوتر و ریاضیات وجود دارد، ما درباره برخی چیزها می‌توانیم با اطمینان صحبت کنیم. نبود تقارن میان یافتن مسائل و تایید صحت آن‌ها یکی از همین واقعیات پذیرفته شده است. نیاز محاسبات به انرژی واقعیت دیگری است. به عبارت دیگر، پیدا کردن سوزن در انبار کاه بسیار مشکل‌تر از بررسی شیء‌ای است که در دستانتان قرار دارد تا ببینید که آیا واقعا یک سوزن است یا خیر؛ و قطعا یافتن سوزن نیازمند کار بسیاری است.

وسعت فضایی که در اختیار آدرس‌ها بیت کوین قرار دارد، سر هر انسانی را به درد خواهد آورد. کما اینکه تعداد کلیدهای خصوصی موجود حتی بیشتر از این است. دانستن اینکه چه مقدار از دنیای مدرن ما بر پایه‌ی امکان‌ناپذیر بودن یافتن سوزن در یک انبار کاه بزرگ خلاصه می‌شود، شگفت‌انگیز است. من این واقعیت را بهتر از هر زمان دیگری دریافته‌ام.

بیت کوین به من یاد داد که اعداد قدرتمند هستند.

درس شانزدهم – اعتماد نکن، تحقیق کن

بیت کوین به دنبال جایگزین کردن، یا حداقل ارائه‌ی گزینه جایگزین، برای ارزهای رایج امروزی است. ارزهای مرسوم همواره با یک مقام صاحب قدرت در ارتباط هستند و این چه در مورد پول‌های قانونی مانند دلار آمریکا و یا پول‌های انحصاری نوین مانند دلارهای فورتنایت (وی‌باکس) صحت دارد. در هر دو مثال ذکر شده شما باید به این مقام در زمان عرضه، مدیریت و گردش پول‌هایتان اعتماد کنید. بیت کوین با گسستن این ارتباط، مسئله اصلی به نام اعتماد را حل می‌کند.

> *مشکل اساسی ارزهای مرسوم لزوم وجود اعتماد برای کارکرد صحیح تمامی آن‌هاست. چیزی که نیاز آن احساس می‌شود، سیستم پرداخت الکترونیکی است که از گواه رمزنگاری به جای اعتماد استفاده کند. – ساتوشی*

بیت کوین مشکل اعتماد را با تمرکززدایی در بالاترین سطح ممکن حل می‌کند، طوری که دیگر نیازی به سرور مرکزی یا طرف‌های مورد اعتماد نباشد. راه‌حل بیت کوین فراتر از اعتماد به طرف سوم مورد اعتماد

است و حتی مسئله‌ی طرف‌های مورد اعتماد را نیز حل می‌کند. وقتی با سیستمی مواجهیم که دیگر مقام مرکزی قدرتمندی در آن وجود ندارد، در واقع لزوم اعتماد به بقیه هم از میان خواهد رفت. تمرکززدایی کامل یک نوآوری محسوب می‌شود که ریشه‌ی سرسخت بودن و دلیل اصلی زنده ماندن آن نیز همین است.

تمرکززدایی دلیل اصلی داشتن نودها، عملیات استخراج، کیف پول‌های سخت‌افزاری و البته بلاک چین است. تنها چیزی که در شبکه بیت کوین باید به آن اعتماد کنید این است که آموخته‌های بشریت از ریاضیات و فیزیک اشتباه نبوده و اکثریت استخراج‌کنندگان در شبکه با نیت صادقانه عمل خواهند کرد (که به خاطر وجود انگیزه‌های اقتصادی این اتفاق نیز رخ می‌دهد).

در حالی که جهان ما بر پایه فرض «اعتماد کن، اما تحقیق هم کن» اداره می‌شود، بیت کوین بر پایه فرض «اعتماد نکن، بلکه تحقیق کن» کار می‌کند. ساتوشی، خالق بیت کوین، به صراحت به اهمیت اعتمادزدایی در مقدمه و نتیجه‌ی وایت‌پیپر بیت کوین اشاره کرد.

نتیجه: ما سیستمی برای تراکنش‌های الکترونیکی معرفی کرده‌ایم که بر اعتماد متکی نیست. – ساتوشی

همانطور که کِن تامپسون، محقق علوم کامپیوتر، در صحبت‌های جایزه تورینگ نیز عنوان کرد، اعتماد موضوع بسیار فریبنده‌ای در دنیای محاسبات و کامپیوترهاست. زمانی که برنامه‌ای را اجرا می‌کنید، باید به انواع مختلف نرم‌افزار (و سخت‌افزار) اعتماد کنید که به صورت نظری می‌توانند نحوه‌ی اجرای برنامه شما را به شیوه‌ی بدخواهانه‌ای تغییر دهند. تامپسون نیز در مقاله‌ی «بازتاب اعتماد کردن به اعتماد» به صورت خلاصه به این مسئله اشاره کرده است:

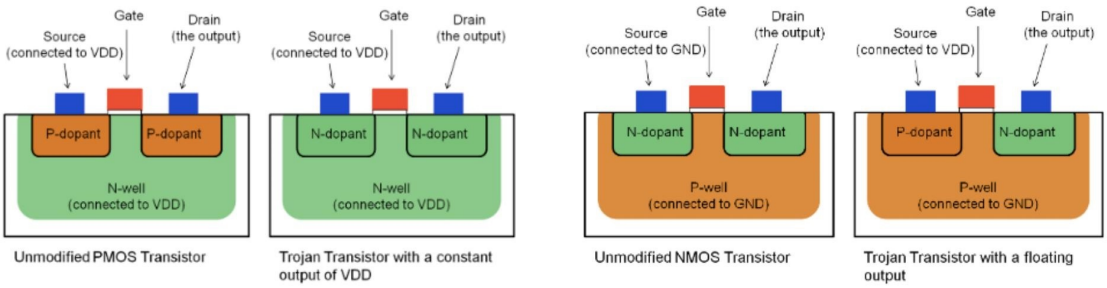
نتیجه واضح است. شما نمی‌توانید به کدی جز آنچه خودتان کاملا ساخته‌اید، اعتماد کنید.

تامپسون همچنین نشان داد که حتی اگر به کد منبع برنامه دسترسی داشته باشید، کامپایلر یا هر برنامه و سخت‌افزاری که وظیفه اجرای نرم‌افزار شما را بر عهده دارد، قدرت به خطر انداختن کدهای شما را خواهد داشت که شناسایی این در پشتی (بک‌دور) کار بسیار سختی است. به همین خاطر در عمل یک سیستم حقیقی غیرمتمرکز نمی‌تواند وجود داشته باشد. برای این کار شما باید تمامی نرم‌افزارها و

سخت‌افزارهایتان از اسمبلرها گرفته تا کامپایلرها و لینکرها را از ابتدا و بدون بهره‌گیری از هیچ نرم‌افزار و ابزار دیگری، خودتان بسازید.

اگر می‌خواهید کیک سیب را از ابتدا بسازید، ابتدا باید جهان را خلق کنید – کارل سیگن

دیدگاه کن تامپسون کاملا مبتکرانه است و به سختی می‌توان آن را رد کرد، پس بیایید نگاه گذرایی به در پشتی غیرقابل شناسایی بیندازیم که کارش را بدون ایجاد تغییر در نرم‌افزارها انجام می‌دهد. محققین موفق شده‌اند که با تغییر قطبیت ناخالصی‌های سیلیکون، روشی برای ساخت سخت‌افزارهای امنیت-بحرانی پیدا کنند. تنها با تغییر خصوصیات فیزیکی اجزای تراشه‌های کامپیوتری، ساخت تولیدکننده اعداد تصادفی امن رمزنگاری ممکن شده است. از آنجا که این تغییر قابل مشاهده نیست، در پشتی با بررسی‌های بصری که یکی از مهمترین سازوکارهای شناسایی دستکاری در تراشه‌هاست نیز قابل شناسایی نخواهد بود.



(a) p-MOS Transistor (b) n-MOS Transistor

تروجان‌های مخفی سخت‌افزاری

ترسناک به نظر می‌رسد، نه؟ حتی اگر قادر به ساختن همه چیز از همان ابتدا باشید، باید در گام بعدی به پیش‌فرض‌های ریاضیات اعتماد کنید. باید به منحنی بیضوی secp۲۵۶k۱ که در پشتی ندارد اعتماد کنید. چرا که احتمال قرار داشتن درهای پشتی خرابکارانه حتی در پایه‌های ریاضیاتی توابع هش نیز وجود دارد که دست کم یک بار هم قبلا اتفاق افتاده است. دلایل بسیاری برای بدگمان بودن وجود دارد که وجود در پشتی در همه چیز شما از سخت‌افزارهایتان گرفته تا نرم‌افزار و منحنی بیضوی تنها بخشی از آن‌هاست.

مثال‌های بالا به خوبی نشان می‌دهند که محاسبات غیرمتمرکز، ایده‌آل‌گرایانه است. بیت کوین احتمالا تنها سیستمی است که به ایده‌آل غیرمتمرکز تا این اندازه نزدیک شده و با این حال هنوز هم نشانه‌هایی از اعتماد حداقلی در آن وجود دارد که در صورت امکان، آن‌ها نیز حذف خواهند شد. به طور منطقی اگر نگاه کنیم، زنجیره اعتماد ته ندارد و همواره باید به محاسباتی که به انرژی نیاز دارند، به پارامتر P که با NP برابر نیست و یا اینکه در واقعیت به سر می‌برید و در دنیای شبیه‌سازی‌شده نیستید اعتماد کنید.

توسعه‌دهندگان بر روی ابزارها و رویه‌هایی کار می‌کنند که اعتماد باقیمانده نیز تا حد زیادی از شبکه حذف شود. برای مثال توسعه‌دهندگان بیت کوین گیتیان (Gitian) را ساخته‌اند که یک روش توزیع نرم‌افزار برای ایجاد ساخت‌های قطعی (deterministic builds) است. ایده پروژه این است که اگر چندین توسعه‌دهنده قادر به بازساخت باینری‌های مشابه باشند، شانس دستکاری خرابکارانه کاهش خواهد یافت. ناگفته نماند که درهای پشتی خیالی تنها شیوه‌های حمله نیستند و از باج‌گیری و زورگیری نیز به عنوان تهدیدهای واقعی نباید غافل شد. اما در پروتکل اصلی، از تمرکززدایی برای کاهش اعتماد استفاده شده است.

تلاش‌های زیادی برای بهبود مسئله‌ی مرغ یا تخم‌مرغ در خودراه‌اندازی (بوت‌استرپینگ) انجام شده که کن تامپسون به آن‌ها اشاره کرده است. یکی از این تلاش‌ها گیکس (Guix) بوده که در نتیجه آن دیگر نیاز نیست به هیچ نرم‌افزار مدیریت سرور اعتماد کنید. اخیرا نیز یک pull-request برای ادغام گیکس در بیت کوین صورت گرفته است.

خوشبختانه بیت کوین به یک الگوریتم یا سخت‌افزار واحد متکی نیست. یکی از نتایج سوگیری رادیکال تمرکززدایی در بیت کوین، مدل امنیت توزیع شده است. هرچند نباید درهای پشتی توصیف شده را جدی نگرفت، بعید است که هر کیف پول نرم‌افزاری، هر کیف پول سخت‌افزاری، هر کتابخانه رمزنگاری، هر برنامه فول نودی یا هر کامپایلری از هر زبان برنامه‌نویسی دستکاری شده باشد. این احتمال وجود دارد، اما بعید است.

نباید فراموش کنید که می‌توانید بدون اتکا به هر سخت‌افزار یا نرم‌افزاری یک کلید خصوصی تولید کنید. شما می‌توانید با انداختن سکه برای چندین بار متوالی، که البته با توجه به خصوصیات سکه شما و نحوه انداختن آن که شاید منبع تولید آنتروپی خوبی نباشد، این کار را انجام دهید. برای همین نیز پروتکل‌های

ذخیره‌سازی نظیر گِلَسیر (Glacier) توصیه می‌کنند که از تاس‌های مورد استفاده در کازینوها به عنوان یکی از دو منبع تولید آنتروپی استفاده شود.

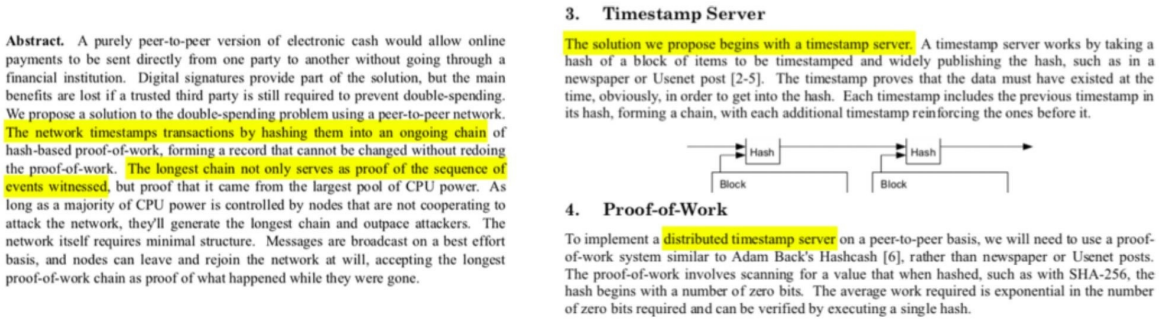
بیت کوین من را وادار کرد تا معنای حقیقی عدم اعتماد به بقیه را درک کنم. بیت کوین آگاهی من را از مسئله‌ی خود راه‌اندازی و زنجیره‌ی بی‌چون و چرای اعتماد در توسعه و اجرای نرم‌افزارها افزایش داد. همچنین در راه آموختن بیت کوین یاد گرفتم که نرم‌افزارها و سخت‌افزارها قابل دستکاری هستند.

بیت کوین به من یاد داد که اعتماد نکنم، بلکه تحقیق کنم.

درس هفدهم – اعلام زمان نیازمند کار است

اغلب گفته می‌شود که استخراج بیت کوین به خاطر وجود هزاران کامپیوتری است که بر روی مسائل ریاضی بسیار پیچیده کار می‌کنند. مطابق این دیدگاه اگر قادر به حل مسئله ریاضی پیچیده شوید، بیت کوین تولید خواهید کرد. در حالیکه درک این دیدگاه ساده‌شده از استخراج بیت کوین شاید راحت باشد، اما یک نکته مهم را نادیده می‌گیرد. بیت کوین تولید یا خلق نمی‌شود و مسائل پیچیده در حقیقت برای حل یک مسئله ریاضی نیست. همینطور خود ریاضیات بیت کوین نیز آنقدرها پیچیده نیست. چیزی که در حقیقت پیچیده است، اعلام زمان در یک سیستم غیرمتمرکز است.

مطابق آنچه در وایت‌پیپر بیت کوین آمده، سیستم اثبات کار یا همان ماینینگ روشی برای پیاده‌سازی یک سرور زمان‌سنج توزیع شده است.



Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

بخشی از وایت‌پیپر بیت کوین؛ بخش‌های اشاره شده به زنجیره زمانی

اولین باری که یاد گرفتم بیت کوین چگونه کار می‌کند، به نظرم رسید که اثبات کار فرایند بیهوده و کم بازدهی است. پس از مدتی دیدگاهم نسبت به نحوه مصرف انرژی در بیت کوین تغییر کرد. هنوز هم نحوه نگاه ما نسبت به اثبات کار بیت کوین پس از گذشت ۱۰ سال از پیدایش آن اشکالاتی دارد.

از آنجا که مسائل ریاضی در فرایند اثبات کار بیت کوین ساختگی هستند، بسیاری از مردم کار انجام شده برای حل آن‌ها را بیهوده در نظر می‌گیرند. اگر به صورت کامل تنها بر روی محاسبات تمرکز کنیم، این نتیجه‌گیری قابل درک است. اما بیت کوین درباره محاسبه کردن نیست، بلکه درباره موافقت کردن مستقلانه بر روی اولویت برخی چیزهاست.

اثبات کار سیستمی است که هر کسی می‌تواند آنچه اتفاق افتاده را به ترتیب وقوع زمانی اعتبارسنجی و تایید کند. تایید مستقلانه فرایندی است که به اجماع و توافقی واحد از سوی افراد مختلف درباره اینکه چه کسی چه چیزی دارد، می‌انجامد.

در محیطی که به سوی تمرکززدایی مطلق گرایش دارد، کالای ارزشمندی تحت عنوان زمان مطلق یافت نمی‌شود. هر ساعتی که توسط یک طرف مورد اعتماد معرفی می‌شود، یک نقطه مرکزی در سیستم به شمار می‌آید که اتکا به آن می‌تواند موجب حمله و اختلال شود. همانطور که گریشا تروباتسکی نیز اشاره کرده، سنجش زمان مشکل ریشه‌ای است.

ساتوشی به صورت نبوغ‌آمیزی این مسئله را با قرار دادن یک ساعت غیرمتمرکز از طریق اثبات کار بلاک چین حل کرد. همگی اعضای شبکه هم‌نظر هستند که زنجیره‌ای که بیشترین کار تجمعی انجام شده را دارد، منبع حقیقت و زنجیره راستین است. در واقع طبق تعریف، این همان چیزی است که واقعا اتفاق افتاده است. از این توافق تحت عنوان اجماع ناکاموتو نیز یاد می‌شود.

شبکه بیت کوین، اثر انگشت زمانی در تراکنش‌ها را با هش کردن آن‌ها بر روی زنجیره‌ی در جریان ثبت می‌کند که در واقع گواهی بر ترتیب رویدادهای به وقوع پیوسته است. – ساتوشی ناکاموتو

بدون حضور روشی پایدار برای اعلام زمان، هیچ راه مطمئنی برای اعلام اولویت زمانی وجود نخواهد داشت. ترتیب‌بندی قابل اطمینان نیز ممکن به همین خاطر ممکن نیست. اجماع ناکاموتو روشی برای اعلام پیوسته‌ی زمان در شبکه بیت کوین است. ساختار انگیزه‌بخش سیستم با استفاده از طمع و علاقه شخصی مشارکت‌کنندگان رقیب، یک ساعت غیرمتمرکز و احتمالاتی به وجود می‌آورد. اینکه ساعت سیستم غیردقیق باشد نیز کاملا اشتباه است، زیرا ترتیب رخدادها در نهایت کاملا واضح بوده و توسط هر کسی قابل تایید است.

به لطف اثبات کار، هم خود کار و هم تایید انجام کار در بهترین حالت ممکن از غیرمتمرکز هستند. هر کسی می‌تواند به اراده خودش وارد شبکه و از آن خارج شود. همه می‌توانند هر زمان که خواستند، هر چیزی را در شبکه صحت‌سنجی کنند. تنها این نیست بلکه هر کسی می‌تواند اعتبار وضعیت سیستم را مستقلا و بدون اتکا به شخص دیگری بسنجد.

درک اثباتِ کار، زمان‌بر است. شاید درک شهودی آن امکان‌پذیر نباشد و در حالی که قوانین ساده‌ای بر آن حاکم است، به پدیده‌ی کاملا پیچیده‌ای ختم شود. برای من تغییر دیدگاهم نسبت به ماینینگ راهگشا بود. مصرف انرژی مفید نه بیهوده، اعتبارسنجی و نه محاسبات، زمان و نه بلاک‌ها.

بیت کوین به من یاد داد که اعلام زمان می‌تواند فریبنده باشند، به خصوص اگر بخواهید غیرمتمرکز باشید.

درس هجدهم – آرام و پیوسته حرکت کن

«سریع حرکت کن و مرزها را بشکاف».

شاید این عبارت در عصر مدرن رایج و تکراری شده باشد اما دنیای تکنولوژی همواره بر پایه این شعار حرکت کرده است. این عقیده که نحوه درست انجام کارها در ابتدا اهمیت ندارد، برگرفته از روحیه‌ی «در ابتدا شکست بخور و زیاد هم شکست بخور» جان‌سی مکسول است. موفقیت با میزان رشد تعبیر می‌شود و تا زمانی که در حال رشد باشید، مشکلی نیست. اگر چیزی ابتدا درست کار نکرد، شیوه انجام آن را تغییر داده و دوباره امتحان می‌کنید. به عبارت دیگر، آنقدری امتحان می‌کنید تا بالاخره نتیجه دهد.

اما بیت کوین به طرز متفاوتی کار می‌کند و طراحی آن فرق دارد. دلیل این تفاوت نیز وجود برخی شرایط غیرقابل تغییر است. همانطور که ساتوشی نیز اشاره کرده، پول‌های الکترونیک پیش از بیت کوین بارها مورد آزمایش قرار گرفته بودند و تمامی آن‌ها به خاطر وجود یک راس قدرت محدودکننده با شکست مواجه شدند. نوآوری بیت کوین به خاطر خلق اژدهایی بدون سر است.

بسیاری از مردم پول‌های الکترونیک را یک شکست می‌بینند که دلیل آن نیز عدم موفقیت شرکت‌ها از دهه ۹۰ بوده است. امیدوارم واضح باشد که تنها ماهیت متمرکز و کنترل‌شونده‌ی این سیستم‌ها سبب شکست آن‌ها شد. – ساتوشی ناکاموتو

یکی از عواقب تمرکززدایی رادیکال در بیت کوین، مقاومت آن در برابر تغییرات است. شعار «سریع حرکت کن و مرزها را بشکاف» هرگز در لایه‌های زیرین و اصلی بیت کوین نمی‌تواند کار کند. حتی اگر این تغییرات به نفع سیستم باشد، اعمال آن با متقاعد کردن همه افراد برای استفاده از نسخه جدید تقریبا یک عمل غیرممکن است. این همان اجماع غیرمتمرکز است که به ماهیت بیت کوین برمی‌گردد.

ماهیت بیت کوین به گونه‌ای است که پس از انتشار نسخه ۰٫۱ (اولین نسخه از پروتکل بیت کوین)، طراحی اصلی آن برای همیشه دست‌نخورده باقی خواهد ماند. – ساتوشی ناکاموتو

این یکی از اساسی‌ترین تناقضات بیت کوین به شمار می‌آید. ما فکر می‌کنیم که هر نرم‌افزاری را به راحتی می‌توان تغییر داد اما ماهیت درنده‌خوی بیت کوین این امر را بسیار سخت کرده است.

همانطور که هاسو در مقاله‌ی «قراردادهای اجتماعی بیت کوین» این مطلب را باز کرده، تغییر قوانین بیت کوین تنها با پیشنهاد ایجاد تغییر و پس از آن متقاعد کردن تمام کاربران به پذیرش این تغییرات وابسته است. برای همین نیز بیت کوین حتی به عنوان یک نرم‌افزار در برابر تغییرات مقاومت شدیدی دارد.

این مقاومت از خصوصیات اصلی بیت کوین است. نرم‌افزارهایی مانند بیت کوین باید از خصوصیت تغییرناپذیری برخوردار باشند تا تعامل میان لایه اجتماعی و فنی آن را تضمین کند. سیستم‌های پولی

همواره ماهیت اختلاف‌برانگیزی داشته‌اند و طبق تجربه‌ی هزار ساله از آن‌ها، بنیادهای مستحکم از ضروریات یک محیط اختلاف‌برانگیز است.

و باران باریده، سیلاب‌ها روان گردید و بادها وزیده، بدان خانه زورآور شد و خراب نگردید زیرا که بر سنگ بنا شده بود. – انجیل متی ۲۴:۷-۲۷

در این مثال از سازندگان احمق و دانا، بیت کوین را نمی‌توان همان خانه پنداشت. بیت کوین همانند سنگی با خصوصیات غیرقابل تغییر، استوار و تامین‌کننده‌ی بنیان سیستم مالی جدید است.

اما به مانند زمین‌شناسان که می‌گویند سنگ‌های پوسته زمین همواره در حرکتند، اگر دقیقتر نگاه کنیم بیت کوین نیز همواره در حال حرکت و تکامل است. فقط باید بدانید که دقیقا به کجا و چگونه نگاه کنید.

معرفی فرمت آدرس‌های P2SH و سگویت گواهی برای امکان تغییر قوانین بیت کوین در صورت پذیرش و استفاده تعداد کافی از کاربران از تغییرات به نفع شبکه است. بروزرسانی سگویت توسعه شبکه لایتنینگ را که خانه‌ای بنا شده بر روی سنگ بیت کوین است، ممکن کرد. بروزرسانی‌های دیگری مانند امضاهای شنور نیز بازدهی و حریم خصوصی را افزایش داده و در کنار آن بهره‌گیری از قابلیت‌های اسکریپت (مانند قرارداد هوشمند) را به لطف متمایزسازی تراکنش‌های عادی با تپ‌روت ممکن خواهد کرد. به راستی که سازندگان دانا کار ساخت و توسعه را بر روی بنیادهای مستحکم ادامه می‌دهند.

ساتوشی از نظر فناورانه تنها یک سازنده دانا نبود. او ضرورت اتخاذ تصمیمات خردمندانه را نیز می‌دانست.

متن‌باز بودن به خاطر آن است که هر کسی می‌تواند مستقل از دیگری کد را بازبینی کند. اگر بیت کوین متن‌بسته بود، هیچکس نمی‌توانست امنیت آن را تایید کند. به نظرم متن‌باز بودن نرم‌افزاری با چنین ماهیتی یک ضرورت است. – ساتوشی ناکاموتو

آزاد بودن بالاترین اهمیت را برای امنیت دارد و متن‌باز بودن نیز ذاتا در راستای جنبش نرم‌افزار آزاد است. طبق گفته‌های ساتوشی، پروتکل‌های امن و کدهایی که آن‌ها را پیاده‌سازی می‌کنند باید در دسترس همه باشند چرا که با عدم شفافیت نمی‌توان به دنبال امنیت بود. مزیت دیگر آن به غیرمتمرکز

بودن برمی‌گردد: کدی که قابل اجرا، مطالعه، اصلاح، رونوشت و توزیع آزادانه باشد، گسترش حداکثری آن را نیز تضمین می‌کند.

تمرکززدایی رادیکال بیت کوین چیزی است که حرکت آن را آرام و پیوسته ساخته است. شبکه‌ای از نودهای مستقل و خودمختار که ذاتا در برابر هر نوع تغییری مقاوم هستند. بدون وجود روشی جهت تحمیل بروزرسانی‌ها به کاربران، تنها روش معرفی و اعمال آن‌ها قانع کردن تدریجی تک تک کاربران به پذیرش تغییرات است. این فرایند بدون هسته مرکزی برای معرفی و اعمال تغییرات، مقاومت شدید آن را در برابر تغییرات خرابکارانه رقم می‌زند. شکستن قوانین و قواعد قبلی در شبکه بیت کوین بسیار دشوارتر از سیستم‌های متمرکز است و برای همین نیز همه در راستای حفظ آن‌ها تلاش می‌کنند.

بیت کوین به من یاد داد که حرکت آرام و پیوسته یک قابلیت است نه یک ایراد.

درس نوزدهم – حریم خصوصی نمُرده است

اگر حرف‌های کارشناسان و صاحب‌نظران را قبول داشته باشید باید بدانید که حریم خصوصی از دهه ۸۰ به بعد مرده است. اما اختراع گمنام و با نام مستعار بیت کوین و برخی رویدادهای عصر حاضر به ما نشان داده که این حرف صحیح نیست. حریم خصوصی همچنان زنده است، هر چند فرار از نظارت‌های گسترده به هیچ وجه آسان نیست.

ساتوشی مسیر طولانی را برای پنهان ساختن رد خود و هویتش طی کرد. بیش از ده سال از اختراع بیت کوین می‌گذرد و هنوز مشخص نیست که ساتوشی ناکاموتو یک شخص بوده است یا یک گروه، مرد، زن، یا حتی یک هوش مصنوعی که برای پیاده‌سازی نقشه‌ی تصاحب جهان، در زمان سفر کرده باشد.

جدا از فرضیه‌های توهم توطئه، ساتوشی انتخاب کرد که پشت یک اسم ژاپنی ناشناس باقی بماند. با اینکه این تنها یک فرضیه است اما برای احترام به جنسیتی که برای خودش انتخاب کرده بهتر است او را با ضمیر مذکر خطاب کنیم.

تصویر منتسب به ساتوشی که به اشتباه چهره شخص دیگری به نام دوریان ناکاموتو را نشان می‌دهد

هویت واقعی ساتوشی هر چه باشد، در پنهان کردن آن کاملا موفق بود. او یک مثال زنده و تجدید آرمانی بود برای تمام کسانی که آرزوی ناشناس ماندن دارند: امکان حفظ حریم خصوصی در فضای آنلاین وجود دارد.

پنهان ساختن اطلاعات جواب می‌دهد. سیستم‌های رمزنگاری که به درستی پیاده‌سازی شده باشند از معدود چیزهایی هستند که می‌توانید به آن‌ها اعتماد کنید. – ادوارد اسنودن

ساتوشی اولین مخترع ناشناس یا با نام مستعار نبود و حتی آخرین آن‌ها هم نیست. بعضی از آن‌ها مانند تام الویس جدوسر که مقاله میمبل‌ویمبل را منتشر کرد، از شیوه‌ی انتشار مقاله‌ی ساتوشی ناکاموتو کاملا تقلید کردند. در حالی که برخی از آن‌ها با وجود ناشناس ماندن، برخی اثبات‌های پیشرفته ریاضی را منتشر کردند.

جهان جدیدی که در آن زندگی می‌کنیم جای عجیبی است. جایی که انتخاب هویت اختیاری بوده، مشارکت‌ها بر پایه‌ی شایستگی‌ها صورت می‌گیرد و مردم می‌توانند آزادانه با هم همکاری و مبادله کنند. برای داشتن احساس راحتی با پارادایم‌های جدید نیازمند برخی تصحیحات هستیم اما من عمیقا معتقدم که تمامی این‌ها پتانسیل ایجاد تغییراتی مثبت را در جهان دارد.

نباید فراموش کنیم که حریم خصوصی یکی از حقوق‌های اساسی بشر است. تا زمانی که مردم در راستای حفظ این حق تلاش کرده و از آن دفاع کنند، جنگ بر سر حریم خصوصی هنوز تمام نشده است.

بیت کوین به من آموخت که حریم خصوصی هنوز زنده است.

درس بیستم – سایفرپانک‌ها کد را می‌نویسند

مثل بسیاری از ایده‌های شگفت‌انگیز دیگر، بیت کوین هم سر و کله‌اش از ناکجاآباد پیدا نشد. ایده‌ی بیت کوین با به کار بستن و ترکیب تعداد زیادی نوآوری و اکتشافات قبلی در حوزه‌های فیزیک، علوم کامپیوتر، ریاضیات و علوم دیگر به ثمر رسید. در نابغه بودن ساتوشی نباید شک کرد اما امکان اختراع بیت کوین بدون وجود غول‌هایی که بر شانه‌ی آن‌ها بایستد، وجود نداشت.

کسی که تنها آرزو می‌کند و امیدوار است، تعامل فعالی با شیوه‌ی وقوع رویدادها نداشته و سرنوشت خویش را شکل نمی‌دهد. – لودویگ فون میزس

اریک هیوز یکی از همین غول‌ها و از بنیان‌گذاران جنبش سایفرپانک‌ها است که مانیفست سایفرپانک را نیز منتشر کرد. تصور اینکه ساتوشی تحت تاثیر این مانیفست نبوده باشد، دور از واقعیت است. در این مانیفست درباره چیزهایی از قبیل تراکنش‌های مستقیم و خصوصی، پول الکترونیک و نقد، سیستم‌های ناشناس و دفاع از حریم خصوصی با امضای دیجیتال و رمزنگاری صحبت شده که تقریبا تمام آن‌ها در بیت کوین وجود دارند.

حریم خصوصی یکی از الزامات جامعه آزاد در عصر الکترونیک است. از آنجا که حریم خصوصی مقصود ماست، باید اطمینان حاصل کنیم که تنها طرفین یک تراکنش درباره آن اطلاعاتی داشته باشند که برای آن تراکنش اساسا ضروری است. [...] بنابرین حریم خصوصی در یک جامعه آزاد نیازمند به کارگیری سیستم‌های مبادلاتی ناشناس است. تاکنون پول نقد چنین کارکردی را دنبال کرده بود؛ یک سیستم مبادلاتی ناشناس را نباید با سیستم مبادلاتی محرمانه اشتباه گرفت. [...] ما سایفرپانک‌ها متعهد شدیم تا چنین سیستم ناشناسی ایجاد کنیم. ما با رمزنگاری از حریم خصوصی خود دفاع می‌کنیم، با سیستم‌های ارسال ایمیل ناشناس، با امضای دیجیتال و با پول الکترونیک. سایفرپانک‌ها کد را می‌نویسند. – اریک هیوز

سایفرپانک‌ها راحتی خود را در امید و آرزو جستجو نمی‌کردند. آن‌ها با شیوه وقوع رویدادها تعامل بسیار نزدیکی داشتند و سرنوشت خود را به دست گرفتند. سایفرپانک‌ها کد را می‌نویسند (به اصطلاح یعنی فقط حرف نمی‌زنند بلکه انجام می‌دهند).

به این ترتیب ساتوشی مثل یک سایفرپانک اصیل بر روی صندلی خود نشست و شروع به نوشتن کدهای بیت کوین کرد. کدی که شکل یک ایده و مفهوم درآمد و به جهان ثابت کرد که کار می‌کند. کدی که بذر واقعیت اقتصادی جدید را کاشت. به خاطر این کد هر کسی می‌تواند تایید کند که سیستم پرداخت جدید واقعا کار می‌کند و حدود هر ۱۰ دقیقه زنده بودن آن را به جهانیان نشان دهد.

```
23  map<uint256, CBlockIndex*> mapBlockIndex;
24  const uint256 hashGenesisBlock("0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f");
25  CBlockIndex* pindexGenesisBlock = NULL;
26  int nBestHeight = -1;
27  uint256 hashBestChain = 0;
28  CBlockIndex* pindexBest = NULL;
    ⋮
675 int64 CBlock::GetBlockValue(int64 nFees) const
676 {
677     int64 nSubsidy = 50 * COIN;
678
679     // Subsidy is cut in half every 4 years
680     nSubsidy >>= (nBestHeight / 210000);
681
682     return nSubsidy + nFees;
683 }
684
685 unsigned int GetNextWorkRequired(const CBlockIndex* pindexLast)
686 {
687     const unsigned int nTargetTimespan = 14 * 24 * 60 * 60; // two weeks
688     const unsigned int nTargetSpacing = 10 * 60;
689     const unsigned int nInterval = nTargetTimespan / nTargetSpacing;
690
691     // Genesis block
692     if (pindexLast == NULL)
693         return bnProofOfWorkLimit.GetCompact();
```

بخشی از کدهای نسخه ۰/۱ بیت کوین

ساتوشی برای اطمینان از برتری نوآوری خود و به واقعیت پیوستن آن، کدهای برنامه را پیش از نوشتن وایت‌پیپر آغاز کرد. او همچنین از عدم تاخیر در انتشار نسخه‌های بعدی نرم‌افزار اطمینان حاصل کرد.

باید کل کد بیت کوین را پیش از آن که خودم را متقاعد به حل تمامی مشکلات می‌کردم می‌نوشتم، پس از آن بود که مقاله را نوشتم. – ساتوشی ناکاموتو

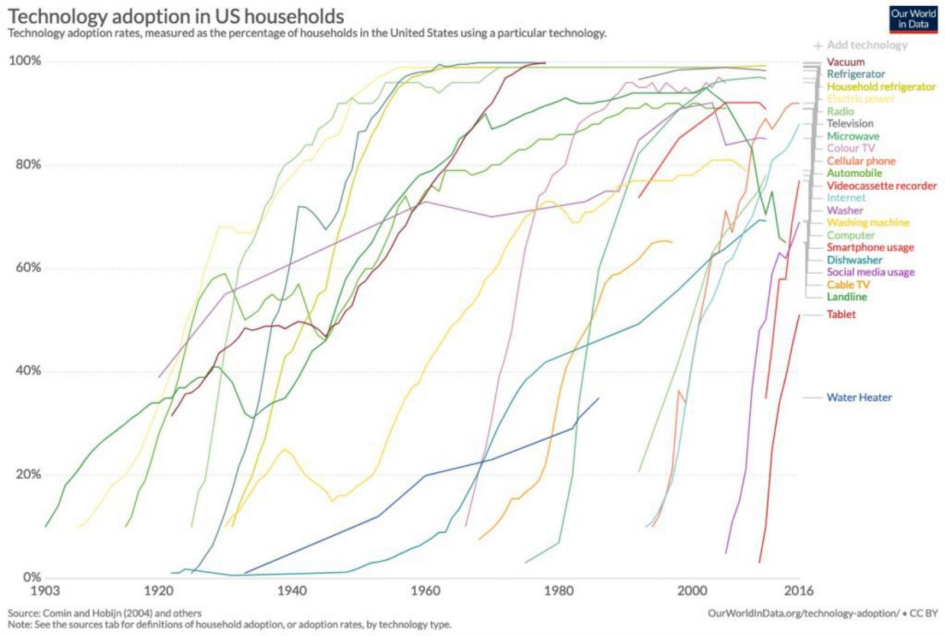
در دنیای بی‌انتهای وعده‌های پوشالی و شک‌برانگیز اجرای عملیات، تلاشی تمرکزیافته برای ساختن شدیدا مورد نیاز بود. ژرف اندیش باشید و خودتان را قانع کنید که واقعا می‌توانید مشکلات را حل کنید و راه‌حل‌ها را یکی یکی پیاده کنید. همه ما باید اندکی از سایفرپانک‌ها یاد بگیریم.

بیت کوین به من یاد داد که سایفرپانک‌ها کد را می‌نویسند.

درس بیست و یکم – تشابهاتی برای آینده بیت کوین

طی چند دهه اخیر روند غیرخطی پیشرفت‌های تکنولوژیکی برای همه آشکار شده است. چه به تکینگی فناوری باور داشته باشید چه نداشته باشید، رشد نمایی نوآوری‌ها در بسیاری از عرصه‌ها غیر قابل انکار است. تنها این نیست و میزان نرخ پذیرش فناوری نیز در حال شتاب گرفتن است و پیش از آنکه به درک این واقعیت برسید، فرزندانتان به جای وسایل بازی مدرسه از اسنپ‌چت استفاده می‌کنند. منحنی‌های نمایی قدرت شوکه کردن شما را پیش از آن که اثراتش را مشاهده کنید دارند.

بیت کوین یک فناوری با رشد نمایی است که زیربنای آن از سایر تکنولوژی‌های نمایی ایجاد شده است. جهان داده به زیبایی افزایش سرعت پذیرش تکنولوژی را به ما نشان می‌دهد که از سال ۱۹۰۳ و با راه‌اندازی خطوط تلفن آغاز شد. خطوط تلفن، الکتریسیته، کامپیوتر، اینترنت و تلفن‌های هوشمند. همگی آن‌ها از الگوی نمایی در ارزش‌گذاری و سرعت پذیرش پیروی کردند. بیت کوین نیز همینطور.



روند پذیرش فناوری‌های جدید در خانواده‌های آمریکایی؛ بیت کوین در این نمودار حضور ندارد

بیت کوین از چندین اثر شبکه‌ای تاثیر می‌گیرد که تمامی آن‌ها از الگوی نمایی پیروی می‌کنند: قیمت، کاربران، امنیت، توسعه‌دهندگان، سهم بازار و پذیرش آن به عنوان پول جهانی.

بیت کوین با زنده ماندن و سپری کردن مراحل اولیه خود، به رشد مداومش در جنبه‌های بیشتر ادامه می‌دهد و با این حال هنوز به پختگی و بلوغ نرسیده است. شاید در میانه‌ی مسیر بلوغش باشد اما اگر روند رشد فناوری را نمایی در نظر گرفتیم، مسیر رسیدن از ناشناخته‌بودن تا فراگیری کوتاه خواهد بود.

تحول تلفن از سال ۱۹۶۵ تا ۲۰۱۹

در سال ۲۰۰۳، جف بزوس برای سخنرانی تد تاک از مثال الکتریسیته برای به تصویر کشیدن آینده وب استفاده کرد. هر سه پدیده‌ی الکتریسیته، اینترنت و بیت کوین دلیل آفرینش تکنولوژی‌ها و شبکه‌های بعدی هستند که خود آن‌ها نیز فناوری‌ها بعدی را ممکن می‌کنند. آن‌ها زیربنایی برای ساختن در اختیار می‌گذارند که در ماهیت بنیادی است.

این حقیقت درباره الکتریسیته که مدتی می‌شود بشر آن را شناخته و از آن استفاده می‌کند صحیح است. همچنین درباره اینترنت که سن کمتری نسبت به الکتریسیته دارد، تقریبا توسط بیشتر مردم پذیرفته شده است. اما بیت کوین کمی بیش از ده سال عمر کرده و طی چرخه هیجانی اخیر خود وارد ذهن عموم مردم شده است. تنها پذیرندگان اولیه این حقیقت را درباره بیت کوین قبول دارند و با گذشت زمان افراد بیشتری بیت کوین را به عنوان آنچه هست خواهند پذیرفت.

در سال ۱۹۹۴ اینترنت گیج‌کننده و درک آن سخت بود. اگر به این کلیپ قدیمی از برنامه تودی‌شو نگاه کنید، این مسئله را که اینترنت هم زمانی به اندازه الان قابل لمس نبود کاملا درخواهید یافت. بیت کوین هنوز برای بسیاری پیچیده و ناآشناست، اما همانطور که اینترنت ماهیت ثانویه اشیای دیجیتال را شکل

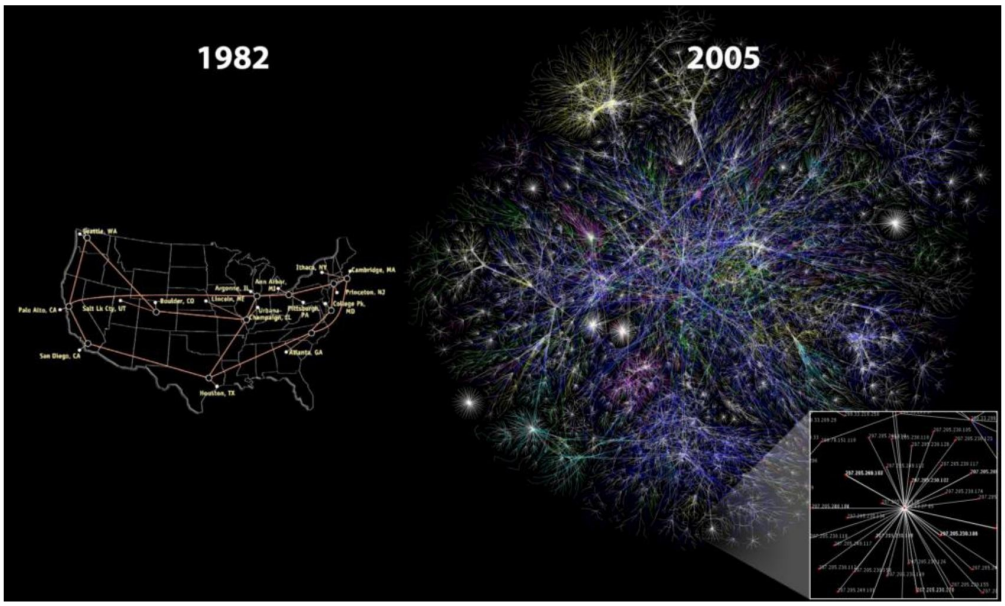
داده، خرج کردن و انباشتن ساتوشی (کوچکترین واحد پولی بیت کوین) نیز ماهیت ثانویه‌ی اشیای بیت کوینی را در آینده شکل خواهد داد.

آینده همینجاست. تنها هنوز به طور یکنواخت پخش نشده است. – ویلیام گیبسون

در سال ۱۹۹۵ حدود ۱۵ درصد از بزرگسالان آمریکایی از اینترنت استفاده می‌کردند. تاریخچه داده‌های مرکز تحقیقاتی پیو از چگونگی در هم تنیده‌شدن اینترنت و زندگی ما حکایت دارد. با استناد به تحقیق میدانی انجام شده در آزمایشگاه کسپرسکای، ۱۳ درصد از افراد از بیت کوین و ارزهای دیجیتال برای خرید کالا در سال ۲۰۱۸ استفاده کرده‌اند. در حالی که پرداخت تنها کاربرد بیت کوین نیست، می‌توان آن را شاخصی از موقعیت رشد مشابه برای اینترنت در نظر گرفت که اوایل تا میانه دهه ۹۰ را در برمی‌گیرد.

در سال ۱۹۹۷ جف بزوس در نامه‌ای به سهامداران نوشت که «این اولین روز از اینترنت است». او با این کار پتانسیل عظیم رشد اینترنت و به تبع آن شرکتش را برای سهامداران توصیف کرد.

مهم نیست امروز در چه روزی از بیت کوین قرار داریم، زیرا وجود پتانسیل دست‌نخورده و نهفته عظیم آن برای همگان و به خصوص ناظرین عادی روشن است.

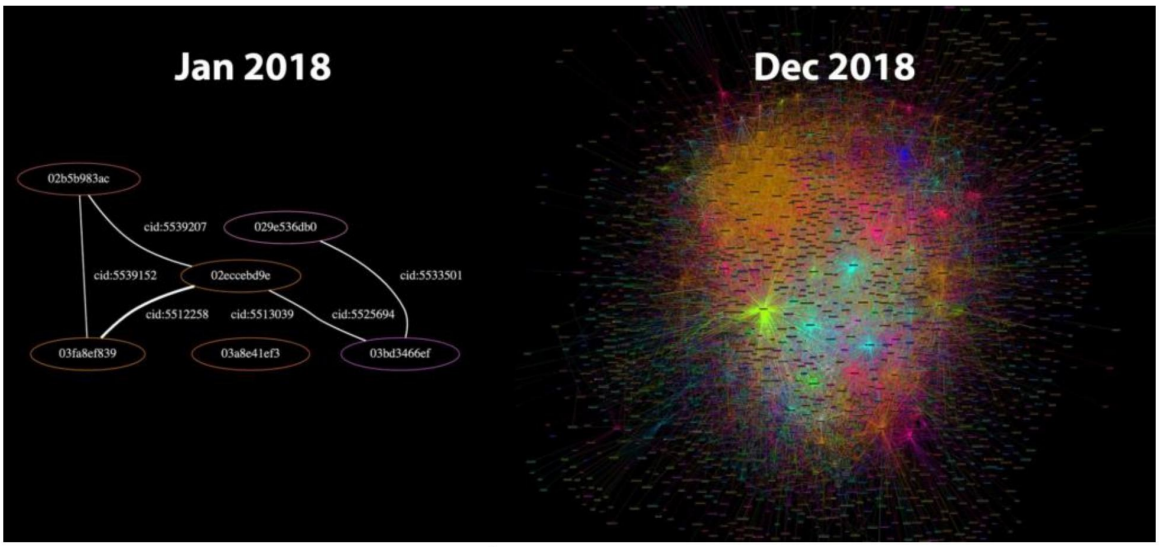


مصورسازی اینترنت در سال ۱۹۸۲ و ۲۰۰۵

اولین نود بیت کوین در سال ۲۰۰۹ و پس از استخراج بلاک جنسیس (اولین بلاک از بلاک چین بیت کوین) فعال و پس از آن اولین نسخه نرم‌افزار عرضه شد. نود ساتوشی برای مدت زیادی در شبکه تنها نبود و هال فینی نیز مدتی بعد جذب ایده بیت کوین شد و به شبکه پیوست. ده سال بعد و در زمان نگارش این مقاله بیش از ۷۵ هزار نود در شبکه بیت کوین در حال اجراست.

تنها لایه اصلی پروتکل بیت کوین شاهد رشد نمایی نیست .شبکه لایتنینگ، یک فناوری لایه دوم، نسبت به شبکه اصلی حتی رشد بیشتری داشته است.

در ژانویه ۲۰۱۸ شبکه لایتنینگ تنها از ۴۰ نود و ۶۰ کانال تشکیل شده بود. در آوریل ۲۰۱۹ این میزان به بیش از ۴ هزار نود و ۴۰ هزار کانال رسید. از یاد نبرید که این فناوری هنوز در مرحله آزمایشی است که احتمال از دست رفتن سرمایه‌های بیت کوین بر روی آن وجود دارد. با این حال روند کاملا مشخص است: هر روزه هزاران نفر برای استفاده از آن مشتاق هستند.



مصورسازی **از رشد شبکه لایتنینگ طی یک سال**

برای من که شاهد رونق وب و فراگیر شدن آن بودم، مشاهده‌ی مشابهات میان این دو کاملا واضح است. هر دو آن‌ها شبکه و فناوری‌های نمایی هستند گزینه‌های جدید، صنایع جدید و شیوه‌های جدید زندگی را ممکن می‌کنند. درست مانند الکتریسیته که از آن برای درک موقعیت خود در دوران اینترنت و اینکه سرانجام به سمت و سویی خواهیم رفت استفاده می‌کردیم، اینترنت نیز بهترین تشابه برای توصیف

موقعیت کنونی و آینده بیت کوین است. یا به قول آندرس آنتونوپولوس، بیت کوین اینترنتِ پول است. این تشابهات بهترین یادآوری به ما انسان‌ها است تا بدانیم با اینکه تاریخ خودش را دقیقا تکرار نمی‌کند اما اغلب الگوی یکسانی را دوباره استفاده می‌کند.

درک فناوری‌های نمایی معمولا سخت است و اغلب دست کم گرفته می‌شوند. حتی با اینکه خود من علاقه زیادی به چنین تکنولوژی‌هایی دارم، همیشه از سرعت رشد نوآوری و پیشرفت آن‌ها شگفت‌زده می‌شوم. مشاهده رشد اکوسیستم بیت کوین مانند مشاهده رونق اینترنت با سرعت چندبرابر است. این تجربه واقعا لذت‌بخش است.

ماموریت من برای درک بیت کوین سبب عبور من از چندین گذرگاه تاریخی شد. درک ساختارهای اجتماعی باستانی، پول‌های قدیمی و چگونگی تکامل شبکه‌های ارتباطی همگی بخشی از این ماجراجویی بودند. از تبرهای دستی تا گوشی‌های هوشمند، فناوری چندین و چند بار دنیای ما را زیر و رو کرده است. ویژگی تحویل‌آفرینی در فناوری‌های شبکه‌ای مانند نوشتن، جاده‌ها، الکتریسیته و اینترنت تشدید یافته‌تر است. همه آن‌ها جهان را برای همیشه تغییر دادند. بیت کوین نیز دنیای مرا برای همیشه تغییر داد و به تغییر تفکرات و احساسات تمامی آن‌هایی که جرئت استفاده از آن را پیدا کنند ادامه خواهد داد.

بیت کوین به من یاد داد که که درک گذشته برای فهم آینده ضروری است. آینده‌ای که تازه در حال شروع شدن است.

نتیجه‌گیری

همانطور که در ابتدا نیز اشاره کردم، به نظرم هرگونه پاسخی به پرسش «چه چیزی از بیت کوین یاد گرفته‌اید؟» همیشه ناقص خواهد بود. از همزیستی موجوداتی که به عنوان سیستم‌های زنده شناخته می‌شوند، یعنی بیت کوین، فضای فناوری و اقتصاد، به درهم‌تنیدگی شدید آن‌ها، موضوعات مورد بحث فراوان‌شان و سرعت فوق‌العاده رشد و فراتر از یادگیری کامل آن‌ها توسط یک نفر می‌توان اشاره کرد.

حتی بدون اینکه نیاز باشد یک نفر کاملا آن را درک کند و با وجود تمام خصوصیات و نقصان‌هایی که شاید داشته باشد، بیت کوین بی‌شک کار می‌کند. بیت کوین به ساخت بلاک‌ها در هر ده دقیقه ادامه می‌دهد و این کار را در نهایت زیبایی انجام می‌دهد. هر چقدر بیت کوین زمان طولانی‌تری به کار خود ادامه دهد، افراد بیشتری به فعالیت در شبکه ترغیب می‌شوند.

این حقیقت دارد که زیبایی چیزها هنگام کار کردن آن‌ها نمود می‌یابد. هنر همان عملکرد است. – گیانینا بارچی

بیت کوین بچه‌ی اینترنت است. به صورت نمایی رشد می‌کند و مرز میان حوزه‌های مختلف را نامشخص‌تر از قبل می‌سازد. اینکه دقیقا در کدام نقطه برای مثال فناوری خالص به پایان راه خود می‌رسد و قلمروی دیگری از علوم آغاز می‌شود، اصلا مشخص نیست. حتی با وجود اینکه بیت کوین برای عملکرد بهینه خود به کامپیوترها احتیاج دارد، اما علوم کامپیوتر به تنهایی برای فهم آن اصلا کافی نیست. بیت کوین علاوه بر اینکه در سازوکارهای داخلی خود مرزی نمی‌شناسد بلکه در رشته‌های آکادمیک هم بدین صورت عمل می‌کند.

اقتصاد، سیاست، نظریه بازی‌ها، تاریخچه پول، تئوری شبکه، علوم مالی، رمزنگاری، نظریه اطلاعات، سانسور، حقوق و قانون‌گذاری، سازمان‌های انسانی، روانشانی؛ تمامی این موضوعات و حتی به همراه تعدادی دیگر، حوزه‌های تخصصی هستند که می‌توانند در ماموریت درک چگونگی کارکرد بیت کوین و اینکه واقعا چه چیزی است، به ما کمک کنند.

هیچ اختراعی را نمی‌توان به تنهایی مسئول موفقیت خود دانست. انقلاب بیت کوین نیز به همین صورت ترکیبی از چندین قطعه نامرتبط است که پیش‌تر کشف شده‌اند و با مشوقی به نام نظریه بازی‌ها به یکدیگر چسبیده‌اند. ترکیب زیبا و ماهرانه‌ی تمامی رشته‌هاست که ساتوشی را یک نابغه ساخته است.

درست مانند هر سیستم پیچیده دیگر، بیت کوین نیز شاهد بده‌بستان‌هایی در مفاهیم بهره‌وری، هزینه، امنیت و بسیاری از خصوصیات دیگر است. همانطور که راه‌حل بی‌نقصی برای بیرون کشیدن یک مربع از دایره وجود ندارد، هر راه‌حلی که بیت کوین برای رفع آن تلاش می‌کند نیز کاستی‌هایی دارد.

به عقیده من نباید پیش از آن که پول را از دست دولت خارج کرده باشیم، دوباره دنبال یک پول خوب دیگر باشیم. به عبارت دیگر نمی‌توانیم این کار را با خشونت انجام دهیم و تنها با معرفی راهکار غیرمستقیم زیرکانه‌ای باید چیزی را معرفی کنیم که قادر به متوقف کردن آن نباشند. – فردریش فون هایک

بیت کوین همان راهکار زیرکانه و غیرمستقیم برای معرفی دوباره پول خوب به جهانیان است. بیت کوین این کار را با قرار دادن قدرت حاکمیت در تمامی نودها انجام می‌دهد، درست مانند داوینچی که برای مسئله‌ی غیرقابل حلِ مربع کردن یک دایره، یک مرد ویترویوسی را در مرکز قرار داد. نودها نیز به طور موثری هر مفهومی از مرکزیت را با ایجاد سیستمی توقف‌ناپذیر و ضدشکننده حذف کرده‌اند. بیت کوین زنده است و قلب آن احتمالا بیش از همه ما خواهد تپید.

امیدوارم که از ۲۱ درس بیت کوین لذت برده باشید. شاید مهمترین درسی که از بیت کوین گرفته باشیم، بررسی همه جانبه آن از زوایای مختلف است تا تصویری نسبتا کامل از آن داشته باشیم. همانطور که جدا کردن یک جزء از سیستم پیچیده کل آن را نابود می‌کند، بررسی جداگانه‌ی اجزای بیت کوین بدون اعتنا به دیگر بخش‌های آن نیز درک ما از آن را دچار مشکل خواهد کرد.

در هر صورت مسیر ماجراجویانه من ادامه خواهد یافت و قصد دارم هرچه بیشتر وارد لانه خرگوش بیت کوین شوم.