حکمرانی کد

بلاکچین و قانون

پریماورا. دفیلیپی، آرون رایت

مترجمان: حامد حیدری، یاسر زندی

Harvard University Press


بسم الله
الرحمن
الرحيم

بلاکچین و قانون

حکمرانی کد

انتشارات راه‌پرداخت

سرشناسه: دفیلیپی، پریماورا. De Filippi, Primavera / عنوان و نام پدیدآور: بلاکچین و قانون/ پریما وراد فیلیپی، آرون رایت ؛ ترجمه حامد حیدری، یاسر زندی. / مشخصات نشر: تهران: راه پرداخت، ۱۴۰۱./ مشـــخصات ظاهری: ۳۲۸ ص.؛ ۱۴/۵×۲۱/۵س‌م./ شـــابک: ۷-۳۴-۷۷۰۲-۶۲۲-۹۷۸/ وضعیت فهرست نویسی: فیپا/ یادداشت: عنوان اصلی: .Blockchain and the law: the rule of code, ۲۰۱۸ / موضوع: بلاک‌چین (پایگاه‌های اطلاعاتی)؛ موضوع:(Blockchain (Databases؛ موضوع: تکنولوژی و قانون؛ موضوع: Technology and law؛ شناسه افزوده: رایت، آرون شناسه افزوده: Wright, Aaron شناسه افزوده: حیدری، حامد، ۱۳۶۷ – ، مترجم شناسه افزوده: زندی، یاسر، ۱۳۶۶–، مترجم / رده‌بندی کنگره: QA۷۶/۹/ رده بندی دیویی:۸۲۴/۰۰۵/ شماره کتابشناسی ملی: ۸۹۰۸۴۶۱

بلاکچین و قانون

حکمرانی کد

پریماورا دفیلیپی
آرون رایت

مترجم:
حامد حیدری (مدرس دانشگاه علامه طباطبائی)
یاسر غرایاق زندی (دانشجوی دکتری مدیریت فناوری اطلاعات)

انتشارات راه‌پرداخت

بلاکچیـــن و قانون:حکمرانی کد / ناشـــر: راه پرداخـــت / مؤلف: پریماورا د فیلیپـــی، آرون رایت/ مترجمان: حامد حیدری و یاســـر زندی/ ویراستار محتوایی: قاسم سرافرازی / ویراستار متن: یلدا شایسته‌فر / صفحه‌آرا: ایمان شاه‌ســـمندی/ نوبت چاپ: اول ۱۴۰۱ / شـــمارگان: ۱۰۰ نسخه / شـــابک ۷-۳۴-۷۷۰۲-۶۲۲-۹۷۸ / تلفن: ۴۴۴۳۹۶۶-۰۲۱ / دورنگار: ۸۹۷۸۴۹۰۲ / پست الکترونیک: info@way2pay.press / پایگاه اینترنتی: w2pshop.ir

فروشگاه انتشارات راه‌پرداخت نشانی: تهران، جنت‌آباد جنوبی، خیابان لاله غربی، روبه‌روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

فهرست

پیشگفتار

پول دقیقاً چیست؟ آیا پول یکی از مهم‌ترین دستاوردهای بشر است؟ فلسفه پول چیست؟ چه ارتباطی بین فلسفه، پول، بانکداری و رسانه‌ها وجود دارد؟ پول همان چرک کف‌دستی که بیشتر ما اکراه داریم اعتراف کنیم که بیشتر فعالیت‌هایمان برای کسب آن است، هنوز هم یک معما است. یک بچه سه‌ساله هم می‌تواند قدرت پول را درک کند، چیزی که با آن به بستنی یا اسباب‌بازی دلخواهش می‌رسد، اما درک ماهیت آن و کاری که می‌کند به این سادگی نیست. آیا پول فقط جسم است یا روح هم دارد؟ درک پول و کارکردش ما را پولدارتر نمی‌کند. بااین‌حال این موضوعی است که فیلسوف‌ها را درگیر خودش کرده و خواهد کرد. فیلسوف‌جماعت هم که قرار نیست با حکمت و فلسفه‌بافی پولدار شود، پس اگر حوصله مباحث فلسفی را دارید، خواندن این مطلب را ادامه دهید.

آیا پول پرده از جوهر درونی حیات برمی‌دارد؟

«راستی پول دقیقاً چیست؟ یک کوه نقره؛ آن‌طور که فاتحان اسپانیایی قاره آمریکا تصور می‌کردند؟ یا لوح‌های گلی و کاغذی که پول چاپی از آن حاصل شد؟ ما چگونه در جهانی زندگی می‌کنیم که پول بیش از آن‌که به چشم دیده شود، نامرئی و کوچک‌تر از اعدادی است که روی صفحه کامپیوتر می‌توانیم ببینیم؟ پول از کجا آمده است و به

کجا می‌رود؟» این سؤال‌ها را نیال فرگوسن در کتاب «برآمدن پول: تاریخ مالی جهان» مطرح می‌کند. گئورگ زیمل، جامعه‌شناس و فیلسوف آلمانی کتابی نوشته است با نام «فلسفه پول» که سال ۱۹۰۰ منتشر شد. زیمل می‌گوید: «پول از وضعیتی استثنایی بهره‌مند است.» به باور زیمل، پول بهتر از هر پدیده‌ای می‌تواند پرده از «جوهر درونی حیات» و «واقعیت اجتماعی سیال و درحرکت» بردارد. از یک‌سو پول پدیده‌ای جزئی و خاص است و از سوی دیگر کلی‌ترین و انتزاعی‌ترین شیء یا کالا محسوب می‌شود. پول کالایی بی‌شکل و انتزاعی است و می‌تواند همه‌چیز را به خود و خود را به همه‌چیز تغییر دهد. به عبارت دیگر هر چیزی را می‌توان با پول خرید و هر چیزی قابل تبدیل شدن به پول است.

سراب جامعه بدون پول

راستی اگر پول نبود چه می‌شد؟ آیا آینده ما به خطر می‌افتاد؟ بله! حتماً آینده ما به خطر می‌افتاد اگر که نمی‌توانستیم با چیزی مثل پول معامله کنیم؛ دلیلش سخت شدن مبادله‌ها است. فکرش را بکنید اگر پول نبود، آیا انگیزه‌ای می‌ماند برای بیشتر تلاش کردن و به دنبال خلاقیت و نوآوری رفتن؟ با وجود خدماتی که پول به بشر کرده است تا همین اواخر هم کسانی بودند که رؤیای جامعه بدون پول را در سر می‌پروراندند؛ کسانی مثل کمونیست‌ها و آنارشیست‌ها، مرتجعان افراطی، مذهبی‌های بنیادگرا و هیپی‌ها. انگلس و مارکس پول را ابزاری برای بهره‌کشی سرمایه‌دارها می‌دانستند که «رابطه پولی» جایگزین همه روابط انسانی حتی روابط خانوادگی شده بود. عقایدی که به این راحتی از بین نمی‌رود حتی تا دهه ۷۰ میلادی هم هنوز کمونیست‌هایی در اروپا بودند که علاقه‌ای به پول نداشتند.

با وجود این آمال، هیچ‌کدام از جوامع کمونیستی نتوانسته‌اند بدون پول کشور را مدیریت کنند؛ همین حالا در کره شمالی هم از پول برای مبادله استفاده می‌شود. در مورد جوامعی که از طریق شکار ارتزاق می‌کردند و از پول هم استفاده نمی‌کردند هم باید در نظر داشت که این جوامع هیچ‌وقت پیشرفت اقتصادی نداشتند که بخواهند نمونه و الگو باشند.

فرگوسن ماجرای قبیله‌ای به نام «نوکاک ماکو» در کلمبیا را تعریف می‌کند که سال‌های سال در انزوا و بدون ارتباط با جوامع انسانی زندگی می‌کردند و بالاخره در سال‌های اول قرن ۲۱ از جنگل‌های حاره‌ای آمازون دل بریدند و به‌طرف منطقه مسکونی سان‌خوزه دل‌گواویار سرازیر شدند. این مردم تصوری از پول نداشتند و فقط از طریق گوشت میمون، شکار و میوه گذران عمر می‌کردند. «امروز، آن‌ها در محوطه‌ای نزدیک شهر به سر می‌برند و برای ارتزاق به کمک‌های دولت اتکا دارند و در پاسخ به این سؤال که آیا دلشان برای جنگل تنگ نشده است، می‌خندند. بعد از یک‌عمر راهپیمایی سخت و دشوار از صبح تا شب برای پیدا کردن غذا، باورشان نمی‌شود کسانی که اصلاً نمی‌شناسندشان مایحتاجشان را تأمین می‌کنند بی آن‌که در عوض چیزی از آن‌ها بخواهند.»

طلا فقط زیبا نیست

پول آن‌قدر انگیزه می‌آورد که می‌تواند باعث از بین رفتن جوامع شود. قرن‌ها پیش، قبل از این‌که پول این‌قدر در دنیا فراگیر شود، جوامعی در دنیا بودند که در صلح و سعادت و بدون این‌که بویی از پول و قدرت آن برده باشند، زندگی می‌کردند. نمونه آن‌ها مردمانی که در سرزمین‌های امپراتوری اینکا، بافرهنگ‌ترین جامعه آمریکای جنوبی در پانصد سال پیش زندگی می‌کردند و هیچ درکی از پول نداشتند. در نظر آن‌ها ارزش طلا به سبب زیبایی آن بود. به دلیل نوع نظام اقتصادی از امپراتوری اینکا به‌عنوان یک تمدن کمونیستی یاد می‌شود.

سال ۱۵۳۲ میلادی بود که «پیزارو» اسپانیایی با همراهانش به «اینکا»ها حمله کرد تا فلزات گران‌بهای این قوم از همه‌جا بی‌خبر را تصاحب کند. قوم اینکا درک نمی‌کردند که چرا طلا و نقره این‌قدر اروپایی‌ها را جادو کرده است. مانکو کاپاک، رهبر آن‌ها در شکایت از پیزارو و افرادش می‌گفت: «اگر همه برف‌های رشته‌کوه آند هم تبدیل به طلا شود، آن‌ها باز هم سیر نمی‌شوند.» او نمی‌دانست ارزش طلا و نقره برای پیزارو فقط دلیل زیبایی‌شناختی ندارد، بلکه این فلزات می‌توانستند تبدیل به پول شوند؛ یعنی واحدی برای شمارش، اندوخته‌ای ارزشمند و قدرتی قابل‌حمل.

پول آنچه تصور می‌کنیم، نیست

پول با تمام خوبی‌هایی که دارد، به‌تنهایی نمی‌تواند سعادت جوامع را سبب شود؛ گرچه این جمله کمی شبیه به موضوع انشای دستمالی‌شده «علم بهتر است یا ثروت» شد، اما حقیقت این است که پول دوست‌داشتنی ما اگر به‌درستی مدیریت نشود، می‌تواند شکست جامعه و اقتصاد آن را در پی داشته باشد. همان اتفاقی که در اسپانیای قرن شانزدهم افتاد، آن‌قدر معادن نقره استخراج شد که این فلز ارزش و قدرت خریدش را نسبت به کالاهای دیگر از دست داد، در نتیجه در دوره زمانی صدساله بین سال‌های ۱۵۴۰ تا ۱۶۴۰ در تمام اروپا، دوره مشهور «انقلاب قیمت» حاکم بود؛ دوره‌ای که قیمت مواد غذایی که ۳۰۰ سال تمایلی به افزایش مستمر نشان نداده بود، به‌طور چشمگیر بالا رفت. به نظر می‌رسد اسپانیایی‌ها پیش از آن‌که کارکرد پول را درک کنند به تولید بیش‌ازحد آن پرداختند. آن‌ها نفهمیده بودند که ارزش فلز قیمتی، مطلق نیست. نمی‌دانستند که پول فقط ارزش چیزی را دارد که کسی حاضر باشد آن را در مقابلش به شما بدهد. افزایش عرضه آن جامعه را ثروتمندتر نمی‌کند، هرچند ممکن است حکومتی را که محصول پول را به انحصار درمی‌آورد، به ثروت برساند.

این همان تصور اشتباهی است که هنوز هم برخی سیاستمداران در دنیا در ذهن دارند و فکر می‌کنند با تزریق پول به جامعه مشکلات اقتصادی هم حل می‌شود. فرگوسن تعریفی از پول در کتابش ارائه داده است که کمی ماهیت این ابزار را روشن می‌کند: «پول موضوعی اعتقادی، حتی ایمانی است؛ اعتقاد به کسی که آن را به ما می‌پردازد؛ اعتقاد به کسی که پول مورداستفاده‌اش را چاپ می‌کند یا مؤسسه‌ای که برای چک‌ها یا انتقال‌هایش احترام قائل است. پول فلز نیست، پشتوانه‌ای مکتوب است و به نظر نمی‌رسد اهمیتی داشته باشد که کجا مکتوب شده است، روی نقره، روی گِل، روی کاغذ یا روی نمایشگر آب‌گونه شفاف. هر چیزی می‌تواند کار پول را بکند، از صدف کائوری جزایر مالدیو تا صفحات سنگی گرد بزرگ که در یِپ (یاپ)، مجمع‌الجزایری در اقیانوس اطلس، استفاده می‌شد و اکنون در عصر الکترونیک به نظر می‌آید که هیچ‌چیز نمی‌تواند کار پول را بکند.»

پول چگونه باعث شکل‌گیری فلسفه در یونان شد؟

حالا از زاویه فلسفه به پول نگاه کنیم، البته قصد ما بررسی فلسفی پول نیست بلکه می‌خواهیم ببینیم پول چه تأثیری روی فلسفه گذاشته است. فلسفه از شش قرن پیش از میلاد در یونان متولد شد؛ اما چرا یونان؟ متفکرانی هستند که می‌گویند پیدایش فلسفه در یونان به دلیل شکل‌گیری نهادهای قضاوت غیرشخصی و نهادهای دموکراتیک و برابری سیاسی شهروندان آتن است اما برخی دیگر مانند «سیفورد» و «شل» این را ربط می‌دهند به پول. به نظر می‌رسد باور سیفورد و شل درباره نقش پول در پیدایش فلسفه در یونان انقلابی‌تر باشد. علی معظمی، پژوهشگر و روزنامه‌نگار حوزه فلسفه، اردیبهشت‌ماه سال ۱۳۹۶ در نشستی در دانشگاه تهران درباره «پول و برآمدن متافیزیک» سخن گفت و این موضوع را روشن کرد.

معتقدان به تأثیر پول و نه دموکراسی در پیدایش فلسفه می‌گویند دموکراسی مدت‌ها پیش از طرح دیدگاه‌های متافیزیکی وجود داشته است و فیلسوف‌ها هم آن زمان خارج از آتن و دور از دموکراسی و تحت سیستمی جبار زندگی می‌کردند. از طرف دیگر سخنان این متفکران از لحاظ فرم و محتوا با فضای بحث آزاد یا نهادهای دموکراتیک همخوانی ندارد و با توجه به این سخنان به نظر نمی‌رسد آن‌ها در شرایط آزادی سیاسی این حرف‌ها را زده باشند. به قول سیفورد «آدم‌ها ممکن است خارج از سیاست زندگی کنند اما خارج از اقتصاد، نه.»

از رواج پول تا رواج فلسفه

پول چگونه در یونان رواج یافت؟ در قرن هشتم تا ششم پیش از میلاد، معابد و نذورات باعث انباشته شدن ثروت و به‌ویژه فلزات قیمتی شد؛ بنابراین مبادله با سکه به‌جای مبادله کالا با کالا رواج یافت. خیلی طول نکشید که دولت‌ها هم به این نکته پی بردند که سکه بهترین وسیله برای پرداخت مزد سربازها و دریافت مالیات و جریمه است.

رواج پول نه‌تنها زندگی افراد را تحت تأثیر قرار می‌دهد بلکه از نظر ذهنی هم

تاثیری عمیق دارد. در ادبیات یونان آن زمـــان برای پول تعاریفی به کار می‌رود مانند پول چیزی است همگن، غیرشـــخصی، مطلوب همگان، پول قدرت بی‌حدومرزی دارد، جمع‌کننده اضداد است چون ماهیتی مجسم دارد اما به آن فرو کاسته نمی‌شود، هم جنبه کالایی دارد و هم انتزاعی اســـت و هیچ‌چیز شـــبیه به پول نیست. به گفته سیفورد این‌ها توصیفاتی هســـتند که تا پیش از پیدایش پول برای هیچ‌چیز دیگری یافت نمی‌شوند.

نکته جالب این‌که در تفکرات فلسفی اولیه صفت‌هایی برای توصیف جهان به کار رفته‌اند که شبیه همین صفت‌های پول هستند. سیفورد با ذکر نمونه‌های متعدد این ادعا را شرح می‌دهد که زمینه شکل‌گیری نگاه متافیزیکی در یونان، اقتصادی تحول‌یافته و به وجود آمدن پول در معنای جدید آن بوده است؛ با برآمدن پول همگن، شکل‌گیری مفاهیم جدید در ذهن ممکن شـــده است؛ سیفورد مدعی اســـت که در یونان پول الهام‌بخش ذهنیت متافیزیکی بوده است.

سوفیست و جبار

اما مارک شل از جنبه دیگری به ارتباط میان پول و فلسفه نگاه می‌کند. شل با بیان روایت‌هایی از یونان باســـتان به این نکته اشاره می‌کند که با داشتن قدرت انجام کار بدون دیده شدن؛ قدرت عمل نامرئی، انسان از هرگونه قید اخلاقی که جامعه بر او گذاشته است، رها می‌شـــود. نامرئی بودن اجازه می‌دهد بدون این‌که به شخص یا اعتبارش لطمه‌ای وارد شود، دست به اعمال شرورانه بزند.

جادوی نامرئی شـــدن چیســـت؟ پول. «پیش از پول معاملات دیدنـــی بودند، با ســـمبل‌هایی که جزئی از آن‌ها بین دو طرف ردوبدل می‌شـــد و در حضور شاهدان حاضر انجام می‌شدند. پول معاملات را نادیدنی می‌کرد چون معامله بی‌شاهد انجام می‌شد و پول، نشانی را از کسی که خرج کرده بود، حمل نمی‌کرد پس منشأ و مقصد خرج کردنش پوشیده می‌ماند.» بنابراین پول ابزاری بود که قدرت نادیدنی می‌آورد.

افلاطون در کتاب «جمهور» خود به دو اصل می‌پـــردازد که همواره در نزاع با هم هستند: پول و فلسفه؛ دو اصلی که حامل ارزش‌اند. «پول ارزش مبادله دارد و فلسفه

ارزش حقیقی. با استفاده از این دو، دو گروه جباران و سوفسطاییان حقیقت را پنهان می‌کنند. سوفسطاییان حقیقت را همچون کالا می‌کنند و جبار پشت روابط نادیدنی قرار می‌گیرد.»

«سوفیست نشـــان داد که حکمت را می‌توان با پول خرید. به‌این‌ترتیب پول معیار حکمت شد. پول تعیین کرد چه حکمتی رواج یابد. درحالی‌که برای فیلسوف، خیر اصل اساسی است، برای سوفسطایی کاسب‌کاری اصل است.»

بانکداری و رسانه‌داری چه شباهتی به هم دارند؟

باورمان نمی‌شـــود اگر بگویند کار جایی مثل روزنامه دنیای اقتصاد یا شبکه‌های صداوسیما یا حتی یوتیوب شبیه به کاری اســـت که بانک‌ها می‌کنند؛ ولی باید باور کنیم. دیدگاه‌هایی وجود دارد که می‌گوید رسانه‌ها کاری شبیه به مؤسسات مالی انجام می‌دهند. اگر بانک‌ها با ابزاری به نام «پول» کار می‌کنند، چرخ رسانه‌ها نیز با مفهومی به نام «توجه» می‌چرخد.

برای این‌که اهمیت توجه را درک کنیم باید ببینیم عصب‌شناســـان و روان‌شناسان شناختی چه نظری در مورد آن دارند. عصب‌شناسان تخمین زده‌اند از ۱۰ به توان ۹ بیت اطلاعاتی که هر ثانیه از طریق حواس وارد مغز انسان می‌شود، ۱۰ به توان ۲ بیت آن موردتوجه قرار می‌گیرد. همان‌طور که دکتر علی‌اکبر فرهنگی، استاد مدیریت و ارتباطات می‌گوید این محدودیت انسان برای نشان دادن توجه به این معنی است که میزان توجه موجود در جهان، به‌یقین محدود است. توجه بیشتر به یک موضوع، ضمن اشغال بخشی از توانایی محاسبه‌ای مغز باعث اختصاص میزان کمتری توجه به دیگر موضوعات می‌شود. برخی همچون «مایکل گلدهابر» از متخصصان مطالعات تغییرات اجتماعی در موسسه برکلی دانشگاه کالیفرنیا، پول توجه را در کنار دو نوع دیگر پول رایج در اقتصاد یعنی پول صنعتی و پول اعتباری (سرمایه‌ای) معرفی می‌کنند.

مقایسه کار بانک‌ها و رسانه‌ها

حالا که ارزش توجه مشخص شـــد، می‌توانیم کار رســـانه‌ها و بانک‌ها را با هم

مقایسه کنیم. اگر بانک‌ها کارشان جمع‌آوری سرمایه‌های خرد و کسب درآمد از این سرمایه‌هاست، کار رسانه هم جلب‌توجه مخاطبان است تا سرمایه‌ای بزرگ از توجه را جمع کند و آن را به متقاضیان ارائه دهـــد. همان‌طور که فرهنگی می‌گوید: «نقش رسانه‌ها در یکپارچه‌سازی منابع توجهی و انتقال آن از سطح فردی به فضای عمومی جامعه، همانند نقش مراکز مالی در جمع‌آوری و انتقال ســـرمایه‌های خرد به سطح کلان اقتصاد است.» اگر بانک‌ها می‌کوشند مشتری و سرمایه آن را جذب خود کنند، رسانه‌ها هم در تلاش برای جذب مخاطب بیشتر و در نتیجه توجه بیشتر هستند تا این توجه را به آگهی‌دهندگان بفروشند.

شباهت بانک‌ها و رسانه‌ها از زبان میکیس تئودوراکیس

میکیس تئودوراکیس شباهت بانک‌ها و رسانه‌ها را به زبانی دیگر بیان می‌کند. او ادعا می‌کند یهودیان برای افزایش نفوذ و قدرتشـــان بانک‌های بزرگ و رسانه‌های آمریکا را قبضه کرده‌اند. رســـانه‌داری و بانکداری به باور این آهنگســـاز بلندآوازه یونانی، قدرتی به ارمغان می‌آورد که سبب شده است یهودیان آمریکا بیشتر بانک‌ها و رسانه‌های عمومی آمریکا را قبضه کنند؛ یعنی جیب و مغز آمریکاییان در دست آنان اســـت. تئودوراکیس که تاکنون چند بار نماینده پارلمان یونان و یک بار وزیر کابینه این کشور بوده است، ســـال ۲۰۰۴ اظهارات خود درباره تسلط یهودیان بر رسانه‌ها و بانک‌های آمریکا را بیان کرد که این اظهارات برای او و دولت یونان سنگین تمام شد زیرا پس از آن یهودیان آمریکا مانع برگزاری کنسرت‌هایش در آن کشور شدند و به‌علاوه، چون دولت یونان درخواست انجمن‌های یهود را برای اعلام برائت نسبت به صحبت‌های تئودوراکیس نپذیرفت، آن‌ها مســـافرت به این کشـــور توریستی را محدود کردند.

درک ارز رمزنگاری‌شـــده و فرار از همه شـــطحیات ناتمام این روزها

این روزها همه می‌خواهند ارز رمزنگاری‌شده خلق کنند. از بانک مرکزی گرفته

تا نهادهای پژوهشی و کسب‌وکارهای مختلف. با این حال مفاهیمی که آنها در حال صحبت درباره آن هستند به هم ریخته است و چیزی که از آن صحبت می‌کنند، گاهی هیچ ربطی به ارزهای رمزنگاری‌شده ندارد. واقعیت این است که بیشتر از ۱۰ سال از زمانی که بیت‌کوین برای اولین بار مطرح شد، نمی‌گذرد؛ اما در یکی، دو سال اخیر و بعد از سروصداهای فراوانی که درباره آن درست شده، هم در ایران و هم در سایر نقاط جهان حکومت‌ها و به‌طور خاص بانک‌های مرکزی و نهادهای مرتبط با آنها نسبت به این مفهوم حساس شده‌اند. هرچند وقت‌یک بار واژه‌هایی می‌شنویم که دقیقاً نمی‌دانیم منظورشان چیست و بعد از بررسی واژه‌ها متوجه می‌شویم که گوینده چند مفهوم را با هم قاطی کرده است و خواسته همگام با مسائل روز چیزی بگوید که متأسفانه نتیجه یک کمدی تراژدی شده است؛ از این دست ترکیب‌های افتضاح، ارز رمزنگاری‌شده ملی است. اساساً وقتی در عالم ارزهای رمزنگاری‌شده صحبت می‌کنیم، چیزی به نام ملی یا حتی دولتی وجود ندارد و نهایتاً ما با ارزهای رمزنگاری‌شده بانک‌های مرکزی طرفیم نه چیزی دیگر. برای درک اینکه چرا بسیاری از مطالبی که این روزها می‌شنویم شطحیات است، به کمک مقاله خوبی که یک سال پیش درباره ارزهای رمزنگاری‌شده بانک‌های مرکزی منتشر شده است، مفاهیم را باز می‌کنیم. این را هم اضافه کنم که این متن بخشی از یک مطلب طولانی است که در راه پرداخت منتشر می‌شود.

ارزهای رمزنگاری‌شده بانک‌های مرکزی

بانک تسویه حساب‌های بین‌المللی سازمانی بین‌المللی است که همکاری و مشارکت‌های پولی و مالی را تقویت می‌کند و به‌عنوان یک بانک به بانک‌های مرکزی، خدمات می‌دهد. این نهاد در ۱۷ مه ۱۹۳۰ میلادی تأسیس شد و قدیمی‌ترین سازمان مالی بین‌المللی جهان به‌شمار می‌رود. از آنجا که مشتریان بانک تسویه بین‌المللی را بانک‌های مرکزی کشورها و سازمان‌های بین‌المللی تشکیل می‌دهند، این نهاد از افراد و شرکت‌های خصوصی سپرده نمی‌گیرد و به آنها خدمت‌رسانی مالی نمی‌کند. یک سال پیش این نهاد مستندی منتشر کرد که یک دسته‌بندی فوق‌العاده از انواع پول در

آن است. این مستند برای همه کسانی که می‌خواهند منطق پول را درک کنند، بسیار جالب توجه است. گل این مستند دیاگرامی است به نام گل پول. این دیاگرام با یک بخش‌بندی همه انواع پول را دسته‌بندی کرده است و به ما کمک می‌کند در این فضای آشفته بتوانیم سره را از ناسره تشخیص دهیم.

بادکنک ارزهای رمزنگاری‌شده

هر روز یک ارز رمزنگاری‌شده جدید معرفی می‌شود؛ نهادهای مختلف دولتی و حاکمیتی هر روز بیشتر علاقه پیدا می‌کنند که نقشی در این میان داشته باشند. خصوصاً بانک‌های مرکزی در جهان و البته ایران به این فکر افتاده‌اند که حضور اثربخش‌تری در این حوزه داشته باشند. برخی از دولت‌ها و بانک‌های مرکزی هم به این فکر افتاده‌اند که ارز رمزنگاری‌شده خودشان را منتشر کنند که در ایران با عنوان «ارز رمزنگاری‌شده ملی» در محافل از آن یاد می‌شود. در این یادداشت می‌خواهیم به این موضوع بپردازیم که ارز رمزنگاری‌شده بانک مرکزی (نه ملی) چیست و چه ویژگی‌هایی دارد؟ و مهم‌تر از همه اینکه چه کاربردهایی دارد. در این متن طبقه‌بندی کاربردی از پول ارائه شده که به ما کمک می‌کند انواع ارزهای رمزنگاری‌شده بانک‌های مرکزی (برای پرداخت‌های خرد و درشت) و تفاوت آن با دیگر انواع فرم‌های پول‌های بانک‌های مرکزی مانند پول نقد (اسکناس و سکه) و سپرده‌های بانکی را درک کنیم. در این متن ویژگی‌های متفاوت ارزهای رمزنگاری‌شده بانک‌های مرکزی و دیگر روش‌های پرداخت را بررسی خواهیم کرد.

غوغای بیت‌کوین

۱۰ سال زمان بیشتر لازم نبود تا بیت‌کوین از موضوع جمعی کوچک به پدیده‌ای جهانی تبدیل شود. ارزش آن افزایش یافته، بالا و پایین داشته و از چند سنت به حدود هشت هزار دلار رسیده است. در این سال‌ها هزاران ارز رمزنگاری‌شده مانند بیت‌کوین معرفی و عرضه شده است. بیت‌کوین و فامیل‌هایش پادشاهی ارزهای سنتی را به لرزه درآورده‌اند و مفاهیمی مانند بلاکچین و دفتر کل توزیع‌شده را به موضوعات

بررسی محافل تخصصی کشانده‌اند. سرمایه‌گذاران خطرپذیر و موسسه‌های مالی در زمینه پروژه‌های دفاتر کل توزیع‌شده سرمایه‌گذاری کرده‌اند و به دنبال این هستند که شیوه تعامل ما با پول را تغییر دهند. بلاگرها، بانکدارهای مرکزی و دانشگاهیان پیش‌بینی می‌کنند که یک تحول یا دگردیسی در پرداخت، بانکداری و سیستم‌های مالی را شاهد خواهیم بود. بانک‌های مرکزی و موسسه‌های پژوهشی با سروصدا اعلام می‌کنند که قصد ورود به این حوزه را دارند و می‌خواهند ارزهای رمزنگاری‌شده بانک مرکزی یا ارزهای دیجیتال خود را ایجاد کنند. در میان این همه هیاهو درک واقعیت هر روز سخت و سخت‌تر می‌شود. بحث‌هایی که شکل می‌گیرد، معمولاً بر مبانی و اصول اشتباه استوار شده و بسیاری از مفاهیم اشتباه درک شده است. در این متن قرار است به یک سؤال ساده پاسخ دهیم؛ ارز رمزنگاری‌شده بانک مرکزی چیست؟ یا وقتی از ارز رمزنگاری‌شده بانک مرکزی صحبت می‌کنیم، داریم درباره چه چیزی حرف می‌زنیم؟

در پایان یک طبقه‌بندی کاربردی از پول معرفی می‌کنیم که بر پایه چهار ویژگی ساخته شده است؛ صادرکننده (بانک مرکزی یا دیگران)، فرم (الکترونیکی یا فیزیکی)، دسترسی (جهانی یا محدود) و مکانیسم انتقال (متمرکز یا غیرمتمرکز). برمبنای این طبقه‌بندی ارزهای رمزنگاری‌شده بانک‌های مرکزی یک فرم الکترونیکی از پولی هستند که بانک‌های مرکزی صادر می‌کنند و می‌توانند به شیوه غیرمتمرکزی مبادله شوند و افراد آن را به هم منتقل کنند؛ به عبارتی تراکنش‌های بین افراد به‌صورت مستقیم انجام می‌شود و پرداخت‌کننده و دریافت‌کننده بدون نیاز به حضور یک واسطه تراکنش‌هایشان را انجام می‌دهند. این تعریف مرزی بین این مفهوم و دیگر انواع پول‌های بانک مرکزی مانند سپرده‌های بانکی می‌کشد که برای تبادل آنها نیاز به یک سیستم مرکزی وجود دارد. برمبنای این طبقه‌بندی دو نوع ارز رمزنگاری‌شده بانک‌های مرکزی قابل شناسایی است؛ نوعی که به‌صورت گسترده قابلیت پذیرش دارد و برای مصارف خرد و روزمره قابل استفاده است و نوع محدودشده که در واقع برای تسویه مبالغ درشت استفاده می‌شود.

این دو نوع ارز رمزنگاری‌شده بانک‌های مرکزی چه چیزی دارند که دیگر انواع

پول‌های بانک‌های مرکزی ندارند؟ در واقع از این طریق به کاربران و مردم این امکان را می‌دهیم که به‌صورت ناشناس در بسترهای دیجیتال پول جابه‌جا کنند، دقیقاً مانند پول نقد. اگر ناشناس بودن اهمیتی نداشته باشد، این مفهوم دیگر اهمیتی ندارد.

اما نوع دوم ارز رمزنگاری‌شده بانک مرکزی قصه دیگری دارد. وقتی درباره تسویه و تصفیه مبالغ درشت صحبت می‌کنیم، ویژگی ناشناس بودن مانند پول نقد مطرح نیست. چون در این حالت تراکنش‌ها برای سیستم مرکزی قابل مشاهده هستند. موضوع مهم در این دسته بهبود کارایی و بهره‌وری و کاهش هزینه‌های تسویه است. پاسخ به سوال‌های این بخش بستگی به مسائل فنی دارد که باید بررسی و حل شوند. برخی از بانک‌های مرکزی در این زمینه فعالیت‌هایی انجام داده‌اند، اما هنوز جایی اعلام نکرده که به‌صورت کامل آماده پذیرش این فناوری است.

در ادامه طبقه‌بندی مقاله‌ای که گفته شد از پول را بررسی می‌کنیم. در ادامه ویژگی‌های دو نوع ارز رمزنگاری‌شده، خرد و درشت بانک مرکزی را بررسی خواهیم کرد. مثال‌ها و پروژه‌هایی که اکنون در حال جلو رفتن هستند را هم بررسی می‌کنیم و برخی از مسائلی را که بانک‌های مرکزی باید بررسی و حل کنند بیان می‌کنیم.

یک فرم جدید از پول بانک مرکزی

بیت‌کوین و آلت‌کوین (جایگزین‌ها و رقبای بیت‌کوین) نوع جدیدی از پول را به ما معرفی کردند. گزارشی مربوط به سال ۲۰۱۵ سه ویژگی برای ارزهای رمزنگاری‌شده معرفی کرده است؛ آن‌ها الکترونیکی هستند؛ هیچ فردی مسئولیتی درباره آنها به عهده نمی‌گیرد و تبادلات فردبه‌فرد را ممکن می‌کنند. ارزهای رمزنگاری‌شده با استفاده از دفترکل توزیع‌شده امکان انتقال ارزش الکترونیکی به‌صورت فردبه‌فرد از راه دور را ممکن می‌کنند؛ آن هم در غیاب اعتماد بین دو طرف معامله. معمولاً فرم الکترونیکی پول برای تبادل نیاز به زیرساخت متمرکز دارد که یک واسطه مورد اعتماد نقش تسویه و تصفیه تراکنش‌ها را بازی کند. تا پیش از ارزهای رمزنگاری‌شده تبادلات نفربه‌نفر محدود به فرم فیزیکی پول یعنی سکه و اسکناس بود.

برخی و نه همه این ویژگی‌ها را دیگر فرم‌های پول داشتند. پول نقد قابل استفاده

به‌صورت نفربه‌نفر است، اما الکترونیکی نیست و بانک مرکزی ارزش آن را ضمانت کرده اســـت. ســـپرده‌های بانکی هم ضمانت بانک‌ها و بانک‌های مرکزی را پشت خودشان دارد. تبادلاتی که بین بانک‌ها انجام می‌شود هم در سیستم متمرکزی جلو می‌رود. برخی پول‌های کالایی (کومودیتی) مانند طلا، سکه‌ها و شمش‌های طلا و دیگر انواع آن قابل استفاده به‌صورت فردبه‌فرد هســـتند اما هیچ‌کسی ارزش آنها را تضمین نکرده و الکترونیکی هم نیستند.

بنابراین برای تعریف ارزهای رمزنگاری‌شده بانک‌های مرکزی باید بگوییم آنها نوعی از تعهد الکترونیکی بانک‌های مرکزی هســـتند که قابلیت استفاده نفربه‌نفر را دارند. منتها این تعریف یک ویژگی مهم دیگر فرم‌های پول‌های بانک مرکزی را نادیده گرفته است؛ دسترسی یا دسترس‌پذیری. در حال حاضر یک نوع از پول بانک مرکزی یعنی اسکناس و سکه برای همه قابل دســـترس هستند، در حالی که تسویه و تصفیه بین حساب‌ها و سپرده‌های بانکی معمولاً محدودیت دارند و صرفاً بانک‌ها می‌توانند تراکنش‌هایی مبتنی بر این سپرده‌ها انجام دهند. به عبارتی وقتی فردی سپرده‌ای در بانکی دارد برای انتقال آن به فرد دیگر نیاز به سیستم بانکی دارد، در حالی که در پول نقد این نیاز وجود ندارد. در این زمینه تعریف دیگری وجود دارد که پول‌ها را از منظر دسترسی تقسیم‌بندی می‌کند. پول‌هایی که به‌صورت گسترده و جهانی قابل دسترسی هستند؛ یعنی به دست آوردن و استفاده از آنها ساده است و سپرده‌های دیجیتالی که در بانک‌ها نگه‌داری می‌شوند.

با ترکیب این تعاریف یک طبقه‌بندی جدید از پول ارائه می‌کنیم. ویژگی‌های مورد نظر برای طبقه‌بندی این موارد اســـت: صادرکننده (بانک مرکـــزی یا دیگران)؛ فرم (الکترونیکی یا فیزیکی)؛ دسترسی (جهانی یا محدود) و مکانیسم انتقال (متمرکز یا غیرمتمرکز مثلاً امکان انتقال فردبه‌فرد). این طبقه‌بندی بین دو نوع ارز رمزنگاری‌شده بانک مرکزی تمایز ایجاد می‌کند؛ هر دو آنها الکترونیکی هستند، بانک‌های مرکزی آنها را صادر می‌کنند و قابل استفاده به‌صورت نفربه‌نفر هستند. یک دسته قابل استفاده برای عامه مردم است (خرد) و یک دســـته فقط قابل استفاده برای موسسه‌های مالی

است (درشت). برای درک این موضوع یک دیاگرام ون به‌خوبی به ما کمک می‌کند که ماجرا را درک کنیم. برای این موضوع چهار بیضی که به آن گل پول می‌گوییم به ما مرز و تمایز دو نوع ارز رمزنگاری‌شده را نشان می‌دهد.

در عمل چهار نوع از پول الکترونیکی بانک مرکزی وجود دارد؛ دو نوع از ارز رمزنگاری‌شده بانک مرکزی و دو نوع از سپرده‌های بانکی. آشناترین نوع سپرده‌های بانک مرکزی سپرده‌های مردم در بانک‌های تجاری هستند. حساب‌های قرض‌الحسنه یا حساب‌های سرمایه‌گذاری بلندمدت و کوتاه‌مدت. نوع دیگر به‌صورت تئوری سپرده‌هایی هستند که بخش‌های عمومی آن را مدیریت می‌کنند مانند اوراق مشارکت.

فرم در دسترس جهانی پول که توسط بانک مرکزی صادر نشده و به‌صورت خصوصی خلق شده، مواردی مانند ارزهای رمزنگاری‌شده، پول کالایی، سپرده‌های بانک‌های تجاری و پول موبایلی است. ارزهای رمزنگاری‌شده بانک مرکزی در دو نوع هستند که در یک ویژگی با هم تفاوت دارند. ارزهای محلی یا فیزیکی به‌عنوان‌مثال ارزهایی که در یک منطقه جغرافیایی خاص یا در سازمان‌ها و جوامع مشخص قابل استفاده هستند در بخش بالا و سمت راست گل مشخص شده‌اند. در آن بالا ارزهای مجازی را داریم که طبق تعریف پول الکترونیکی هستند که معمولاً توسط توسعه‌دهندگانی که آن را صادر می‌کنند کنترل می‌شود. موارد مصرف ارزهای مجازی در جوامع یا موجودیت‌های مجازی است. همچنین نوع دیگری از ارزهای رمزنگاری‌شده خصوصی برای مبالغ درشت وجود دارد. این نوع خاص قابلیت انتقال فردبه‌فرد را از طریق دفتر کل توزیع‌شده دارد، منتها به‌جای افراد موسسه‌های مالی از این مدل استفاده می‌کنند.

در ادامه این طبقه‌بندی و مثال‌های آن را از گذشته تا امروز و آینده شرح می‌دهیم.

مثال‌ها

ارز رمزنگاری‌شده بانک مرکزی (خرد): با فدکوین شروع می‌کنیم. این مفهوم اولین بار سال ۲۰۱٤ توسط کونینگ خلق شد و توسط فدرال رزرو تأیید نشد که از طریق آن ارز رمزنگاری‌شده بانک مرکزی خلق شود. فدکوین می‌تواند در کنار پول نقد و

سپرده‌های بانکی سه ستون پول دولتی را بسازند.

ارز رمزنگاری‌شـــده بانـــک مرکزی (درشـــت): کَدکویـــن مثالـــی از ارزهای رمزنگاری‌شده درشت بانک‌های مرکزی است. این نامی است که برای دارایی‌های دیجیتال بانک کانادا استفاده می‌شـــود. بانک کانادا این مفهوم را در تعامل با سیستم پرداخت کانادا، کنسرسیوم R3 و تعداد زیادی از بانک‌های کانادایی پیش برده است.

حساب‌های سپرده ارزی: دینرو الکترونیکو خدمت پرداخت موبایلی است که در اکوادور کاربرد دارد و بانک مرکزی پشتیبان آن است. شهروندان اکوادوری می‌توانند به‌سادگی و با دانلود یک اپلیکیشن و با کمک شماره ملی و پاسخ به چند سؤال امنیتی یک حساب باز کنند. آن‌ها می‌توانند از طریق اپلیکیشن پول در حسابشان بگذارند یا حتی به کمک آن در محل‌های طراحی‌شده برای انجام تراکنش پول بردارند.

ارز رمزنگاری شده: بیت‌کوین مثالی از ارز دیجیتال غیر بانک‌های مرکزی است. این ارز توسط برنامه‌نویس ناشناسی به نام ساتوشی ناکاموتو توسعه داده شده و نرم‌افزار متن‌باز آن در سال ۲۰۰۹ همراه با وایت پیپری که ویژگی‌های فنی طراحی‌اش را شرح داده بود منتشر کرد.

ارز مجازی: پوک‌کوین ارزی اســـت که برای خریدهای درون بازی پوکمون‌گو استفاده می‌شود و مثالی از ارز مجازی است.

ارز رمزنگاری‌شده (درشت): سکه تســـویه یوتیلیتی (USC) مثال از تلاش بخش خصوصی برای ایجاد ارز رمزنگاری‌شده عمده است. این مفهومی است که توسط همراهی و همـــکاری بانک‌های خصوصی و کســـب‌وکارهای فین‌تک برای ایجاد توکن‌های دیجیتالی اســـت که برای تبادل از طریق پلتفرم دفتر کل توزیع‌شـــده در کشورهای مختلف استفاده می‌شود.

بانک آمستردام در سال ۱۶۰۹ برای تسهیل تجارت ایجاد شد. اولین بار این بانک مرکزی سپرده‌هایی مردم را گرفت و به آنها رسید داد. تاجران و مردم از این رسیدها برای مبادله استفاده می‌کردند و این اولین بار بود که مفهوم پول به صورت امروزی خلق شد. بانک مرکزی آلمان سال ۱۸۱۴ تأسیس شد و بانک آمستردام در سال ۱۸۲۰

تعطیل شد.

سال ۱۹۳٤ طلاهایی که معادل ۱۰۰ هزار دلار بود توسط خزانه‌داری آمریکا خلق شد که صرفاً برای تراکنش‌های رسمی بین بانک‌های فدرال رزرو استفاده می‌شد. این درواقع باارزش‌ترین اسکناس دلاری است که ایجاد شده و کاربرد عمومی پیدا نکرد این اسناد نمونه‌هایی از پول غیرالکترونیکی، محدود، با پشتیبانی دولت و قابل استفاده به صورت نفربه‌نفر بود.

ارزهای محلی: پوند بریستول یک مثال از ارزهای محلی است که در فروشگاه‌ها و برای پرداخت‌های خرد قابل استفاده است.

پول کالایی: سکه‌های طلا مثال‌هایی از پول کالایی هستند. این طلا هم می‌تواند برای تولید استفاده شود و هم به عنوان وسیله مبادله قابلیت استفاده دارد. پول کالایی مفهومی مربوط به گذشته است و این روزها صرفاً در مواردی مانند مهریه استفاده می‌شود.

پول موبایلی: ای‌گولد، ام‌پسا و ونمو نمونه‌هایی از پول موبایلی و سپرده‌های بانکی هستند. این ابزارها امکان انتقال پول بین افراد از طریق پیام‌های متنی را فراهم می‌کنند.

و در پایان

هیچ‌گاه به اندازه امروز مفهوم پول مورد توجه قرار نگرفته بود. اکنون که تکنولوژی به این عرصه ورود کرده است ما شاهد تغییرات شگرفی خواهیم بود و قطعاً در سال‌های آینده درک ما از مفاهیمی مانند ارزش، ثروت، قیمت، دارایی و سرمایه تغییر خواهد کرد. حتی اگر فرض کنیم که چیزی به نام بیت‌کوین هم شکست بخورد ما دیگر به روزهای سابق باز نخواهیم گشت. دریچه‌ای که ساتوشی ناکاموتو به روی ما باز کرد حتی در صورت شکست خوردن خبر از دنیای دیگری داد که مطمئناً در سال‌های آتی به سمت این دنیا می‌رویم. آن چیزی که در پس همه اتفاق‌های این روزها ارزش توجه دارد این است که متوجه شدیم می‌شود جور دیگر زندگی کرد؛ می‌شود جور دیگر تجارت کرد. به عبارتی هر آن چه که تا امروز در ذهن‌مان کرده بودیم را باید بیرون بریزیم و به دنیای قشنگ نو سلام کنیم. راه دور است و بیابان در

پیش. خوشحالیم که با تلاش تیمی خستگی ناپذیر در راه پرداخت کتاب «بلاکچین و قانون» منتشر شد. لازم اســـت از همه همکارانمان در راه پرداخت که با همکاری آنها این کتاب آماده و منتشر شد تشکر کنیم. امیدواریم بتوانیم این راه را ادامه دهیم.

رضا قربانی /مینا والی /رسول قربانی

مقدمه

در سال ۱۹۸۸، تیموتی می، یکی از بنیان‌گذاران جنبش «سایفرپانک»[1]، هشدار داد که «هیولایی در حال ایجاد رعب و وحشت در دنیای مدرن است». این هیولا نه تروریسم سیاسی، نه کشمکش نژادی و نه بحران زیست‌محیطی است. در عوض، رشد و انبساط شکل جدیدی از هرج‌ومرج است که می آن را به‌صورت «هرج‌ومرج رمزی»[2] تعریف کرد. آن‌طور که می در اثر خود با نام «رساله هرج‌ومرج‌گرایان رمزی»[3] توضیح می‌دهد، اینترنت و پیشرفت‌ها در رمزنگاری کلیدی عمومی – خصوصی به‌زودی افراد را قادر می‌سازد تا به‌صورت ناشناس‌تر با یکدیگر ارتباط و تعامل داشته باشند. با تکیه بر شبکه‌های غیر قابل ردیابی و «جعبه‌های مهر و موم‌شده[4] اجرای پروتکل‌های رمزنگاری»، افراد می‌توانند «کسب‌وکار و قراردادهای الکترونیکی خود را بدون نیاز به دانستن نام حقیقی یا هویت قانونی طرف مقابل اجرا کنند».

در پایان، «می» پیش‌بینی کرد که افراد از این وضعیت رها می‌شوند و همین امر باعث تغییر کامل «ذات قوانین دولتی، توانایی در پرداخت مالیات و کنترل مراودات اقتصادی و توانایی در مخفی نگه‌داشتن اطلاعات می‌شود» و مفاهیمی نظیر اعتماد و شهرت نیز

1. cypherpunk
2. crypto anarchy
3. Crypto Anarchist Manifesto
4. tamper- proof boxes

حفظ می‌شـــود. پروتکل‌های امنیتی رمزی باعث از رده خارج‌شدن «سیم‌خارداری» می‌شود که به‌واسطه مالکیت فکری ایجاد شده است، جریان اطلاعات آزاد می‌شود، افراد با توانایی نوینی برای خودسازمان‌دهی آشنا می‌شوند و تمامی جنبه‌های شرکت‌های تجاری و دولت‌ها تغییر می‌کند. از دیدگاه می، این گسترش گریزناپذیر است. آن‌طور که او در نوشته‌های بعدی‌اش توضیح می‌دهد؛ «غول چراغ جادو بیرون آمده است» و چیزی جلودار موج سهمگین هرج‌ومرج فناورانه نیست.

از بسیاری جهات، بلاکچین‌ها[1] جعبه‌های مهر و موم‌شده‌ای هستند که ایده آن تقریبا ۳۰ سال پیش توسط می بیان شد. آنها چندین فناوری را با یکدیگر ترکیب می‌کنند که از جمله می‌توان به شبکه‌های همتابه‌همتا، رمزنگاری کلید عمومی ـ خصوصی و مکانیسم اجماع[2] اشاره کرد. از این فناوری‌ها برای ایجاد چیزی استفاده می‌شود که می‌توان آن را پایگاه داده ضدتغییر و بســـیار ارتجاعی در نظر گرفت که افراد در آن قادرند داده‌ها را به‌شیوه‌ای شـــفاف و تغییرناپذیر ذخیره کنند و به‌طور نیمه‌ناشناس وارد بسیاری از تراکنش‌های اقتصادی شوند. بلاکچین، انتقال ارز دیجیتال، دیگر دارایی‌های ارزشمند، مدیریت مالکیت اموال و اسناد حســـاس را فراهم می‌کند و احتمالا ایجاد فرایندهای رایانه‌ای را که به قراردادهای هوشمند مشهور هستند، تسهیل می‌کند و می‌توان آن را به‌طور خودمختار اجرا کرد.

بلاکچین، متفاوت از پایگاه‌های داده‌ای ابتدایی عمل می‌کند. در این حالت، آنها به‌طور متمرکز نگهداری نمی‌شوند. آنها را به‌طور جمعی و به‌واسطه شبکه‌ای همتابه‌همتا از رایانه‌ها مدیریت می‌کنند (که به آنها همتایان یا گره‌ها[3] می‌گویند). در اغلب موارد نیز در سراسر دنیا پراکنده هستند. این گره‌ها نسخه‌ای دقیق یا تقریبا دقیق از بلاکچین را ذخیره می‌کنند و با استفاده از پروتکل نرم‌افزاری که به‌طور مشخص چگونگی ذخیره‌سازی اطلاعات، انجام تراکنش‌هـــا و اجرای کدهای نرم‌افزاری را برای شـــبکه‌های فرایند مشخص کرده‌اند، بین آنها هماهنگی ایجاد می‌کنند.

---

1. BlockchAIns
2. consensus mechanisms
3. nodes

از آنجا که بلاکچین به‌طور گسترده تکثیر می‌شود، هر نوع داده ذخیره‌شده در بلاکچین به‌شدت ارتجاعی است و می‌تواند باقی بماند، حتی اگر نسخه‌ای از بلاکچین خراب شود یا حتی اگر یکی از گره‌ها در شبکه با شکست مواجه شود. بنابراین، تا زمانی که نسخه‌ای معتبر از بلاکچین در جایی وجود داشته باشد، می‌توان بلاکچین را ذخیره کرد و دیگران آن را تکثیر کنند تا اسناد قدیمی را بازیابی کند و در تراکنش‌های جدید وارد شود.

برای اطمینان از ثبت منظم اطلاعات و بهبود امنیت بلاکچین، هر بلاکچین شامل یک مکانیسم اجماع خواهد بود (مجموعه‌ای از قوانین مشخص با طرح‌های تشویقی از پیش‌تعریف‌شده و ساختارهای هزینه) که حذف یا اصلاح داده‌های ذخیره‌شده روی بلاکچین را دشوار و هزینه‌بر می‌کند. مکانیسم‌های اجماع به شبکه مبتنی بر بلاکچین کمک می‌کند تا به‌طور دوره‌ای درباره وضعیت کنونی پایگاه داده مشترک به توافق برسند؛ حتی اگر اعضا ندانند یا به یکدیگر اعتماد نداشته باشند.

با استفاده از رمزنگاری کلید عمومی ـ خصوصی، هر بلاکچین اعتبار یکپارچگی داده‌های ذخیره‌شده روی بلاکچین را تایید می‌کند و افراد را قادر می‌سازد تا به‌طور نیمه‌ناشناس تراکنش‌ها را انجام دهند، بدون آنکه لازم باشد هویت واقعی خود را فاش کنند. از آنجا که بلاکچین به‌طور متمرکز حفظ نمی‌شود، هیچ گروهی ضرورتا نیازمند کنترل دسترسی به آنها نیست. بر همین اساس، در بلاکچین با دسترسی عام، هر کسی می‌تواند یک حساب بلاکچین ایجاد کند که متشکل از آدرسی عمومی و کلیدی خصوصی است (رمز عبور) و می‌تواند با کمترین نگرانی از بابت مداخله گروه ثالث (واسطه) با دیگران تراکنش انجام دهد.

همچنین، بلاکچین پیشرفته‌تر نیز سیستم‌های رایانش غیرمتمرکز[1] را با یکدیگر یکپارچه می‌سازد؛ به عبارتی دیگر، یک ماشین مجازی توزیع‌شده[2]. همچنین، زبان‌های کامل برنامه‌نویسی تورینگ[3] طرف‌های قرارداد را قادر می‌سازد تا برنامه‌های قراردادهای

1. decentralized computing systems
2. distributed virtual machine
3. Turing

هوشمند را بنویسند و به‌کار ببندند. این برنامه‌ها روی بلاکچین ذخیره می‌شود و توسط چندین عضو از شبکه اصلی همتابه‌همتای بلاکچین اجرا می‌شود و فرایندهای رایانه‌ای را ایجاد می‌کند که ناشناس هستند و به‌طور بالقوه خاموش کردن آنها، پس از به‌راه‌افتادن، دشوار است.

از زمان عرضه بیت‌کوین در ۲۰۰۹ تاکنون، بلاکچین بر استحکام برخی از سرویس‌های آنلاین افزود که به‌دنبال استفاده از فناوری برای ذخیره‌سازی اطلاعات هستند و فرایندهای رایانه‌ای را اجرا می‌کنند. برخی از این نرم‌افزارهای کاربردی با هدف رسیدن به چشم‌انداز می عرضه شدند و در عین حال دیگر نرم‌افزارها نیز به تقویت خدمات قانونی کنونی کمک می‌کنند.

همان‌طور که بیت‌کوین نشان داده است، فناوری بلاکچین از سیستم‌های انتقال ارزش جهانی و غیرمتمرکز حمایت می‌کند که هم بین‌المللی و هم ناشناس‌اند. با استفاده از بلاکچین، هر کسی می‌تواند ارزهای دیجیتال (نظیر بیت‌کوین)، یا دیگر دارایی‌های ارزشمند را، بدون نیاز به اتکا بر موسسات تهاتر[1] و بدون آشکارکردن هویت خود، تبادل کند. بلاکچین در سیستم‌های رمیتنس همتابه‌همتا قرار دارد که از هزینه فرستادن پول به خارج می‌کاهد. این فناوری در صنعت خدمات مالی نیز جایگاهی برای خود دست‌وپا کرده است؛ امکان اجرای سیستم‌های جدید غیرمتمرکز را فراهم آورده که در مرکز امور مالی جهان قرار می‌گیرد که شامل اوراق بهادار غیرمتمرکز[2] و تبادل اوراق مشتقه[3] می‌شود.

طی فقط چند سال، بلاکچین به فراتر از حوزه محصولات پرداخت و امور مالی وارد شد و به پشتیبانی از سیستم‌های خودمختار و جدید کمک کرد تا به تعاملات اجتماعی و اقتصادی با کمترین نیاز به واسطه‌ها شکل دهد. از قراردادهای هوشمند برای اجرای تمامی بندهای توافقات قانونی و انعقاد قراردادهای تجاری پویا استفاده می‌شود که ایجاد اختلال در آنها دشوار است.

---

1. clearing house
2. decentralized securities
3. derivatives exchanges

دولت‌ها در سراسر دنیا در حال استفاده از بلاکچین برای امن‌کردن و مدیریت اسناد عمومی حساس هستند که از جمله می‌توان به اطلاعات و اموال حیاتی اشاره کرد. با اهرم‌کردن ذات تغییرناپذیر و ارتجاعی بلاکچین، دولت‌ها به‌دنبال تضمین یکپارچگی و صلاحیت اطلاعات کلیدی دولتی هستند. با گذشت زمان، بلاکچین می‌تواند زیرساخت‌های عمومی جدیدی ایجاد کند و به‌طور بالقوه، حتی سیستم‌های بین‌المللی و جهانی ایجاد کند که فقط با اتصال به اینترنت در دسترس همگان قرار خواهد گرفت. همچنین، بلاکچین در حال شکل‌دهی به تلاش‌های جمعی است که از آن جمله می‌توان به ساختارهای جدید سازمان‌های مدیریت‌شده دیجیتال بر حسب روش کار اشاره کرد؛ حداقل به‌طور جزئی.

از آنجا که بلاکچین به‌طور گسترده پذیرفته شده و می‌تواند تراکنش‌های اقتصادی را تسهیل کند، برای مدیریت عملیات‌ها در نهادهای قانونی و به‌صورت نقطه مرکزی هماهنگ‌سازی، از بلاکچین استفاده می‌شود. قراردادهای هوشمند نیز قوانین آیین‌نامه‌ای را اجرا می‌کنند که قادرند هزینه و دشواری مدیریت گروه را کاهش دهند. بلاکچین حتی در حال ایجاد شکل‌های جدید سازمانی است که شفاف‌تر باشد و سلسله‌مراتب کمتری در آن دیده شود. در نتیجه، به گروه‌ها کمک می‌کند تا بدون نیاز به شناختن یکدیگر به توافق برسند. چون بلاکچین امکان اجرای خودمختار آیین‌نامه‌ها را فراهم می‌سازد، با گذشت زمان، ممکن است آنها زیرساختی برای ایجاد سازمان‌هایی به وجود آورند که به‌طور کامل بر سیستم‌های الگوریتمی و هوش مصنوعی برای مدیریت فعالیت گروه‌ها وابسته‌اند. مدیریت این سازمان‌ها به نیروی انسانی وابسته نیست، در عوض بر قوانین آیین‌نامه‌ای و دیگر ابزارهای حاکمیت الگوریتمی[1] به‌منظور شکل‌دهی به عملیات‌های خودمتکی هستند.

از بلاکچین به‌طور روزافزون برای کنترل ادوات و دستگاه‌ها استفاده می‌شود و قراردادهای هوشمند نیز عملیات این ادوات متصل به اینترنت را تعریف می‌کنند. در نتیجه، کاربردهای بلاکچین از هماهنگ‌سازی فعالیت‌های انسانی فراتر می‌رود. در

1. algorithmic governance

نهایت، ممکن است بلاکچین به لایه‌ای بنیادی تبدیل شـــود که به ماشین‌ها در ورود به تراکنش‌های اقتصادی همراه با انســـان‌ها و نیز دیگر ماشـــین‌ها کمک می‌کند. اگر این اقدامات موفقیت‌آمیز باشد، می‌توان از بلاکچین برای مدیریت بازه گسترده‌ای از فعالیت‌ها استفاده کرد و در نتیجه، عصر جدیدی از تعاملات ماشین با ماشین و ماشین با انسان[1] را پایه‌گذاری کرد که می‌تواند به‌طور بالقوه ذات رابطه ما را با کالاهای فیزیکی تغییر دهد.

با این حال، همه نرم‌افزارهای کاربردی و خدمات مبتنی بر بلاکچین از قوانین و قواعد کنونی پیروی نمی‌کنند. ارزهای دیجیتال مبتنی بر بلاکچین به‌صورت بین‌المللی کار می‌کنند و غالبا به مقررات کنونی در ارتباط با انتقال پول و پولشویی اهمیت نمی‌دهند. همچنین، قوانینی را که با هدف کمک به دولت‌ها، بانک‌ها و دیگر نهادهای خصوصی برای ردیابی جریان پول در جهان تدوین شده‌اند، در نظر نمی‌گیرند. اگر فناوری‌های نوظهور به‌خوبی مدیریت نشـــوند، ممکن اســـت از آنها برای انجام کلاهبرداری و پولشویی، تامین مالی تروریست‌ها یا دیگر فعالیت‌های خرابکارانه استفاده شود.

همچنین، بلاکچین در بازارهای عمومی نیز دیده می‌شـــود؛ افراد را قادر می‌سازد تا میلیاردها دلار توکن[2] رمزی به‌فروش برسانند (برخی از آنها شبیه اوراق بهادار هستند) و اوراق مشتقه و دیگر محصولات مالی را با استفاده از تبادلات خودمختار و آیین‌نامه‌ای مبادله کنند. این سیســـتم‌های مبتنی بر بلاکچین غالبا از موانع قانونی که از بازارهای مالی کنونی حمایت می‌کنند، غافل می‌شـــوند و قوانین خوش‌ساختی را که با هدف محدودکردن کلاهبرداری و حفاظت از سرمایه‌گذاران وضع شده‌اند، سست می‌کنند.

خارج از دنیای مالی، از بلاکچین برای پشـــتیبانی از نرم‌افزارهایی استفاده کرده‌اند که محدودیت‌هایی بر فعالیت‌های قمار آنلاین و تجارت الکترونیکی اعمال و از کازینوهای اتوماسیون‌شده پشـــتیبانی می‌کند؛ کازینوهایی که برای کنترل به گروه ثالث و همچنین، بازارهای الکترونیکی غیرمتمرکز که خریدوفروش کالا را بدون اتکا بر سایت‌هایی نظیر eBay، CrAIgslist، یا حتی Silk Road، تسهیل می‌کنند، نیازی ندارند. این نرم‌افزارها باعث

1. machine- to- machine and machine- to- person interactions
2. tokens

فروش آســـان‌تر داروهای غیرمجاز می‌شـــود و در صورت پذیرش کافی از سوی بازار می‌توانند محدودیت‌های دولتی و دیگر حوزه‌ها را در هم بشکنند.

بلاکچین به آزادسازی جریان اطلاعات، تامین انرژی لازم برای اشتراک‌گذاری فایل بین همتاها، بسترهای ارتباطاتی غیرمتمرکز و شبکه‌های اجتماعی کمک فراوانی می‌کند که بر ویژگی‌های بلاکچین که از جمله ذات غیرمتغیر و ارتجاعی آن است، متکی است. همچنین به دیگر شبکه‌های همتابه‌همتا نیز در ترویج یا محدودسازی مطالب دارای حق نشر و حاوی مواد تحریک‌آمیز کمک می‌کند. اگر از این خدمات به‌درستی و در سطح گسترده استفاده شـــود، می‌توانند به اقدامات دولتی و شرکتی در جهت کنترل، فیلتر و سانسور اطلاعات آنلاین، بدون توجه به هزینه‌های اجتماعی و سیاسی کمک کنند.

اگر بلاکچین برحسب سرعت، عملکرد، کاربردپذیری و دسترسی بهبود یابد، ممکن است این فناوری در گذر زمان شروع به ســـاخت سازمان‌هایی کند که با شرکت‌های سنتی و دیگر نهادهای دولتی رقابت کنند و شـــاید حتی به ظهور ادوات خودمختار و ربات‌هایی منجر شود که مستقل از گروه ثالث فعالیت می‌کنند؛ رها از کنترل دولت‌ها و اپراتورهای میانجی.

همان‌طور که در این کتاب بحث خواهیم کرد، توانایی بلاکچین در تسهیل و حمایت از سیســـتم‌های خودمختار به‌طور فزاینده‌ای باعث ایجاد چالش در دولت‌ها و برای قانون‌گذاری می‌شود که به‌دنبال کنترل، شـــکل‌دهی یا تاثیرگذاری بر توسعه فناوری بلاکچین هستند. درست مانند بسیاری دیگر از فناوری‌ها، بلاکچین را می‌توان برای حمایت و اجرای قوانین کنونی به‌کار برد، اما آنچه باعـــث توانمندی ویژه بلاکچین می‌شود، توانایی آن در تسهیل ایجاد سیستم‌های ارتجاعی، تغییرناپذیر و خودکار مبتنی بر کدنویسی است که در سطح جهانی فعالیت کنند و ابزارهای مالی و قراردادی جدیدی را در اختیار مردم قرار دهند تا بتوانند جای امور کلیدی اجتماعی را بگیرند.

با وجود بلاکچین، مردم می‌توانند نظام قانونی یا قراردادهای هوشمند منحصربه‌خود را بســـازند و پروتکل‌هایی بنیادی در شـــبکه‌های مبتنی بر بلاکچین وضع کنند. این

سیستم‌ها بدون قانون به نظم می‌رسند و آنچه را که چارچوب قوانین خصوصی[1] نام دارد، اجرا می‌کنند؛ در سراسر این کتاب به آن lexcryptographica، خواهیم گفت (واژه‌ای لاتین به‌معنای قوانین رمزی/قانونی رمزی). آنها قدرتی به توسعه‌دهندگان نرم‌افزار می‌دهند که بتوانند ابزارها و خدماتی خلق کنند که درگیر احکام قضایی نشوند و به‌طور بین‌المللی برای هماهنگ‌کردن فعالیت‌های اقتصادی و اجتماعی کار کنند.

قوانین رمزی با سیستم‌های موجود از احکام مبتنی بر کد که توسط نرم‌افزار آنلاین امروزی اجرا می‌شوند، فرق دارند. در حال حاضر، بیشتر خدمات آنلاین به‌طور عمومی یا به‌صورت یک میانجی عمل می‌کنند که بر دیگر میانجی‌ها وابسته است (نظیر ارائه‌دهندگان رایانش ابری، موتورهای جست‌وجو، پردازنده‌های پرداخت، ثبت‌کنندگان نام دامنه و شبکه‌های اجتماعی) تا از خدمات آنها پشتیبانی کنند. این واسطه‌ها قدرت اعمال و اجرای قوانین و احکام خود را دارند و به‌راحتی می‌توان حوزه قضایی آنها را شناسایی کرد، آنها همچنین به‌عنوان نقاط متمرکز کنترل برای نهادهای قانون‌گذار عمل می‌کنند.

کنترل و تعیین مقررات برای سیستم‌های مبتنی بر بلاکچین (که اساسا یا انحصارا بر قوانین رمزی متکی هستند) دشوارتر خواهد بود. بلاکچین نیاز به وجود واسطه‌ها را کاهش می‌دهد و سیستم‌هایی ایجاد می‌کند که پروتکل‌ها و دیگر احکام مبتنی بر کد بر آن حاکم هستند و به‌طور خودکار توسط شبکه‌های مبتنی بر بلاکچین اجرا می‌شوند. از طریق استفاده از بلاکچین و قراردادهای هوشمند، نرم‌افزارهای آنلاین جدیدی را می‌توان طراحی کرد که تا حد زیادی خودمختار باشند و به‌طور فزاینده‌ای از واسطه‌های متمرکز، مستقل رفتار کنند. این نرم‌افزارها از هیچ‌چیز جز کد ساخته نشده‌اند و توسط پروتکل مبتنی بر بلاکچین به شیوه‌ای توزیع‌شده اجرا می‌شوند (صرف‌نظر از اینکه آیا با قوانین دولتی سازگار هستند یا خیر) در نتیجه، تنش‌هایی با نهادهای قانونی به وجود می‌آورند که بر واسطه‌های متمرکز قانون‌گذار متمرکز هستند و در حال حاضر به تسهیل فعالیت‌های آنلاین کمک یا آنها را کنترل می‌کنند.

1. private regulatory frameworks

با وجود وعده‌های درخشان بلاکچین، شبکه‌های مبتنی بر بلاکچین با ریسک ایجاد خطرات گسسته مواجه هستند که ممکن است بانکداری متمرکز، بازارهای مالی و اداره توافقات تجاری را ناپایدار و از شکل‌های جدیدی از فعالیت‌های خرابکارانه حمایت کند. این خطرات به‌طور ویژه حاد هستند، زیرا این فناوری برای دوباره‌کاری سیستم‌های بنیادی و نهادهای اساسی به‌کار می‌رود که جامعه مدرن را تعریف می‌کنند. از بین این موارد می‌توان به سیستم‌های پرداخت، بازارهای مالی، توافقات تجاری و بسیاری از ساختارهای سازمانی اشاره کرد که جامعه ما را مردمی می‌کنند.

امروزه، تمرکز بر حاکمیت اجتماعی از سوی نهادها و سیستم‌های اداری تحمیل می‌شود. آنها بر قوانین و سلسله‌مراتب سازمانی برای نظم‌دهی به جامعه متکی هستند. نرم‌افزارهای بلاکچین برای شکل‌دهی به توابع خود به این قوانین وابسته نیستند؛ در عوض آنها به قوانین رمزی برای سازمان‌دهی فعالیت‌های اقتصادی و اجتماعی متکی هستند.

همان‌طور که فناوری به بلوغ بیشتری می‌رسد، بلاکچین نیز می‌تواند انتقال ساختار قدرت از احکام قانونی دولتی را به قوانین رمزی و پروتکل‌هایی که شبکه‌های بلاکچین غیرمتمرکز بر آن حاکمیت دارند، تسریع کند. پروتکل‌های مبتنی بر کد و تصمیمات مرتبط با توسعه آنها در نهایت چگونگی کارکرد این سیستم‌ها را مشخص می‌کند و ابزارهای تعامل ما را شکل می‌دهد. ما می‌توانیم به‌طور روزافزون خود را در معرض «حاکمیت کدها» قرار دهیم؛ کدهایی که ممکن است هیچ گروهی بر آنها کنترل نداشته باشد و امکان دارد طبق «حاکمیت قوانین» عمل کنند یا عمل نکنند.

در این کتاب به‌دنبال استفاده‌های نوظهور از بلاکچین می‌گردیم و منافع و چالش‌های درک‌شده آن را توصیف می‌کنیم و همچنین به نمادهای قوانین رمزی اشاره می‌کنیم. ما این ایده را رد می‌کنیم که بلاکچین به ایجاد یک هرج‌ومرج مبتنی بر رمز منجر خواهد شد که خالقان این فناوری در ذهن خود آن را ترسیم کرده بودند. همچنین به استراتژی‌های مرتبط با وضع قوانین اشاره خواهیم کرد.

وقتی اینترنت برای اولین‌بار عرضه شد، تفکرات مرتبط با هرج‌ومرج و بی‌قانونی را در

بین مردم رواج داد (که البته، آن شک‌وتردیدها درست بود). همان‌طور که جان پری بارلو در رساله خود در سال ۱۹۹۶؛ «بیانیه استقلال فضای مجازی» گفته بود، اینترنت در آغاز به‌صورت دنیایی درک شده بود که در آن «مفاهیم قانونی سنتی درباره اموال، مالکیت، هویت، انتقال مالکیت و بافت اعمال نمی‌شود». این دنیا به‌واسطه حضور کاربرانش معنا می‌یابد و آنها نیز بر شبکه‌های غیرمتمرکز برای سازمان‌دهی و حکومت بر امور خود متکی هستند؛ بدون آنکه از جانب نهادهای متمرکز دخالتی صورت بگیرد.

با این حال، با بلوغ اینترنت، دیدگاه بارلو صرفا رویایی از یک آرمان‌شهر بود. گرچه طرح اصلی اینترنت به‌دنبال تمرکززدایی قدرت و ترویج آزادی ارتباطات بود (حتی به‌ازای وجود اسپم‌ها، کلاهبرداری‌ها و جرائم مختلف) اما با گذشت چند دهه، به‌طور فزاینده‌ای متمرکز و قانون‌محور شـــد؛ ظهور گوشی‌های موبایل، فروشگاه‌های اپل و پلتفرم‌های رایانش ابری به پایه‌گذاری شـــبکه‌های متمرکزتر منجر شد که فقط چند شرکت بر آن تســـلط داشـــتند و جریان اطلاعات و تراکنش‌های اقتصادی را در آن کنترل می‌کردند.

امروزه، گرایش‌های نامنظم در اینترنت تا حد زیادی اصلاح شده است. دولت‌ها از طریق متمرکز کردن کانون قوانین روی ارائه‌دهندگان سرویس‌های اینترنت (ISP)[1] و واسطه‌های بزرگی که در خلق و استقرار ســـرویس‌های اینترنتی سهیم بودند، به‌طور روزافزون وظایف سیاست‌گذاری بر اینترنت را به این نهادها واگذار می‌کنند. برخی از کشورها، به‌ویژه در اروپا، کارهای خاصی را آغاز کرده‌اند؛ قطعه‌قطعه‌کردن اینترنت و اجرای الزامات بومی‌سازی داده‌ها برای پرهیز از جمع‌آوری و ذخیره‌سازی اطلاعات از سوی شرکت‌های خارجی درباره شهروندان‌شان. کشورهایی نظیر چین، روسیه، کره شمالی و ایران حتی گامی فراتر برداشتند و از دیوارهای آتشین ملی[2] برای خلق اینترنت عاری از تاثیرات غربی یا دگراندیشانه داخلی استفاده می‌کنند.

استدلال ما این است که رشد و توســـعه فناوری بلاکچین از مسیری مشابه پیروی خواهد کرد. حتی اگر بلاکچیـــن به‌طور فزاینده‌ای خودمختار باشـــد و به‌طور بالقوه

1. Internet ser vice providers (ISPs)
2. national firewalls

شامل سیستم‌های بی‌قانون باشد، همچنان ابزارهایی برای شکل‌دهی و کنترل استفاده و نحوه استقرار آنها وجود دارد. بلاکچین ممکن است نیاز به واسطه‌ها را کاهش دهد، اما بعید است که آنها خودشان را حذف کنند. حتی می‌توان از این فرض که بلاکچین به واسطه‌زدایی در سطح وسیع منجر می‌شود و اجرای قوانین، تقویت نیروهای بازار، هنجارهای اجتماعی و خود کدها را در پی خواهد داشت، برای حفاظت و صیانت از حاکمیت قانون استفاده کرد.

دولت‌ها برای شکل‌دهی و منحرف‌کردن این فناوری حین توسعه و رسیدن به پذیرش روزافزونش به ابزارهای متعددی دسترسی دارند. آنها می‌توانند فعالیت کاربران نهایی را تنظیم کنند و به‌سبب هرگونه استفاده از این سیستم‌ها یا حتی حمایت از نرم‌افزارهای مبتنی بر بلاکچین آنها را مجـــرم معرفی کنند. به‌طور جایگزین، یـــا علاوه بر آن، آنها می‌توانند فشارهای زیادی روی توسعه‌دهندگان نرم‌افزار اعمال کنند که از این سیستم‌ها حفاظت می‌کنند. همچنین، فشارهایی بر تولیدکنندگان سخت‌افزار و واسطه‌هایی که در سطوح پایین TCP/IP فعالیت می‌کنند، اعمال می‌شود.

برای مثال، دولت‌هـــا می‌توانند قوانین را بر ISPها و واســـطه‌های اطلاعاتی اعمال کنند (نظیر موتورهای جســـت‌وجو) و در نتیجه ممکن اســـت این واسطه‌ها به‌طور هدفمند از اندیس‌گذاری بر چندین نرم‌افزار بلاکچیـــن ممانعت کنند. آنها می‌توانند قوانینی برای گروه‌هایی وضع کنند که از شـــبکه‌های بلاکچین حمایت و پشـــتیبانی می‌کنند (معدن‌کاوها/معدن‌چی‌ها) یا درباره توسعه‌دهندگان نرم‌افزار یا تولیدکنندگان ســـخت‌افزار این کار را انجام دهند که ابزارهای مورد نیاز را برای این شبکه‌ها تامین می‌کنند. تنظیم مقررات برای این گروه‌ها را می‌توان یا به‌طور مستقیم از طریق اعمال قوانین خاص روی این بازیگران یا به‌طور غیرمستقیم از طریق تغییر طرح‌های تشویقی اقتصادی و ساختارهای پرداخت‌شان انجام داد.

بلاکچین همچنان نابالغ اســـت؛ بنابراین دولت‌ها می‌توانند هنجارهای اجتماعی نوظهور مرتبط با فناوری را از طریق آموزش، گروه‌های کاری بین‌المللی رســـمی یا دیگر ابزارهای غیررسمی شکل دهند. همچنین، آنها می‌توانند برای دستیابی به اهداف

خاص سیاسی، رمزگذاری بر قوانین و مقررات خاص به‌صورت شبکه‌های بلاکچین و قراردادهای هوشمند از این فناوری بهره ببرند.

در این کتاب به‌دنبال ذات دوگانه بلاکچین هستیم که ظهور قوانین رمزی را تشریح می‌کند و به حوزه‌های بالقوه قانون‌گذاری اشـــاره خواهد کرد. فرض ما این است که دانشی درباره بلاکچین نداریم و بنابراین ابتدا تاریخچه‌ای مفصل و مروری فنی از این فناوری خواهیم داشت و سپس تولید بیت‌کوین و اتریوم[1] و دیگر فناوری‌های مرتبط را توضیح می‌دهیم. سپس، ویژگی‌های اصلی بلاکچین را مشخص می‌کنیم و توضیح می‌دهیم که چرا این ویژگی‌ها باعث تسهیل قوانین رمزی می‌شود و ما را به‌سوی افزایش کنترل الگوریتمی و قوانین رمزی سوق می‌دهد. همچنین، چگونگی حمایت بلاکچین از قوانین کنونی و چگونگی استفاده از این فناوری برای اثرگذاری بر نهادهای سیاسی و اجتماعی فعلی را در بافت‌های گوناگون بررسی می‌کنیم. از سیستم‌های پرداخت، قوانین قراردادی و امور مالی گرفته تا سیســـتم‌های مخابراتی و اطلاعاتی یا تعاملات ماشین با ماشین که از طریق اجرای قوانین رمزی به این موضوعات می‌پردازیم. پس از توصیف چالش‌های قانونی بلاکچین، به چگونگی وضع قوانین برای سیستم‌های مبتنی بر بلاکچین، در کنار هزینه‌های انجام این کار اشاره می‌کنیم. کار خود را نیز با ورود به آینده، سنجش چگونگی پشتیبانی یا تکمیل قوانین از سوی بلاکچین به‌وسیله تبدیل همه بخش‌های قوانین به کد و بررسی برخی از خطرات این مسیر به پایان می‌رسانیم. هدف ما ارائه دیدگاهی درباره چگونگی کارکرد بلاکچین، استفاده‌های بالقوه این فناوری، ویژگی‌های متمایز قوانین رمزی و حوزه‌های بالقوه وضع قوانین است.

1. Ethereum

فصل یک
فناوری

بخش یک

بلاکچین‌ها، بیت‌کوین و پلتفرم‌های رایانش غیرمتمرکز

بلاکچین، در مرکز خود، پایگاه داده غیرمتمرکزی اســـت که شبکه‌ای توزیع‌شده از رایانه‌ها آن را کنترل می‌کنند. آنها به‌واسطه فناوری‌های گوناگونی با یکدیگر ترکیب می‌شوند؛ از جمله، شبکه‌های همتابه‌همتا، رمزنگاری کلیدهای عمومی ـ خصوصی و مکانیسم‌های اجماع تا بدین صورت نوع جدیدی از پایگاه داده را خلق کنند. در اینجا، ما توصیفی کوتاه از چگونگی کارکرد بلاکچین ارائه می‌کنیم و سپس بافت اساسی اجزای کلیدی این فناوری را تشریح می‌کنیم.

تا پیش از ظهور اینترنت، رایانه‌ها دچار انزوا بودند. آنهـــا جزایری دورافتاده از هم بودند که هیچ‌راهی برای اتصال به یکدیگر نداشـــتند، جز اینکه از کابل‌های طویل و قطور استفاده کنند. در اواخر دهه ۵۰ میلادی، این حالت تغییر کرد. پس از آنکه شوروی فضاپیمای اسپوتنیک[1] را با موفقیت به فضا فرستاد و ترس از ادامه پیدا کردن جنگ سرد وجود داشت، پژوهشگران شرکت راند[2] شروع به توســـعه الگوی رایانشی جدیدی کردند. آنها امید داشتند سیستمی را توســـعه دهند که بتواند در برابر فجایع هسته‌ای ایستادگی کند. در آگوست ۱۹٦٤، پس از سال‌ها تحقیق، پاول بارن[3] یکی از پژوهشگران این شرکت، اکتشافی مهم را گزارش کرد. بارن توانسته بود با اتکا بر فناوری‌ای که پکت سوئیچینگ[4] نام داشـــت، چند قطعه اطلاعات را از یک رایانه به رایانه دیگر بفرستد و

1. Sputnik
2. Rand Corporation
3. Paul Baran
4. packet switching

دوباره این قطعه‌ها را سر هم کند. این اتفاق در آن دوران شبیه معجزه بود.

نهاد پروژه‌های تحقیقاتی پیشرفته در صنایع دفاع آمریکا (ARPA)[1]، با اتکا بر تحقیقات بارن، از این فناوری برای خلق اولین شبکه رایانه‌ای استفاده کرد؛ ARPAnet. بعدها نام دارپانت (DARPAnet) را بر آن گذاشتند، زیرا واژه «دفاع» («Defense») به ابتدای نام آن نهاد افزوده شده بود و به پژوهشگران و دانشگاهیان کمک می‌کرد تا فایل‌ها را به اشتراک بگذارند و منابع را با یکدیگر تبادل کنند. طی چند دهه بعد، قدرت این شبکه بیشتر شد، همان‌طور که بر تعداد لایه‌های این فناوری افزوده شد نظیر TCP/IP، (برنامه کنترل انتقال و پروتکل اینترنت)[2] و خدمات نام دامنه (DNS) برای آسان‌تر کردن احراز هویت رایانه‌ها در این شبکه و نیز تضمین اینکه اطلاعات به‌طور مناسبی هدایت می‌شوند، از این فناوری استفاده می‌شد. رایانه‌ها هم دیگر در انزوا نبودند. اکنون، آنها با استفاده از لایه‌های نازک کد به یکدیگر متصل بودند.

رمزگذاری بر کلیدهای عمومی ـ خصوصی و امضای دیجیتال

همان‌طور که دارپانت روزبه‌روز پیشرفت می‌کرد، دومین انقلاب آن دوران به‌وقوع پیوست؛ الگوریتم‌های جدید رمزنگاری در حال خلق ابزارهای جدیدی برای افراد و ماشین‌ها بودند تا پیام، فایل و دیگر اطلاعات را به‌طور امن و معتبر ارسال کنند. در سال ۱۹۷٦، وایت‌فیلد دای‌فی و مارتی هلمن،[3] دو رمزنگار از دانشگاه استنفورد، با نبوغ فراوان مفهوم «رمزنگاری کلید عمومی ـ خصوصی» را مطرح کردند که یکی از مشکلات بنیادی حوزه رمزنگاری را حل می‌کرد (نیاز به توزیع کلید امن) و در واقع بنیاد نظری را برای امضاهای دیجیتالی[4] معتبر فراهم کرد.

پیش از ظهور رمزنگاری کلید عمومی ـ خصوصی، فرستادن پیام‌های خصوصی دشوار بود. پیام‌های رمزی روی کانال‌های ناامن انتقال می‌یافتند و آنها را در برابر استراق سمع آسیب‌پذیر می‌کرد. برای فرستادن یک پیام رمزی، آن پیام باید با استفاده از یک

1. Advanced Research Projects Agency
2. Transmission Control Program and Internet Protocol
3. Whitfield Di4e and Marty Hellman
4. Digital signatures

«کلید» (که به آن سایفر[1] می‌گفتند) در هم می‌ریخت و در نتیجه رشته‌ای نفوذناپذیر متنی پدید می‌آمد. وقتی آن پیام درهم‌ریخته به مقصد خود می‌رسید، دریافت‌کننده از همان کلید برای رمزگشایی از متن رمزی استفاده می‌کرد و پیام نهفته را آشکار می‌کرد.

یکی از محدودیت‌های اصلی این سیستم رمزگذاری این بود که آن کلید برای محرمانه نگه‌داشتن هر نوع پیام ارسالی در مرکز فرایند قرار داشت. گروه‌هایی که از این سیستم‌ها استفاده می‌کردند باید پیش از آنکه پیام را تبادل می‌کردند، بر سر آن کلید به توافق می‌رسیدند یا آن کلید باید به‌نحوی به دست گروه دریافت‌کننده می‌رسید. به‌سبب این محدودیت‌ها، کلیدها به‌آسانی دچار تغییر می‌شدند. اگر گروه ثالثی به یک کلید دست پیدا می‌کردند، می‌توانستند در ارتباط اختلال ایجاد کنند و یک پیام رمزی را رمزگشایی کنند.

رمزنگاری کلید عمومی ـ خصوصی این مشکل را حل کرد؛ به نحوی که فرستادن پیام‌های رمزی را بدون نیاز به کلید مشترک ممکن کرد. طبق مدل «دی‌فای و هل‌من»، هر دو گروه بر سر یک کلید عمومی توافق می‌کنند و هر گروه کلید خصوصی منحصربه‌فرد خود را تولید می‌کند. کلید خصوصی به‌صورت یک کلمه عبور سری عمل می‌کرد که گروه‌ها نیازی به اشتراک‌گذاری آن نداشتند و در عین حال کلید عمومی به‌عنوان نقطه مرجعی عمل می‌کرد که می‌توانستند به‌راحتی آن را مخابره کنند. با ترکیب کلید عمومی با کلید خصوصی گروه دیگر و سپس ترکیب خروجی با کلید خصوصی دیگر گروه‌ها، «دی‌فای و هل‌من» متوجه شدند که امکان تولید کلید پنهان مشترکی وجود دارد که بتوان از آن برای رمزگذاری و رمزگشایی پیام‌ها استفاده کرد.

در سال ۱۹۷۸، مدتی کوتاه پس از آنکه دی‌فای و هل‌من به‌طور علنی انتشار تحقیق بنیادی خود را اعلام کردند، گروهی از رمزنگاران دانشگاه MIT ـ ران ریوست، ادی شامیر و لن ادل‌من[2] ـ بر پایه تحقیقات دی‌فای و هل‌من دست به کار شدند. آنها الگوریتمی با نام الگوریتم RSA توسعه دادند (که از حرف اول نام توسعه‌دهندگان اقتباس شده است) تا مجموعه‌ای متصل و ریاضی از کلیدهای خصوصی و عمومی را با

1. cipher
2. Ron Rivest Adi Shamir, and Len Adleman

ضرب دو عدد اول بزرگ تولید کنند. این رمزنگارها متوجه شدند که ضرب دو عدد اول بزرگ نسبتا ساده است، اما به‌طور استثنایی دشوار است (حتی این کار برای رایانه‌های قدرتمند نیز دشوار است) و محاسبه آن اعداد اول مورد استفاده سخت می‌شود (فرایندی که فاکتوریزاسیون عدد اول[1] نام داشت).

با در نظر گرفتن مزیت این فرایند شگفت‌انگیز ریاضی، الگوریتم مذکور امکان مخابره گسترده کلیدهای عمومی را فراهم می‌کرد، البته با دانستن اینکه کشف کلیدهای خصوصی بسیار دشوار و تقریبا غیرممکن باشد. برای مثال، اگر آلیس بخواهد اطلاعات حساسی را به باب بفرستد، او باید اطلاعات را با استفاده از کلید عمومی خود و کلید عمومی باب رمزگشایی کند و پیام رمزی را به‌طور عام نشر دهد. با وجود الگوریتم RSA و به‌سبب استفاده از فاکتوریزاسیون عدد اول، فقط کلید خصوصی باب می‌تواند آن رمز را آشکار سازد.

کاربردهای استفاده از کلید خصوصی ـ عمومی فراتر از پیام‌های رمزنگاری محض است. همان‌طور که دی‌فای و هل‌من گفته‌اند، از طریق ساخت سیستم‌های رمزی جدید که در آنها «رمزنگاری و رمزگشایی به‌واسطه کلیدهای متمایز» انجام می‌شود، رمزنگاری کلیدهای عمومی و خصوصی می‌تواند امضاهای دیجیتالی معتبر و امنی را ممکن سازد که در برابر تغییرات به‌شدت مقاوم باشند؛ بنابراین، جای امضاهای مکتوب را که «نیازمند ابزارهای کاغذی و قراردادهای کاغذی هستند»، می‌گیرد.

برای مثال، با استفاده از الگوریتم RSA، گروه فرستنده می‌تواند یک پیام را با امضای دیجیتال همراه کند که با ترکیب پیام با کلید خصوصی گروه فرستنده تولید شده است. پس از ارسال، گروه گیرنده می‌تواند از کلید عمومی گروه فرستنده برای بررسی اعتبار و تمامیت پیام استفاده کند. با استفاده از رمزنگاری کلید عمومی ـ خصوصی و امضای دیجیتال، اگر آلیس می‌خواست پیامی را به باب بفرستد، او می‌توانست پیام را با استفاده از کلید خصوصی خود و کلید عمومی باب رمزنگاری کند و سپس پیام را با استفاده از کلید خصوصی خودش امضا کند. پس، باب می‌توانست از کلید عمومی آلیس برای

1. prime factorization

تایید اعتبار پیام آلیس و اینکه طی انتقال دچار تغییر نشـــده است، استفاده کند. سپس، باب می‌توانســـت با امنیت کامل با اســـتفاده از کلید خصوصی خود و کلید عمومی آلیس، رمزگشـــایی را انجام دهد. رمزگذاری کلید عمومی ـ خصوصی نقطه آغاز کار گروه بزرگی از دانشمندان علوم رایانه، ریاضی و دانشگاهیان بود که شروع به طراحی سیستم‌های جدیدی کردند تا بتوان با استفاده از این تکنیک‌های جدید رمزنگاری آن را ساخت. با تکیه بر رمزنگاری کلیدهای عمومی ـ خصوصی و امضای دیجیتال، از لحاظ نظری پول الکترونیکی، نام مستعار و سیستم‌های توزیع محتوا و نیز شکل‌های جدیدی از قراردادهای هوشمند ممکن می‌شود.

شبکه‌های همتابه‌همتا و اینترنت تجاری

در سال‌های پس از تولد اینترنت و اختراع رمزنگاری کلیدهای عمومی ـ خصوصی، حوزه رایانش متحول شد. هزینه رایانه‌ها به‌سرعت کاهش می‌یافت و این ماشین‌های رمزنگار نیز از زیرزمین شرکت‌های بزرگ و نهادهای دولتی به روی میز کار ما آمدند و وارد منازل‌مان شدند. پس از آنکه شرکت اپل رایانه شخصی اسطوره‌ای خود را عرضه کرد (Apple II)، بازه گســـترده‌ای از رایانه‌های ارزان وارد بازار شد؛ انگار که یک‌شبه رایانه‌ها وارد زندگی روزانه ما شدند.

تا اواســـط دهه ۹۰ میلادی، اینترنت در مرحله انبساط و تجاری‌سازی سریع به سر می‌برد. رشـــد دارپانت به فراتر از مناســـبات آکادمیک اولیه خود رسیده بود و با چند به‌روزرسانی، به اینترنت مدرن مبدل شد. میلیون‌ها نفر در سراسر دنیا به‌دنبال شکل‌های معتبر «فضای مجازی» بودند که با پروتکل‌هـــای جدید نرم‌افزاری تعامل می‌کردند و افراد را قادر می‌ساختند تا پیام‌های الکترونیکی را بفرســـتند (از طریق پروتکل ساده انتقال ایمیل،[1] SMTP)، فایل‌ها را انتقال دهند (از طریق پروتکل انتقال فایل،[2] FTP) و رسانه‌هایی را که روی رایانه‌ها میزبانی می‌شوند، توزیع و لینک کنند (از طریق پروتکل

1. simple mAIl transfer protocol
2. file transfer protocol

انتقال هایپرمتن، HTTP).[1] در این بین، مجموعه‌ای از ISPهـــا نیز حضور دارند. طی چند سال، اینترنت از یک دوران عقب‌ماندگی وارد شکل جدیدی از زیرساخت شد؛ آن‌طور که نیویورک‌تایمز گزارش کرد: «برای جریان اطلاعات... همان کاری که راه‌آهن بین‌قاره‌ای برای جریان کالا در یک قرن گذشته انجام می‌داد».

در ابتدا، خدمات اینترنتـــی غالبا با اســـتفاده از مدل «کلاینت ـ ســـرور»[2] (یا مدل سرویس‌گیرنده–سرویس‌دهنده) شکل یافت. سرورها که شـــرکت‌های «دات‌کام» مالک آن بودند، یک یا چند برنامه رایانه‌ای اجرا می‌کردند که وب‌سایت‌ها میزبان آن بودند و انواع نرم‌افزارهای کاربردی را مهیا می‌کردند و کاربران اینترنت می‌توانســـتند از طریق ایستگاه‌های پردازشگر به آنها دسترسی پیدا کنند. اطلاعات، به‌طور عمومی یک‌طرفه جریان داشتند؛ از یک سرور به یک کلاینت. سرورها می‌توانند منابع خود را با کلاینت‌ها به اشتراک بگذارند، اما مشتریان غالبا نمی‌توانستند منابع خود را با سرور یا دیگر ایستگاه‌های متصل به همان سرور اینترنت به اشتراک بگذارند.

سیستم‌های اولیه کلاینت ـ سرور نســـبتا امن بودند، اما غالبا به‌عنوان گلوگاه عمل می‌کردند. هر کدام از سرویس‌های آنلاین مجبور بودند تا سرورهایی را داشته باشند که سرپا نگه‌داشتن آنها و اجرای آنها بسیار گران تمام می‌شد. اگر یک سرور متمرکز از کار می‌افتاد، کل سرویس ممکن بود متوقف شود و اگر یک سرور بیش از اندازه از سوی کاربران درخواست دریافت می‌کرد، ممکن بود دچار بار اضافی شود و همین امر باعث شود که آن سرویس به‌طور موقت از دسترس خارج شود.

در ابتدای قرن بیست‌ویکم، مدل‌های جدیدی برای تحویل خدمات آنلاین معرفی شد. به‌جای تکیه بر سرورهای متمرکز، گروه‌ها شروع به استفاده از شبکه‌های همتابه‌همتا کردند که بر زیرساخت‌های غیرمتمرکز تکیه داشـــتند که در آنها هر شرکت‌کننده در شبکه (که عموما به آنها همتا یا گره[3] می‌گویند) هم به‌عنوان تامین‌کننده و هم به‌عنوان مصرف‌کننده منابع اطلاعاتی عمل می‌کرد. این مدل جدید با عرضه Napster، محبوبیت

1. hypertext transfer protocol
2. client-server model
3. Node

زیادی به‌دست آورد. با اجرای این نرم‌افزار، هر کسی می‌توانست موسیقی را از دیگر کاربران (که به‌عنوان کلاینت عمل می‌کردند) دانلود کند و در عین حال به‌طور همزمان فایل موسیقی را برای دیگران نیز بفرستد (که به‌عنوان سرور عمل می‌کنند). با استفاده از این شیوه، نپستر (Napster) میلیون‌ها رایانه را در سراسر جهان به یکدیگر متصل کرد و کتابخانه بزرگی از موسیقی به وجود آورد.

با این حال، محبوبیت نپستر زیاد دوام نیاورد. شبکه همتابه‌همتای این نرم‌افزار یک اندیس متمرکز و مدام در حال به‌روزرسانی از تمام موسیقی‌های موجود در این شبکه بود. این اندیس اعضا را به سمت فایل‌های موسیقی که می‌خواستند، هدایت کرد و به‌عنوان رکن اساسی کل شبکه عمل می‌کرد.

گرچه این کار برای کارکرد شبکه مذکور لازم بود، اما این اندیس متمرکز ثابت کرد که نقص اصلی نپستر است. دادگاه‌ها، پس از اعلام دادخواهی علیه نپستر، این سایت را مسئول تخطی از قوانین حق نشر یافتند، زیرا این سایت از اندیس مذکور استفاده می‌کرد. نپستر مجبور شد فایل‌های موجود برای همتایان را روی شبکه با دقت بیشتری مدیریت کند و این سایت اندیس حق نشر موسیقی را اعمال کرد. پس از اجرای این مورد، محبوبیت نپستر دچار افول شد و کاربران نیز به‌تدریج آن سایت را رها کردند.

پس از شکست نپستر، دومین نسل از شبکه‌های همتابه‌همتا عرضه شدند که اشتراک‌گذاری فایل را برای مخاطبان گسترده‌تری ممکن می‌ساختند. شبکه‌های جدید همتابه‌همتا، نظیر گنوتلا و بیت‌تورنت،[1] باعث شدند که مردم بتوانند اطلاعات موجود در رایانه شخصی‌شان را بدون نیاز به اندیس‌های متمرکز به اشتراک بگذارند. با گنوتلا، کاربران می‌توانستند فایل‌ها را از طریق فرستادن یک درخواست جست‌وجو پیدا کنند. آن درخواست بین رایانه‌ها انتقال می‌یافت تا به شبکه مورد نظر برسد و سپس فایل درخواستی روی رایانه یکی از همتایان پیدا می‌شد. بیت‌تورنت رویکردی دیگر در پیش گرفت؛ معرفی ایده بخش‌بندی کردن فایل به‌صورت قطعات کوچک که بتوان از چندین کاربر به‌طور همزمان آن را دانلود کرد، بنابراین غالبا انتقال فایل سریع‌تر و کارآمدتر انجام می‌شود. بیت‌تورنت انتقال این قطعات را با استفاده از فایل‌های کوچکی با پسوند

1. Gnutella and BitTorrent

«torrent» آغاز کرد تا بتوان آنها را روی سرورهای مختلف میزبانی کرد، بنابراین نیازی به سرویس‌های متمرکز نبود.

با ظهور این شبکه‌های همتابه‌همتای متمرکز نسل دوم، حالت جدیدی برای تحویل محتوا آغاز شد و در نتیجه تبادل اطلاعات از اپراتورهای بزرگ آنلاین ممکن شد. این شبکه‌های متمرکز فاقد مرکز قابل تشخیص بودند و فقط چند واسطه از این شبکه‌ها پشتیبانی می‌کردند و بر خلاف نپستر، از کارانداختن این شبکه‌ها تقریبا غیرممکن می‌شد.

ارز دیجیتال

ایده شبکه‌های همتابه‌همتای ارتجاعی از نظر رمزنگاران و دیگر فعالان عرصه فناوری به پیشرفت‌هایی در رمزنگاری کلیدهای عمومی ـ خصوصی منجر شد. این افراد که هم به رمزنگاری و هم به حریم خصوصی علاقه داشتند، متوجه قدرت شبکه‌های همتابه‌همتا و رمزگذاری آنها شدند و هر دو را ابزاری برای مقابله با آزادی رو به زوال افراد یافتند.

این افراد عقیده داشتند که بدون بررسی و نظارت‌های مناسب، استقرار فناوری اطلاعاتی مدرن باعث کاهش حیطه حریم شخصی افراد می‌شود و در نتیجه دولتی مستولی‌شونده و نظارت‌های شرکتی را درپی خواهد داشت. بر اساس گفته‌های دیوید چوآم،[1] رمزنگار و یکی از بنیان‌گذاران انجمن بین‌المللی تحقیقات رمزنگاری،[2] فناوری رایانشی در گذر زمان، باعث کاهش توانایی افراد در رصد و کنترل اطلاعات‌شان می‌شود؛ اطلاعاتی که دولت‌ها و شرکت‌ها خواستار جمع‌آوری آنها هستند و برای بررسی سبک زندگی، عادات و مکان زندگی افراد از آنها استفاده می‌کنند و از داده‌های مربوط به تراکنش‌های روزمره افراد نیز بهره می‌برند.

برای مقابله با این خطرات، این افراد از استقرار انبوه ابزارهای رمزنگاری حمایت می‌کنند و عقیده دارند که این کار باعث حفاظت از حریم خصوصی و در عین حال تسلط دولت‌ها در جهان می‌شود. آنها به‌دنبال دموکراتیک کردن دسترسی به رمزنگاری،

1. David Chaum
2. Association for Cryptologic Research

ساخت سیستم‌های پیام‌رسان امن، قراردادهای دیجیتالی، سیستم‌های احراز هویت و شکایت‌های خصوصی و «جعبه‌های تغییرناپذیر»[1] هستند. با نگارش آزادانه و گسترده نرم‌افزارهایی که نتوان آنها را تخریب کرد یا آنها را از کار انداخت، آنها امید داشتند جامعه‌ای آزاد بسازند که بتواند از قید و بند کنترل دولتی یا شرکتی فرار کند.

زیرساخت ضروری این رویا نقدینگی بی‌نام و نشان و دیگر سیستم‌های غیرقابل ردیابی پرداخت بود. این افراد و دیگر رمزنگاران که کار خود را از ۱۹۸۳ آغاز کردند، بررسی استفاده از رمزنگاری کلید خصوصی ـ عمومی را برای ساخت سیستم‌های جدید پولی شروع کردند. در آن سال، چوآم سیستمی را پیشنهاد داد تا خلق و انتقال نقدینگی الکترونیکی که نیازمند اطلاعات محرمانه نباشد را ممکن سازد. این سیستم در نهایت به دیجی‌کش[2] تبدیل شد؛ شرکتی که چوآم در ۱۹۹۴ راه‌اندازی کرد.

دیجی‌کش بر رمزنگاری کلیدهای عمومی ـ خصوصی به‌منظور صدور ارز دیجیتال تکیه داشت و از سیستم امضای دیجیتال چوآم استفاده می‌کرد (که به آن امضای ترکیبی می‌گفتند) تا تراکنش‌ها را بین گروه‌ها اعتبارسنجی کند. این شرکت به‌صورت یک شرکت تسویه وجوه متمرکز عمل کرد، عرضه پول را تثبیت و تراکنش‌های دیجی‌کش را پردازش می‌کرد. با این حال، دیجی‌کش، نظیر نپستر، یک محدودیت فنی داشت؛ به‌واسطه مدل کلاینت ـ سرور فعالیت می‌کرد که در این حالت شرکت چوآم مجبور بود تا هر تراکنش را در شبکه دو بار بررسی کند. موفقیت دیجی‌کش کاملا به سرنوشت یک شرکت وابسته بود و وقتی آن شرکت در ۱۹۹۸ ورشکسته شد، دیجی‌کش نیز با آن سرنگون شد.

با این حال، ایده خلق یک ارز دیجیتالی ناشناس همچنان باقی ماند. پس از دیجی‌کش، چندین سایفرپانک[3] (علاقه‌مندان به رمزنگاری و حریم خصوصی)، از جمله هال فینی، وای دای و نیک‌زابو،[4] سفر یک‌دهه‌ای را برای ساخت یک ارز دیجیتال ناشناس آغاز کردند که کنترل متمرکز نداشته باشد. این سایفرپانک‌ها می‌دانستند که برای خلق چنین

1. Tamper-proof boxes
2. DigiCash
3. cypherpunks
4. Hal Finney, WAI DAI, and Nick Szabo

سیستمی، به بهره‌گیری از چندین فناوری نیاز دارند که هم عرضه ارز دیجیتال را کنترل کند و هم امنیت اسناد و سوابق معتبر افراد را حفظ کند. ارز دیجیتال مجموعه‌ای از بیت‌ها بود که روی حافظه یک یا چند دستگاه ذخیره می‌شد و برخلاف اسکناس یا سکه‌های فلزی، جسم نداشت. از این رو، مثل هر منبع دیجیتال دیگری، واحدی از ارز دیجیتال را می‌توان به‌طور نامتناهی کپی و بازتولید کرد. به‌سبب این ویژگی‌های ذاتی، رمزارز محل مناسبی برای کلاهبرداری شد. بدون یک موسسه تهاتر متمرکز یا هر نوع واسطه دیگری که بتواند تراکنش‌ها را اعتبارسنجی کند و موجودی حساب‌ها را به‌روزرسانی کند، هر کسی که یک واحد ارز دیجیتال داشته باشد، توانایی فرستادن منابع مالی را به دو گروه به‌طور همزمان خواهد داشت و در نتیجه مشکل «خرج کردن دوباره» (دوبار خرج کردن)[1] به وجود می‌آید. برای مثال، اگر باب معادل پنج دلار ارز دیجیتال داشته باشد، می‌تواند آن مقدار را به آلیس و جان در یک زمان منتقل کند، در نتیجه حدود ۱۰ دلار در مجموع به‌طور غیرقانونی خرج می‌کند.

هر سیستم پرداخت غیرمتمرکز باید این مشکل خرج‌کردن دوباره را حل کند و باید این کار را به طریقی انجام دهد که به واسطه‌های متمرکز وابسته نباشد. کل مقدار ارز در گردش در هر زمان معینی باید ثابت باشد یا به‌واسطه یک پروتکل نرم‌افزاری کنترل شود، بنابراین از بی‌ارزش‌کردن ارز مورد نظر از طریق تولید منابع مالی اضافی نامعتبر جلوگیری می‌شود. همچنین، این سیستم باید سابقه امن و غیرقابل تغییری از هر تراکنش داشته باشد تا بتواند جریان کل ارز دیجیتال در سیستم را زیر نظر بگیرد. بدون این ویژگی‌های ضروری، تعیین اعتبار کسانی که ارز دیجیتال دارند در هر لحظه از زمان بدون اتکا بر نهادی معتمد یا موسسات تهاتر غیرممکن است.

بیت‌کوین

در اواخر سال ۲۰۰۸، یک یا چند توسعه‌دهنده گمنام با نام ساتوشی ناکاموتو[2] این مشکل را حل کردند. آنها از طریق ترکیب رمزنگاری کلید عمومی ـ خصوصی، امضای

1. double spending problem
2. Satoshi Nakamoto

دیجیتال و فناوری‌های همتابه‌همتا برای خلق پایگاه داده‌های جدید توزیع‌شده که با نام بلاکچین معرفی شدند، این مساله را حل کردند. با استفاده از بلاکچین، ناکاموتو یک ارز دیجیتالی غیرمتمرکز ساخت که می‌توانست بدون نیاز به واسطه‌های متمرکز کار کند.

برخلاف دیجی‌کش چوآم که بر اپراتور غیرمتمرکز متکی بود، سیستم ناکاموتو بر شبکه‌ای از رایانه‌ها متکی بود که کار اعتبارسنجی و حفاظت از اسناد کل تراکنش‌های بیت‌کوین را بر عهده داشتند. طی یک مقاله کوتاه ۹ صفحه‌ای با عنوان «بیت‌کوین: سیستم نقدینگی الکترونیکی همتابه‌همتا» به این مطلب اشاره شده بود. بر اساس این مدل، تراکنش‌ها در یک مخزن داده مشترک ثبت می‌شدند و نرم‌افزار بیت‌کوین نیز عرضه ارز دیجیتال را کنترل و اعتبارسنجی تراکنش‌ها را هماهنگ می‌کرد، در نتیجه نیاز به کنترل متمرکز از میان برداشته می‌شد.

بیت‌کوین از زمان عرضه‌اش در سال ۲۰۰۹ تاکنون، به یکی از بزرگ‌ترین سیستم‌های پرداخت در دنیا مبدل شده و همچنان پایه‌های فنی‌اش از نظر بسیاری همچنان به‌اندازه راه‌اندازی‌اش عجیب و اسرارآمیز است. یک راه برای مفهومی‌سازی چگونگی کارکرد بیت‌کوین این است که به ایمیل فکر کنیم. امروزه، یک آدرس ایمیل ما را قادر می‌سازد تا به هر کسی که به اینترنت متصل است، ظرف کمتر از چند ثانیه پیام‌های الکترونیکی بفرستیم یا از او دریافت کنیم. آدرس ایمیل غالبا به هویت فردی ما مربوط نمی‌شود؛ ممکن است نیمه‌آشنا باشد و به‌عنوان نقطه مرجعی برای دریافت پیام‌های الکترونیکی عمل کند. با آنکه بسیاری از کاربران بر اپراتورهای ثالث برای مدیریت ایمیل‌ها اتکا می‌کنند، پروتکل بنیادی برای ارسال و دریافت پیام‌ها غالبا یک پروتکل رایگان، آزاد و چندکاربری است که می‌توان بدون درخواست مجوز از کسی از آنها استفاده کرد. دسترسی به یک ایمیل و داشتن یک رمز عبور افراد را قادر می‌سازد تا حساب‌های ایمیل خود را کنترل کنند؛ چه از طریق واسطه‌های کاربری تحت وب نظیر جی‌میل یا از طریق ایستگاه‌های ایمیل نظیر مایکروسافت آت‌لوک[1] یا تاندربرد.[2]

بیت‌کوین نیز شبیه همین حالت است. بیت‌کوین یک پروتکل آزاد است که یک

1. Microsoft Outlook
2. Thunderbird

گروه یا فرد به‌طور متمرکز آن را کنترل نمی‌کند. بیت‌کوین بر رمزنگاری کلید عمومی ـ خصوصی برای توانمندسازی افراد به‌منظور خلق حساب‌های بیت‌کوین نیمه‌ناشناس متکی است؛ بدون آنکه از کسی درخواست اجازه و مجوز کند. با داشتن یک حساب بیت‌کوین، افراد می‌توانند بیت‌کوین را برای هر کسی در دنیا بفرستند یا از او دریافت کنند، آن هم ظرف چند دقیقه، از طریق اجرا و امضای دیجیتالی یک تراکنش بیت‌کوین با یک کلید خصوصی. پس از امضای تراکنش، اعضای شبکه بیت‌کوین متوجه می‌شوند که تراکنش معتبر است و در نتیجه موجودی حساب بیت‌کوین مرتبط را به‌روزرسانی می‌کنند.

افراد در حال کلی با شبکه بیت‌کوین با استفاده از یک «کیف پول» در تعامل هستند. درست مانند ایستگاه‌های پردازشگر ایمیل، کیف پول‌های بیت‌کوین به افراد حاضر در شبکه بیت‌کوین کمک می‌کند تا حساب‌های خود را مدیریت کنند. افراد کیف پول خود را روی رایانه شخصی ذخیره کرده یا با استفاده از برنامه کاربردی از آن محافظت می‌کنند که غالبا توسط گروه‌های ثالث نگهداری می‌شود و در نتیجه از طریق یک مرورگر وب یا یک گوشی هوشمند معمولی به بیت‌کوین دسترسی پیدا می‌کنند. برای افزایش امنیت، برخی افراد کیف پول‌های خود را به‌طور آفلاین روی یک فلش‌درایو USB یا دیگر شکل‌های سخت‌افزارهای امن ذخیره می‌کنند که غالبا به آنها کیف پول‌های سرد[1] می‌گویند. تراکنش‌های بیت‌کوین، مانند ایمیل، نامحدود است و آزادانه بین مرزهای ملی در جریان است. هیچ گروه متمرکزی انتقال ارز دیجیتال را کنترل نمی‌کند و هیچ کسی نباید یک تراکنش را تایید کند یا عضویت را روی شبکه از پیش معین کند. هر کسی با داشتن یک حساب بیت‌کوین می‌تواند بیت‌کوین را در مقادیر کوچک و بزرگ بفرستد (از ۰٫۰۰۰۰۰۰۰۱ بیت‌کوین تا حدود ۰٫۰۰۰۱۷۵۸۹۹۵$).

سوابق تراکنش روی شبکه بیت‌کوین در بلاکچین بیت‌کوین ذخیره می‌شود و با نرم‌افزارهای منبع‌باز و رایگانی که به آنها پروتکل بیت‌کوین می‌گویند، مدیریت می‌شود. به‌جای انتقال موسیقی یا فایل‌های چندرسانه‌ای، رایانه‌ها در شبکه بیت‌کوین اطلاعاتی

1. Cold wallet

درباره تراکنش‌های جدید در شبکه تبادل می‌کنند. پروتکل بیت‌کوین شامل مکانیسمی است که به اعضای شبکه کمک می‌کند تا به اجماع برسند؛ درباره اینکه آیا تراکنش مذکور معتبر است یا اینکه باید روی بلاکچین بیت‌کوین ثبت شود.

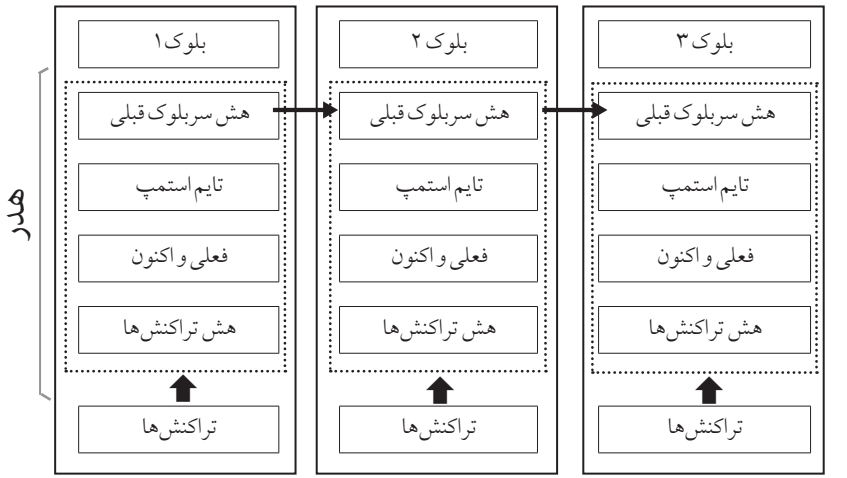
بر خلاف ارز و سکه‌های فیزیکی (یعنی آنچه دست‌به‌دست می‌چرخد، بدون آنکه ردی از خود بر جای بگذارد) همه تراکنش‌های بیت‌کوین روی بلاکچین بیت‌کوین ذخیره می‌شوند و به‌طور عمومی قابل ممیزی (بلاکچین) هستند. هر کسی که بخواهد به شبکه بیت‌کوین ملحق شود، می‌تواند یک نسخه کامل از بلاکچین بیت‌کوین را دانلود یا مرور کند و از طریق تراکنش‌های بیت‌کوین آن را ردیابی کند. به سبب ذات آزاد و شفاف بیت‌کوین، بلاکچین بیت‌کوین به‌طور گسترده توزیع شد و در حال حاضر روی هزاران رایانه در بیش از ۹۷ کشور وجود دارد. کپی‌هایی از بلاکچین بیت‌کوین را می‌توان در بین کشورهای بزرگ صنعتی یافت؛ آمریکا و چین و حتی کشورهای کوچک نظیر کامبوج و کشـــور بلیز (Belize). از آنجا که بلاکچین بیت‌کوین در سراسر دنیا ذخیره می‌شود، به‌سبب اتکای شبکه پرداخت بر یک شبکه همتابه‌همتا، بیت‌کوین قابلیت ارتجاع دارد و به‌طور استثنایی از کار انداختن آن دشوار است. بنابراین، تا زمانی که یک رایانه نسخه‌ای از بلاکچین بیت‌کوین را داشته باشد، شـــبکه بیت‌کوین همچنان وجود دارد. حتی در صورت وقوع بلایای طبیعی یا اقدام یک دولت مرکزی برای از کار انداختن شـــبکه مذکور، می‌توان بلاکچین بیت‌کوین را کپی و آن را ظرف چند ساعت تکثیر کرد (در صورت وجود سرعت بالا در اتصالات اینترنتی).

از بسیاری جهات، بلاکچین بیت‌کوین را می‌توان «کتابی» مقاوم در برابر تغییر دانست که نسخه‌های مشابه آن روی چندین رایانه در سراسر دنیا ذخیره شده است. هر کسی می‌تواند محتوای جدیدی به این کتاب اضافه کند و پس از آنکه آن محتوای جدید اضافه شد، همه نسخه‌های کنونی کتاب روی رایانه‌هایی که پروتکل بیت‌کوین را اجرا می‌کنند، به‌روزرسانی می‌شود.

با این حال، بر خلاف کتاب، بیت‌کوین به‌واسطه صفحات سازمان‌دهی می‌شود. در عوض، چندین دسته از تراکنش‌های بیت‌کوین در قالب بلوک‌های مجزا گروه‌بندی

می‌شوند و پروتکل بیت‌کوین آنها را به یکدیگر پیوند می‌دهد تا زنجیره‌ای متوالی و با ثبت زمانی تشکیل شود. هر بلوک حاوی اطلاعاتی درباره انتقال بیت‌کوین‌ها از یک عضو به عضو دیگر شبکه است و اطلاعات دیگری نیز وجود دارد که ممکن است به هر تراکنش پیوست شود (نظیر یک شعر، دعا، مرجع یک عکس یا دیگر فایل‌ها). هر بلوک نیز حاوی یک راس است که از آن برای سازمان‌دهی پایگاه داده مشترک استفاده می‌شود.

اجزای اصلی سربلوک (block header) مانند اثر انگشت منحصربه‌فرد هستند (که به آنها هش (hash) می‌گویند) و برای همه تراکنش‌های آن بلوک است و در کنار ثبت زمانی (تایم‌استمپ)[1] قرار می‌گیرد که در واقع یک هش (درهم) از بلوک قبلی است. هش‌ها را با استفاده از توابع هشینگ رمزی استاندارد تولید می‌کنند که آژانس امنیت ملی آمریکا (NSA) اختراع کرده و روشی برای بازنمایش تراکنش‌های یک بلوک به‌صورت رشته‌ای از کاراکترها و اعداد است که به‌طور منحصربه‌فرد با تراکنش بلوک در ارتباط هستند.



شکل ۱،۱: بلاکچین ساده‌شده بیت‌کوین

با آنکه کتاب بر شـــماره صفحاتش تکیه دارد تا محتوای داخلی‌اش را نظم دهد (و همین مطلب باعث می‌شود که صحافی یک کتاب با نظم خاص ممکن شود) بلاکچین

1. timestamp

بیت‌کوین به داده‌های ذخیره‌شده در هر ســـربلوک برای سازمان‌دهی پایگاه داده‌های مشترک متکی است که شامل یک هش از بلوک قبلی و یک تایم‌استمپ است و در نتیجه زنجیره‌ای متوالی تولید می‌شود (به شکل ۱,۱ نگاه کنید).

برای امنیت و یکپارچگی بلاکچین بیت‌کوین، ناکاموتو یک سیستم مبتکرانه ساخت که اضافه‌کردن اطلاعات را به بلاکچین بیت‌کوین دشـــوار می‌سازد و حتی اصلاح یا پاک‌کردن اطلاعات را پس از ذخیره‌شدن‌شان سخت‌تر می‌کند. ذخیره‌سازی اطلاعات در بلاکچین بیت‌کوین نیازمند زمان است و فقط می‌توان از طریق تلاش جمعی آن را انجام داد. پروتکل بیت‌کوین رویه‌ای سفت‌وسخت برای اضافه‌کردن بلوک‌های جدید به پایگاه داده مشترک دارد و همه بلوک‌ها نیز برای اطمینان از اینکه آنها حاوی تراکنش‌ها و هش‌های معتبر هستند، تایید می‌شوند.

با آنکه تولید یک هش در هر بلوکی نباید چالش‌برانگیز باشـــد، پروتکل بیت‌کوین به‌طور هدفمند این کار را با مطرح‌کردن یک شرط دشوار می‌سازد؛ هش هر بلوک باید با یک عدد خاص همراه با صفر مقدم[1] آغاز شود. این کار با استفاده از یک بازی حدسی ریاضی انجام می‌شود که معمولا نوعی «اثبات کار»[2] است. برای تولید یک هش معتبر با تعداد مورد نیاز صفر مقدم، گروه‌های هر شبکه باید یک معمای ریاضی را حل و تضمین کنند که راهکار آنها حاوی حداقل صفر مقدم مورد نیاز است که در پروتکل بیت‌کوین مشخص شده و در آن لحظه نیاز است.

هر رایانه‌ای سعی دارد تا هش معتبری تولید کند که در سراسر محاسبات تکرارشده اجرا می‌شود تا با الزامات سفت‌وسخت آن پروتکل هم‌خوانی و مطابقت داشته باشد. یافتن یک راهکار برای این معمای ریاضی نیازمند محاسبات دلخواه نیست؛ صرفا یک بازی صحیح و خطا است که غالبا از آن با عنوان «معدن‌کاوی»[3] یاد می‌کنند.

پروتکل بیت‌کوین دشواری معمای ریاضی را تعدیل می‌کند که به تعداد معدن‌چیان در شبکه بیت‌کوین بستگی دارد که اثبات کار را انجام می‌دهند تا بدین صورت مطمئن

1. leading zeros
2. proof of work
3. mining

شوند که شـــبکه یک بلوک جدید در هر ۱۰ دقیقه اضافه می‌کند. هر چقدر گره‌های بیشتری در شبکه بیت‌کوین با قصد حل این معما وجود داشته باشد، تولید یک هش معتبر با یک تعداد مناسب از صفرهای مقدم دشوارتر می‌شود.

پس از آنکه معدن‌کاو یک هش معتبر برای یک بلوک خـــاص پیدا کرد، راهکار را به شبکه بیت‌کوین مخابره می‌کند. پس از مخابره، دیگر گره‌ها در شبکه یک محاسبه ساده انجام می‌دهند تا مطمئن شوند که هش حاصله با مشخصات و الزامات پروتکل بیت‌کوین مطابقت دارد. اگر معتبر باشد، آن بلوک به بلاکچین بیت‌کوین افزوده می‌شود و روی هارددرایوهای گره‌های فعال ذخیره می‌شـــود. از طریق این فرایند، شـــبکه به این توافق می‌رسد که چه کسی مالک آن مقدار از بیت‌کوین در آن لحظه است. گاهی اوقات، بخش‌های مختلف این شبکه به بلوک متفاوتی در بلاکچین می‌پیوندند و شبکه بیت‌کوین دچار انشعاب[1] می‌شود یا به چندین نسخه تقسیم می‌شود. گاهی، انشعاب‌ها در نتیجه تقسیم‌شدن شبکه رخ می‌دهد؛ احتمالاً به سبب حمله خرابکارانه این اتفاق رخ می‌دهد. در دیگر مواقع، انشعاب‌ها وقتی رخ می‌دهند که نسخه به‌روزشده‌ای از ایستگاه پردازش برای اجرای شبکه بیت‌کوین منتشر شود و چندین گره متصل به این شبکه در به‌روزرسانی نرم‌افزار خود با شکست مواجه شوند؛ در نتیجه غفلت یا انکار واقعی در پذیرش تغییرات فناورانه در یک پایگاه کد جدید نیز ممکن است این اتفاق رخ دهد.

وقتی بلاکچین بیت‌کوین دچار انشعاب می‌شود، ساختار پایگاه داده به‌تدریج شبیه درخت می‌شـــود تا یک زنجیره خطی. برای اطمینان از اینکه این ش‌ب‌که در نهایت به‌سوی شاخه‌ای از آن درخت حرکت می‌کند، پروتکل بیت‌کوین یک قانون خاص را اجرا می‌کند (انتخاب انشعاب)[2] و قید می‌کند که در صورت به وجود آمدن یک انشعاب، معدن‌کاوها باید همیشه بلندترین زنجیره را در پیش بگیرند؛ در این صورت، شاخه‌ای که بیشترین بلوک تاییدشده را داشته باشد (که بر اساس قدرت محاسباتی اندازه‌گیری شده است) اجازه اعتبارسنجی بلوک‌ها را دارد.

این قانون باعث می‌شود که پروتکل بیت‌کوین اجماع را در سراسر شبکه حفظ کند.

1. fork
2. fork choice

اگر اکثریت شبکه بر سر زنجیره خاصی از تراکنش‌ها به توافق برسند، آن زنجیره معتبر فرض می‌شود. بنابراین، کسانی که بیت‌کوین دارند در هر زمانی به آن اعتماد دارند، کسانی که اکثریت قدرت پردازشی حمایت‌کننده از شبکه بیت‌کوین را کنترل می‌کنند، مطابق قوانین پروتکل عمل می‌کنند و تراکنش‌ها را تایید و بلوک‌های جدید را روی بلندترین زنجیره ثبت می‌کنند.

اثبات کار (بازی حدس‌زدن) فقط برای تضمین ذخیره‌سازی منظم اسناد در بلاکچین بیت‌کوین مفید نیست. این الگوریتم اجماعی همچنین مانع آن می‌شود که افراد تراکنش‌های قلابی ایجاد کنند یا اسناد ذخیره‌شده در بلاکچین بیت‌کوین را تغییر دهند. چون راس هر بلوک شامل یک هش از سربلوک‌های قبلی است، هر کسی که بخواهد محتوای ذخیره‌شده در بلوک را تغییر دهد، ناگزیر زنجیره را می‌شکند. حتی یک تغییر کوچک باعث ایجاد هش جدید و منحصربه‌فردی می‌شود که به بلوک تغییریافته مربوط است و لزوما تغییری را در هش‌های همه بلوک‌های بعدی ایجاد می‌کند.

هر کسی که بخواهد حتی یک سند را در بلاکچین بیت‌کوین اصلاح کند، باید کار پرهزینه و طاقت‌فرسای تولید هش‌های جدید را به ازای هر بلوک در بلاکچین بیت‌کوین انجام دهد. هر چقدر تراکنش‌های بیشتری روی شبکه رخ دهد و بلوک‌های بیشتری به بلاکچین بیت‌کوین متصل شوند، اصلاح بازگشتی تراکنش‌های ثبت‌شده نیز دشوارتر می‌شود. علاوه بر این، چون بلاکچین بیت‌کوین از طریق اجماع کار می‌کند، یک مهاجم یا گروه مهاجمان باید تاریخچه تراکنش مورد نظر را در بلاکچین بیت‌کوین بازنویسی کنند؛ آن هم سریع‌تر از اکثر گره‌های معتبری که روی شبکه وجود دارد.

ممکن‌ترین شیوه برای تغییر یک سند در بلاکچین بیت‌کوین این است که «حمله ۵۱٪» را انجام دهند و به‌طور موثر شبکه را در دست بگیرند، به‌طوری که آنها بتوانند تراکنش‌ها را با نرخی که از باقی شبکه سریع‌تر است، تایید کنند. با توجه به مقیاس شبکه توزیع‌شده بیت‌کوین، چنین حمله‌ای به‌طور فزاینده‌ای غیرممکن می‌شود. معدن‌کاوهای بیت‌کوین که در سال ۲۰۱۵ کار خود را شروع کردند، طبق گفته نشریه اکونومیست، ۱۳ هزار برابر بیش از مجموع قدرت محاسبات عددی ۵۰۰ ابررایانه بزرگ دنیا قدرت دارند. با توجه

به رشد این شبکه، هماهنگ‌کردن چنین حمله‌ای تا به امروز صدها میلیون‌ها دلار هزینه خواهد داشت. عملیاتی که برای بیشـــتر گروه‌های خصوصی یا ائتلاف‌های هکری مستقل هزینه سرسام‌آوری در پی خواهد داشت.

برای متوازن‌کردن هزینه ورود به معدن‌کاوی بیت‌کوین، ناکاموتو یک طرح تشویقی زیرکانه راه انداخت تا مردم را تشویق کند که بلاکچین بیت‌کوین را حفظ کنند و امن نگه دارند. هر بار که یک معدنچی یک هش معتبر برای یک بلوک جدید از تراکنش‌ها تولید کند، شبکه بیت‌کوین با مقداری بیت‌کوین به آن معدنچی پاداش می‌دهد که به آن «پاداش بلوک»[1] می‌گویند و این مقدار علاوه بر دستمزد تراکنش است. بنابراین معدن‌کاوها در شبکه بیت‌کوین طرح تشویقی اقتصادی دارند تا تراکنش‌ها را اعتبارسنجی کنند و در اثبات کار متعهد باشند و باانگیزه رفتار کنند. آنها، با معطوف‌کردن منابع محاسباتی خود، می‌توانند به ازای هر بلوکی که اعتبارسنجی می‌کنند به پاداش بلوکی و کارمزد تراکنش برسند و ارز دیجیتال را در بازار آزاد به دیگران بفروشند.

چون پروتکل بیت‌کوین فقط برنامه‌ریزی‌شده است تا ۲۱ میلیون بیت‌کوین تولید کند، ناکاموتو پذیرش اولیه را توصیه می‌کند. پاداش بلوکی به‌طور تدریجی با گذشت زمان کاهش می‌یابد؛ تقریبا هر چهار سال یک‌بار نصف می‌شود و این فرایند از زمان معرفی این شبکه در ۲۰۰۹ شروع شده است و تقریبا تا ۲۱۴۰ ادامه خواهد داشت. معدن‌کاوها از این شبکه در روزهای اول پشتیبانی می‌کنند، بنابراین فرصت رسیدن به بیت‌کوین‌های بیشتری را خواهند داشت.

با ترکیب الگوریتم اثبات اجماع کار و طرح‌های تشویقی پاداش بلوکی، ناکاموتو طرحی را توســـعه داد که از طریق ســـاخت یک سیســـتم غیرمتمرکز بتواند عرضه بیت‌کوین را محدود کند و تراکنش‌ها را بدون نیاز به موسسات متمرکز تهاتر انجام دهد و مشـــکل دوبار خرج‌کردن را حل کند. ســـرانجام، ناکاموتو «سیســـتم انتقال وضعیت»[2] را ایجاد کرد. هر ۱۰ دقیقه، شـــبکه بیت‌کوین وضعیـــت خود را به‌روز می‌کند و موجودی همه حســـاب‌های فعلی بیت‌کوین را محاسبه می‌کند. الگوریتم

1. block reward
2. state transition system

اجماع اثبات کار به‌عنوان یک تابع انتقـــال وضعیت عمل می‌کند که وضعیت کنونی پاداش شبکه بیت‌کوین را در نظر می‌گیرد و آن را با مجموعه‌ای از تراکنش‌های جدید بیت‌کوین به‌روز می‌کند.

برای ارزیابی اینکه آیا کاربر برای اجرای تراکنش، بیت‌کوین کافی دارد یا خیر، پروتکل بیت‌کوین در سراسر تراکنش‌های قبلی جست‌وجو می‌کند و از اولین بلوک بیت‌کوین این کار را آغاز می‌کند (بلوک مولد/بلوک زاینده[1]). اگر کاربر، بیت‌کوین کافی داشته باشد، تراکنش معتبر فرض می‌شود و در بلوک جای می‌گیرد. پس از آنکه معدن‌کاو هش معتبری با اثبات کار تولید کند که دیگر معدن‌کاوها آن را تایید می‌کنند، وضعیت شبکه بیت‌کوین به‌روز می‌شود که شامل موجودی حســـاب‌های دخیل در تراکنش‌های آن بلوک نیز هست. البته اگر کاربر، بیت‌کوین کافی نداشته باشد، تراکنش از طرف شبکه رد می‌شـــود. معدن‌کاوها تراکنش را در یک بلوک وارد نمی‌کنند و تراکنش نامعتبر بر وضعیت شبکه اثری ندارد.

از طریق این طراحی فنی، حتی با وجود اینکه بیت‌کوین موسسه تهاتر متمرکز ندارد، کاربران مطمئن می‌شـــوند که هر حســـاب بیت‌کوین در لحظه معین دقیق است. این پروتکل به صورتی اجرا شده که تعامل قابل اعتماد همتابه‌همتا بین افرادی که یکدیگر را نمی‌شناسند ممکن شود و بنابراین لزوما نباید به یکدیگر اعتماد داشته باشند. به همین علت است که بیت‌کوین و فناوری بلاکچین در حالت کلی به‌صورت سیستمی بی‌نیاز از اعتماد تعریف شده است. به‌جای اتکا بر یک نهاد معتمد متمرکز یا یک واسطه، افراد باید به کدهای بنیادی و معدن‌کاوهایی اعتماد کنند که از بلاکچین بیت‌کوین حمایت می‌کنند.

اتریوم

با عرضه و رشد سریع بیت‌کوین، بسیاری از برنامه‌نویســـان شروع به بررسی این فناوری برای استفاده در خارج از حوزه ارز دیجیتال کردند. پس معرفی بیت‌کوین، صدها بلاکچین و ارزهای دیجیتال جدید ظاهر شدند که انگار یک‌شبه این اتفاق رخ داده است و خدمات کیف‌پول متمرکز به وجود آمد تا به مردم در پیوستن به شبکه بیت‌کوین کمک

1. genesis block

کند. همچنین تبادلات باعث شد که معامله بیت‌کوین در ازای ارزهای سنتی رایج نظیر دلار آمریکا، یورو و یوآن چین ممکن شود. بنابراین قیمت بیت‌کوین به‌سرعت بالا رفت و برای مدت اندکی به سقف ۱۲۰۰ دلار رسید (در سال ۲۰۱۳) و علاقه به بیت‌کوین بیشتر شد و سرمایه‌گذاران جسور و کسب‌وکارهای سنتی، نظیر مایکروسافت و دل نیز از بیت‌کوین به‌عنوان یکی از گزینه‌های پرداخت استفاده می‌کردند.

با این حال، هر چقدر افراد بیشتری وارد بیت‌کوین می‌شدند، محدودیت‌های آن نیز بیشتر هویدا می‌شد. بیت‌کوین به‌عنوان پلتفرمی برای تسهیل تبادل ارز دیجیتال عرضه شده بود، اما بدون به‌روزرسانی پروتکل‌های خود، نمی‌توان از آن استفاده فراوانی کرد. شبکه بیت‌کوین کند بود (فقط هر ۱۰ دقیقه یک‌بار موفق می‌شد تا به اجماع برسد و تراکنش‌ها را تایید کند) بنابراین، پرسش‌هایی درباره میزان اطلاعاتی که بیت‌کوین می‌تواند ذخیره کند، شکل گرفت. ساختار غیرمتمرکز بیت‌کوین باعث شد که به‌روزرسانی و بهبود آن دشوار شود و این شبکه فاقد حاکمیت رسمی بود و بر تلاش گروه کوچکی از توسعه‌دهندگان متکی بود که به کندی ایرادات را در نرم‌افزار اصلی رفع می‌کردند.

در همین حین پروژه‌های جدید مبتنی بر بلاکچین به کار افتاد، با این امید که این محدودیت‌ها برطرف شود. آنها به‌دنبال بهره‌مندی از قدرت بلاکچین بودند؛ نه فقط برای ذخیره‌سازی اطلاعات مرتبط با انتقال ارز دیجیتال، بلکه برای ساخت محیطی که از نرم‌افزارهای غیرمتمرکز[1] میزبانی کند (در اختصار به آنها dapps می‌گویند) که حداقل تا حدودی برای اجرای توابعش بر بلاکچین متکی بود.

در سطح عمومی، به سبب آنکه بلاکچین یک سیستم ذخیره‌سازی داده است، ممکن است از این فناوری برای کارهایی بیش از ذخیره داده‌های مرتبط با تراکنش‌های بیت‌کوین استفاده شود. بلاکچین‌ها می‌توانند دیگر انواع اطلاعات را نیز ذخیره کنند که از آن جمله می‌توان به برنامه‌های کاربردی در رایانه‌های کوچک اشاره کرد که فعالان این عرصه به آنها قراردادهای هوشمند می‌گویند.

1. decentralized applications

اولین بلاکچین‌ها که می‌توانستند قراردادهای هوشمند پیچیده را ایجاد و اعمال کنند بلاکچین‌های اتریوم بودند. دومین نسل از شبکه‌های مبتنی بر بلاکچین‌ها که بر اساس بیت‌کوین ساخته شده بود، اما کاربردپذیری بیشتری داشت و گروه‌ها را قادر می‌ساخت تا از قراردادهای هوشمند روی بلاکچین‌ها استفاده کنند؛ درست مانند آنکه فرد بخواهد کدهای یک وب‌سایت را همین امروز روی یک سرور بارگذاری کند و در فوریه ۲۰۱۴ معرفی شد و تقریبا یک سال‌ونیم بعد عرضه شد.

اتریوم، مانند بیت‌کوین، شبکه‌ای همتابه‌همتاست که یک پروتکل منبع‌باز و آزاد آن را کنترل می‌کند. اتریوم ارز دیجیتال منحصربه‌خود را دارد (اتر)[1] که به معدن‌کاوهایی اختصاص می‌یابد که از شبکه پشتیبانی می‌کنند و می‌توان آن را نیز مانند بیت‌کوین منتقل کرد. بلاکچین اتریوم از یک مکانیسم اثبات کار مشابه برای به‌روزرسانی وضعیت بلاکچین اتریوم استفاده می‌کند. با این حال، بر خلاف بیت‌کوین، اتریوم سریع‌تر است و برای قراردادهای هوشمند ظرفیت بیشتری دارد. بلاکچین اتریوم تقریبا هر ۱۲ ثانیه به‌روز می‌شود (نه هر ۱۰ دقیقه). همچنین، اتریوم یک زبان برنامه‌نویسی تورینگ کامل[2] را اجرا می‌کند که سالیدیتی[3] نام دارد که نوشتن قراردادهای هوشمند و استفاده از نرم‌افزارهای غیرمتمرکز را ممکن می‌سازد. با وجود سالیدیتی، امکان اجرای محاسبات پیچیده روی شبکه همتابه‌همتا از لحاظ نظری وجود دارد.

بر خلاف بیت‌کوین که فقط یک نوع حساب داشت، در شبکه اتریوم، دو نوع حساب متفاوت وجود دارد؛ یکی برای کاربران هر روزه شبکه (که به آن حساب با مالکیت خارجی[4] می‌گویند) و دیگری برای نرم‌افزارهای قراردادهای هوشمند (که به آن حساب قرارداد[5] می‌گویند). یک حساب قراردادی دارای آدرس عمومی روی شبکه اتریوم است، اما کلید خصوصی ندارد. کدهای استخراج‌شده از قرارداد هوشمند را ذخیره می‌کند و می‌تواند اتر را جمع‌آوری یا توزیع کند، داده‌ها را روی بلاکچین اتریوم ثبت

1. ether
2. Turing- complete programming langua
3. Solidity
4. externally owned account
5. contract account

کند، اطلاعات را پردازش کند و احتمالا اجرای دیگر قراردادهای هوشمند را ممکن سازد. یک حساب با کنترل خارجی متفاوت است. درست مانند بیت‌کوین، این حساب به یک آدرس عمومی اختصاص می‌یابد و هر کسی که به آن کلید خصوصی دسترسی داشته باشد، می‌تواند اتر را به دیگر اعضای شبکه بفرستد و با قراردادهای هوشمند ذخیره‌شده در حساب قرارداد تعامل داشته باشد.

آن بخشی از پروتکل اتریوم که مسئول پردازش قراردادهای هوشمند است، ماشین مجازی اتریوم (EVM)[1] نام دارد. از دیدگاه عملی، می‌توان EVM را نوعی ماشین مجازی غیرمتمرکز دانست که روی چندین برنامه از قراردادهای هوشمند کار می‌کند. به‌عنوان قانونی کلی، هر کسی می‌تواند اجرای قرارداد هوشمند را با فرستادن یک اتر تراکنش به حساب قرارداد مرتبط اجرا کند و در نتیجه چرخ اتریوم این‌گونه به حرکت درمی‌آید.

قراردادها یا با پیام فرستنده یا با پیام گیرنده تعامل می‌کنند. پیام یک شیء حاوی مقدار خاصی اتر و آرایه‌ای از داده‌ها، آدرس فرستنده و آدرس مقصد است (که یا می‌تواند حساب قرارداد دیگری باشد یا یک حساب با مالکیت خارجی). وقتی قرارداد یک پیام دریافت می‌کند، گزینه بازگشت دادن پیام به فرستنده اصلی را دارد؛ تا حد زیادی مانند یک تابع استاندارد رایانه‌ای عمل می‌کند.

بر اساس طراحی، هر عملیاتی که ماشین مجازی اتریوم آن را پردازش می‌کند، به‌واسطه گره‌های فعال در شبکه اتریوم اجرا می‌شود. از طریق این اجرا، هر نوع تضادی با EVM اتریوم می‌تواند قرارداد دیگری را به ازای هزینه صفر فعال کند. برای پرهیز از این سوءاستفاده، پروتکل اتریوم کارمزد کمی را مطالبه می‌کند که به آن «گاز» (یا سوخت/بنزین) به ازای هر مرحله محاسباتی می‌گویند.

برای پرهیز از نوسانات اضافی قیمت، قیمت گاز ثابت نیست، بلکه به‌طور دینامیکی از سوی معدن‌چیان و مبنای قیمت بازار اتر تنظیم می‌شود. همچنین، پروتکل اتریوم را می‌توان در یک بلوک جای داد و معدن‌چیان شبکه اتریوم را مجبور کرد تا کارمزد گاز مطالبه کنند که با هزینه تراکنش دیگران در شبکه متناسب است.

1. Ethereum Virtual Machine (EVM)

ذات آزاد و غیرمتمرکز اتریوم به قراردادهای هوشمند اجازه می‌دهد تا به‌طور نیمه‌ناشناس مستقر شوند و به‌طور خودمختار کار کنند. چون همه گره‌های فعال روی اتریوم کد مربوط به تمام قراردادهای هوشمند را اجرا می‌کند، این کد از سوی یک گروه کنترل نمی‌شود و تغییر نمی‌کند. از یک جهت، قرارداد هوشمند مانند یک نماینده خودمختار فعالیت می‌کند که به‌طور خودکار به ورودی‌های دریافتی از حساب‌های با مالکیت خارجی یا دیگر برنامه‌های مرتبط با قراردادهای هوشمند که روی این شبکه اجرا می‌شوند، پاسخ می‌دهد.

از زمان عرضه اتریوم تاکنون، صدها هزار قرارداد هوشمند به‌کار گرفته شدند که این قراردادهای هوشمند توانایی پردازش منطق ابتدایی را دارند («اگر این شد، پس آن شود»[1]) و می‌توان از آن برای تولید و انتقال توکن‌ها (مربوط به دارایی‌های فیزیکی و دیجیتالی)، تایید امضاها، ثبت آرا و اجرای سیستم‌های حاکمیت مبتنی بر بلاکچین جدید استفاده کرد.

با این حال، با توجه به طرح بنیادی شبکه، اجرای کد از طریق EVM اتریوم کند است و به‌طور بالقوه گران تمام می‌شود. با وجود این محدودیت‌ها، اتریوم راه را برای الگوی جدید رایانش هموار می‌سازد؛ به‌طوری که نرم‌افزارهای کاربردی دیگر از سوی نهادی متمرکز کنترل نشوند، بلکه در عوض به‌طور خودمختار روی شبکه‌ای غیرمتمرکز و همتابه‌همتا اجرا شوند.

اشتراک‌گذاری فایل غیرمتمرکز و شبکه‌های همپوشان

برای گسترش توانمندی‌های بیت‌کوین، اتریوم و دیگر بلاک‌چین‌ها، پروتکل‌های غیرمتمرکز جدید توسعه می‌یابند و مدیریت انتقال دارایی‌های اضافی را برای بلاکچین ممکن می‌سازند (یعنی علاوه بر ارز دیجیتال). همچنین، قراردادهای هوشمند را قادر می‌سازند تا با دیگر فایل‌های دیجیتال تعامل و به‌طور بالقوه آنها را کنترل کنند. این پروتکل‌ها به‌عنوان «شبکه‌های همپوشان»[2] عمل می‌کنند که توانایی و مفیدبودن این

1. if this, then that
2. overlay networks

ساختارهای داده‌ای جدید را بسط و توسعه می‌دهند.

برای مثال، پروتکل‌هایی نظیر کالرکوین[1] گروه‌ها را قادر می‌سازد تا از شبکه بیت‌کوین برای خلق توکن‌هایی استفاده کنند که بازنمودی از بازه دارایی‌های ارزشمند است. گروه‌ها با استفاده از پروتکل کالرکوین می‌توانند تراکنشی را برای یک مقدار اسمی از بیت‌کوین (یا دیگر ارزهای دیجیتال) بفرستند و چند فراداده را به تراکنش ضمیمه کنند تا نشان دهند که آن تراکنش در حقیقت بازنمودی از انتقال دارایی‌های محسوس یا دارایی‌های دیجیتال است؛ نظیر یک گواهی سپرده و سهام، مالکیت اثری که حق نشر آن محفوظ است یا دادن رای. به‌عبارتی دیگر، با استفاده از پروتکل کالرکوین، انتقال مقادیر بسیار اندک از بیت‌کوین (در حد ۰,۰۰۰۰۰۰۰۰۰۱) می‌تواند امکان انتقال سهام گوگل را نیز ممکن سازد.

علاوه بر این، پروتکل‌های غیرمتمرکز اشتراک‌گذاری فایل، افراد را قادر می‌سازد تا فایل‌ها را روی شبکه همتابه‌همتا ذخیره کنند و دسترسی به آن فایل‌ها را با استفاده از قراردادهای هوشمند، ایجاد ابزارهای جدید برای ساخت نرم‌افزارهای غیرمتمرکز پیچیده و منسجم و دیگر موارد کنترل کنند. چون بلاکچین می‌تواند فقط یک مقدار محدود از اطلاعات را به ازای هر تراکنش ذخیره کند و اینکه بلاکچین اتریوم به ازای هر مرحله محاسباتی کارمزدی را در برنامه قرارداد هوشمند مطالبه می‌کند، غالبا ساخت نرم‌افزارهای کاربردی غیرمتمرکز که برای ذخیره فایل به یک بلاکچین متکی باشند، هزینه‌بر است.

پلتفرم‌های ذخیره‌سازی توزیع‌شده جدید و سرویس‌های توزیع محتوا، نظیر سوآرم و فایل‌کوین (که از پروتکل‌های IPFS استفاده می‌کنند) به‌دنبال رفع این محدودیت‌ها به‌منظور پشتیبانی از کاربردهای پیشرفته بلاکچین هستند. هدف از این سیستم‌های جدید تامین امنیت و ذخیره‌سازی ارتجاعی همتابه‌همتا در شبکه‌های مبتنی بر بلاکچین است که هیچ نیازی به مدیریت متمرکز نداشته باشند، زمان از کارافتادگی آنها صفر باشد و بتوانند حتی در صورتی که برخی اعضا از شبکه خارج شدند، به فعالیت خود ادامه دهند.

---

1. Color Coin

درست مانند بیت‌کوین و اتریوم، این شبکه‌های همپوشان نیز مکانیسم‌های تشویقی درون‌ساخت دارند تا پذیرش و اســـتفاده را ترویج کنند. اعضای این شبکه‌ها در ازای ذخیره‌سازی داده، پاداش دریافت می‌کنند و آن را به گروه ثالث انتقال می‌دهند. آن پهنای باند یا فضای اضافی روی هارددرایو می‌تواند در این شـــبکه‌ها استفاده شود و به‌طور داوطلبانه برای ذخیره‌سازی بخش‌های کوچکی از فایل‌ها به‌توافق برسند (که به آنها قطعه درشت یا قطعه ریز[1] می‌گویند) که در صورت تقاضا از سوی این پروتکل‌های غیرمتمرکز اشتراک‌گذاری فایل، دوباره مونتاژ می‌شوند.

از طریق انباشت پهنای باند و منابع ذخیره‌سازی، تصور می‌شود که فناوری‌های پشت این سیستم‌های غیرمتمرکز از طریق قدرت اعداد بتوانند در سرویس‌های آنلاین کنونی گامی فراتر بردارند. به جای ساخت یک نرم‌افزار کاربردی آنلاین از طریق کرایه‌کردن فضا از یک ارائه‌کننده سرویس ســـنتی ابری نظیر آمازون، مایکروسافت یا آی‌بی‌ام، یا اتکا بر واســـطه‌های بزرگ غیرمتمرکز نظیر فیس‌بوک و گوگل، برای میزبانی داده‌ها، نرم‌افزارهای غیرمتمرکز جدید برای هماهنگ‌سازی و ذخیره‌سازی بر فناوری بلاکچین و شبکه‌های همتابه‌همتا متکی خواهند بود. اگر این کار با موفقیت انجام شود، بلاکچین و این پروتکل‌های غیرمتمرکز جدید ممکن است بر معماری اینترنتی کاملا جدیدی استوار شوند (که گاهی اوقات به آنها نسخه سوم وب می‌گویند).

بلاکچین مجوزدار

چون بلاکچین غیرمتمرکز است و امکان اجرای کدهای خودمختار را ممکن می‌سازد، تلاش‌هایی برای مهار قدرت بلاکچین به شیوه‌ای کنترل‌شده و قابل پیش‌بینی، در دست انجام است. بیت‌کوین، اتریوم و دیگر بلاکچین‌ها بی‌نیاز از مجوز، برای همگان آزاد و در دسترس هستند. هر کسی که به اینترنت متصل باشد، می‌تواند آن نرم‌افزار منبع‌باز را که بر این بلاکچین حاکمیت می‌کند، دانلود کرده و در شـــبکه مشارکت کند، بدون آنکه لازم باشد هویت واقعی خود را فاش کند یا به‌دنبال مجوز باشد. ذات نیمه‌ناشناس و غیرمتمرکز و آزاد بلاکچیـــن بی‌نیاز از مجوز، زمانی باعث نگرانی می‌شـــود که در

1. chunks or shards

محیط‌های به‌شدت مقرراتی نظیر بانکداری و امور مالی به‌کار رود و نیازمند آن است که موسسات مالی، گروه‌ها را زیر نظر بگیرند و فعالیت‌های مشکوک را گزارش کنند.

در امتداد بیت‌کوین و اتریوم، چندین بلاکچین به وجود آمده است. این بلاکچین‌ها بر شبکه همتابه‌همتا متکی هستند، اما هر کسی نمی‌تواند به آنها ملحق شود. در عوض، یک نهاد متمرکز یا ائتلاف، گروه‌های مجاز را برای مشارکت در این شبکه بلاکچین انتخاب می‌کند و محدودیت‌هایی را درباره کسانی که می‌توانند به اطلاعات دست یابند یا آن را روی پایگاه داده مشترک ثبت کنند، اعمال می‌کند. اعضای ائتلاف در نهایت عضویت را کنترل می‌کنند، بنابراین محیطی ایجاد می‌شـــود که در آن هر گروه در شبکه هویت مشخصی دارد یا تا حدی قابل اعتماد است.

بلاکچین‌های مجوزدار کنونی غالبا هدف‌محور هستند. به‌طور مثال، پروتکل ریپل[1] از یک بلاکچین مجوزدار برای تسهیل تبادل ارزش و دیگر ارزش‌ها نظیر دلار آمریکا، یورو و حتی طلا استفاده می‌کنند. پروتکل ریپل یک مکانیسم ائتلاف جایگزین است که با اثبات کار بیت‌کوین و اتریوم فرق دارد که بر شبکه‌های فرعی معتمد جمعی در شبکه ریپل بزرگ‌تر اتکا دارند تا تراکنش‌ها را پردازش و آنها را تایید کنند.

در حال حاضر، یکی از مزیت‌های قابل توجه بلاکچین مجوزدار سرعت آن است. در یک شبکه آزاد و بی‌نیاز از مجوز، نظیر اتریوم و بیت‌کوین، گره‌های فعال باید درباره تایید هر تراکنش به اجماع برسند. در بیت‌کوین، این شبکه‌ها می‌توانند فقط تراکنش‌ها را هر ۱۰ دقیقه یک‌بار پردازش کنند و در اتریوم هر ۱۲ ثانیه این اتفاق رخ می‌دهد که از پایگاه‌های مدرن داده عقب می‌افتند، چون این پایگاه‌ها ظرف چند میلی‌ثانیه اطلاعات را ذخیره می‌کنند. به سبب آنکه بلاکچین مجوزدار تمایل دارد فقط با چند شرکت‌کننده از پیش‌تعیین‌شده کار کند، آنها می‌توانند شیوه‌های جایگزینی برای سنجش اعتبار و تایید تراکنش‌ها اجرا کنند که غالبا به شیوه‌ای سریع‌تر انجام می‌شود.

با وجود ایجاد منافع بر حسب ســـرعت و پیش‌بینی‌پذیری، بلاکچین مجوزدار در نهایت دچار یک نقص مهم می‌شود؛ اعتماد، ناپایدار است. در بلاکچین مجوزدار، هیچ

1. Ripple protocol

تضمینی وجود ندارد که گروه‌ها با یکدیگر تبانی نکنند تا بلاکچین اصلی را به شیوه‌ای تغییر دهند که ممکن است در نهایت به دیگر اعضای شبکه خسارت وارد کند. اگر فقط چند گروه بتوانند اطلاعات را اعتبارسنجی کرده و آنها را روی بلاکچین ذخیره کنند، این گروه‌ها به نقاط یکتای شکست (و کنترل) تبدیل می‌شوند که ممکن است خرابی‌های فنی، دستکاری یا هک‌کردن در پی داشته باشد. این محدودیت‌های امنیتی ممکن است سرانجام به پیامدهای فاجعه‌بار منجر شود؛ به‌ویژه اگر بلاکچین مجوزدار برای پشتیبانی از سیستم‌های اقتصادی و اجتماعی مهم رشد کند.

دغدغه امنیتی غالبا به‌واسطه بلاکچین مجوزدار در حال توسعه برطرف می‌شود. استدلال برخی این است که بلاکچین مجوزدار در نهایت باعث حذف نیاز به بلاکچین عمومی نظیر بیت‌کوین و اتریوم می‌شود. دیگران این موارد را به‌صورت راهکاری موقت می‌بینند؛ درست مانند اینترانت‌ها[1] که در اواسط دهه ۹۰ میلادی بر شرکت‌های آمریکایی تسلط داشتند.

حداقل در کوتاه‌مدت، احتمالا آینده فناوری بلاکچین شامل بلاکچین مجوزدار و بی‌نیاز از مجوز خواهد بود که در کنار یکدیگر با هماهنگی کار می‌کنند. تراکنش‌های سریع ممکن است روی بلاکچین مجوزدار رخ دهد، در حالی که (به‌سبب امنیت) وضعیت این شبکه‌ها ممکن است از طریق بلاکچین بی‌نیاز از مجوز و آزاد ایمن شود. اساسا، یک نفر می‌تواند آینده‌ای را تصور کند که طی آن بلاکچین بی‌نیاز از مجوز و آزاد به‌صورت ستونی برای اکوسیستم عمل می‌کند و شامل بلاکچین‌های مجوزدار گوناگون است که بر استفاده‌های خاص تمرکز دارند.

در حال حاضر، جنبه‌های نوآورانه واقعی بلاکچین در بلاکچین مجوزدار و خصوصی قرار ندارد؛ در زنجیره‌هایی قرار دارد که عمومی و بی‌نیاز از مجوز هستند. بلاکچین عمومی را می‌توان برای اهداف قانونی استفاده کرد، اما آنها می‌توانند از ادغام چندین سیستم غیرقانونی نیز پشتیبانی کنند که تغییر و کنترل آنها دشوار است.

بلاکچین‌های عمومی و بی‌نیاز از مجوز، به سبب ویژگی‌های منحصربه‌فردشان،

1. intranets

هیچ ندیده‌ای هنوز

انتشارات راه‌پرداخت

برای سفارش اینترنتی این کتاب به وبسایت انتشارات راه‌پرداخت مراجعه کنید
way2pay.shop

کتاب بلاکچین و قانـون به بررسـی موانع حقوقی و قانونی گسـترش اسـتفاده از بلاکچین و لزوم تصویب مقررات نویـن در این خصوص می‌پردازد. در این کتاب به این موضوع پرداخته می‌شـود که بلاکچین می‌تواند بر دولت‌ها نیز تاثیر داشته باشد و به شکل‌گیری ساختارهای نوین سـازمانی که تصمیم‌گیری‌های مشـارکتی در آن پررنگ‌تر است، بینجامد. حذف واسطه‌ها اصلی‌ترین مزیت بلاکچین به‌شمار می‌رود و همین مزیت به کاهش قدرت قوانین و مقررات سنتی منجر می‌شود. بلاکچین با حذف واسـطه‌هایی نظیر شـرکت‌های بزرگ و چندملیتی، ممکن است توان دولت‌ها برای نظارت بر بانکداری، کسب‌وکار، قانون و سایر حوزه‌های حساس را کاهش دهد. لذا برای بهره‌گیری هرچه بهتر از این فناوری به مقررات و رویکردهای قانونی نوین نیاز داریم که این کتاب به طور مفصل به آن پرداخته است.

Harvard University Press

کتاب بلاکچین و قانون با حمایت کارخانه نوآوری رسانه راه‌کار منتشر شده و ناشر اصلی آن انتشارات دانشـگاه هاروارد است

راه‌کار

انتشارات راه‌پرداخت

ناشـر فنـاوری و نـوآوری

way2pay.press

ISBN 978-622-7702-34-7

۱۹۰ هـزار تومـان