ویرایش سوم

راهنمای ورود به دنیای بیت کوین
اتریوم و ارزهای دیجیتال برای مبتدی‌ها

یک ساتوشی

محمد آذرنیوار / نیما ملک‌پور

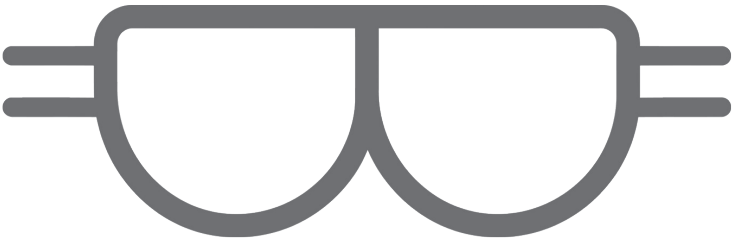
چاپ شانزدهم

انتشارات راه پرداخت

بسم الله
الرحمن
الرحيم

The mark of responsible forestry
FSC™ C009732

سرشناسه : آذرنیوار، محمد، ۱۳۷۶
عنوان و نام پدیدآور : یک ساتوشی: راهنمای ورود به دنیای بیت‌کوین، اتریوم و ارزهای دیجیتال برای مبتدی‌ها
نویسنده : محمد آذرنیوار، نیما ملک‌پور
وضعیت ویراست : [ویراست۳]
مشخصات نشر : تهران: راه پرداخت، ۱۴۰۱
مشخصات ظاهری : ۳۱۹ ص.: مصور، جدول، نمودار.
شابک: ۲-۲۶-۷۷۰۲-۶۲۲-۹۷۸
وضعیت فهرست نویسی : فیپا
یادداشت : چاپ شانزدهم
یادداشت : کتابنامه: ص. ۳۱۸
عنوان دیگر : راهنمای ورود به دنیای بیت‌کوین، اتریوم و ارزهای دیجیتال برای مبتدی‌ها
موضوع : بیت‌کوین
موضوع: Bitcoin
موضوع : ارز مجازی
موضوع : Digital currency
موضوع : بازرگانی الکترونیکی
موضوع : Electronic commerce
شناسه افزوده : ملک‌پور، نیما، ۱۳۷۴-
رده بندی کنگره: HG۱۷۱۰
رده بندی دیویی : ۳۳۲/۱۷۸
شماره کتابشناسی ملی : ۸۸۲۹۳۸۳



ویرایش سوم

راهنمای ورود به دنیای بیت کوین
اتریوم و ارزهای دیجیتال برای مبتدی‌ها

یک ساتوشی

محمد آذرنیوار / نیما ملک‌پور

چاپ شانزدهم

۱

انتشارات
راه‌پرداخت

عنوان : یک ساتوشی: راهنمای ورود به دنیای بیت‌کوین، اتریوم و ارزهای دیجیتال برای مبتدی‌ها

ناشر : راه پرداخت

نویسندگان: محمد آذرنیوار، نیما ملک‌پور

ویراستار ارشد : مینا والی

ویراستار محتوایی: قاسم سرافرازی

ویراستار فنی: یلدا شایسته‌فر

بازبینی نهایی متن: رضا قربانی

صفحه‌آرا: علیرضا کیوان

ناظر چاپ : قادر شهبازی

نوبت چاپ: شانزدهم ۱۴۰۱

شمارگان : ۱۰۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۲۶-۲

تلفن : ۰۲۱-۴۴۴۴۳۹۶۶

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل : publisher@way2pay.press

وب‌سایت : way2pay.press

لیتوگرافی: هنر اشکان

چاپ و صحافی: واژه

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

@Way2Pay press Way2Pay.press @Way2Pay press

فهرست

[یادداشت نویسندگان بر ویرایش دوم]

محمد آذرنیوار- نیما ملک‌پور

دنیای ارزهای دیجیتال از زمان اتمام نگارش کتاب پیش رو، که نزدیک به دو سال از آن می‌گذرد، تغییرات شگفت‌انگیزی داشته است. شروع استفاده واقعی از قابلیت قراردادهای هوشمند و گسترش آن‌ها چنان به‌سرعت اتفاق افتاد که انتظار آن را نداشتیم. شاهد بودن این تغییرات، درس‌ها و تجارب ارزشمندی نیز برای خود ما به همراه داشت. فناوری غیرمتمرکز که هیچ‌یک از ما در تاثیرگذاری آن شک نداریم، بیش از اینکه جایگزین یا به‌عبارت بهتر نابودکننده‌ی نظام‌های پولی و اقتصادی فعلی شود، یکی از اجزای مهم شکل‌دهنده به دنیایی است که تاروپود آن از ساختارهای موجود در کنار ساختارهای جدید تشکیل شده است. در این میان ما به‌عنوان دوستداران فناوری غیرمتمرکز بر این باور هستیم که تاثیر این پدیده نه‌تنها در جنبه‌های اقتصادی و پولی، بلکه در سایر بخش‌های اجتماعی، سیاسی و فرهنگی نیز به‌نمایش درخواهد آمد. از این رو روایت ظهور بیت‌کوین و تلاش برای آموزش مفاهیم دنیای غیرمتمرکز به زبان ساده قطعات پازلی هستند که تصویر کلی آن نگرشی فراتر از کسب درآمد یا

آموزش شیوه‌های پول درآوردن از ارزهای دیجیتال ارائه می‌دهد. از این رو امیدواریم که خوانندگان «یک ساتوشی» پس از اتمام خوانش آن، شوق بیشتری برای یادگیری و غرق‌شدن در این دنیای بی‌انتها پیدا کنند.

کتاب پیش رو همان‌طور که از نام فرعی آن پیداست، با هدف نمایش مسیر ورود به دنیای ارزهای دیجیتال و سرمایه‌گذاری در آن‌ها نوشته شد. استقبال از سادگی و قابل‌فهم بودن «یک ساتوشی» ما را بر آن داشت که در ویرایش جدید، مفاهیم و اصطلاحات پرکاربرد دو سال اخیر را به کتاب اضافه و ابزارهای معرفی‌شده را به‌روز کنیم. البته باید اشاره کرد که با وجود اضافه‌شدن مفاهیم جدید در نسخه پیش رو، ویرایش کلی تا حد امکان مختصر بود و تلاش شده تا همچنان بر روی آموزش مفاهیم برای مبتدیان پایبند باشیم. در انتها نیز باید افزود که با شنیدن اصطلاحات و لغات پرکاربرد جدید، نیاز مداوم به دنبال‌کردن و به‌روز بودن بیش از هر زمان دیگری در این حوزه احساس می‌شود و تاکید می‌کنیم که برای همگام‌شدن با این فناوری بهتر است هرگز به این کتاب اکتفا نکنید.

[یادداشت نویسندگان بر ویرایش اول]

محمد آذرنیوار- نیما ملک‌پور

اولین باری که نام بیت‌کوین را شنیدیم به سادگی از کنار آن رد شدیم تا چند سال بعد همه نگاه‌ها از جمله نگاه حسرت‌آمیز ما دوباره به آن جلب شد. چیزی که در ابتدا شبیه به سکه‌های مجازی در بازی‌های آنلاین به نظر می‌رسید و امکان تصور کاربردی برای آن وجود نداشت، با گذشت زمان به غول بزرگی تبدیل شده بود که به این راحتی‌ها متوقف نمی‌شد. یادگیری درباره آن ما را وارد دنیایی کرد که اولین دستاوردش دور ریختن تمام باورهای قدیمی از پول بود. بیت کوین طراحی خارق‌العاده‌ای را به ما نشان داد که نفع هر نفر در راستای منافع کلی شبکه قرار می‌گرفت. سیستمی که رشوه و فساد در آن معنی نداشت و همچنین به لطف بلاکچین، برای اولین بار توانستیم به‌جز پول، به جهانی غیرمتمرکز هم فکر کنیم.

مشاهده رشد سریع حوزه ارزهای دیجیتال و آینده غیرقابل انکار با سیستم‌های غیرمتمرکز، ما را بر آن داشت تا هر آنچه از دانش اندک خودمان تا منابعی که

می‌شناختیم را برای گردآوری کتابی مناسب برای کسانی که هنوز با این پدیده آشنا نشده‌اند، زیر و رو کنیم. در این مسیر، افراد زیادی به ما یاری رساندند که تشکر از آنها را وظیفه خود می‌دانیم. در اینجا لازم می‌دانیم از آقای حمیدرضا شعبانی، بنیان‌گذار و مدیر مجموعه ارزدیجیتال، به سبب حمایت‌های همیشگی ایشان و آقای رضا قربانی، بنیان‌گذار و مدیر مجموعه راه پرداخت، به سبب کمک شایان در انتشار این کتاب، تشکر ویژه خود را اعلام کنیم. همچنین از آقایان و خانم‌ها بهزاد ناصرفلاح، مجید جهادی، امیرمحمد غلامی، محمد کثیری، سعید عزتی، امین عربی، محسن قره داغلی، سجاد مقصودی، علیرضا مقدم، بهاره رضاجو، ثریا نیل درار، سولماز محمدزاده، محمد غرقابی و تمامی کسانی که در زمینه محتوا و بازبینی این کتاب ما را یاری رساندند تشکر می‌کنیم.
کتاب پیش رو را به پدر و مادر خود که زمینه یادگیری و رشد ما را فراهم کردند تقدیم می‌کنیم تا هدیه ناچیزی در برابر بخشی از زحمات ایشان باشد.

[یادداشت ناشر]

رضا قربانی- انتشارات راه پرداخت

خوشحالم که کتاب «یک ساتوشی» به چاپ هفتم رسیده است. نه ما در انتشارات راه پرداخت و نه نویسندگان کتاب انگیزه انتفاعی از انتشار این کتاب نداشته‌ایم و به همین دلیل قیمت پشت جلد این کتاب بسیار کم‌تر از میانگین بازار نشر است. قیمت پشت جلد کتاب در حدی است که صرفاً هزینه‌های چاپ و کاغذ و توزیع را تأمین کند. هدف نویسندگان و ما صرفاً این بوده است که افراد بیشتری دنیای بیت‌کوین و رمزارزها را به شیوه درست بشناسند. سؤال بسیاری در این زمانه پرهیاهو این است که چگونه وارد دنیای بیت‌کوین شوند و در پاسخ به این پرسش‌ها شاهد بوده‌ایم که انبوهی سروصدا خلق شده است. در این‌همه سروصدا تشخیص سره از ناسره هر روز سخت‌تر می‌شود. ما مطمئن هستیم آنهایی که مبانی را درست آموخته‌اند در ادامه راه کم‌تر دچار خطا می‌شوند. البته که هیچ راهی برای دوری از خطا وجود ندارد و حرفه‌ای‌ترین‌ها هم دچار خطا و اشتباه می‌شوند. ولی مطالعه درست و آشنایی با اصول و مبانی به ما کمک می‌کند ادامه مسیر با قطب‌نمای دقیق‌تری انجام شود. دقیق‌ترین قطب‌نماها هم نمی‌توانند کشتی را از غرق شدن نجات

دهند ولی اگر از قطب‌نما به‌موقع و درست استفاده کنیم در ادامه راه از بسیاری ریسک‌ها جلوگیری می‌کنیم.

بنابراین مطالعه کتاب یک ساتوشی در این چند سال اولین توصیه ما برای کسانی بوده است که می‌خواستند وارد دنیای بیت‌کوین شوند. برخی افرادی که در چند سال گذشته سعی کردند از مسیر درست وارد این دنیای هیجان‌انگیز شوند امروز به حرفه‌ای‌های این حوزه تبدیل گشته‌اند و در کسب‌وکارهای نامداری مشغول فعالیت هستند. دنیای رمزارزها فراتر از این است که رمزارزی را بخریم و به انتظار بنشینیم که گران شود و ما یک‌شبه پول‌دار شویم. دنیای رمزارزها دنیایی ناشناخته است که هر روز بُعد جدیدی از آن را کشف می‌کنیم. ولی این دنیای جدید ناشناخته مبنی بر اصولی است که در این سال‌ها تغییری نکرده است.

نویسندگان کتاب یک ساتوشی به‌صورت کاملاً حرفه‌ای و مسلط برای مخاطب ناآشنا مفاهیم را بسته‌بندی و در یک ساختار منطقی ارائه کرده‌اند. قاعدتاً این تازه شروع راه است؛ راهی که رهروان آن باید آن را به‌تنهایی طی کنند. در این مسیر استعاره کرگدن را دوست

دارم. آنهایی که می‌خواهند در این مسیر موفق باشند چاره‌ای ندارند جز این که طریقت کرگدن را انتخاب کنند. همان گونه که کرگدن تنها سفر می‌کند و پوست کلفتی دارد رفتن در این مسیر برای آنهایی مناسب است که طاقت تنهایی دارند و می‌توانند تنها سفر کنند. قاعدتاً راه بی‌رهرو سخت است و تنها سفر کردن کاری است طاقت‌فرسا. به همین دلیل لازم است که برای خودمان توشه راه برداریم که در این راه سخت و طولانی کم نیاوریم. کتاب یک ساتوشی به‌مثابه همان توشه راهی است که برای زدن به دل جاده باید با خود برداریم. این کتاب را اگر یک‌نفس بخوانیم در کم‌تر از یک روز خوانده می‌شود و تمام. ولی توصیه من به همه آنهایی که این کتاب را دست گرفته‌اند این است که با طمأنیه بخش‌های گوناگون کتاب را بخوانند، درباره آن فکر کنند و سعی کنند در دستگاه مختصات فکری خود جایی برای آن باز کنند. پیشنهاد می‌کنم هیچ چیزی را چشم‌بسته قبول نکنید و به هر ادعایی که در کتاب می‌رسید از خودتان سؤال بپرسید که چرا؟ بپرسید که چرا این ادعا درست است و یا حتی چرا غلط است؟ سعی کنید ذهنتان را درگیر کنید و بیش‌تر از اینکه قیمت لحظه‌ای رمزارزها را دنبال کنید، منطق پشت این تغییر را بیابید. قطعا آنهایی که منطق این دنیا را درک کنند در تسلط یافتن به ابزارها و روش‌های گوناگون راه ساده‌تری در پیش دارند. سعی کنید این کتاب دریچه‌ای باشد برای شما که ذهن‌تان را به روی دنیای جدید باز کند. این فرصتی است که حیف است آسان از دست بدهید.

در پایان لازم است از همه همکاران و دوستانم که در انتشار و رسیدن این کتاب به دست شما ما را یاری کردند تشکر کنم.

مقدمه

به عصر ارزهای دیجیتال و تمرکززدایی سلام کنید. سال‌ها بود که نقش قدرت‌های مرکزی در کنترل و انتشار اطلاعات به سبب ظهور اینترنت کمرنگ شده بود، اما نیاز به جریانی که قدرت حاکم بر پول را از چنگ بانک‌های مرکزی و دولت‌ها دربیاورد نیز احساس می‌شد. معرفی بیت‌کوین در اواخر سال ۲۰۰۸ میلادی آغازگر جریان غیرمتمرکزسازی پول بود که در ادامه مسیر خود به «غیرمتمرکزکردن همه چیز» تبدیل شد. فناوری بی‌نظیر مورد استفاده در بیت‌کوین یعنی بلاکچین، راه خود را به اغلب صنایع پیدا کرد و سودای تغییرناپذیری و گاهی اوقات هم شفافیت در سرلوحه اهداف استارت‌آپ‌ها قرار گرفت. امروزه روند شتاب‌گرفته این فناوری نفوذ آن را تا عمق تسهیلات بانکی ممکن کرده و هر خدمتی که پیش‌تر تنها با نظام بانکداری یا سیستم‌های سازمان متمرکز امکان‌پذیر بود، هم‌اکنون با ترکیب بلاکچین و رمزنگاری خارج از بانک‌ها قابل پیاده‌سازی است. نمی‌توان منکر آن شد که شکل دنیای ما در سال‌های آینده به‌شدت تحت تأثیر فناوری بلاکچین و ارزهای دیجیتال قرار خواهد گرفت و این فناوری در دیجیتالی‌شدن تمامی عناصر زندگی انسان‌ها نقش پررنگی ایفا خواهد کرد. از این رو، اهمیت فعالیت در فضای پیرامون این فناوری که پتانسیل بالایی را برای خلق ارزش در سال‌های آینده دارد، به‌خوبی درک می‌شود. تجربه اولین آشنایی با بیت‌کوین و ارزهای دیجیتال که بیشتر افراد را به درون یک لانه خرگوش بی‌انتها کشانده نیز اغلب با رشد قیمت‌های نجومی آنها رقم خورده است.

کتاب حاضر تلاشی برای راهنمایی افرادی است که تنها در حد شنیدن واژه بیت‌کوین یا دنبال‌کردن قیمت ارزهای دیجیتال با این فناوری آشنا هستند و به‌دنبال شناخت جنبه‌های بیشتر و روش‌های سرمایه‌گذاری در آنها می‌گردند. از کوچک‌ترین واحد پولی بیت‌کوین به پاس خدمات سازنده آن تحت عنوان «ساتوشی» یاد می‌شود. یک ساتوشی جزئی از صد میلیون واحد کوچک دیگر است که در کنار یکدیگر یک واحد بیت‌کوین را تشکیل می‌دهند. انقلاب پولی که بیش از یک دهه قبل شروع شد، هم‌اکنون به جایگاهی رسیده که رسانه‌ها؛ رویدادها و حوادث آن را از نزدیک دنبال می‌کنند و چشم‌های بسیاری به آینده آن دوخته شده است. یک ساتوشی نمادی برای سهیم‌شدن در این انقلاب است؛ مشارکتی که با کوچک‌ترین واحد پولی آغازگر این

انقلاب انجام می‌شود. یک ساتوشی می‌تواند دارایی ارزشمندی در آینده باشد و طبق جمله معروفی که در جامعه بیت‌کوین رایج است، باید ساتوشی‌ها را روی هم انباشت[1].

تمرکز کتاب پیش‌رو بیشتر روی معرفی اصول و روش‌های سرمایه‌گذاری در ارزهای دیجیتال به همراه معرفی و توضیح انواع تحلیل در این حوزه است، با این حال نگاهی هم به خود فناوری بیت‌کوین و ارزهای دیجیتال داشته‌ایم. کتاب حاضر به سه بخش تقسیم شده و در بخش اول گریزی به تاریخچه پول و مفاهیم اولیه در مباحث ارزهای دیجیتال، بیت‌کوین و بلاکچین زده‌ایم. در بخش دوم، اصول اولیه‌ای که برای سرمایه‌گذاری در ارزهای دیجیتال باید بدانید و انواع شیوه‌های سرمایه‌گذاری را شرح داده‌ایم. در بخش سوم نیز انواع روش‌های تحلیل برای سرمایه‌گذاری در ارزهای دیجیتال را به همراه نکات لازم توضیح داده‌ایم.

همچنین کتاب حاضر به نحوی نگارش شده که پاسخگوی سؤالات کاربران مبتدی باشد و امیدواریم در نیل به این مقصود موفق بوده باشیم. اگرچه توجه به این نکته الزامی است که با پیشرفت فناوری و ارائه ابزارهای جدید و بهینه، برخی ابزارها یا روش‌های معرفی‌شده در این کتاب ممکن است دیگر مورد استفاده قرار نگیرند. از این رو در بخش به‌روز باشید از این کتاب برای کسب محتوای به‌روز می‌توانید اطلاعاتی کسب کنید.

دیباچه

با وجود اینکه پریسا احمدی بهترین دانش‌آموز کلاسش در بین تمام دختران دبیرستان حتیفی در شهر هرات افغانستان بود، خانواده‌اش ابتدا در برابر ثبت‌نام او در کلاس‌های مهارت اینترنت و شبکه‌های اجتماعی که توسط یک سرمایه‌گذار خصوصی برگزار می‌شد و حتی در ازای تلاش این دانش‌آموزان پول پرداخت می‌کرد، مقاومت می‌کردند. او در یک ایمیل نوشت: «اینجا در افغانستان، زندگی یک زن محدود به دیوارهای اتاق و مدرسه‌اش است.»

دختران افغانستان به اینترنت دسترسی ندارند؛ چه در خانه، چه در مدرسه. اگر

1. Stack sats (satoshies)

احمدی پافشاری نمی‌کرد، بعید نبود که وضعیت برای او به همان شیوه قبلی ادامه یابد. او شاگرد اول کلاسش بود و حتی می‌خواست در کلاس‌های بیشتری هم شرکت کند. او به اندازه کافی برای کاری که می‌خواست انجام دهد، دلیل داشت. طبق چیزی که خودش می‌گفت، حتی خانواده‌اش را به‌شدت تحت فشار قرار داده بود.

شرکت سرمایه‌گذاری حامی این کلاس‌ها یعنی فیلم آنکس[1]، یک شرکت هنری آمریکایی بود که با استفاده از شبکه اجتماعی و یک وب‌سایت به ۳۰۰ هزار وبلاگ‌نویس و فیلم‌سازی که در آثارشان همکاری می‌کنند، حمایت مالی می‌رساند. فعالیت فیلم انکس در افغانستان به یک برنامه سوادآموزی دیجیتال به نام زنان انکس منتهی شد که با همکاری «رویا محبوب»، تاجر افغان شکل گرفت که به ۵۰ هزار دختر افغان در سراسر این کشور آموزش می‌دهد. محبوب مانند یک ستاره شناخته می‌شود و نامش در میان یکصد شخصیت تأثیرگذار دنیا در مجله تایم قرار گرفت. او که یک شرکت نرم‌افزاری به نام «افغان سیتادل» را اداره می‌کند، از معدود مدیران زن افغانستان است و انگیزه اصلی خود را آموزش زنان افغانی قرار داده است. برنامه زنان انکس کلاس‌های خود را در دبیرستان‌های محلی افغانستان برپا می‌کند و مدرسان آن همگی زن هستند. به‌دلیل همین ویژگی زن‌بودن مدرسان، خانواده احمدی سرانجام قانع شدند و اجازه ثبت‌نام دخترشان را دادند.

احمدی کلاس‌هایش را در سال ۲۰۱۳ آغاز کرد. او و هم‌کلاسی‌هایش در حال یادگیری در مورد شبکه جهانی وب، شبکه اجتماعی و وبلاگ‌ها بودند. دختر فیلم‌دوستی که همچنین عاشق نوشتن درباره فیلم‌های تکان‌دهنده زندگی‌اش بود. او نوشتن در یک وبلاگ را آغاز کرد و اعضای آن واکنش مثبتی نسبت به دیدگاهایش نشان دادند که همین امر باعث شد اولین درآمد واقعی دوران جوانی خود را کسب کند.

هنوز هم یکی از چیزهایی که دختران در افغانستان از آن بی‌بهره هستند، یک حساب بانکی است. اگر این نوجوان افغان پولی داشته باشد، مجبور است آن را به حساب بانکی پدر یا برادرش منتقل کند و این موضوع درباره بیشتر دختران محل زندگی او صدق می‌کند، اما در این‌باره او خوش‌شانس بود.

1. Film Annex

در سال ۲۰۱۴ شانس به احمدی رو کرد. «فرانچسکو رولی»، بنیان‌گذار شرکت آمریکایی فیلم انکس، متوجه مشکل پیش روی زنانی مانند احمدی شد و از طرفی هزینه‌های بالای تراکنش در ارسال مبالغ نسبتاً کوچک به‌صورت بین‌المللی، او را مجبور به پیاده‌سازی تغییرات جامعی در سیستم پرداخت فیلم آنکس کرد.

او تصمیم گرفت که به وبلاگ‌نویس‌هایش به‌عنوان دستمزد بیت‌کوین پرداخت کند. ارز دیجیتالی که با فداکاری سفت‌وسخت گروه کوچکی از خوره‌های فناوری، به هر گوش شنوایی مژده تغییر جهان را می‌داد و در سال ۲۰۱۳ آوازه آن در دنیا طنین‌انداز شده بود. رولی خیلی زود بیت‌کوین را درک کرد و مزایای آن را برای افرادی مانند احمدی که تنها یکی از هفت هزار زن جوان افغان مشارکت‌کننده در فیلم انکس بود، به کار برد. بیت‌کوین‌ها در حساب‌های بانکی دیجیتالی به نام «کیف پول‌ها» نگهداری می‌شوند که توسط هر کسی در خانه و تنها با دسترسی به اینترنت می‌تواند ایجاد شود. دیگر به افتتاح حساب در بانک، ارائه مدارک یا اثبات اینکه شما یک مرد هستید، نیازی نیست. در واقع بیت‌کوین نام یا جنسیت شما را نمی‌داند و به این ترتیب به زنان در جوامع مردسالار، یا حداقل به آنهایی که به اینترنت دسترسی دارند، اجازه داشتن کنترل روی پول‌هایشان را می‌دهد.

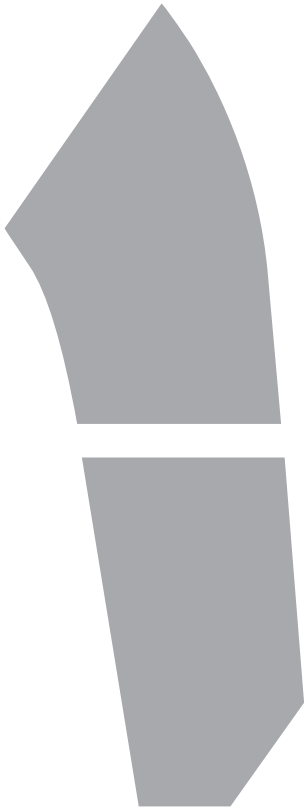
بیش از این نمی‌توان بر اهمیت این موضوع تأکید کرد. چیزی که این زنان می‌سازند برای خودشان است، نه پدران و برادران‌شان. در حالی که بیت‌کوین علاج همه دردها نیست، اما این جریان پیشگام فناوری در قرن بیست‌ویکم برای آزادی توده مردم یک وعده واقعی ارائه می‌دهد. بسیاری از مشارکت‌کنندگان فیلم آنکس در ایالات متحده، بریتانیا، ایتالیا و دیگر کشورهای ثروتمند از راحت‌نبودن با ارزهای دیجیتال اظهار گلایه کردند. تنها کسب‌وکارهای محدودی آن را به‌عنوان روش پرداخت پذیرفتند و برای بسیاری دیگر تمام ماجرا هنوز شیادانه به نظر می‌رسید. این شکایات به مشارکت‌کنندگان فیلم آنکس منحصر نمی‌شد؛ تصور بیت‌کوین برای خیل عظیمی از مردم یک کلاهبرداری نیمه‌پخته است؛ برنامه‌ای که برای خالی‌کردن دست احمق‌ها از پول‌هایشان ترتیب داده شده است.

از این گذشته احمدی دغدغه‌های مشترکش در رابطه با بیت‌کوین را که همتایانش

در کشورهای دیگر درباره آن گلایه می‌کنند، به مباحثه می‌گذارد. به‌خصوص گزینه‌هایی که برای خرج‌کردن آن در اقتصاد عقب‌افتاده‌ای مانند اقتصاد افغانستان وجود دارد، هنوز بسیار محدود است. جهت مقابله با این مشکلات، فیلم آنکس در سال ۲۰۱۴ یک سایت تجارت الکترونیکی راه‌اندازی کرد که به اعضایش اجازه مبادله بیت‌کوین با گیفت‌کارت سایت‌های بین‌المللی مانند آمازون که به کابل، هرات و دیگر شهرهای افغانستان ارسال می‌شد را می‌داد. در نتیجه، فیلم آنکس اقتصاد محصورشده بیت‌کوین خود را به وجود آورد که با تغییر نام تجاری‌اش به «بیت‌لندرز» آن را قدرت بخشید.

احمدی بیت‌کوین‌هایش را برای خرید یک لپ‌تاپ استفاده کرد. امری که تنها چند سال قبل، غیرممکن محسوب می‌شد. او با نمایش اینکه چگونه مستقل باشیم، چگونه برای خودمان تصمیم بگیریم و مهم‌تر از همه چگونه روی پای خودمان بایستیم، جنبه‌های مثبت بیت‌کوین را یادآور شد. بیت‌کوین به احمدی اجازه تصور آینده‌ای را داد که در آن دیگر یک ضمیمه فرعی به مردان زندگی‌اش نبود؛ آینده‌ای که خود او می‌توانست آن را ترسیم کند. «من خودم را یک دکتر زن تحصیل‌کرده و فعال در آینده می‌بینم»؛ این را پریسا احمدی گفت.[۱]

۱. از مقدمه کتاب عصر ارزهای دیجیتال (Age of Cryptocurrency)؛ نوشته پاول وینا و مایکل کیسی



فصل اول

مفاهیم پایه

از آنجایی که این کتاب برای تمام افراد ـ چه تازه‌کار و چه حرفه‌ای ـ نوشته شده است، قبل از رفتن به سراغ مباحث مربوط به سرمایه‌گذاری و معامله، به درک و یادگیری مفاهیم پایه نیاز است. یادگیری مفاهیم پایه حوزه ارزهای دیجیتال را می‌توان مانند آموختن الفبا برای فراگیری یک زبان در نظر گرفت. همان‌طور که اگر الفبای یک زبان خارجی را یاد نگیرید، نمی‌توانید از آن استفاده کنید، عدم یادگیری مفاهیم پایه این فضای نوپا هم در ادامه مسیر، مشکلات زیادی برای شما ایجاد می‌کند.

اگر قصد سرمایه‌گذاری در ارزهای دیجیتال را دارید، به هیچ‌عنوان سرمایه‌گذاری کورکورانه و با این فکر که «باید در ارزهای دیجیتال سرمایه‌گذاری کنم، چون بقیه هم سرمایه‌گذاری می‌کنند» را توصیه نمی‌کنیم. نه فقط در ارزهای دیجیتال؛ بلکه سرمایه‌گذاری در هر بازاری مستلزم شناخت درست از آن است. به بیان ساده، باید به‌طور دقیق بدانید که روی چه چیزی سرمایه‌گذاری می‌کنید و وقت می‌گذارید. در زمان نگارش این کتاب، فقط حدود ۱۳ سال از آغاز دوران واقعی ارزهای دیجیتال غیرمتمرکز (یا به عبارت دیگر ۱۳ سال از معرفی بیت‌کوین) می‌گذرد؛ بنابراین نسبت به پدیده‌های سنتی، درک ماهیت دارایی‌های دیجیتال با چالش‌های بیشتری همراه است.

در این بخش، ابتدا تاریخچه پول و روند تکامل آن را به‌صورت مختصر مرور می‌کنیم تا به درک درستی از پول و چگونگی تحول آن در طول زمان برسید و سپس به سراغ مفاهیمی می‌رویم که دانستن آنها قبل از ورود به دنیای ارزهای دیجیتال ضروری است.

تاریخچه پول

بسیاری از دانشمندان، پول را بزرگ‌ترین ابتکار تاریخ بشریت می‌دانند. بدون پول، احتمالاً هنوز در جنگل‌ها و دشت‌های پهناور، با نیزه‌های دست‌ساز به‌دنبال شکار حیوانات و پیدا کردن غذا بودیم، یا شاید شب و روزمان به کشاورزی می‌گذشت. پول به بشر نظم و انگیزه پیشرفت داد و باعث ظهور تمدن‌های بزرگ شد. بدون این ابتکار بی‌نظیر، هیچ پیشرفتی قابل تصور نبود. در این فصل به بیان چیستی پول و شرح تاریخچه مختصری از آن پرداخته می‌شود که به درک شما از ارزهای دیجیتال کمک شایانی خواهد کرد.

پول چیست؟

پول از نظر بسیاری از اقتصاددانان کلاسیک هر چیزی است که: ۱. واسط تبادل باشد؛ یعنی بتوان با آن تبادل کالا انجام داد و نیازهای خود را برطرف کرد. ۲. واحد حساب باشد؛ یعنی بتوان بهای یک چیز را با آن تعیین کرد و ۳. ذخیره ارزش باشد؛ یعنی چیزی که بتوان آن را ذخیره کرد تا در آینده که همچنان دارای ارزش است، مورد استفاده قرار بگیرد. پول به‌عنوان یک کالا مصرفی یا کالای سرمایه‌ای خریداری نمی‌شود؛ بلکه کارکرد اصلی آن معاوضه با کالاهای دیگر است. هرچند خرید کالای سرمایه‌ای با هدف ایجاد درآمد انجام می‌شود، تقاضا برای پول همیشه وجود دارد و کالای سرمایه‌ای نمی‌تواند جایگزین آن شود. به گفته لودویگ فون میزس، اقتصاددان بزرگ مکتب اتریش، عدم قطعیت در مورد آینده دلیل اصلی تمایل انسان‌ها به نگه داشتن پول است و اگر افراد از تمام هزینه‌ها و درآمدهای خود آگاه بودند، می‌توانستند پول خود را به صورت بهینه برنامه‌ریزی کنند تا مجبور نباشند پول نقد نگهداری کنند. اقتصاددانان تعریف «پول» و «ارز» را یکی نمی‌دانند. به عقیده آنها، پول سیستمی از حساب‌ها و اعتبارات است که ارز به آن جان می‌بخشد. مثلاً دلار یک سیستم پولی است که ارز آن همان اسکناس دلار است. در گذشته، اقتصاددانان سنتی، پول را به اشیای قابل لمس مثل اسکناس، سکه یا هر کالای فیزیکی دیگری محدود می‌کردند، اما از نظر صاحب‌نظران معاصر، حتی گاهی یک چیز (مثل لباس یا مدل مو) در بازی کامپیوتری هم می‌تواند به‌عنوان پول در نظر گرفته شود. نسلی که با فروشگاه‌ها و کالاهای واقعی و فیزیکی بزرگ شده، امروز برایش عجیب است که چرا یک نفر در یک بازی کامپیوتری سکه‌های مجازی می‌خرد. از نظر اغلب اقتصادانان عصر حاضر، پول‌بودن یک چیز کاملاً بین‌الاذهانی است. به عبارت دیگر، یک چیز وقتی ارزشمند می‌شود و به‌عنوان پول مورد استفاده قرار می‌گیرد که عده‌ای ارزشمندی آن را می‌پذیرند. برای اینکه مفهوم بین‌الاذهانی‌بودن پول را بهتر درک کنید، به بررسی نمونه‌ای به‌جز ارزهای رایج ملی نیاز داریم؛ چراکه برای مدت زیادی از این ارزها استفاده کرده‌ایم و پیش‌زمینه ذهنی ما از پول‌های رایج اجازه نمی‌دهد تا از عدم ارزش ذاتی

آنها اطمینان حاصل کنیم. با داستانی از جامعه‌ای شروع کنیم که تا اوایل دهه ۱۹۰۰ در جزایر «میکرونزی» زندگی می‌کردند و «یپ»[1] نام داشتند. اهالی یپ دارای پولی عجیب بودند. پول مردم این جزیره سنگ‌های غول‌پیکری به نام «رای»[2] بود. سنگ‌های رای واقعاً سنگین بودند و بزرگ‌ترین‌شان چهار تن وزن داشت و قطرش ۳.۵ متر بود؛ واحد پولی که چند صد کیلو وزنش بود. به یک اسکناس فکر کنید که ۲۰۰ کیلوگرم وزن داشته باشد. اما مردم یپ سنگ‌های رای را جابه‌جا نمی‌کردند، یا به شکلی که ما از اسکناس و سکه استفاده می‌کنیم، آن را مبادله نمی‌کردند، بلکه آنها فقط ثبت می‌کردند که چه کسی مالک چه قسمتی از کدام سنگ است. به‌عنوان مثال، فرض کنید یک سنگ رای دو تنی روی کوه قرار دارد. مالک سنگ برای خرید مایحتاج خود نیاز ندارد که سنگ را با خودش جابه‌جا کند. فقط کافی است که مالکیت سنگ یا بخشی از سنگ را به فرد دیگری منتقل کند؛ درنتیجه سنگ همچنان سر جایش باقی می‌ماند. حتی روایتی وجود دارد که یک بار یکی از سنگ‌های رای که روی یک کشتی قرار داشته است، به‌دلیل توفان به دریا می‌افتد. با این حال، ارزش سنگ همچنان حفظ می‌شود و با آن معامله صورت می‌گیرد، چون حتی اگر سنگ در کف دریا باشد، می‌توان به‌صورت قراردادی مالکیت آن را منتقل کرد.

عکس ۱-۱: سنگ‌های رای که اهالی یپ از آنها به‌عنوان پول استفاده می‌کردند.

1. Yap
2. Rai

مردم جزیره یپ هنوز از این سنگ‌ها استفاده می‌کنند. شاید فکر کنید این فقط مختص این جزیره است، اما اگر کمی دقیق‌تر نگاه کنید و ادامه این فصل را بخوانید، خواهید فهمید که حتی ارزهای رایج ملی مثل دلار یا ریال هم از چنین مفهومی پیروی می‌کنند. چیزی مانند اسکناس دلار یا سنگ ذاتاً ارزشمند نیست. تنها دلیلی که باعث می‌شود این چیزها ارزش داشته باشند، این است که ما همگی این تصمیم را گرفته‌ایم و چون ما این تصمیم را گرفته‌ایم، آنها ارزشمندند. پول در تبادل و معامله‌ای که با هم داریم، معنی پیدا می‌کند. پول چیزی واقعی نیست. یک داستان مشترک است که ما از ارزش آن به یکدیگر می‌گوییم؛ یک افسانه که همه آن را باور کرده‌اند.

خاستگاه و منشاء پول

چه زمانی پول پدیدار شد؟ پاسخ این سؤال به این بستگی دارد که شما پیرو چه تفکری باشید. بحث درباره تاریخچه پول به‌طور اجتناب‌ناپذیری به بحث درباره تاریخ‌نگاری پول گره خورده است؛ چراکه شرح تکامل پول، بدون شرح‌دادن چگونگی تفکر درباره آن غیرممکن است. به‌طور کلی، دو تفکر درباره منشاء پول وجود دارد؛ تفکر «متالیسم» که بسیار قدیمی و رایج است و تفکر «چارتالیسم» که بیشتر در عصر معاصر به آن پرداخته می‌شود و کمتر در میان عموم ترویج شده، اما دارای اعتبار علمی بیشتری است. در ادامه، هر دو تفکر را به اختصار شرح می‌دهیم و این بر عهده شماست که پیرو کدام‌یک از آنها باشید. هر دو تفکر در نگاه اول منطقی هستند و صاحب‌نظران بزرگی پشت آنها قرار دارند. از این رو، نمی‌توان با قطعیت گفت که کدام‌یک کاملاً درست است. هر کدام از این دو نظریه حرفی برای گفتن دارند و به نظر می‌رسد که واقعیت، ترکیبی از این دو باشد.

پیروان تفکر متالیسم درباره منشاء پول دیدگاهی آشنا دارند؛ دیدگاهی که بیشتر مردم هم به آن واقف هستند و در کتاب‌های درسی درباره آن زیاد نوشته شده است؛ همه چیز از مبادله کالابه‌کالا یا همان سیستم دادوستد پایاپای آغاز شد. به زبان ساده، هزاران سال پیش و در زمان انقلاب کشاورزی، انسان متوجه شد که نمی‌تواند همه نیازهایش را خودش تأمین کند و باید با دیگران تعامل داشته باشد. کشاورز

زحمت‌کشی که گندم تولید می‌کرد، گندم‌های اضافی‌اش را با آهنگری که ابزار می‌ساخت، عوض می‌کرد، به این صورت، هر دو می‌توانستند نیازهای خود را برطرف کنند. با این حال، خیلی زود مشخص شد این سیستم مشکلات زیادی دارد. آیا ارزش این کیسه گندم با ارزش این داس برابر است؟ اگر آهنگر به گندم نیاز نداشت و نیازش چیز دیگری بود، چه؟ چطور کیسه‌های سنگین گندم را با خود حمل کنیم؟

ارسطو درباره خاستگاه پول می‌گوید: «وقتی ساکنان یک کشور به ساکنان کشورهای دیگر بیشتر وابسته شدند و آنچه را که نیاز داشتند، وارد کردند و آنچه را که مقدار زیادی از آن داشتند، صادر کردند؛ نیاز به استفاده از پول به وجود آمد.» این نظریه می‌گوید تجارت در مقطعی به حدی پیچیده شد که سیستم کالابه‌کالا دیگر نمی‌توانست نیازها را برطرف کند. دو هزار سال بعد از ارسطو، «آدام اسمیت» در یکی از آثارش به نام «ثروت ملل»، این نظریه را احیا کرد. اسمیت تمدن موجود در پرو و دیگر نقاط دنیا را شرح داد که سیستم پایاپای را تحمل می‌کردند تا اینکه اروپاییان نبوغ ضرب سکه را به آنجا بردند. دیدگاه اسمیت برای پاسخ به اینکه «چرا ما از سیستم کالابه‌کالا به سمت پول و بدهی حرکت کردیم»، حیاتی بود. به عقیده اسمیت، از آنجایی که انسان‌ها نسبت به استعدادهایشان تقسیم وظیفه کردند، بنابراین کالاهای مازاد برای تجارت تولید می‌کردند تا به‌وسیله تجارت آنها با کالاهای مورد نیازشان امرار معاش کنند، اما در اینجا مشکلی وجود داشت که در دنیای اقتصاد به آن «همسویی نیازها» می‌گویند. به عبارت دیگر، اگر شما یک آهنگر تولیدکننده سرنیزه بودید و از این راه زندگی خود را تأمین می‌کردید، هیچ تضمینی وجود نداشت که همیشه فردی مایل باشد گوسفندهایش را به ازای سرنیزه‌های تولیدی شما بدهد. بنابراین متالیست‌ها منشاء پول را سیستم مبادله کالابه‌کالا می‌دانند که بعدها به ایجاد پول منجر شد.

در نقطه مقابل، دیدگاه چارتالیسم قرار دارد. اگر چارتالیست باشید، نقطه شروع تاریخی شما بسیار متفاوت است. اول از همه، داستان سیستم دادوستد پایاپای را افسانه می‌دانید و رد می‌کنید. یک چارتالیست به تحقیقات معاصر و نوین تاریخی و اقتصادی تکیه می‌کند. انسان‌شناسان معاصر مناطقی را کشف کرده‌اند که در آنجا هیچ ارزی مورد استفاده قرار نمی‌گرفت. به گفته این دانشمندان، در برخی نواحی،

هیچ‌گونه شـواهدی مبنی بر اسـتفاده از سیسـتم کالابـه‌کالا، حتی به‌عنوان سیسـتم تبادل اولیه وجود ندارد. چارتالیسـت‌ها می‌گویند: پول قبل از اینکه به‌صورت امروزی درآید، یک سیسـتم ثبت جرائم یا بدهی بوده است؛ سیسـتمی که نشان می‌دهد هر نفر چقدر به یک نفر دیگر مدیون است. سیستم‌های باستانی عدالت کیفری به‌صورت ادای دین در قبال جرم عمل می‌کردند، مثلاً اگر یک نفر برادر کسی را کشت، دینش ۲۰ بز است. به عبارت دیگر، پول در ابتدا یک سیستم ثبت بدهی ساده بوده که اگر کمی دقت کنیم، اکنون هم همین‌طور است؛ البته با پیچیدگی‌های بسیار زیاد.

سیستم پول کالایی

به گـواه مورخان، اولین سیسـتم پولی تاریخ حدود سـه هزار سـال قبـل از میلاد، در میـان‌رودان، عراق امـروزی، به وجود آمـد؛ زمانی که مردمان بابل باسـتان نقـره و جو را به‌عنوان وسایل مبادله و واحدهای ارزش عمومی پذیرفتند و شروع به استفاده از آنها کردند. واحد وزن جو در بابل «شکل»[1] نام داشت. این جریان با نگارش قانون حمورابی، یکی از قدیمی‌ترین لوح‌های به‌جامانده و اولین نمونه قانون مکتوب، مصادف بود. قانون حمورابی شامل یکسری دسـتورات پرداخت هم هست که در آن چگونگی حل‌وفصل بدهی‌ها با گندم و جو آورده شده است. بر اساس آن دستورالعمل‌ها، حسابداران بابلی هر روز سوابق تبادلات جامعه را ثبت می‌کردند. آنها این کار را با استفاده از حک‌کردن یکسـری دندانه روی لوح‌های گلی انجام می‌دادند. این روش نگهداری سوابق، موجب ایجاد نوعی سبک نوشتن آسان‌تر به نام «خط میخی» شد و جای خط تصویری مصر باسـتان را گرفت؛ بنابراین شاید بتوان گفت که حسـابداری و پول عامل اصلی اختراع خط بوده است.

فلزاتی از جنس طـلا، نقره و مـس به‌دلیل حمل آسـان، کمیابـی و دوام بـالا و برخی کالاهای اساسـی در زندگی مردم مانند گندم، جو و نمک به‌عنـوان مهم‌ترین پول‌های کالایی در طول تاریخ شناخته می‌شوند. البته از آنجایی که پول یک پدیده بین‌الاذهانی است، همیشه کالاهای مصرفی به‌عنوان پول مورد استفاده قرار نمی‌گرفتند. به‌عنوان

1. Shekel

نمونه و به گفته مورخان بزرگ تاریخ، در بسیاری از نقاط آفریقا و جنوب آسیا از صدف که کاربرد خاصی در زندگی مردم هم نداشت، برای تبادلات استفاده می‌کردند. یا در غرب آفریقا یک نوع فلز برنزی به شکل نعل اسب، پول رایج مردم بود، در حالی که اگر همان فلز برنزی به شکل چیز دیگری بود، تا حد زیادی ارزشش را در میان جامعه از دست می‌داد و در میان قبایل به‌سادگی پذیرفته نمی‌شد.

دوران سکه

بخش بزرگی از تاریخچه پول به سکه‌های فلزی اختصاص دارد که هزاران سال به‌عنوان پول رایج مورد استفاده قرار می‌گرفتند. اولین سکه یا به‌طور دقیق‌تر یکی از اولین ارزهایی که به دست یک حکومت صادر شد، سکه‌ای به نام «استاتر» بود. استاترها، آلیاژی از طلا و نقره (الکتروم) بودند که پادشاهی لیدیه (غرب ترکیه کنونی) آنها را ضرب می‌کرد. نکته قابل توجه درباره این سکه‌ها، منقش‌بودن به سر یک پادشاه است؛ پادشاهی که روی این سکه‌ها نقش بسته، «الیاتس» است. نشان موجود روی استاترها، نشان‌دهنده اقتدار پادشاه الیاتس بود و احتمالاً پادشاهی لیدیه شروع‌کننده ارتباط چندهزارساله بین ارز و کار هنری بوده است. مرسوم‌شدن نقش‌ونگار روی ارز، به این اشیای بی‌جان، قدرت، اهمیت و ارزش مضاعف بخشید. البته پدیده سکه‌های فلزی خیلی به شکل آن مربوط نیست؛ بلکه صادرشدن آن از سوی یک حکومت به آن مفهوم می‌بخشد. فلزات طلا، نقره و مس به‌دلیل ویژگی‌های منحصربه‌فرد خود، بیشترین استفاده را برای ضرب سکه داشتند، ولی بعدها نیکل جای آنها را گرفت. حکومت‌ها با استفاده از انحصار در دریافت مالیات‌ها، به تنها راه جبران بدهی‌ها و ایجاد اعتبارات تبدیل شدند. مالیات‌هایی که حکومت‌ها دریافت می‌کردند، فقط با سکه همان امپراتوری قابل پرداخت بود. امروزه نیز پول همچنان به‌عنوان نشانه قدرت یک حکومت یا دولت در نظر گرفته می‌شود.

عصر پول‌های کاغذی

تاریخ پول کاغذی بسیار مفصل و پر از جزئیات ریز و درشت است؛ بنابراین به‌دلیل

محدودیت کلمات و حجم بالای مطالب باقی‌مانده، در اینجا تنها به‌صورت مختصر این تاریخ پرفرازونشیب را مرور می‌کنیم.

حمل مقدار زیادی سکه فلزی مشکلات زیادی برای بازرگانان ایجاد کرده بود و هزینه‌ها و خطرات تجارت را افزایش می‌داد. در قرن یازدهم میلادی، امپراتوری چین ایده‌ای جالب را عملی کرد؛ ذخیره سکه‌ها در مکان‌های امن و صدور رسیدهای کاغذی برای آنها. مردم به‌مرور به جای حمل طلا و سکه شروع به ذخیره فلزات گران‌بهای خود در مراکز امانت‌داری کردند.

این مراکز پر از نگهبان بود و امنیت طلاها را برقرار می‌کرد. به‌طور کلی و به بیان ساده، نحوه کار این مراکز به این صورت بود که به محض اینکه شخصی طلا یا نقره خود را به مرکز می‌سپرد، متصدی یک کاغذ به‌عنوان رسید به آن شخص می‌داد که مقدار طلا یا نقره او با تمام جزئیات در آن ذکر شده بود.

عکس ۲-۱: اولین پول کاغذی جهان که دولت چین صادر کرد. روی این کاغذ نوشته شده است: «جاعلان را گردن می‌زنیم».

رسیدی که مراکز امانت‌داری به مردم می‌دادند، نشان‌دهنده ارزش و اعتبار طلایی

بود که آنها به امانت سپرده بودند؛ بنابراین انتقال آن رسید کاغذی می‌توانست به معنای انتقال خود طلا باشد. به این ترتیب بود که شکل جدیدی از پول در بین مردم رواج پیدا کرد. مردم شروع به مبادله رسیدهای کاغذی به جای سکه‌های طلا کردند که جابه‌جایی و نگهداری آن از طلا آسان‌تر بود و نسبت به حمل طلا امنیت بیشتری را به ارمغان آورد. مردم همچنین می‌توانستند رسیدهای خود را در قبال سکه‌های طلا و نقره با مراکز امانت‌داری مبادله کنند. با گذشت زمان، دولت‌ها و بانک‌ها جایگزین مراکز امانت‌داری شدند و رسیدهای کاغذی جای خود را به اسکناس‌های امروزی دادند.

استاندارد طلا

تا اواخر قرن بیستم، ارزش تمام ارزهای رایج دنیا بر این مبنا بود که طلایی به‌عنوان پشتوانه در بانک‌ها یا نزد دولت‌ها وجود داشت. در واقع اسکناس‌ها، کاغذهایی بودند که طبق قاعده باید معادل آنها در بانک یا نزد دولت‌ها طلای ذخیره وجود می‌داشت و این چیزی بود که به این کاغذها ارزش و اعتبار می‌بخشید. طبق قانون، مردم می‌توانستند با مراجعه به بانک ملی یا مرکزی در قبال پول‌هایشان، طلا دریافت کنند.

استاندارد طلا در اواخر قرن هفدهم میلادی بیش از پیش رایج شد و مردم برای اینکه دولت‌ها و شرکای بانکی آنها نتوانند برای منافع شخصی خود، پول عمومی را نابود کنند، لازم دانستند که پول را به طلا، این فلز قابل لمس و کمیاب، گره بزنند. این سیستم در پایین نگه‌داشتن نرخ تورم موفق بود و به حفاظت از ذخایر ثروت کمک می‌کرد. با این حال، محدودیت منابع پول و ارزش بالای طلا موجب می‌شد تا در بحران‌ها مردم از خرج‌کردن خودداری کنند و ترجیح می‌دادند پول‌هایشان را ذخیره کنند.

در اوایل قرن بیستم، با وقوع جنگ جهانی اول و سپس بحران‌هایی مانند «رکود بزرگ» نظام استاندارد طلا، دولت‌ها را با کمبود شدید نقدینگی روبه‌رو کرده بود و در مقاطع متعددی این نظام پولی برای چاپ بیشتر پول، بارها از سوی دولت‌های بریتانیا و آمریکا نقض شد. در اواسط دهه ۱۹۳۰ دولت‌ها سعی می‌کردند استاندارد طلا را دوباره

زنده کنند، اما وقوع جنگ جهانی دوم معادلات را برهم زد. در فاصله دو جنگ جهانی، نبرد بر سر دستیابی به هژمونی و سلطه پولی میان قدرت‌های جهان شدت گرفت، تا از میان آنها سرانجام ایالات متحده آمریکا به‌عنوان قدرت برتر سربرآورد. اقتصاد بکر و روبه‌رشد، دور بودن از صحنه جنگ جهانی و نفوذ بالا در محافل سیاسی، سرانجام باعث تبدیل‌شدن دلار آمریکا به ارز ذخیره جهانی شد.

قدرت‌نمایی دلار

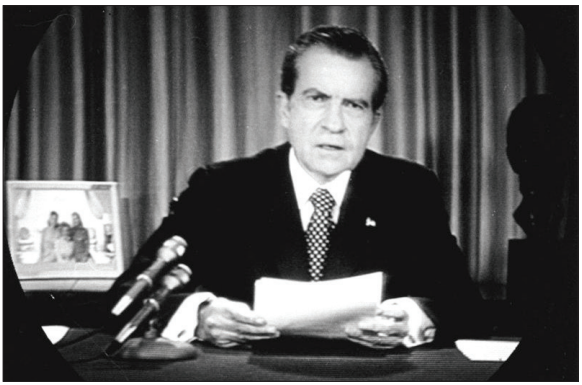
در اواخر جنگ جهانی دوم و در ۲۲جولای ۱۹۴۴، بیش از ۷۰۰ نماینده از ۴۴ کشور جهان در محلی به نام «برتون وودز» گرد هم آمدند تا یک نظام پولی جدید را شکل دهند. در جریان این گردهمایی، توافق‌نامه برتون وودز امضا شد که به‌طور خلاصه شرح آن این بود: «تمام کشورهای امضاکننده توافق‌نامه، به‌جای طلا، دلار ذخیره کنند و آمریکا به میزان دلارهای صادرشده، در خزانه خود طلا نگهداری کند. بانک‌های مرکزی کشورهای امضاکننده موافقت‌نامه‌های برتون وودز می‌توانستند هر زمان اراده کنند، ذخایر دلار خود را که پس از قرارداد پشتوانه پول‌های ملی‌شان شده بود، از راه مراجعه به بانک مرکزی آمریکا (فدرال‌رزرو) به طلا تبدیل کنند.» آمریکا، با تکیه بر این تعهد، در عمل به تنها ضامن نظام پولی بین‌المللی بدل شد؛ بنابراین کشورهای زیادی شروع به ذخیره دلار آمریکا کردند که نتیجه‌ای جز قدرتمندی مطلق ایالات متحده نداشت.

همزمان، با امضای موافقت‌نامه‌های برتون وودز دو نهاد جهانی هم ایجاد شد؛ صندوق بین‌المللی پول و بانک جهانی. نهاد اول باید نقش سرپرست را در نظام پولی جدید بر عهده بگیرد و از راه نظارت بر رابطه میان پول‌ها و اعطای کمک به کشورهای گرفتار مشکل، مانع از آن شود که نظام پولی به آشفتگی کشیده شود. و اما بانک جهانی وظیفه داشت با اعطای اعتبارهای آسان، به بازسازی کشورهای آسیب‌دیده از جنگ کمک کند. با توجه به موقعیت مالی ایالات متحده در آن زمان، تردیدی نبود که این قدرت در هر دو نهاد، جایگاهی بسیار نیرومند یافت.

اما عمر نظام پولی برتون وودز به ۳۰ سال نکشید. در اواخر دهه ۱۹۶۰ میلادی، محدودیت‌های سیستم برتون وودز (که مستقیماً روی فدرال‌رزرو فشار وارد می‌کرد)

آن را برای آمریکا غیرقابل تحمل کرد.

این کشـور که از هزینه‌های جنـگ ویتنام می‌نالیـد و در رقابت با تولیـدات خارجی ارزان‌تر ناتوان بود، نتوانسـت بین ورود کافی ارز خارجی و پرکردن دوباره ذخایر طلای خود تعادل برقرار کند. از سـوی دیگر، کشورهایی مانند فرانسـه که تقاضای دریافت طلا در قبال دلارهایشـان را داشتند، موجب شـدند تا ذخایر طلای آمریکا رو به اتمام برود. سـرانجام در ۱۵ اکتبـر ۱۹۷۱، ریچارد نیکسـون، رئیس‌جمهور وقـت آمریکا، در اقدامی ناگهانی امکان دریافت طلا در ازای دلار را لغو و به‌صورت غیررسمی پایان عصر اسـتاندارد طلا را اعلام کرد. تلاش‌های مجدد برای بازگشـت به اسـتاندارد طلا نیز به نتیجه نرسید و تا پایان دهه ۱۹۷۰ تمام کشورهای دنیا از استاندارد طلا خارج شدند.



عکس ۳-۱: نیکسون، رئیس‌جمهور وقت آمریکا، در حال اعلام پایان استاندارد طلا

اگرچه استاندارد طلا دیگر وجود ندارد، اما سلطه دلار همچنان پابرجاست. چیزی که ما به آن امتیاز دلار یا همان هژمونی دلار می‌گوییم، از طریق موقعیت این ارز در تجارت بین‌المللی به دست می‌آید.

اصلی‌ترین کالایی که با دلار خریدوفروش می‌شـود، نفت اسـت؛ بنابراین هر کشور و شـرکتی که بخواهـد نفت بخـرد، مجبور اسـت دلار ذخیره کنـد یـا وام دلاری بگیرد. به‌دلیل کاربرد دلار در خریـد نفت، تجارت بین‌المللی هم به سـمت کار بـا دلار تمایل

پیدا می‌کند. در نتیجه، نقدشوندگی دلار از هر ارز دیگری بیشتر است. بنابراین در بحران‌های نقدینگی، جریان سرمایه به سمت دلار می‌رود و این به معنای تقاضای بیشتر برای دلار است. تقاضا برای دلار، تورم آن را خنثی می‌کند و به بیان دقیق‌تر، این روند معکوس می‌شود. فدرال‌رزرو ذخایر دلار را افزایش می‌دهد تا به تقاضای شدید جهان پاسخ دهد.

به این ترتیب، ارزش دیگر ارزها نسبت به دلار کاهش می‌یابد و به عبارت دیگر، تورم دلار به بیرون از مرزهای آمریکا کشیده می‌شود. اگرچه آمریکا کالاهای زیادی تولید و به سراسر جهان صادر می‌کند، اما با استفاده از چیزی که ما به آن «امتیاز گزاف» می‌گوییم، این کشور دلار هم صادر می‌کند و با پولی که خودش چاپ کرده، کالاهای وارداتی را می‌خرد.

گسترش یا همان انبساط پولی (بخوانید تسهیل کمی، تسهیلات اعتباری، چاپ پول)، نوعی مالیات پنهان است. هرگز نمی‌توانیم بدون پرداخت بهای یک چیز، آن را دریافت کنیم و تأثیر گسترش پولی چند تریلیون دلاری، به معنای برداشت ارزش پول از دارندگان آن است که از نظر مفهومی همان مالیات تلقی می‌شود. اما به علت اینکه دلار ارز ذخیره جهانی است، آمریکا بیشترین منفعت را می‌برد. از آنجایی که تعداد زیادی از دارندگان دلار در داخل آمریکا حضور ندارند، در عمل دولت آمریکا دارد از کسانی هم که اصلاً در آمریکا زندگی نمی‌کنند، مالیات می‌گیرد و این فقط به‌خاطر سیاست‌های پولی فدرال‌رزرو است. تمام مردم، شرکت‌ها و کشورهایی که دلار نگهداری می‌کنند، بدون اینکه بخشی از آمریکا باشند، به دولت این کشور مالیات می‌دهند، بدون اینکه خیلی از آنها این موضوع را بدانند.

در میان عموم مردم، هنوز این تفکر وجود دارد که پول‌های ملی دارای پشتوانه طلا یا دیگر فلزات گران‌بها هستند، در حالی که امروزه این یک دروغ خنده‌دار است. اگرچه بانک‌های مرکزی دنیا هنوز طلا نگهداری می‌کنند، اما دیگر نه دلار، نه ریال و نه هر ارز دیگری هیچ پشتوانه‌ای ندارند. ارزشمندی پول‌های سراسر دنیا به اعتماد کردن مردم به یک دولت یا حکومت و به‌طور کلی عرضه و تقاضا بستگی دارد. این مردم هستند که با پذیرش و استفاده از یک پول به آن ارزش می‌دهند. امروزه همه دولت‌ها می‌توانند

بدون توجه به ذخایر طلا، به مقدار دلخواه پول چاپ کنند.

عصر نوین پول؛ پول‌های الکترونیکی

ظهور و گسترش کامپیوتر و اینترنت پس از دهه ۱۹۸۰ میلادی، پول را وارد عصر جدیدی کرد؛ عصر پول‌های الکترونیکی، پول‌هایی که در بستر اینترنت جابه‌جا می‌شوند؛ حالا دیگر پول‌های کاغذی هم دوران‌شان رو به اتمام است. همان‌طور که «یووال نوح هراری» در کتاب خود می‌نویسد، مجموع کل پول جهان به‌طور تقریبی ۶۰ تریلیون دلار است.

با این وجود، مجموع کل سکه‌ها و اسکناس‌ها کمتر از شش تریلیون دلار است. بیش از ۹۰ درصد از تمام پول دنیا نیز، بیش از ۵۰ تریلیون دلاری که در حساب‌های ما به چشم می‌خورد، صرفاً در سرورهای رایانه‌ای وجود دارند. به همین شکل، بیشتر تراکنش‌های مربوط به کسب‌وکارها با انتقال داده‌های الکترونیکی از یک فایل رایانه‌ای به دیگری و بدون هیچ‌گونه مبادله پول نقد فیزیکی انجام می‌شوند. فقط یک مجرم است که مثلاً یک خانه را با ارائه کیفی پر از اسکناس خریداری می‌کند. زمانی که با اینترنت یا خودپرداز از حساب خود به حساب دوست‌تان پول واریز می‌کنید، تنها عملی که رخ می‌دهد، این است که از رقم حساب شما مقداری کسر شده و به رقم حساب دوست‌تان مقداری اضافه می‌شود؛ بدون اینکه هیچ انتقال فیزیکی صورت بگیرد.

ظهور بیت‌کوین؛ عصر ارزهای دیجیتال

اندکی پس از آرام‌گرفتن بحران اقتصادی فاجعه‌بار در سال ۲۰۰۸، شکل جدیدی از دارایی و شاید پول که بشر تاکنون به خود ندیده بود، معرفی شد؛ بیت‌کوین ، یک سیستم پولی که متعلق به هیچ دولت، نهاد یا شرکتی نیست. سیستمی که هیچ‌کس نمی‌تواند به‌تنهایی روی آن کنترلی داشته باشد. یک سیستم غیرمتمرکز؛ پول مردم.

بحران مالی سال ۲۰۰۸، بدترین بحران اقتصادی از زمان رکود بزرگ در سال ۱۹۲۹ است. در فاصله سال‌های ۲۰۰۷ تا ۲۰۰۸، ده‌ها بانک و شرکت با چند میلیارد دلار ارزش

ورشکستی خود را اعلام کردند و روزی نبود که اخبار سقوط بورس تیتر اول رسانه‌ها نباشد. با وجود تلاش‌های فراوانِ ابرقدرت‌هایی مانند آمریکا و بریتانیا، جهان دو سال درگیر یک بحران بزرگ و موجی از بیکاری شد. برای این بحران دلایل زیادی ارائه شده است؛ برخی بازار آشفته مسکن را به آن ربط می‌دهند و برخی دیگر دولت‌های وقت را مقصر این بحران می‌دانند. اما ریشه تمام دلایل به یک چیز بازمی‌گردد؛ سیستم پولی فاسد.

بانک‌ها و مؤسسات مالی نه‌تنها در این بحران؛ بلکه در بحران‌های پیشین هم در صف متهمان اصلی قرار داشتند. دیگر کافی بود. سیستم پولیِ دارای خطا و نیازمند به اعتماد، دیگر نمی‌توانست کسی را راضی کند. ما به یک سیستم پولی جدید نیاز داشتیم؛ سیستمی شفاف با سیاست‌های مشخص. در اواخر سال ۲۰۰۸، زمانی که جهان هنوز در شوک بحران مالی بود، فرد یا گروه ناشناسی که خود را «ساتوشی ناکاموتو» می‌خواند، بیت‌کوین را معرفی کرد.

بیت‌کوین پدیده‌ای انقلابی است که به عقیده بسیاری، جرقه تحول گسترده در نظام مالی دنیا را زده است و انقلاب ارزهای دیجیتال مثل یک بهمن هر چیزی را که سد راهش باشد، از میان برمی‌دارد. ظهور بیت‌کوین آغاز تلاشی برای رسیدن به یک هدف بود؛ حذف اعتماد متمرکز.

این ایده که مردم بتوانند بدون نیاز به اعتماد کردن به بانک‌ها و نهادهای متمرکز، به‌صورت مستقیم تبادلات مالی خود را انجام دهند، ایده توزیع غیرمتمرکز پول که آن را تحت عنوان «استخراج» می‌شناسیم، ایده یک دفتر حسابداری جهانی و ایده یک ارز جهانی (ارزی که هیچ مرز و جغرافیایی را نمی‌شناسند) چیزهایی نیست که بتوان به‌سادگی از کنار آنها گذشت.

حالا که در زمان نگارش این کتاب حدود ۱۳ سال از ظهور بیت‌کوین می‌گذرد، دیگر این ارز دیجیتال تنها نیست. در حال حاضر هزاران ارز دیجیتال گوناگون وجود دارد و همچنان این رقم در حال افزایش است. به عقیده بسیاری از صاحب‌نظران علوم اقتصاد، از جمله «جیم ریکاردز»، حرکت دنیا به سمت حریم خصوصی و حذف اعتماد، نشان می‌دهد که حتی اگر بیت‌کوین از بین برود، ارزهای دیجیتال غیرمتمرکز

به راه خـود ادامه می‌دهنـد. حالا که بـه درک درسـتی از چگونگی پیدایـش و ذات پول رسـیده‌اید، در ادامـه وارد دنیـای نامحـدود ارزهـای دیجیتال می‌شـویم تا ایـن پدیده پیچیده را با بیانی ساده تشریح کنیم.

فصل دوم

بیت‌کوین

بیت‌کوین اولین ارز دیجیتال غیرمتمرکز دنیاست. در زمان نوشتن این فصل از کتاب، بازار بیت‌کوین حدود ۴۰ درصد از کل بازار ارزهای دیجیتال را به خود اختصاص داده بود. می‌توان گفت که آشنایی با بیت‌کوین کلید شناخت تمام دنیای کریپتو است، زیرا با شناختن درست آن، درک سایر مفاهیم برایتان بسیار راحت‌تر خواهد بود و بالعکس اگر بیت‌کوین را درست نشناسید، در درک سایر مفاهیم هم احتمالاً با مشکل مواجه خواهید شد. این فصل را به‌طور کامل به بیت‌کوین و تمام جنبه‌های مرتبط با آن اختصاص می‌دهیم.

بیت‌کوین به زبان ساده

در ساده‌ترین تعریف، بیت‌کوین یک ارز و پول دیجیتال و همچنین یک شبکه برای پرداخت‌های مستقیم و بدون واسطه است. چیزی که بیت‌کوین را از سایر پول‌ها و سیستم‌های پیش از خود متمایز می‌کند، غیرمتمرکز بودن آن است. غیرمتمرکز بودن یعنی اینکه قدرت کنترل یک سیستم، برنامه، شبکه، دولت یا هر چیز دیگری بین افراد مختلف تقسیم شود. هیچ‌کس نمی‌تواند به‌تنهایی کنترل یک سیستم غیرمتمرکز را در دست داشته باشد و هیچ‌کس مالک اصلی آن نیست. به همین ترتیب، هیچ بانک، مؤسسه، نهاد یا دولتی، بیت‌کوین را کنترل نمی‌کند. در حقیقت می‌توان گفت کنترل بیت‌کوین به دست تمام مشارکت‌کنندگان و افراد فعال در جامعه آن است. در سیستم‌های سنتی، برای انتقال پول و ارزش مجبور هستید به سازمان‌های متمرکزی مانند بانک اعتماد کنید، اما با بیت‌کوین می‌توانید بدون نیاز به اعتماد به هیچ مؤسسه و نهادی، به تمام جهان به‌صورت مستقیم و همتابه‌همتا، پول (بیت‌کوین) ارسال کنید. در واقع در بیت‌کوین اعتماد از واسطه‌های متمرکز ـ که می‌توانند مرتکب اشتباه عمدی یا سهوی شوند ـ به ریاضیات منتقل شده؛ دو به علاوه دو، همیشه چهار می‌شود، حتی اگر یک قدرت متمرکز مخالف این حقیقت باشد.

از بیت‌کوین می‌توان همانند پول‌های رایج برای خرید کالا، تبادل و انتقال پول استفاده کرد و همچنین مانند طلا آن را با هدف سرمایه‌گذاری ذخیره کرد. واحد اختصاری ارز بیت‌کوین، BTC است، مثل دلار که واحد اختصاری آن USD است.

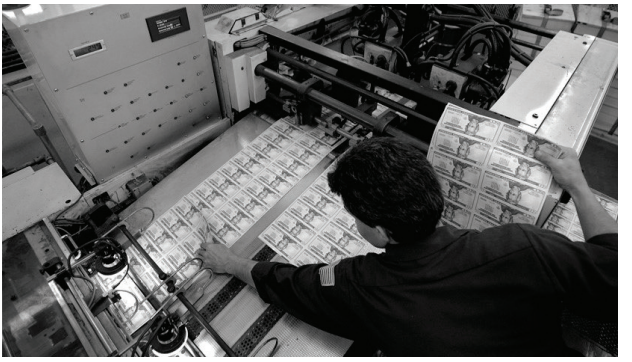
این نکته را فراموش نکنید که بیت‌کوین هیچ‌گونه شـکل و فرم فیزیکی ندارد و فقط به شکل دیجیتالی منتقل می‌شـود. امروزه هر کس به‌راحتی می‌تواند بیت‌کوین بخرد و در نرم‌افزار کیف پولی که روی گوشی موبایل خود نصب کرده، آن را ذخیره کند. سپس در عرض چند سـاعت بیت‌کوین را برای فرد دیگری در هر نقطه کره زمین ارسـال کند، بدون اینکه نیاز باشـد از بانک یا هر گونه واسـطه‌ای کمـک بگیرد. این پدیـده در واقع کنترل و مالکیـت واقعی پول را به دسـت خود افـراد برگردانـده و هویـت در آن با کلمه عبور ویژه‌ای که «کلید خصوصی» نام دارد، تعیین می‌شود. بر خلاف آنچه در سیستم بانکداری می‌بینیـم، بیت‌کوین بـه هیچ‌عنوان قابل مصادره یا قابل سانسـور نیسـت، البته تا زمانی که آن را خودتان نگهداری کنید و در نگهداری آن به سیستم‌های متمرکز متکی نباشید.

بیت‌کوین همچنین یکی از بزرگ‌ترین چالش‌های موجود در اینترنت را برطرف کرد. پول‌های دیجیتال همواره با یک مشکل بزرگ روبه‌رو بوده‌اند که «دو بار خرج‌کردن» نام دارد. در دنیای دیجیتال خیلی راحت می‌توان از یک فایل یا متن هزاران کپی تهیه کرد، اما پول نباید کپی شود. این مشکل در اسکناس‌های کاغذی و پول‌های فیزیکی وجود ندارد. برای مثال، نمی‌توانید اسکناسی را که برای خرید یک غذا خرج کرده‌اید، دوباره برای خرید یک کالای دیگر اسـتفاده کنید، اما در دنیای دیجیتـال، اگر پول مانند یک فایل باشـد، می‌توانید آن را همزمان در دو محل جداگانه خرج یا به عبارتی پول را کپی کنید. به خاطر همین مسئله، تا قبل از ظهور ارزهای دیجیتال غیرمتمرکز، همیشه یک سازمان مرکزی برای بررسـی موجودی‌های اشخاص وجود داشـت تا جلوی کپی‌شدن پـول را بگیرد، امـا بـا پیدایـش بیت‌کوین این سـازمان مرکـزی از میان برداشـته شـد و مسئولیت بررسـی این تراکنش‌ها به کل افراد شـبکه محول شـد. پس دیگر دستاورد مهم بیت‌کوین، حل مشکل دو بار خرج‌کردن بدون اعتماد به فردی دیگر بود.

تعداد واحدهای بیت‌کوین محدود بوده و این ارز ضدتورمی است. بر خلاف ارزهای رایج (فیـات= بـدون پشـتوانه) کـه دولت‌ها بـه تعـداد نامحـدود آنهـا را چـاپ و صادر می‌کننـد، در پروتکل یا همـان کد بیت‌کوین مشـخص شـده که بیت‌کوین‌هـا محدود باشـند و تعداد آنها فقط ۲۱ میلیون واحد خواهد بود. پس از رسیدن تعداد واحدهای

بیت‌کوین‌ها به رقم ۲۱ میلیون، دیگر هیچ بیت‌کوینی تولید نخواهد شد. محدود بودن واحدهای بیت‌کوین، شعار نیست و از آنجایی که همه می‌توانند در مالکیت شبکه نقش ایفا کنند، این مسئله کاملاً اثبات شده است.

در مقابل پول‌های رایج که بانک‌های مرکزی تنها مرجع صدور پول هستند، واحدهای بیت‌کوین به دست سازمان خاصی تولید و صادر نمی‌شوند، بلکه افراد داوطلبی به نام استخراج‌کننده یا به اصطلاح «ماینر» این وظیفه را بر عهده می‌گیرند. در شبکه بیت‌کوین هر کسی می‌تواند با اختصاص‌دادن قدرت پردازش سخت‌افزارهای کامپیوتری خود به شبکه، ماینر شود. طی فرایند استخراج، علاوه بر تأیید تراکنش‌ها و حفظ امنیت شبکه، بیت‌کوین تولید می‌شود و به‌عنوان پاداش به ماینرها تعلق می‌گیرد. این‌گونه است که واحدهای بیت‌کوین تولید شده و به گردش درمی‌آیند. برای اولین‌بار در تاریخ، با بیت‌کوین حق توزیع پول از دولت به مردم واگذار شده است. در صفحات پیش‌رو درباره استخراج بیشتر می‌خوانید.



شکل ۱-۲: یکی از مهم‌ترین ویژگی‌های بیت‌کوین عدم امکان افزایش عرضه آن توسط یک گروه یا نهاد خاص است.

بیت‌کوین غیرقابل جعل و تراکنش‌های آن غیرقابل بازگشت است. کسی نمی‌تواند تراکنش ساختگی در شبکه ایجاد کند و بیت‌کوینی خارج از قوانین موجود وارد شبکه کند یا بیت‌کوین‌های افراد دیگر را به سرقت ببرد. اساس غیرقابل جعل‌بودن بیت‌کوین

به خاطر تکنیک‌های رمزنگاری است که در آن استفاده شده است. همچنین زمانی که بیت‌کوین ارسال می‌کنید، بر خلاف سیستم‌های سنتی، بانک یا نهاد خاصی نمی‌تواند مانع از تراکنش شما شود. زمانی هم که بیت‌کوین به دست گیرنده می‌رسد، هیچ‌کس قادر نیست که آن را برگشت بزند، مگر با خواست (یا کلید خصوصی) گیرنده.

بیت‌کوین با کمک یک پایگاه داده و یک دفتر کل توزیع‌شده به نام «بلاکچین» فعالیت می‌کند. در فصل‌های بعد با بلاکچین و دفتر کل توزیع‌شده بیشتر آشنا می‌شوید، اما به‌طور خلاصه، بلاکچین مثل یک دفترچه یادداشت دیجیتالی است که می‌توان هر نوع اطلاعات را روی آن به‌صورت اشتراکی و غیرقابل تغییر، ثبت کرد. زمانی که یک داده روی این دفترچه دیجیتالی ثبت شود، کسی نمی‌تواند آن را پاک کند یا تغییری در آن دهد. این داده هر چیزی می‌تواند باشد، اما در بیت‌کوین، اطلاعاتی که روی بلاکچین ثبت می‌شود، تاریخچه تراکنش‌هاست. بنابراین، تمام سوابق تراکنش‌های بیت‌کوین روی یک دفتر دیجیتال به نام بلاکچین ثبت می‌شود و هرکسی که به شبکه بیت‌کوین متصل می‌شود (که اصطلاحاً نود[1] نام دارد)، یک کپی کامل از آن را دریافت می‌کند. کامپیوترهای متصل به شبکه یا همان نودها هر تراکنشی که به بیت‌کوین ارسال می‌شود را اعتبارسنجی می‌کنند و با رأی اکثریت مشخص خواهد شد که تراکنش معتبر است یا خیر. بلاکچین باعث می‌شود که نتوان جلوی تراکنش‌های بیت‌کوین را گرفت، آنها را برگشت زد یا در آن تغییری ایجاد کرد.

بیت‌کوین را شخص (یا شاید گروهی) به نام ساتوشی ناکاموتو خلق کرده است. ساتوشی ناکاموتو نامی است که خالق بیت‌کوین پای مقاله معرفی شاهکار خود نوشته بود. هویت این نابغه، کسی که به عقیده صاحب‌نظران باید جایزه نوبل بگیرد، تاکنون ناشناس مانده و تنها چیزی که از هویت او در دست داریم، فقط حدس و گمان است. یکی از نکات جالب درباره بیت‌کوین هم همین راز خالق آن است. بیت‌کوینرها (طرفداران سرسخت بیت‌کوین) معتقدند مخفی‌بودن هویت ساتوشی نشان می‌دهد که این پدیده به هیچ‌کس وابسته نیست و راه خودش را طی می‌کند.

شاید در ابتدا با شنیدن نام مخترع بیت‌کوین گمان کنید که او اهل ژاپن یا یکی از

1. Node

کشورهای شرقی باشد، اما اسم او لزوماً شرقی بودنش را اثبات نمی‌کند و حتی طبق مدارک موجود از نوشته‌های او، احتمال غربی‌بودن ناکاموتو بیشتر است. در ادامه کتاب بیشتر درباره چگونگی پیدایش و گسترش بیت‌کوین و هویت ساتوشی ناکاموتو می‌خوانید.

در بحث بها و قیمت بیت‌کوین، ارزش این دارایی همان‌طوری تعیین می‌شود که ارزش طلا، دلار، ریال، یورو، پوند انگلیس یا هر ارز رایج دیگری تعیین می‌شود. در واقع عرضه و تقاضای بیت‌کوین در صرافی‌های آنلاین یا بازارهای غیررسمی، قیمت آن را مشخص می‌کند. بدیهی است که هر چقدر تقاضا برای بیت‌کوین بیشتر باشد، قیمت آن هم افزایش می‌یابد. کمیابی و تعداد محدود واحدهای این ارز دیجیتال هم در بها و ارزش آن تأثیر بسزایی دارد؛ چراکه محدود بودن عرضه اگر با افزایش تقاضا همراه شود، موجب افزایش قیمت خواهد شد.

قیمت بیت‌کوین در روزهای اولیه معرفی این ارز دیجیتال کمتر از ۰/۱ دلار بوده و اکنون که در حال نوشتن این بخش از کتاب هستیم، با چندصد هزار درصد افزایش طی ۱۳ سال، بیش از ۳۰ هزار دلار آمریکا قیمت دارد. قیمت بیت کوین لحظه‌ای تغییر می‌کند و شاید وقتی در حال خواندن این قسمت هستید، بیت کوین ارزشی متفاوت از آنچه که اکنون هست داشته باشد. کسانی که کمتر از یک دهه پیش فقط ۱۰۰ دلار بیت‌کوین خریدند و نگهداری کردند، امروز در زمره میلیونرها قرار دارند. بیت‌کوین در سراسر جهان روی سایت‌های صرافی به ازای ارزهای رایج و همچنین ارزهای دیجیتال دیگر خریدوفروش می‌شود و به‌راحتی می‌توان از طریق صرافی‌های آنلاین بیت‌کوین خریداری کرد یا آن را به فروش رساند. در فصل‌های بعد در مورد خریدوفروش ارزهای دیجیتال به‌طور مفصل می‌خوانید.

برای ذخیره، ارسال یا دریافت بیت‌کوین به «کیف پول» نیاز دارید. اگر بخواهیم خیلی مختصر توضیح بدهیم، کیف پول بیت‌کوین ابزاری است که با استفاده از آن می‌توانید بیت‌کوین‌هایتان را ذخیره کنید، آنها را انتقال دهید یا از فرد دیگری بیت‌کوین دریافت کنید. این ابزار می‌تواند نرم‌افزار رایگانی در گوشی و کامپیوتر شما باشد یا سخت‌افزار قابل حملی که در حد و اندازه یک فلش مموری است. تعداد نرم‌افزارهای کیف پول خیلی زیاد است و به‌صورت رایگان در نام‌های مختلف عرضه می‌شوند.

بنابراین به‌سادگی می‌توانید در کمتر از چند دقیقه یک کیف پول بیت‌کوین رایگان روی کامپیوتر یا تلفن همراه هوشمند خود نصب کرده و از آن استفاده کنید.

امروزه به لطف توسعه‌دهندگانی که شبانه‌روز روی بیت‌کوین کار می‌کنند، همه افراد با کمترین سطح از دانش فنی می‌توانند از بیت‌کوین استفاده کنند و ارسال و دریافت بیت‌کوین به‌سادگی ارسال و دریافت پیامک است. در صفحات پیش رو، به‌صورت کامل به مبحث کیف پول‌ها پرداخته شده است.

داستان ظهور بیت‌کوین

«چیزی که به آن نیاز داریم، یک سیستم پرداخت الکترونیکی است که به جای اعتماد، بر رمزنگاری استوار باشد.»

ساتوشی ناکاموتو

۳۱ اکتبر سال ۲۰۰۸، ساعت ۱۴:۱۰ به وقت نیویورک؛ چندصد نفر از اعضای یک انجمن اینترنتی شامل متخصصان و دوستداران علم رمزنگاری، ایمیلی از شخصی که خود را «ساتوشی ناکاموتو» می‌خواند، دریافت می‌کنند؛ «من در حال کار کردن روی یک سیستم پرداخت الکترونیکی بوده‌ام که کاملاً همتابه‌همتاست و هیچ طرف سومی در آن دخالت ندارد.»

ساتوشی ناکاموتو در این پیام شرحی مختصر از سیستم انقلابی خود ارائه کرده و در جزئیات بیشتر به یک مقاله ۹صفحه‌ای (وایت‌پیپر) پیوند داده بود که در آن ایده بیت‌کوین با جزئیات بیشتری توضیح داده شده است.

افرادی که پیام ساتوشی ناکاموتو را دریافت کردند، خود را «سایفرپانک» می‌نامند. سایفرپانک نام جنبشی است که تلاش می‌کند علم رمزنگاری را به‌منظور امنیت و حریم خصوصی در اینترنت بین مردم و شرکت‌ها گسترش دهد. از مطرح‌ترین افرادی که دعوت پنهانی ساتوشی ناکاموتو را دریافت کردند، می‌توان به «آدام بک» ، «نیک زابو»، «وی دای»، «هال فینی» و «دیوید چام» اشاره کرد. این افراد پیش از معرفی بیت‌کوین بارها تلاش کرده بودند تا با استفاده از رمزنگاری یک سیستم پولی

همتابه‌همتا ایجاد کنند، اما همگی‌شان با شکست مواجه شده بودند. ساتوشی نام بسیاری از این سایفرپانک‌ها را در مقاله معرفی بیت‌کوین آورده است و بارها به تأثیری که این افراد در خلق بیت‌کوین داشته‌اند، اشاره کرده است.

آدام بک مخترع «هش‌کش»[1] است. هش‌کش راهکاری بود که در زمان اوج‌گیری استفاده از اینترنت، برای جلوگیری از اسپم یا همان هرزنامه ساخته شده بود. این متخصص رمزنگاری برای جلوگیری از ارسال پیام‌های بیهوده از طرف اسپمرها که با هدف مختل‌کردن سیستم‌ها انجام می‌شد، در ابتکار خود این الزام را ایجاد کرد که کاربران برای ارسال پیام باید با سخت‌افزار کامپیوتر خود (CPU) یکسری محاسبات ریاضی انجام می‌دادند که نیازمند زمان و مصرف برق بود. به این ترتیب، اگر کسی می‌خواست هرزنامه‌ای ارسال کند، مجبور بود مقدار زیادی قدرت پردازش سخت‌افزاری داشته باشد که این خود مستلزم مصرف‌کردن برق بود. به این روش «اثبات کار» می‌گویند که در بیت‌کوین با نام «ماینینگ» یا همان استخراج می‌شناسیم.

نیک زابو، خیلی قبل‌تر از بیت‌کوین و در سال ۱۹۹۸ به‌دنبال ساخت چیزی شبیه بیت‌کوین بود که «بیت‌گولد» نام داشت. پروژه بیت‌گولد به‌دلیل مشکلات فنی شکست خورد و هیچ‌وقت عملیاتی نشد، اما از آن به‌عنوان «پایه‌گذار معماری بیت‌کوین» یاد می‌کنند.

زابو، محقق کامپیوتر، پژوهشگر در زمینه حقوق و در کل انسان همه‌فن‌حریفی است. او تاکنون گنجینه‌ای از مقالات را در زمینه‌های اقتصاد، علوم کامپیوتر، سیاست، انسان‌شناسی و حقوق به رشته تحریر درآورده است. زابو همچنین خالق ایده «قرارداد هوشمند» است که در فصل بعد درباره آن خواهید خواند. بسیاری از اعضای جامعه بیت‌کوین معتقدند که او خود ساتوشی ناکاموتو است؛ چیزی که زابو بارها آن را رد کرده است.

وی دای هم پیش از بیت‌کوین، در سال ۱۹۹۸ ارز دیجیتال خود را ساخته بود. او که متخصص علم رمزنگاری و عاشق ریاضیات و فلسفه است، پروژه‌ای به نام بی‌مانی

1. HashCash

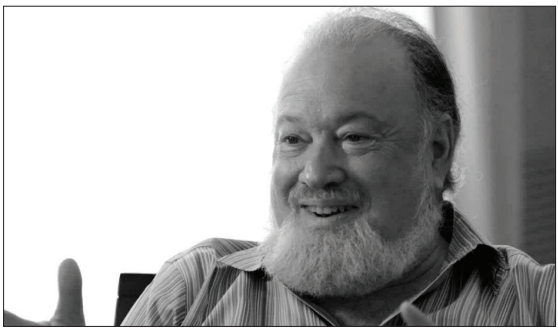
را معرفی کرد که مانند بیت‌کوین با تراکنش‌های همتابه‌همتای ناشناس و دفتر کل مشترکی که هر عضو شبکه می‌توانست با آن تراکنش‌ها را اعتبارسنجی کند، مطرح شد. در سیستم بی‌مانی، برای تأیید تراکنش‌ها پاداش و برای تقلب مجازات در نظر گرفته شده بود. شرکت‌کنندگان در شبکه باید مقداری پول را به حساب خاصی واریز می‌کردند که در صورت اثبات سوءنیت مجازاتی وجود داشت. تصورش سخت نیست که نقطه‌ضعف این راه‌حل، در تشویق به همدستی بود. چگونه یک جامعه بدون وجود نهاد اجرایی مرکزی می‌تواند مجازات در نظر بگیرد؟ داوری و قضاوت به عهده چه کسی خواهد بود؟ بی‌مانی به همین دلیل شکست خورد. اما راه‌حل بیت‌کوین این بود که مسئله تنها به دادن پاداش متکی باشد، نه اعمال مجازات.

هال فینی یکی دیگر از متخصصان بزرگ رمزنگاری بود. او به‌عنوان یکی از اعضای برجسته و اولیه جنبش سایفرپانک‌ها، با نوآوری‌های گوناگون خود مانند «بازفرستنده ایمیل ناشناس»[1] که به مردم اجازه می‌داد بدون مشخص‌شدن هویتشان ایمیل ارسال کنند، اعتباری برای خود دست‌وپا کرده بود. سال ۲۰۰۴ فینی نسخه پول الکترونیکی خود را ساخت، اما هرگز آن را برای عموم منتشر نکرد. همانند بیت‌کوین، مدل فینی نیز از «اثبات کار» استفاده می‌کرد. در ارتباط با بیت کوین، فینی یکی از اولین کسانی بود که نرم‌افزار بیت‌کوین را نصب کرد و به استخراج این ارز دیجیتال پرداخت. اولین تراکنش تاریخ بیت‌کوین را هم که ۱۰ واحد بیت‌کوین بود، هال فینی از ساتوشی ناکاموتو دریافت می‌کند که همین موضوع یکی دیگر از دلایلی است که احتمال ساتوشی‌بودن هال فینی را پررنگ کرده است. او در سال ۲۰۱۴ به‌دلیل یک بیماری نادر درگذشت.

بدون اغراق می‌توان گفت معروف‌ترین نمونه پول الکترونیکی قبل از بیت‌کوین «دیجی‌کش»[2] است که خالقش دیوید چام بود. این پروژه حتی قبل از جنبش سایفرپانک‌ها و در سال ۱۹۸۹ معرفی شد. شرکت دیجی‌کش در هلند آغاز به کار کرد و به نظر می‌رسید که در دنیای روبه‌رشد اینترنت یک پروژه انقلابی باشد. ساخته فکری چام یک زیرساخت رمزنگاری بود که از هویت پرداخت‌کننده محافظت می‌کرد و در عین حال

1. Anonymous remailer
2. DigiCash

به او اجازه می‌داد به‌طور انکارناپذیری در صورت نیاز، گیرنده را شناسایی کند.



شکل ۲-۲: دیوید چام از پیشگامان رمزنگاری و توسعه فناوری‌های حریم خصوصی‌محور به حساب می‌آید.

دیجی‌کش خیلی زود مذاکراتی را با شرکت‌های بزرگی مثل مایکروسافت آغاز کرد و با چند بانک هم برای گسترش آن قرارداد همکاری امضا کرد، اما در اواخر دهه ۱۹۹۰ با ظهور شرکت‌های پرداخت اینترنتی از جمله پی‌پال این پروژه که برای ادامه کار به یک سیستم مرکزی نیاز داشت، در رقابت شکست خورد و شرکت دیجی‌کش خیلی زود اعلام ورشکستگی کرد.

سرانجام بعد از سال‌ها شکست، به بیت کوین رسیدیم. تنها حدود سه ماه پس از معرفی بیت‌کوین، در ژانویه ۲۰۰۹ اولین نسخه از نرم‌افزار آن عرضه شد و ساتوشی ناکاموتو، خالق آن، به‌عنوان اولین مشارکت‌کننده، اولین بلوک (بلوک شماره صفر) از بلاکچین بیت‌کوین را استخراج کرد که به آن «بلوک پیدایش» (جنسیس) هم می‌گویند. با ایجاد اولین بلوک، ۵۰ واحد بیت‌کوین تولید (استخراج) شد و به این ترتیب، این پدیده به موجودیت رسید. یکی از نکات جالب در بیت‌کوین این است که سازنده بلوک می‌تواند پیام دلخواه خود را در آن ثبت کند. در اولین بلوک بیت‌کوین، ساتوشی این پیام را ثبت کرده است: «نشریه تایمز/ سوم ژانویه ۲۰۰۹/ رئیس خزانه در آستانه دومین کمک مالی به بانک‌ها». این پیام به یکی از اخبار منتشرشده در روزنامه تایمز اشاره می‌کند؛ مبنی

بر اینکه رئیس خزانه (سلطنتی) وقتِ بریتانیا برای نجات بانک‌ها از بحران، به‌دنبال کمک مالی به آنهاست. به گفته صاحب‌نظران، ساتوشی با ثبت این پیام قصد داشته ضعف سیستم بانکداری را نشان دهد و هدف ایجاد بیت‌کوین را به رخ بکشد. همچنین، با توجه به زمان انتشار روزنامه، ساتوشی با این پیام توانسته زمان تولد بیت‌کوین را هم اعلام کند. خالق بیت‌کوین تا اواخر سال ۲۰۱۰ با کمک جامعه بیت‌کوین این نوزاد نوپا را کمی به جلو برد. در روز ۱۲ دسامبر ۲۰۱۰، ساتوشی بعد از انتشار آخرین پست خود برای همیشه ناپدید شد و ادامه گسترش بیت‌کوین را به جامعه آن سپرد. او هیچ مطلبی مبنی بر خداحافظی منتشر نکرد و آخرین یادداشت برجای‌مانده از او هم یک مطلب فنی مربوط به به‌روزرسانی بیت‌کوین است. البته در سال ۲۰۱۴ زمانی که بحث در مورد احتمال ساتوشی‌بودن فردی به نام «دوریان ناکاموتو» داغ بود، یکی از حساب‌های کاربری منتسب به ساتوشی ناکاموتو چنین نوشته‌ای را منتشر کرد: «من دوریان ناکاموتو نیستم.»

ساتوشی ناکاموتو کیست؟

هرچه بیت‌کوین بزرگ‌تر می‌شود، هویت ساتوشی ناکاموتو، خالق آن، اهمیت بیشتری می‌یابد. تاکنون ده‌ها خبرنگار و بنیاد تحقیقاتی برای کشف هویت ساتوشی تلاش کرده‌اند، اما همه آنها در نهایت به در بسته خورده‌اند. گروهی معتقدند که بیت‌کوین نمی‌تواند ساخته دست یک نفر باشد و به احتمال زیاد ساتوشی ناکاموتو یک گروه متشکل از چند برنامه‌نویس است. گروهی دیگر عقیده دارند که یک یا چند نفر از همان سایفرپانک‌هایی که قبل از بیت‌کوین برای ایجاد پول دیجیتال تلاش کرده بودند. مثل نیک زابو، هال فینی یا آدام بک. همان ساتوشی هستند که البته همه‌شان این ادعا را رد کرده‌اند.

با شنیدن نام ساتوشی ناکاموتو در ابتدا این حس القا می‌شود که مخترع بیت‌کوین یک فرد یا گروهی از کشورهای شرقی مانند ژاپن است. با این حال، بررسی‌ها در سبک نگارش و منطقه زمانی او. بر اساس زمان مطالبی که منتشر شده است. نشان می‌دهد احتمال بریتانیایی‌بودن ساتوشی بیشتر از ژاپنی‌بودن اوست. هیچ نشانه روشنی از ساتوشی وجود ندارد و گویا قرار نیست این راز هیچ‌گاه فاش شود. طبق اولین آدرس‌های

ثبت‌شده در شبکه بیت‌کوین، گفته می‌شود ساتوشی ناکاموتو بیش از یک میلیون از واحدهای بیت‌کوینی که در ابتدای کار شبکه استخراج شده است را در اختیار دارد؛ یک میلیون بیت‌کوینی که در زمان نوشتن این کتاب معادل حدود ۱۰ میلیارد دلار است. اگر هویت ساتوشی ناکاموتو مشخص بود، او با این دارایی که مدام به ارزشش افزوده می‌شود، اکنون در میان ثروتمندترین افراد دنیا قرار داشت.

برخی بیت‌کوین را حاصل همکاری مخفیانه چند شرکت بزرگ فناوری می‌دانند و برخی دیگر با پیروی از تئوری توطئه، معتقدند که این ارز دیجیتال پروژه یک سازمان دولتی مثل آژانس امنیت ملی آمریکا (NSA) است. همچنین طی این سال‌ها که از عمر بیت‌کوین می‌گذرد، افراد زیادی ادعای ساتوشی ناکاموتو بودن کرده‌اند که به‌دلیل عدم ارائه مدارک کافی، تمام این ادعاها از طرف حامیان بیت‌کوین رد شده است. مهم‌ترین فردی که دعوی ساتوشی‌بودن دارد، «کریگ رایت»، از اولین فعالان حوزه بیت‌کوین است که در ادامه به آن می‌پردازیم. دلیل مخفی‌بودن ساتوشی ناکاموتو، خودش یک موضوع مورد بحث دیگر است. بعضی ساتوشی را یک خوره کامپیوتر (گیک) می‌دانند که با ایمان به آرمان‌های اینترنت ناشناس، مایل به فاش‌شدن هویتش نبوده است. گروهی دیگر می‌گویند ساتوشی ناکاموتو از ترس جانش به‌عنوان شروع‌کننده جریان پول غیرمتمرکز خودش را مخفی کرده است. گروهی دیگر حدس می‌زنند که ساتوشی دستگیر یا کشته شده باشد. گروهی نیز معتقدند که ساتوشی ناکاموتو احتمالاً تاکنون خودش را بارها معرفی کرده است، اما کسی حرف او را باور نمی‌کند. هرچه هست، به عقیده اغلب اعضای جامعه بیت کوین، مخفی‌بودن ساتوشی اتفاقی مثبت برای بیت‌کوین تلقی می‌شود، چون انعکاسی از فلسفه جاودانه‌بودن این پول دیجیتال است. ناشناسی ساتوشی به حدی عمیق است که دوست شما، همکارتان و حتی اعضای خانواده‌تان هم می‌توانند ساتوشی ناکاموتو باشند. اما در این میان برخی ناکاموتو«تر» از بقیه هستند. در ادامه با چند شخصیتی آشنا می‌شوید که از آنها به‌عنوان نزدیک‌ترین افراد به هویت خالق بیت‌کوین یاد می‌شود.

گوین اندرسن

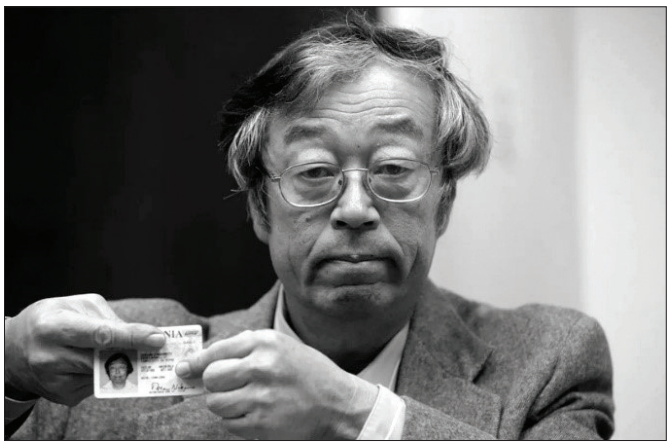
«گوین اندرسن» فردی است که پس از آنکه ناکاموتو میدان را ترک کرد، سکان

هدایت بیت‌کوین را به وی سپرد. او از همان ابتدا کمک‌های زیادی به ترویج بیت‌کوین کرد و ماه‌ها به‌صورت شبانه‌روزی روی کد بیت‌کوین کار کرد تا قابلیت‌های آن را افزایش دهد.

ساتوشی و گوین اندرسن می‌توانند یک نفر باشند؛ چراکه در این صورت ناکاموتو می‌تواند بدون آنکه میدان را ترک کند، با یک هویت جدید به توسعه بیت‌کوین ادامه دهد. به‌علاوه، طی یک تحقیق سبک‌شناسی، قلم اندرسن شباهت زیادی به قلم ناکاموتو دارد. با این حال، خود او این ادعا را رد کرده است. اندرسن در سال ۲۰۱۶ مدعی شد که احتمالاً محقق استرالیایی یعنی کریگ رایت همان ساتوشی ناکاموتو است، اما مدتی بعد دوباره در این باره ابراز شک و تردید کرد و گفت که «خودش را از این بازی کنار می‌کشد».

دوریان ساتوشی ناکاموتو

یکی دیگر از گزینه‌های احتمالی، یک فرد ژاپنی-آمریکایی ساکن کالیفرنیا به نام «دوریان پرینتیس ساتوشی ناکاموتو» است. تشابه اسمی فوق‌العاده نزدیک به ساتوشی و سابقه او در فیزیک، باعث قوت‌گرفتن این احتمال شد.



شکل ۳-۲: دوریان ناکاموتو

نام دوریان ساتوشی اولین‌بار در یک هفته‌نامه خبری در مارس ۲۰۱۴ مطرح شد. در آن مقاله، نویسنده به تدریس ناکاموتو به‌عنوان فیزیکدان در دانشگاه «کال پولی» پاناما و سابقه آزادی‌خواهانه‌اش در گذشته، به‌عنوان مدارکی برای هویت او اشاره کرد. بزرگ‌ترین مدرک در مورد او پاسخ ناکاموتو درباره سؤالی در رابطه با بیت‌کوین است که این فرد در جواب گفته بود: «من دیگر با این موضوع کاری ندارم، به همین خاطر دیگر نمی‌توانم درباره آن نظری بدهم، حالا دیگر این موضوع در دست افراد دیگری است و آنها مسئولش هستند و من دیگر هیچ ارتباطی با این ماجرا ندارم.» این مصاحبه باعث افزایش شایعات در رسانه‌ها و حتی تعقیب خودروی وی توسط خبرنگاران شد. او بعدها در مصاحبه‌ای گفته خودش را انکار کرد و اذعان داشت که سؤال خبرنگار را اشتباه متوجه شده و فکر می‌کرده که سؤال در مورد شغل محرمانه سابق او به‌عنوان پیمانکار نظامی بوده است.

هال فینی

احتمال ساتوشی‌بودن این محقق و برنامه‌نویس برجسته در علوم رمزنگاری، بسیار بیشتر از دو گزینه قبلی است. به گفته بسیاری از فعالان حوزه ارزهای دیجیتال، حتی اگر او خالق بیت‌کوین نباشد، ساتوشی ناکاموتو را به‌خوبی می‌شناخته است.

فینی مدت‌ها قبل از بیت‌کوین زندگی خودش را وقف رایانه و علوم رمزنگاری کرده بود و شخص دوم بعد از ناکاموتو محسوب می‌شود که از نرم‌افزار بیت‌کوین استفاده کرد، باگ‌های کد را گزارش داد و برای بهبود شبکه نظرات خود را بیان کرد. همچنین او اولین کسی بود که از طریق یک تراکنش، بیت‌کوین دریافت کرده است. خود او در مصاحبه‌ای گفته است که وقتی برای اولین‌بار ساتوشی قصد آزمایش تراکنش را داشته، برای او ۱۰ واحد بیت‌کوین فرستاده است. طبق گزارش نشریه فوربس، خانه او فقط چند ساختمان با دوریان پرینتیس ساتوشی ناکاموتو فاصله داشته و این شک را بیشتر می‌کند که هال فینی از اسم همسایه خود برای ساخت یک هویت جعلی استفاده کرده باشد. وی در ۲۸ آگوست ۲۰۱۴ بر اثر یک بیماری نادر درگذشت. نکته جالب در مورد فینی این است که به خواست خودش، بدن او به‌وسیله نیتروژن مایع

فریز شده، با این امید که در آینده با پیشرفت فناوری دوباره به زندگی بازگردد.

کریگ رایت

کریگ رایت، متخصص کامپیوتر استرالیایی و از اولین فعالان جامعه بیت‌کوین و مهم‌ترین شخصی است که خودش ادعا می‌کند ساتوشی است. البته تا زمان نگارش این کتاب، او هنوز مدرک درستی دال بر ادعای خود ارائه نکرده است.

در سال ۲۰۱۵، پس از انتشار گزارشی مبنی بر اینکه کریگ رایت همان ناکاموتو است، پلیس استرالیا به خانه او یورش برد، اما اعلام شد که این مسئله ربطی به بیت‌کوین ندارد. از آن زمان او چندین بار خودش را سازنده بیت‌کوین معرفی کرده و ادعا می‌کند که برای حرف‌هایش مدرک دارد. همان‌طور که اشاره شد، حداقل تا زمان نگارش این کتاب او مدرک درستی برای اثبات ادعای خود منتشر نکرده و به فردی جنجالی در فضای ارزهای دیجیتال تبدیل شده است. در جامعه بیت‌کوین از کریگ رایت اغلب با لقب «دروغگو» یاد می‌شود.

دیوید کلیمن

ادعا می‌شود دیوید کلیمن در کنار کریگ رایت، ساتوشی ناکاموتو هستند، یا حداقل در تیمش فعالیت می‌کرده‌اند. کلیمن، یک متخصص رایانه و از طرفداران پروپاقرص پول رمزنگاری‌شده بود و در فهرست اولیه ساتوشی برای معرفی بیت‌کوین نیز حضور داشت. او همچنین روی پروژه‌ای با هدف ایجاد یک «سیستم رمزنگاری‌شده و تغییرناپذیر در حوزه سوابق محاسباتی علوم رایانه‌ای» با بنیاد S-doc همکاری می‌کرده است.

طبق گزارش‌های رسمی، او یک میلیون واحد بیت‌کوین استخراج کرده که با تعداد بیت‌کوین‌های ساتوشی ناکاموتو مشابه است. کلیمن در نهایت فقر و بیچارگی در سال ۲۰۱۳ درگذشت. جسد پوسیده او در حالی یافت شد که بطری‌های الکل در اطرافش دیده می‌شدند و یک اسلحه پر در کنارش بود. یک سوراخ برجامانده از گلوله در تشک او کشف شد، اما هیچ پوکه‌ای در صحنه وجود نداشت.

نیک زابو

بدون شک نیک زابو را هم می‌توان گزینه‌ای نزدیک به ساتوشی ناکاموتو دانست. اینکه زابو یک مهندس علوم رایانه و نگارنده مقاله «بیت‌گولد» بوده، دلیل محکمی بر این موضوع است.

در سال ۲۰۰۸، زابو در وبلاگ خود تاریخ مقاله‌ای را که در سال ۲۰۰۵ نوشته بود و در آن گفته بود قصد دارد یک پول دیجیتال ایجاد کند، به‌روز کرد. کمی بعد شبکه بیت‌کوین راه‌اندازی شد. به‌علاوه، عبارت‌هایی مانند «قیمتی که کسی قابلیت تعیین آن را ندارد» در مقاله او و اشاره‌هایی به هال فینی، به گمانه‌زنی‌ها پیرامون ساتوشی‌بودن زابو دامن می‌زند. مانند بیشتر گزینه‌ها، خود او این برچسب را برای خود نمی‌پذیرد. او در سال ۲۰۱۴ گفت: «متأسفم که باید بگویم اشتباه می‌کنید و من ساتوشی ناکاموتو نیستم، اما دیگر عادت کرده‌ام.» از طرف دیگر، شاید بتوان گفت این مسئله که ناکاموتو در مقاله معرفی بیت‌کوین نامی از بیت‌گولد نبرده، خود مدرکی محکم در ارتباط با هویت اصلی‌اش باشد.

پاول لرو

در سال ۲۰۱۹ چند پادکست و مقاله معتبر درباره احتمال ساتوشی ناکاموتو بودن یکی از مرموزترین تبهکاران تاریخ یعنی پاول لرو که با نام مستعار «مسترمایند» نیز شناخته می‌شود، منتشر شد. این مقالات دلایل زیادی برای ادعای خود ارائه داده‌اند که نمی‌توان از آنها چشم‌پوشی کرد.

نام کامل او «پاول سولوتشی کالدر لروکس» است که علاوه بر جنایات مرموزش، سابقه درخشانی در برنامه‌نویسی متمرکز بر رمزنگاری دارد. او توابع رمزنگاری E4M و TrueCrypt را ساخته و در سال ۱۹۹۸ یک مانیفست شبیه به متن وایت‌پیپر بیت‌کوین منتشر کرده بود. لرو در مانیفست خود که در سایت E4M منتشر شده بود، با لحنی ساده می‌نویسد که رسیدن به حریم خصوصی در جهان در حال سخت‌تر شدن است و دولت‌ها به‌دنبال اعمال نظارت زیادی بر کار مردم هستند. او رمزنگاری را تنها راه مقابله با نقض حریم خصوصی می‌داند. پاول لرو در سال ۲۰۱۲ دستگیر شد و طبق گفته‌ها هم‌اکنون در زندان به سر می‌برد.

گزینه‌های نامحدود

به همان جمله اول برمی‌گردیم: شما، دوست شما، همکارتان و حتی اعضای خانواده‌تان هم می‌توانند ساتوشی ناکاموتو باشند. به نظر می‌رسد به نقطه‌ای رسیده‌ایم که شاید هرگز ساتوشی ناکاموتوی واقعی پیدا نشود. حتی اگر همین امروز یک نفر پیدا شود و با انتقال یک میلیون واحد بیت‌کوین که متعلق به ساتوشی ناکاموتو است، خودش را به‌عنوان ساتوشی معرفی کند و دلایل کافی برای آن داشته باشد، باز هم عده زیادی باور نخواهند کرد.

به‌جز افرادی که معرفی کردیم، افراد مشهور دیگری از جمله «ایلان ماسک»، کارآفرین افسانه‌ای، «آدام بک»، متخصص کامپیوتر و حتی یکی از اعضای باند «پابلو اسکوبار»، قاچاقی مشهور مواد مخدر هم در میان گزینه‌ها قرار دارند و این فهرست به‌صورت نامحدودی به‌روز می‌شود. هرکس در خیال خودش می‌تواند برای خود یک ساتوشی ناکاموتو داشته باشد.

یکی که غرق در نوآوری بیت‌کوین شده، می‌تواند ایلان ماسک، این کارآفرین نابغه را مخترع بیت‌کوین بداند و یکی که به آن مشکوک است، می‌تواند سازمان‌های جاسوسی آمریکا و بریتانیا را به‌عنوان خالق بیت‌کوین در نظر بگیرد. هر چه هست، تأثیر امروز بیت‌کوین در دنیای مالی را نمی‌توان انکار کرد.

بیت‌کوین چگونه کار می‌کند؟

برای کار با بیت‌کوین و سرمایه‌گذاری در آن نیازی نیست بدانید چگونه کار می‌کند، همان‌طور که برای فعالیت در اینترنت نیازی نیست که با زیرساخت‌های اصلی شبکه جهانی وب آشنا باشید. بنابراین، اگر مایل به خواندن مفاهیم فنی نیستید، می‌توانید این بخش از کتاب را نادیده بگیرید و به سراغ بخش‌های بعدی بروید. با این حال، برای تکمیل مطالب کتاب در این بخش سعی می‌کنیم برای افرادی که به آشنایی با زیرساخت بیت‌کوین علاقه‌مند هستند، چگونگی کار بیت‌کوین را توضیح بدهیم. پس از خواندن این قسمت، اگر درباره کارکرد بیت‌کوین کمی گیج شدید، جای نگرانی نیست؛ زیرا گستردگی و تازه‌بودن مفاهیم این حوزه حتی کارشناسان خبره را هم

سـردرگم می‌کند. وقتی خودتان با بیت‌کوین کار کنیـد، به‌مرور نحوه کار این سیسـتم برای شما روشن‌تر خواهد شد.

چه چیزی بیت‌کویـن را از سیسـتم‌های متمرکز متمایز می‌کند؟ درسـت حدس زدید، اصلی‌ترین نقطه تمایز بیت‌کوین با سیستم‌هایی مانند بانک این است که همه می‌توانند در کنترل سیسـتم و تأییـد تراکنش‌های بیت‌کوین نقش داشـته باشـند. تاریخچه تمام تراکنش‌های بیت‌کوین روی یک دفتر دیجیتال به نام بلاکچین ثبت می‌شود. هر کسی که به شبکه بیت‌کوین متصل می‌شود (که اصطلاحاً نود نام دارد) یک کپی کامل از بلاکچین را دریافت می‌کند. طبق قوانین شـبکه، هر تراکنشـی که به بیت‌کوین ارسال می‌شود، توسـط این کامپیوترها بررسـی خواهد شـد و هر کامپیوتر به آن تراکنش رأی می‌دهد. گروهی تراکنش را تأیید می‌کننـد و گروهی آن را غیرمعتبر می‌داننـد. در نهایت با رأی اکثریت مشخص خواهد شد که تراکنش معتبر است یا خیر.

در بیت‌کوین، با استفاده از مفهوم بلاکچین، هیچ‌کس نمی‌تواند یک تراکنش را برگشت بزند، جلوی یک تراکنش را بگیرد و در سیستم تقلب کند. تفاوت بلاکچین با دفاتر دیجیتالی و بایگانی‌های دیگر این است که اطلاعات ذخیره‌شده روی آن میان همه افراد به اشتراک گذاشته می‌شود. در نتیجه با اسـتفاده از رمزنگاری و توزیع داده‌ها، امکان هک، حذف و دست‌کاری اطلاعات ثبت‌شده، تقریباً از بین می‌رود. اگر اندکی درباره همین ویژگی تغییرناپذیری داده‌ها در بلاکچین تفکر کنیم، انقلابی‌بودن این فناوری به‌خوبی احساس می‌شود. حفظ و امنیت اطلاعات و سوابق در دنیای دیجیتال همیشه دغدغه مهمی بوده است.

به لطف بلاکچین، زمانی که فردی بخواهد مقداری بیت‌کوین برای دیگری ارسال کند، درخواست خود را در قالب پیام تراکنش به اعضای شبکه (نودها) مخابره می‌کند. نودها دفترچه‌های دیجیتالی‌شـان را ورق می‌زنند و موجودی فرسـتنده را به دست می‌آورند تا از امکان‌پذیری انجام ایـن تراکنش اطمینان حاصـل کنند. دفترچه دیجیتالـی نودها از برگه‌هایی تشـکیل شـده که در بلاکچین آنها را با نام «بلوک» می‌شناسـیم و درون آنها اطلاعات و داده ثبت می‌شـود. در صورتی که تراکنش با قوانین شـبکه مغایرتی نداشته باشد، تراکنش معتبر شناخته می‌شود و همانند خط تولید یک کارخانه منتظر ورود به مرحله بعدی، یعنی فرایند تأیید تراکنش می‌شود.

تراکنش‌ها پس از آنکه از سمت نودها معتبر شناخته شدند، در محلی مجازی به نام «مم‌پول»[1] منتظر می‌مانند تا فرایند تأیید را طی کنند. برای درک بهتر چگونگی کار کردن تراکنش‌ها در شبکه بیت‌کوین بهتر است آن را با یک مثال توضیح دهیم. مم‌پول را می‌توانیم ایستگاه اتوبوسی فرض کنیم که مسافرانش (تراکنش‌ها) منتظر آمدن اتوبوس‌ها هستند تا آنها را به مقصد برسانند (تأیید کنند). رانندگان اتوبوس همان ماینرها یا استخراج‌کنندگان هستند که پس از واردشدن به ایستگاه، تا جایی که می‌توانند اتوبوس خود را از این مسافران پر می‌کنند. اتوبوس‌ها نیز در شبکه بیت‌کوین نقش بلوک را دارند. حالا باید در این مثال کمی تغییر ایجاد کنیم تا شرایط واقعی شبکه را نشان دهد.

فرض کنید یک مسافر می‌تواند به‌طور همزمان در چند اتوبوس نشسته باشد؛ همان‌طور که یک تراکنش بیت‌کوین می‌تواند از سوی چندین ماینر انتخاب شود و در بلوک آنها قرار بگیرد. مسافران هم‌اکنون در اتوبوس‌ها نشسته‌اند و منتظر هستند رانندگان حرکت خود را به سمت مقصد نهایی آغاز کنند. این مقصد نیز در واقع همان تأییدشدن تراکنش است. با آغاز مسابقه‌ای که ماینینگ یا استخراج نام دارد، رانندگان اتوبوس (ماینرها) تلاش می‌کنند که سریعتر از بقیه، تراکنش‌هایشان را به مقصد برسانند؛ زیرا راننده اولی که موفق به انجام این کار شود، پاداش خوبی از شرکت واحد اتوبوسرانی (شبکه بیت‌کوین) دریافت خواهد کرد.

ماینرها پس از انتخاب تراکنش و قرار دادن آن در بلوک‌هایشان، در رقابتی که استخراج نام دارد و لازمه‌اش مصرف انرژی و صرف توان پردازشی[2] است، مشغول حل‌کردن معمای ریاضی بلوک می‌شوند. این معمای ریاضی از کنار هم گذاشتن تراکنش‌ها و عبور آنها از فرایندهای رمزنگاری به نام «توابع هش»، به وجود می‌آید. حل‌کردن این معماها کار دشواری است که با قدرت پردازش سخت‌افزارهای کامپیوتری انجام می‌شود. یافتن پاسخ این مسائل ریاضی در نهایت به تأییدشدن تراکنش‌های قرارگرفته در آن بلوک منجر می‌شود.

پس از یافتن پاسخ معمای ریاضی، بلوک مورد نظر در کنار سایر بلوک‌هایی که پیش

---

1. Mempool

۲. استخراج بیت‌کوین درحال‌حاضر با سخت‌افزارهایی که ای‌سیک یا اسیک (ASIC) نامیده می‌شود، انجام می‌گیرد.

از این حل شده‌اند، با یک ترتیب زمانی مشخص قرار گرفته و زنجیره‌ای به‌هم‌پیوسته از بلوک‌ها شکل می‌گیرد. این زنجیره به‌هم‌پیوسته از بلوک‌ها همان بلاکچین (زنجیره بلوکی) است. به فرایند تأیید تراکنش با انجام یک کار مشخص (که در دایره لغات شبکه بیت‌کوین همان مصرف انرژی است)، فرایند اثبات کار نیز گفته می‌شود. با وجود سازوکار استخراج در شبکه بیت‌کوین، برای حمله به این شبکه یک عامل بازدارنده قدرتمند وجود دارد. یعنی اگر کسی بخواهد به شبکه بیت‌کوین حمله کند و طبق میل خود بلاکچین را تغییر دهد، مجبور است از نیمی از تمام ماینرها قدرت پردازش بیشتری داشته باشد. فراهم‌کردن چنین قدرتی تقریباً غیرممکن است و توجیه اقتصادی ندارد. اما ماینرها برای انجام تمام این کارها که شامل تهیه سخت‌افزارهای مخصوص و مصرف برق است، به یک انگیزه نیاز دارند. چه انگیزه‌ای ماینرها را به فعالیت در شبکه وامی‌دارد؟ چه انگیزه‌ای بهتر از پول و درآمد؟

بیت‌کوین از کجا می‌آید؟

پاسخ این سؤال که بیت‌کوین‌ها توسط چه کسی ساخته می‌شوند با این سؤال که انگیزه ماینرها برای فعالیت در شبکه چیست، یکی است. اولین استخراج‌کننده‌ای که در شبکه زودتر از بقیه موفق شود پاسخ معمای ریاضی بلوک را پیدا کند، با واحدهای پولی خود شبکه، یعنی همان بیت‌کوین پاداش دریافت می‌کند. این پاداش برای ماینرها از دو منبع اساسی تأمین می‌شود:

- کارمزد یا هزینه تراکنش‌ها که کاربران مشخص می‌کنند.
- پاداش بلوک که پس از حل بلوک، به استخراج‌کننده برنده تعلق می‌گیرد.

تراکنش‌های بیت‌کوین رایگان نیستند و کاربران برای جلب توجه ماینرها جهت تأییدکردن تراکنش‌هایشان، باید مبلغ مشخصی بیت‌کوین را به‌عنوان هزینه و کارمزد آن تعیین کنند. ماینرها نیز به‌طور منطقی به انتخاب تراکنش‌هایی علاقه نشان می‌دهند که کارمزدشان نسبت به بقیه بالاتر است. یافتن پاسخ بلوک‌ها، منجر به آزاد شدن بیت‌کوین‌ها در شبکه می‌شود. زمان حدودی اضافه‌شدن هر بلوک به بلاکچین نیز حدود ۱۰ دقیقه است. برای افزایش کمیابی بیت‌کوین، پس از دوره‌های زمانی

حدود چهارساله، تعداد بیت‌کوین‌هایی که به واسطه ماینرها در شبکه آزاد می‌شوند، به نصف کاهش می‌یابد که به آن «هاوینگ» (نصف‌شدن پاداش بلوک) می‌گویند. در حال حاضر بیش از ۱۸ میلیون از ۲۱ میلیون واحد بیت‌کوین در شبکه استخراج شده و با توجه به هاوینگ، استخراج تمام واحدهای بیت‌کوین تا سال ۲۱۴۰ به طول می‌انجامد.

نحوه کار بیت‌کوین از نظر فنی

با یک نگاه بنیادی، بیت‌کوین یک برنامه کامپیوتری است. بخش بزرگی از این برنامه یک فایل دیجیتال است و دفتر کل نام دارد که شبیه به دفتر حساب‌وکتاب سنتی عمل کرده و حساب‌ها و موجودی هر نفر را در خود ثبت می‌کند.

LEDGER
(دفتر کل)

مالک حساب	ارزش
مریم	٤
محمد	٥٦
محسن	٨٣
سارا	١٦
رضا	١٨٧
بهروز	٢٣
...	...

شکل ۴-۲: تصویر فرضی از یک دفتر کل

یکی از اساسی‌ترین مواردی که بیت‌کوین را از سیستم‌های متمرکز متمایز می‌کند، نحوه نگهداری و به‌روزرسانی دفتر کل است. همان‌طور که بالاتر هم اشاره شد، در بیت‌کوین به جای یک نهاد مرکزی، دفتر کل به‌صورت گروهی و اشتراکی، توسط اعضای شبکه نگهداری می‌شود. این یعنی هر کسی می‌تواند از دفتر کل نگهداری کرده و آن

را به‌روز کند. به هر کامپیوتری که به‌طور مستقیم به شبکه متصل شود و دفتر کل را دریافت کند، نود گفته می‌شود.

تمام چیزی که در بیت‌کوین با آن سروکار داریم را می‌توان در این یکی، دو جمله خلاصه کرد: سیستمی که به همه (کامپیوترها یا همان نودها یا گره‌ها) اجازه می‌دهد در نگهداری سابقه تراکنش‌ها سهیم باشند، به اضافه ویژگی‌های امنیتی برای جلوگیری از تقلب و حمله به شبکه.

زمانی که بیت‌کوین ارسال می‌کنید، چه اتفاقی رخ می‌دهد؟

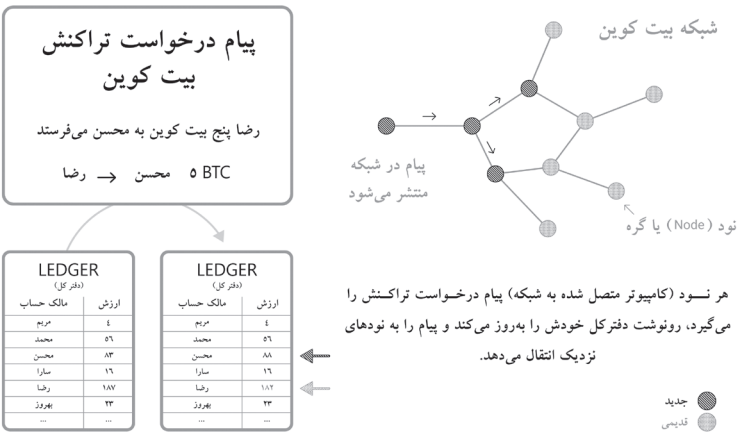
گفتیم که همه افراد می‌توانند در حفظ و نگهداری دفتر کل بیت‌کوین سهیم باشند. به عبارت ساده‌تر، هنگام ارسال بیت‌کوین، به شبکه اعلام می‌کنید که مقداری از حساب شما کسر شود و به حساب گیرنده واریز شود.

در واقع هنگام ارسال بیت‌کوین مالکیت مقداری از سکه‌هایی که در اختیار شماست را به فرد دیگری واگذار می‌کنید و فرایند تغییر مالکیت نیز با تکنیک‌های رمزنگاری صورت می‌گیرد. نودها یا همان کامپیوترهای موجود در شبکه بیت‌کوین، بعد از دریافت پیامِ تغییر مالکیت سکه‌هایی که قصد ارسال آن‌ها را دارید، پس از صحت‌سنجی و بررسی مالکیت آن‌ها با امضای دیجیتال، محتوی پیام را به سایر نودها ارسال می‌کنند. به‌این ترتیب تمامی حاضرین در شبکه پس از بررسی تراکنش شما و تأییدشدن آن توسط ماینرها، آن را به زنجیره بلوکی خود اضافه و دفترکل خود را به‌روز می‌کنند.

بانک‌ها هم یک دفتر کل دیجیتال دارند که تراکنش‌ها و دارایی مشتریان در آن ثبت شده است. فرض کنیم محسن ۱۰ میلیون تومان پول دارد و سارا ۵ میلیون تومان. این اطلاعات روی دفتر کل بانک‌ها ثبت می‌شود و وقتی سارا ۵ میلیون تومان برای محسن می‌فرستد، در دفتر کل موجود در بانک این مبلغ از حساب سارا کسر می‌شود و به موجودی حساب محسن افزوده می‌شود.

در هنگام انجام تراکنش بانکی، پول فیزیکی منتقل نمی‌شود؛ بلکه فقط مالکیت پول تغییر می‌کند. در بیت‌کوین، اگر رضا بخواهد برای محسن پنج بیت‌کوین ارسال

کند، باید درخواستش را به شبکه اعلام کند که «پنج بیت‌کوین از موجودی من کم کن و به محسن اضافه کن.» هر نود در شبکه، پیام را دریافت کرده و کپی دفتر حساب‌وکتاب خود را طبق این درخواست به‌روز می‌کند و تمام این فرایند به‌صورت دیجیتالی انجام می‌شود.



شکل ۵-۲: پیام درخواست تراکنش در شبکه بیت‌کوین

امضای دیجیتال و کلیدهای عمومی و خصوصی

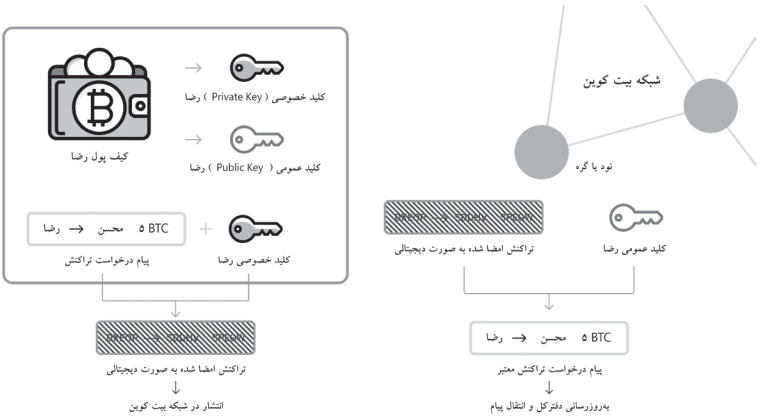
همان‌طور که اشاره شد، درخواست تراکنش از سوی یک کاربر به شبکه ارسال می‌شود و کامپیوترهای فعال در شبکه آن را اعمال می‌کنند. اما آنها چگونه مطمئن می‌شوند که این درخواست معتبر است؟ اگر کسی که این پیام را فرستاده است، واقعاً بیت‌کوین نداشته باشد، چه؟

وقتی یک چک را برای نقد کردن به بانک می‌برید، اولین چیزی که کارمند بانک برای انجام درخواست شما بررسی می‌کند، چیست؟ درست حدس زدید: امضای فرد دارنده دسته‌چک. در شبکه بیت‌کوین هم هر پیام تراکنش باید امضای معتبر داشته باشد تا قبول شود، اما نه امضای دست‌نویس؛ امضایی از جنس دیجیتال، چیزی که نتوان

آن را جعـل کـرد. در درون هر کیف پـول بیت‌کوین، دو رشـته متنی وجـود دارد که مجزا هستند، اما با هم ارتباط مکمل دارند؛ کلید عمومی و کلید خصوصی. هر کس برای ارسال بیت‌کوین باید پیام تراکنش را با کلید خصوصی کیف پولش امضا و به شبکه ارسال کند. به این شکل، بدون اینکه نیازی به استفاده از نام و مشخصات هویتی در شبکه بیت‌کوین باشد، مشخص می‌شود که بیت‌کوین‌ها دقیقاً از طریق کیف پول دارنده بیت‌کوین ارسال شده‌اند و فرد دیگری به دروغ این پیام را به شبکه نفرستاده است.

داشتن کلید خصوصی به منزله داشتن دارایی‌هاست و برای همین گفته می‌شود که هرگز نباید کلید خصوصی کیف پول خود را در اختیار فرد دیگری قرار بدهید. هر نود، امضای تراکنش فرد را بررسی می‌کند تا از درسـتی آن مطمئن شود، اما چگونه شبکه می‌تواند بدون داشـتن کلیـد خصوصی، از اعتبـار امضای دیجیتـال اطمینان حاصل کند؟ اینجاست که کلید عمومی به کار می‌آید. با استفاده از کلید عمومی که افشای آن هیچ مشکلی ندارد، نودها می‌توانند بدون مشاهده کلید خصوصی، از اعتبار امضای تراکنش اطمینان حاصل کنند.

امضـای دیجیتـال بـرای هـر تراکنـش منحصربه‌فـرد اسـت و بـا هرگونـه تغییـر در درخواست تراکنش، امضا به‌طور کامل تغییر می‌کند. به این ترتیب، نمی‌توان پیام‌های درخواست تراکنش را تغییر داد.



شکل ۶-۲: امضای دیجیتال در تراکنش بیت‌کوین

اما به عبارت دقیق‌تر سیستم بیت کوین میزان موجودی حساب‌ها را ذخیره نمی‌کند و اصلاً در بطن این شبکه چیزی به نام «حساب» تعریف نشده است. در بیت‌کوین تنها چیزی که ثبت می‌شود، تاریخچه تراکنش‌هاست. به عبارت دیگر، دفتر کل بیت‌کوین فقط سوابق تراکنش‌ها را ذخیره می‌کند؛ بنابراین به جای ذخیره موجودی حساب‌ها، مالکیت در بیت‌کوین بر اساس تراکنش‌های قبلی تعیین می‌شود.

LEDGER

(دفتر کل)

ارزش	تراکنش ها
۱۰.۰۰۰	محمد → مریم
۰.۳۴۵	سارا → محمد
۱۸.۴۳۳۲	رضا → محسن
۷.۱۵۶	محسن → سارا
۱۲.۳۴۰۲	مریم → رضا
۳.۰۲۹۳۸۱	سارا → بهروز
...	...

شکل ۷-۲: شکلی ساده‌شده از دفتر کل بیت‌کوین

تا به اینجا می‌دانیم که با الزام امضای دیجیتال در تراکنش‌های بیت‌کوین، کسی نمی‌تواند پیام غیرمعتبر خود را در شبکه اعمال کند، اما فرض کنیم که مالک یک کلید خصوصی هستید و با امضای معتبر تراکنش را ارسال می‌کنید، شبکه چگونه متوجه می‌شود که موجودی کافی دارید؟ اگر به‌عنوان مثال ۰/۱ بیت‌کوین موجودی داشته باشید، اما بخواهید ۱ بیت‌کوین برای کسی ارسال کنید، شبکه چگونه متوجه این ایراد می‌شود؟

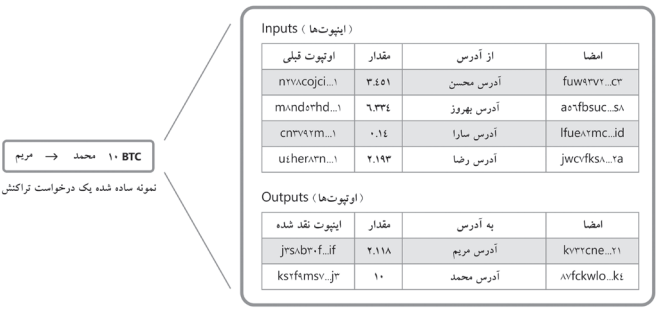
تراکنش‌های بیت‌کوین بر مبنای سیستمی تحت عنوان خروجی تراکنش خرج‌نشده یا «UTXO» کار می‌کنند. یک «خروجی تراکنش خرج‌نشده»، مانند پولی می‌ماند

که متعلق به کاربر است و کاربر می‌تواند در یک تراکنش دیگر آن را خرج کند. در واقع، سیستم بیت‌کوین از این نظر بر خلاف بانک‌ها کار می‌کند. در بانک‌ها برای اینکه مشخص شود هر کس چه مقدار موجودی دارد، یک فهرست از موجودی کاربران در اختیار بانک قرار دارد که در زمان تراکنش از موجودی یک نفر کم می‌کند و به موجودی فرد دیگری اضافه می‌کند، اما در بیت‌کوین این‌گونه نیست و هیچ فهرستی در کار نیست که موجودی کاربران را ثبت کند، اما به جای آن، از مدل UTXO استفاده می‌شود. در مدل‌های UTXO، شبکه بر اساس تمام تراکنش‌هایی که شما در کیف پول خود دریافت یا ارسال کرده‌اید، متوجه می‌شود که آیا دارایی کافی برای انجام تراکنش دارید یا خیر.

برای اینکه این مفهوم را بهتر درک کنید، فرض کنید ۷۵ هزار تومان پول در کیف پول‌تان دارید. از آنجایی که اسکناس ۷۵ هزار تومانی نداریم، پس در کیف پول شما ترکیبی از اسکناس‌های مختلف وجود دارد که جمع آن در کل ۷۵ هزار تومان می‌شود. هر اسکناس را به‌عنوان یک خروجی تراکنش خرج‌نشده (UTXO) در نظر بگیرید. هر اسکناس دارای مقدار ارزشی است که می‌توانید در تبادلات بعدی خود از آن استفاده کنید. حالا مثال بالا را یک قدم جلوتر ببریم. فرض کنید می‌خواهید با ۲۸ هزار تومان از ۷۵ هزار تومان خود ناهار بخرید. برای خرید ناهار باید به رستوران چند اسکناس (خروجی تراکنش خرج‌نشده) بدهید تا مبلغ ناهار را پرداخت کنید. فرض کنیم ۷۵ هزار تومان شما شامل هفت اسکناس ۱۰ هزار تومانی و یک اسکناس ۵ هزار تومانی می‌شود. پس به‌طور کلی شما هشت خروجی تراکنش خرج‌نشده دارید. حالا برای خرید یک ناهار ۲۸ هزار تومانی به فرض سه خروجی تراکنش خرج‌نشده (سه اسکناس ۱۰ هزار تومانی) پرداخت می‌کنید و رستوران به شما دو هزار تومان برمی‌گرداند. آن سه اسکناس ۱۰ هزار تومانی را که پرداخت کردید، به‌عنوان همان خروجی تراکنش خرج‌نشده در نظر بگیرید، آن دو هزار تومان بقیه را هم یک خروجی تراکنش خرج‌نشده در نظر بگیرید که به شما برمی‌گردد.

یک مثال دیگر؛ اگر فردی قصد ارسال ۱۰ بیت‌کوین را داشته باشد، درخواست تراکنش او دارای پیوندهایی به تراکنش‌های ورودی قبلی است که جمع میزان آنها باید

حداقل ۱۰ بیت‌کوین باشد تا تراکنش انجام شود. به این پیوندها اصطلاحاً «اینپوت» یا ورودی می‌گویند. به بیان ساده، وقتی قصد ارسال بیت‌کوین دارید، به شبکه بیت‌کوین تراکنش‌های قبلی خود را نشـان می‌دهید و می‌گویید اینها مدارکی هسـتند که نشان می‌دهند این میزان بیت‌کوین را دارید؛ بنابراین داشـتن بیت‌کوین بدان معناسـت که در شبکه بیت‌کوین تراکنش‌هایی دارید که خرج نشده است.



شکل ۸-۲: شکل یک درخواست تراکنش در شبکه بیت‌کوین

بی‌نهایت آدرس

هرکس می‌تواند بدون نیاز به واردکردن نام یا مشـخصات خود، به شبکه بیت‌کوین متصل شود. شبکه بیت‌کوین اجازه ساخت هر تعداد کیف پولی را به کاربران می‌دهد و هر کیف پول کلید خصوصی خاص خودش را دارد. شاید فکر کنید که تولید یک کلید عمومی برای سـاخت آدرس کیف پول، به معنای مشخص‌شدن هویت شخصی شما باشد، اما این قدم هم ناشناس است و حتی می‌تواند بدون نیاز به اینترنت انجام شود. به‌سادگی و با یک کلیک می‌توانید کلیدهای جدید بسازید.

اما یک مسـئله؛ در هنگام سـاخت کیف پـول امکان بررسـی تکراری‌بـودن یا نبودن آدرس یا کلید وجود ندارد. بـرای درک بهتر این جمله، فرایند سـاخت ایمیل را در نظر بگیرید. هنگامی که قصد دارید ایمیل ایجاد کنید، سرویس ایمیل‌دهی (مثل جی‌میل) از شما می‌خواهد یک آدرس ایمیل برای خود مشخص کنید. آدرس دلخواه خود را وارد می‌کنید، اما سیسـتم به شما می‌گوید که این آدرس قبلاً ثبت شـده و نمی‌توانید آن را

برای خود برگزینید. در بیت‌کوین این‌گونه نیست و اگر بتوانید کلید خصوصی یک نفر را حدس بزنید، به دارایی‌های او دسترسی خواهید داشت، اما حدس کلید خصوصی تقریباً محال است. چرا؟

حداکثر تعداد آدرس‌های احتمالی بیت‌کوین $۲^{۱۶۰}$ است، یعنی:

۱۴۶۱۵۰۱۶۳۷۳۳۰۹۰۲۹۱۸۲۰۳۶۸۴۸۳۲۷۱۶۲۸۳۰۱۹۶۵۵۹۳۲۵۴۲۹۷۶ احتمال برای آدرس‌های بیت‌کوین وجود دارد. برای اینکه بزرگی این عدد را خوب درک کنید، به این مثال توجه کنید؛ تخمین زده می‌شود تعداد دانه‌های شن و ماسه در دنیا تقریباً ۷٫۵ میلیون تریلیون باشد. حالا فرض کنید هر دانه شن یک کره زمین باشد و با احتساب شن‌های این کره‌های زمین، باز هم رقمی که به دست می‌آید، خیلی پایین‌تر از احتمال آدرس‌های بیت‌کوین است. این موضوع باعث می‌شود تا هک یا حملات سایبری با استفاده از حدس‌زدن کلیدها غیرممکن باشد.

بلوک و بلاکچین

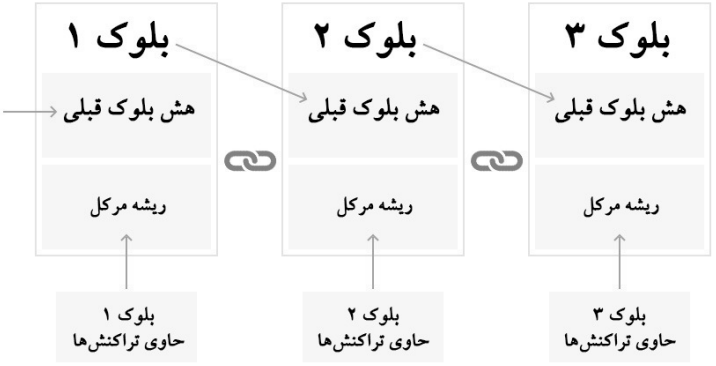
تا اینجا به لطف امضای دیجیتال و مفهوم ورودی و خروجی در تراکنش‌ها، مطمئن هستیم کسی نمی‌تواند تراکنش غیرمعتبر ارسال کند یا بیشتر از موجودی خود انتقال دهد، اما باز هم امنیت به شکل کامل در شبکه بیت‌کوین برقرار نشده است. همان‌طور که پیش‌تر گفته شد، تراکنش‌ها پس از ارسال به شبکه، از نودی به نود دیگر منتقل می‌شوند؛ بنابراین ترتیب رسیدن دو تراکنش مختلف به یک نود می‌تواند متفاوت باشد.

به‌عنوان مثال، یک کاربر خرابکار می‌تواند به بهانه خرید کالا از یک فروشنده به او بیت‌کوین بفرستد و بعد از اینکه آن فرد کالا را تحویل داد، تراکنشی مخالف تراکنش قبلی بفرستد و در این صورت، به‌دلیل عدم وجود ترتیب زمانی، نودها ممکن است تراکنش دوم را زودتر دریافت کنند و عملاً بیت‌کوین‌ها دو بار خرج شوند.

پس چگونه می‌توان فهمید که چه تراکنشی زودتر ارسال شده است؟ برای حل این مشکل، در شبکه بیت‌کوین سیستم بلاکچینی در نظر گرفته شده است. شبکه بیت‌کوین تراکنش‌ها را با گذاشتن آنها در بسته‌هایی به نام «بلوک» مرتب می‌کند.

حداکثر حجم بلوک بیت‌کوین حدود یک مگابایت است و در هر بلوک بیت‌کوین، به‌طور میانگین حدود ۲٫۵ هزار تراکنش جای می‌گیرد. بلوک‌های بیت‌کوین به‌طور میانگین هر ۱۰ دقیقه یک بار طی فرایند ماینینگ ایجاد می‌شوند که در ادامه درباره آن می‌خوانید. هر بلوک یک هش (بخوانید شناسه منحصربه‌فرد) و هش بلوک قبلی را در خود دارد.

در واقع بلوک‌ها به‌ترتیب به یکدیگر متصل هستند و یک زنجیره را شکل داده‌اند. اگر چیزی داخل یک بلوک تغییر کند، هش بلوک هم تغییر می‌کند و به این ترتیب با توجه به مرتبط‌بودن هش‌ها، بلوک‌های دیگر غیرمعتبر می‌شوند. از این رو گفته می‌شود بلاکچین تغییرناپذیر است.



شکل ۹-۲: ساختار فرضی بلوک‌ها در بلاکچین

تمام تراکنش‌هایی که در یک بلوک خاص قرار دارند، به‌عنوان تراکنش‌های ارسال‌شده در یک زمان در نظر گرفته می‌شوند و تراکنش‌هایی که هنوز در بلوک وارد نشده باشند، به‌عنوان تأییدنشده[1] تلقی می‌شوند. زمانی که تراکنش در بلوک ثبت شود و آن بلوک به شبکه ارسال شود، تراکنش یک تأیید یا کانفرم می‌خورد، همچنین

1. Unconfirmed

زمانی که بلوک‌های جدیدی روی بلوک تراکنش قبلی ثبت شوند، تعداد تأیید هم به همان میزان بالا می‌رود.

ماینینگ بیت‌کوین

ماینینگ اصلی‌ترین چیزی است که امنیت شبکه بیت‌کوین را تأمین می‌کند. هر نود می‌تواند تراکنش‌ها را در یک بلوک قرار دهد و آنها را به دیگر نودها مخابره کند، اما برای جلوگیری از ایجاد بلوک‌های متعدد، دست‌کاری بلاکچین و حمله به بیت‌کوین، برای ساخت بلوک، یک شرط وجود دارد و آن این است که نود باید ماینر یا استخراج‌کننده باشد.

برای اینکه بلوک‌ها به بلاکچین اضافه شوند، هر بلاک باید دارای جواب یک مسئله ریاضی پیچیده باشد. با بهره‌مندی از فناوری «تابع هش رمزنگاری»، تنها راه حل‌کردن مسئله ریاضی، حدس‌زدن اعداد است. به عمل پیداکردن پاسخ معادله بلوک‌ها، «استخراج» یا همان ماینینگ می‌گویند. حدس‌زدن مداوم اعداد هم فقط با سخت‌افزارهای کامپیوتری که قدرت پردازش دارند، قابل انجام است و این فرایند برق مصرف می‌کند.

نام علمی ماینینگ، «اثبات کار» است. در واقع استخراج‌کنندگان با قدرت پردازش سخت‌افزارهای خود اثبات می‌کنند که به پروتکل بیت‌کوین پایبند هستند. اگر کسی بخواهد به شبکه بیت‌کوین حمله کند، مجبور است بیش از ۵۰ درصد از قدرت پردازش بیت‌کوین را از آن خود کند. با توجه به گستردگی شبکه بیت‌کوین، این کار بسیار هزینه‌بر است و از نظر منطقی توجیه ندارد.

برای ایجاد انگیزه در ماینرها جهت افزایش امنیت شبکه و همچنین تولید واحدهای بیت‌کوین جدید به‌صورت غیرمتمرکز، در ازای پیدا کردن جواب معادله بلوک‌ها پاداش اهدا خواهد شد. پاداش بلوک بیت‌کوین ابتدا ۵۰ واحد بیت‌کوین بود، اما این پاداش پس از هر ۲۰۰ هزار بلوک (تقریباً هر چهار سال یک بار) نصف می‌شود. در حال حاضر، پاداش بلوک بیت‌کوین ۶٫۲۵ واحد است.

همچنین، تراکنش‌های بیت‌کوین دارای کارمزد هستند. ماینرها اغلب تراکنش‌هایی را در داخل بلوک قرار می‌دهند که کارمزد بهتری دارند و بنابراین تراکنش‌هایی که کارمزد بالاتر دارند، زودتر تأیید خواهند شد. کاربر خودش حق دارد که کارمزد تراکنش‌اش را مشخص کند، اما

اگر برای تراکنش خود کارمزد مناسب مشخص نکند، تأیید تراکنش می‌تواند تا چند روز طول بکشد یا اصلاً تأیید نشود. علاوه بر پاداش بلوک، میزان کل کارمزد تراکنش‌های یک بلوک هم به ماینر تعلق می‌گیرد.

سختی استخراج

به‌دلیل اینکه میانگین زمان ایجاد شدن بلوک بیت‌کوین ۱۰ دقیقه است، تقریباً هر ۱۰ دقیقه بیت‌کوین‌های جدید تولید می‌شوند و به یک ماینر تعلق می‌گیرند. حالا ممکن است که یک ماینر بسیار قدرتمند بتواند جواب معادله را مثلاً در پنج دقیقه پیدا کند که این امر باعث اختلال در کار شبکه و استخراج سریع تمام واحدهای بیت‌کوین خواهد شد.

به همین منظور، چیزی به نام سختی شبکه در بیت‌کوین تعبیه شده است. شبکه به‌طور خودکار نسبت به قدرت پردازش موجود، سختی پیداکردن پاسخ معادلات را کم و زیاد می‌کند تا ماینرها بتوانند به‌طور میانگین در ۱۰ دقیقه به جواب برسند، نه بیشتر و نه کمتر. با اضافه‌شدن قدرت پردازش ماینرها، سختی افزایش می‌یابد و با کم‌شدن آن، سختی هم کمتر می‌شود. در شبکه بیت‌کوین، سختی شبکه بعد از هر ۲,۰۱۶ بلوک (تقریباً هر دو هفته یک بار) تنظیم می‌شود.

استخر استخراج

به‌دلیل بالا رفتن سختی شبکه بیت‌کوین و سخت‌بودن انجام عمل ماینینگ به‌صورت فردی، ماینرها به‌صورت گروهی در محل‌های مجازی که «استخر استخراج» نام دارند، جمع می‌شوند تا برای استخراج از قدرت پردازش جمعی استفاده کنند.

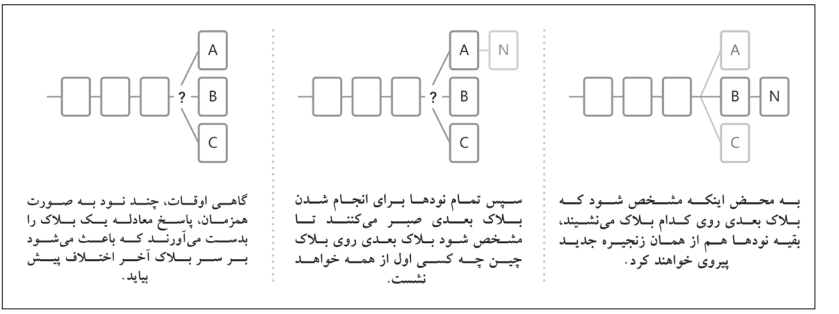
به عبارت دیگر، ماینرهای سراسر دنیا دستگاه‌های استخراج خود را به استخرهای استخراج معتبر متصل می‌کنند و استخر استخراج به نمایندگی از همه و با مجموع قدرت پردازشی که دارد، برای ماینینگ و به دست آوردن پاداش بلوک تلاش می‌کند. در این روش، هر استخراج‌کننده معمولاً بر اساس توان پردازشی خود سود می‌برد، اما پاداش اصلی بلوک به استخر استخراج تعلق می‌گیرد. البته در صورتی که یک ماینر عادی بخواهد به‌تنهایی و به شکل مستقیم برای استخراج بیت‌کوین اقدام کند،

شانس او نزدیک به صفر خواهد بود.

استخراج دو بلوک همزمان

اگر به فرض محال دو نود (ماینر) همزمان معادله را حل کنند و همزمان بلوک‌های خود را به شبکه بفرستند، چه؟

در این مورد، هر دو بلوک به شبکه اعلام می‌شوند و هر نود، بلوکی را که اول دریافت کرده است، در بلاکچین خود قرار می‌دهد، اما طبق قوانین بیت‌کوین، هر نود باید بلندترین زنجیره موجود از بلاکچین را دنبال کند؛ بنابراین اگر بر سر آخرین بلوک توافق حاصل نشود، به محض اینکه معادله آخرین بلوک حل شد، همه نودها بلندترین زنجیره را خواهند پذیرفت.



شکل ۱۰-۲: پذیرش زنجیره طولانی‌تر توسط نودهای شبکه بیت‌کوین

عدم توافق بر سر آخرین بلوک در زنجیره می‌تواند باعث تقلب و دو بار خرج‌کردن شود. اگر یک تراکنش در بلوک زنجیره کوتاه‌تر باشد، زمانی که بلوک بعدی استخراج شود، این تراکنش و تمام تراکنش‌های آن بلوک دوباره به‌صورت تأییدنشده درمی‌آیند.

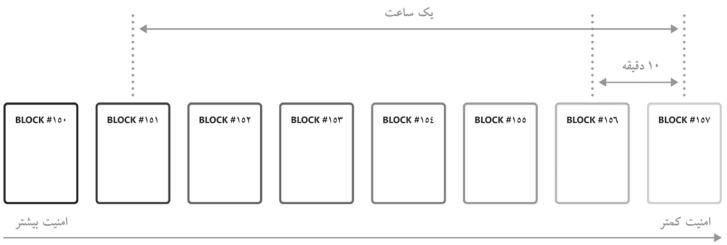
فرض کنید که فرد خرابکاری می‌خواهد از فرد دیگری با بیت‌کوین، یک فایل بخرد. خرابکار بیت‌کوین را برای فروشنده می‌فرستد و فروشنده پس از دیدن اولین تأیید، فایل را به خرابکار می‌دهد. حالا اگر خرابکار بتواند در شبکه بیت‌کوین زنجیره‌ای

طولانی‌تر بسازد که یک تراکنش با مبلغ یکسان به کیف پول خودش داخل آن باشد، می‌تواند پول خود را برگشت بزند و در عمل بیت‌کوین را دو بار خرج کند.

اما این کار تـا چه میزانی عملی اسـت؟ در صورتی که یک ماینر خرابـکار بیش از ۵۰ درصد قدرت پردازش شبکه را داشته باشد و به عبارتی «حمله ۵۱ درصدی» به شبکه انجام دهـد. او برای انجـام این کار باید بـا کامپیوترهای زیـادی که در حـال رقابت برای یافتن جواب معادله بلوک هستند، رقابت کند.

حتـی اگر بـه فـرض محـال او بتواند یـک بلـوک را پیـش از بقیه حـل کنـد، احتمال حل‌شدن بلوک‌های دوم، سوم، چهارم و... به‌شدت پایین است و هرچه جلوتر می‌رویم، پایین‌تر نیز می‌آید. اگر یک خرابکار بیش از ۵۰ درصد قدرت شبکه را در اختیار داشته باشد، شانس او برای حل‌کردن بلوک بیش از ۵۰ درصد خواهد بود، اما برای حل‌کردن دو بلوک متوالی او فقط ۲۵ درصد شانس خواهد داشت و هرچه تعداد بلوک‌ها بیشتر می‌شوند، شانس خرابکار نیز کمتر و کمتر خواهد شد تا به نزدیک صفر برسد.

به همین دلیل است که فروشندگان و صرافی‌ها برای تأیید تراکنش و ارائه خدمات، حداقل دو الی شش تأیید را ضروری می‌دانند. شش تأیید امن‌ترین حالت ممکن برای تراکنش است و بعد از آن، تراکنش دیگر مشکلی نخواهد داشت.



شکل ۱۱-۲: امنیت تراکنش‌ها در شبکه بیت‌کوین نسبت به تعداد تأیید

قیمت بیت‌کوین

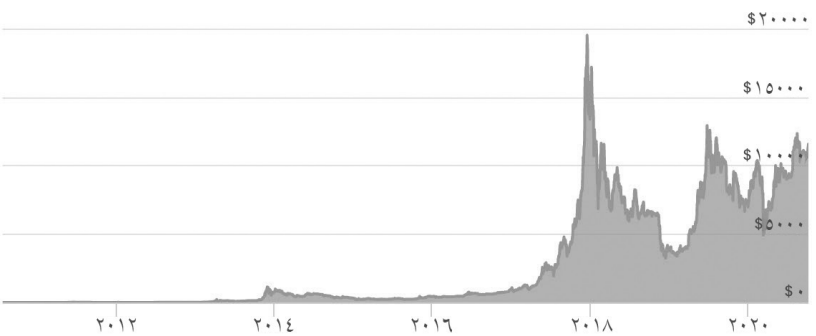
طبق نتایج چندین نظرسـنجی معتبر، در سـال ۲۰۱۷ اغلب افراد تـازه‌وارد به دنیای بیت‌کوین، به‌دلیل رشـد شـدید قیمت ایـن ارز دیجیتال جذب آن شـده بودند و حتی

شاید شما هم در ابتدا به‌دلیل افزایش چندهزار درصدی قیمت بیت‌کوین علاقه‌مند به یادگیری درباره آن شده باشید. پتانسیل بیت‌کوین برای تغییر نظام مالی دنیا و همچنین کمیابی بی‌نظیر آن باعث شده است تا این دارایی روزبه‌روز باارزش‌تر شود. البته این ارز دیجیتال به‌دلیل نوپا بودن و عدم قانون‌گذاری صحیح، بسیار پرنوسان است و ده‌ها بار شاهد نوسان بیش از ۲۰ درصد در یک روز هم بوده است؛ نوساناتی که در بازارهای سنتی خیلی کمتر رخ می‌دهد. در این بخش به‌صورت خلاصه تاریخچه جالب قیمت بیت‌کوین را بررسی می‌کنیم.

بیت‌کوین راه خود را با ارزش صفر دلار در سال ۲۰۰۹ آغاز کرد و در سال ۲۰۱۰ با قیمت هر واحد حدود ۰٫۰۰۳ دلار وارد اولین صرافی به نام «بیت‌کوین مارکت» شد و همین‌طور به رشد خود ادامه داد تا اینکه در سال ۲۰۱۷ به اوج قیمتش یعنی ۲۰ هزار دلار رسید. در زمان نگارش این کتاب، هر واحد بیت‌کوین حدود ۳۰ هزار دلار قیمت دارد و شاید زمانی که این کتاب را می‌خوانید قیمتی بالاتر یا پایین‌تر داشته باشد. با توجه به قیمت اولیه بیت‌کوین یعنی ۰٫۰۰۳ دلار و با فرض قیمت ۳۰ هزار دلار، قیمت این دارایی از سال ۲۰۱۰ تاکنون بیش از ۹ میلیون درصد رشد کرده است. اگر در سال‌های ابتدایی بیت‌کوین فقط چند صد دلار روی بیت‌کوین سرمایه‌گذاری می‌کردید، امروز میلیون‌ها دلار ثروت داشتید.

اما روند قیمت بیت‌کوین همیشه صعودی نبوده است. در تاریخچه کوتاه قیمت بیت‌کوین، بارها شاهد سقوط‌های ۹۰درصدی هم بوده‌ایم. به عبارت دیگر، همان‌طور که بیت‌کوین بسیاری را به ثروت رسانده، خیلی‌ها را هم به ورشکستگی سختی دچار کرده است. به‌عنوان یک نمونه جدید، در پایان سال ۲۰۱۷، با گذشت حدود ۱۰ سال از معرفی بیت‌کوین، ارزش بازار این ارز دیجیتال به ۳۲۰ میلیارد دلار رسیده بود، اما در سال ۲۰۱۸، درست زمانی که اغلب مردم کم‌کم با بیت‌کوین آشنا می‌شدند، به یکباره سقوطی شدید همه را به شوک فرو برد. با سقوط حدود ۹۰درصدی بیت‌کوین، ارزش بازار این ارز در کمتر از چند ماه به ۷۰ میلیارد دلار کاهش یافت و تمام سال ۲۰۱۸، روند نزولی شدیدی در بازار حاکم بود. سرمایه‌گذارانی که در سال ۲۰۱۷ با قیمت ۲۰ هزار دلار بیت‌کوین خریده بودند، طعم ضرر حدود ۹۰درصدی را به‌خوبی چشیدند. با بررسی

نمودارهای بیت‌کوین، به چندین نمونه از این فرازها و فرودها دست می‌یابید و با توجه به اینکه تاریخ تکرار می‌شود، در این سرمایه‌گذاری باید آماده هر چیزی بود.



نمودار۱-۲: نمودار ۱۰ ساله قیمت بیت‌کوین از ۲۰۱۰ تا اواسط ۲۰۲۰

قیمت بیت‌کوین مانند هر دارایی دیگری به‌شدت تحت تأثیر عوامل بیرونی و درونی قرار دارد. از نظر بیرونی، هر چیزی که مردم را نسبت به آینده بیت‌کوین امیدوار کند، می‌تواند موجب افزایش قیمت آن شود، مثل خبر پذیرش بیت‌کوین به‌عنوان روش پرداخت توسط یک شرکت بزرگ. از طرف دیگر، اخبار منفی که نگرانی درباره آینده بیت‌کوین را افزایش دهد، می‌توانند موجب سقوط شدید قیمت آن شوند. از جمله رویدادهای منفی بیرونی که بر قیمت بیت‌کوین تأثیرگذار هستند، می‌توان به اخبار مربوط به وضع مقررات سخت‌گیرانه توسط دولت‌ها یا هک‌شدن یک صرافی بزرگ اشاره کرد.

همچنین، ارزش بیت‌کوین به‌شدت تحت تأثیر عملکرد شبکه‌اش قرار دارد. با وجود هک صرافی‌ها و کیف پول‌ها، خود شبکه بیت‌کوین تاکنون هک نشده و تا زمان نگارش این کتاب هیچ‌گونه حمله موفقی به زیرساخت‌های اصلی شبکه انجام نشده است. بیت‌کوین با مفاهیمی مثل ضدسانسور بودن، تراکنش‌های برگشت‌ناپذیر و تمرکززدایی زنده است و نقطه تمایز آن با سیستم‌های دیگر در همین‌هاست. اما اگر اتفاقی مثل برگشت یا جلوگیری از یک تراکنش رخ بدهد یا به هر نوعی تمرکززدایی آن

زیر سؤال برود، قیمت بیت‌کوین با خطر سقوط مواجه خواهد شد؛ چراکه امیدواری به آینده آن کاهش می‌یابد.

به‌طور کلی اصلی‌ترین عامل در افزایش قیمت بیت‌کوین، کمیابی آن است. تعداد تمام بیت کوین‌هایی که وجود خواهند داشت، حداکثر به ۲۱ میلیون واحد محدود است و بیشتر از این مقدار بیت‌کوین استخراج نخواهد شد. از سوی دیگر، سازوکاری در بیت‌کوین به نام هاوینگ وجود دارد که هر چهار سال یک بار پاداش استخراج آن را نصف می‌کند. اینها میزان کمیابی بیت‌کوین را افزایش می‌دهند و در نتیجه روی کاغذ (و نه حتماً) احتمال افزایش قیمت بالا می‌رود. طبق برآوردها، استخراج تمام واحدهای بیت‌کوین تا سال ۲۱۴۰ طول خواهد کشید.

به عقیده گروهی از فعالان این حوزه، بیت‌کوین هنوز نتوانسته آن‌طور که باید، به آرمان‌های خود جامه عمل بپوشاند و کاربرد به‌عنوان پول و ابزار پرداخت یکی از چالش‌های فعلی بیت‌کوین است. در سال ۲۰۱۰، یکی از طرفداران بیت‌کوین برای کاربردی‌کردن آن با ۱۰ هزار واحد بیت‌کوین دو عدد پیتزا خرید؛ بیت‌کوین‌هایی که امروزه میلیون‌ها دلار ارزش دارند. کاربردی‌شدن بیت‌کوین با افزایش قیمت آن رابطه مستقیمی دارد، اما در حال حاضر، به‌دلیل سرعت پایین تراکنش‌ها و نوسانات شدید قیمت، از بیت‌کوین بیشتر به‌عنوان یک ابزار سرمایه‌گذاری و ذخیره ارزش استفاده می‌شود تا یک روش پرداخت. همچنین، باید این حقیقت را گفت که در حال حاضر در دارک‌وب (وب تاریک) از بیت‌کوین برای خریدوفروش کالاهای غیرقانونی مثل مواد مخدر استفاده می‌شود. از سوی دیگر، اگرچه شبکه بیت‌کوین شفاف است، اما در مقایسه با سیستم‌های مالی بانکی و شرکت‌های متمرکز، رهگیری تراکنش‌های بیت‌کوین بسیار مشکل است. این اتفاق برای قیمت بیت‌کوین مثبت تلقی می‌شود، اما به‌طور غیرمستقیم می‌تواند موجب ممانعت از پذیرش توسط دولت‌ها شود.

به‌دلیل کوچک‌بودن بازار بیت‌کوین در مقایسه با سایر بازارهای سنتی، قیمت بیت‌کوین تحت تأثیر دست‌کاری هم قرار می‌گیرد. تعداد زیادی معامله‌گر و شرکت دانه‌درشت در بازار بیت‌کوین که به «نهنگ» مشهور هستند، می‌توانند با ثبت سفارش‌های سنگین خرید یا فروش و اقداماتی از این قبیل، قیمت را در جهت

منافع خود دست‌کاری کنند. با این حال هر چقدر که بازار بیت‌کوین بزرگ‌تر شود و قانون‌گذاری درست‌تری برای آن صورت بگیرد، احتمال دست‌کاری بازار کاهش می‌یابد. در حال حاضر افراد زیادی روی بیت‌کوین سرمایه‌گذاری بلندمدت انجام می‌دهند یا با استفاده از نوسانات این ارز دیجیتال، معامله روزانه انجام می‌دهند و از سرمایه‌گذاری کوتاه‌مدت سود می‌برند. در فصل‌های بعد به‌طور مفصل نحوه سرمایه‌گذاری در بیت‌کوین را توضیح داده‌ایم.

دولت‌ها، قانون و بیت‌کوین

آیا بیت‌کوین و ارزهای دیجیتال قانونی هستند؟ در بیشتر کشورها از جمله ایران، قانون‌گذاران هنوز پاسخ درستی به این سؤال نداده‌اند. به عبارت دیگر، از آنجایی که این حوزه بسیار جدید است و فرصت‌ها و تهدیدهای آن هنوز به‌خوبی شفاف نیست، اغلب دولت‌ها و دستگاه‌های قضایی سراسر جهان سیاست «صبر کن و ببین» را در پیش گرفته‌اند؛ یعنی در بیشتر کشورهای دنیا ارزهای دیجیتال نه قانونی هستند، نه غیرقانونی.

در بعضی از حوزه‌های قضایی مانند ژاپن، سوئیس، آمریکا و کانادا، ارزهای دیجیتال به رسمیت شناخته شده و فضای کار و فعالیت بسیار باز است. از طرف دیگر، در زمان نگارش این بخش از کتاب، چند کشور از جمله چین و روسیه محدودیت‌های سختی بر خریدوفروش ارزهای دیجیتال اعمال کرده‌اند. با این حال، به‌دلیل ذات غیرمتمرکز این فناوری، ممنوعیت کامل ارزهای دیجیتال خیلی منطقی به نظر نمی‌رسد و تاکنون کشورها نگهداری و خریدوفروش ارزهای دیجیتال را برای مردم جرم‌انگاری نکرده‌اند. بیشتر محدودیت‌های قانونی در این حوزه نیز برای کسب‌وکارهایی مانند صرافی‌ها و مزارع استخراج اعمال می‌شود. به‌عنوان نمونه، به‌دلیل تراکنش‌های ناشناس ارزهای دیجیتال، صرافی‌ها موظف به احراز هویت از مشتریان‌شان هستند.

به‌طور خلاصه، اگر قصد نگهداری و خرید ارزهای دیجیتال را دارید، اکنون از نظر قانونی هیچ مشکلی وجود ندارد، اما اگر به‌عنوان مثال قصد دارید صرافی ارز دیجیتال راه‌اندازی کنید، موضوع متفاوت است.

همان‌طور کـه گفتیم، در ایران، ارزهای دیجیتال هنوز رسـمی و قانونی نیسـتند، اما استفاده، خرید و نگهداری این دارایی‌ها به خودی خود برای افراد عادی جرم نیست و تا اواسط سـال ۱۳۹۹ هیچ قانون مدونی برای این حوزه وضع نشده است. طبق ماده ۲ قانون مجازات عمومی؛ «هر فعل یا ترک فعل که مطابق قانون قابل مجازات یا مستلزم اقدامـات تأمینی یا تربیتی باشـد، جرم محسـوب اسـت و هیچ امـری را نمی‌توان جرم دانست؛ مگر آنکه به موجب قانون برای آن مجازات یا اقدامات تأمینی یا تربیتی تعیین شـده باشـد.» بنابراین در حال حاضر به‌دلیل عدم وجود مجازات بـرای خریدوفروش ارزهای دیجیتال یا نگهداری بیت‌کوین، نمی‌توان این اعمال را جرم دانست.

جرم‌نبودن اسـتفاده از بیت‌کوین و نگهداری آن تنها در صورتی است که بیت‌کوین ابزار جرم دیگری نباشـد یا قانون بالادسـتی را نقض نکنـد. به‌عنوان مثـال، از آنجایی که پول‌شـویی جرم اسـت، اگر با بیت‌کوین پول‌شـویی یا هر فعالیـت مجرمانه دیگری انجام شـود، مشـمول مجازات خواهد بـود. نهادهایی ماننـد نیروی انتظامـی در قبال کلاهبرداری‌های حوزه فناوری مسئولیت و اختیار دارند؛ بنابراین جدای بحث چیستی ارزهای دیجیتال، به‌عنوان یک فناوری، قانون می‌توانـد پیگیری‌های لازم را تا جایی که ممکن باشـد انجام دهـد. در صـورت رخ‌دادن هرگونه کلاهبـرداری، هک یـا عدم وفای به عهد در فضـای ارزهای دیجیتال، یک فرد می‌تواند شـکایت رسـمی ارائه دهد و قوه قضائیه به آن رسیدگی خواهد کرد.

در مورد شـرایط برای کسـب‌وکارهای ارز دیجیتال در ایران، باید گفـت که هم‌اکنون صرافی‌های ارز دیجیتال، درگاه‌های پرداخت مربوط به ارزهای دیجیتال و... در کشـور فعالیت دارند، اما هیچگونه مجوز رسمی برای تأسیس صرافی یا سایت خریدوفروش ارزهای دیجیتال از سوی بانک مرکزی صادر نمی‌شود و تمامی سایت‌ها و مراکز فعلی به‌صورت غیررسمی فعالیت می‌کنند. در بهمن ۱۳۹۷، بانک مرکزی پیش‌نویس قوانین ارزهای دیجیتال را منتشـر کرد. قـرار بود ایـن پیش‌نویس پس از چند مـاه به تصویب نهایی برسد، اما هنوز (حداقل در زمان نگارش این کتاب) چنین اتفاقی رخ نداده است. در این پیش‌نویس، صرافی‌ها می‌توانند با دریافت مجوز فعالیت کنند، اما استفاده از بیت‌کوین به‌عنـوان ابزار پرداخت ممنوع اسـت. به‌طور کلی خریدوفـروش و نگهداری

بیت‌کوین بـرای مردم جـرم نیسـت، اما در مقیـاس وسـیع و حـوزه پرداخت‌های کلان کشور، فعلاً مجوز خاصی صادر نشده است.

ماینینگ، اسـتخراج بیت‌کوین یا هر ارز دیجیتال دیگری در ایران قانونی اسـت، اما برای انجام اسـتخراج بیت‌کوین باید از وزارت صنعت، معدن و تجـارت مجوز دریافت شـود؛ چراکه اسـتخراج ارزهای دیجیتال بدون مجوز از وزارت صمـت، غیرمجاز اعلام شـده اسـت. همچنین باید از وزارت نیرو، برق مخصوص ماینینگ بـا تعرفه صادراتی دریافت کرد.

فراموش نکنید که احتمال تغییر سریع مقررات در این حوزه بسیار بالا است و قبل از هر اقدامی لازم است که اطلاعات خود را نسبت به مقررات فعلی به‌روز کنید.

فصل سوم

ارزهای دیجیتال پس از بیت‌کوین

بیت‌کوین توانست برای اولین‌بار پول و نقل‌وانتقال آن را غیرمتمرکز کند، اما به‌دلیل پتانسیل‌های بلاکچین در کاربردهای بسیار بیشتر و همچنین نقص‌هایی که برخی برنامه‌نویسان به بیت‌کوین نسبت دادند، امروزه بیش از ۳۵۰۰ ارز دیجیتال با اسم‌ها و نمادهای مختلف در بازار ارزهای دیجیتال خرید‌وفروش می‌شود. به‌طور کلی می‌توان گفت که ارزهای دیجیتال پس از بیت‌کوین به دو دلیل عمده ساخته شدند؛ حل مشکلات بیت‌کوین یا ارائه کاربردی فراتر از پول. از همان روزهای اول معرفی بیت‌کوین، تعداد زیادی از توسعه‌دهندگان و علاقه‌مندان به عدم تمرکز، معتقد بودند که بیت‌کوین به‌دلیل محدودیت‌هایی مثل سرعت پایین تراکنش‌ها نمی‌تواند به‌عنوان روش پرداخت برای نیازهای روزمره مورد استفاده قرار بگیرد. البته این ظاهر موضوع است. تعداد زیادی از توسعه‌دهندگانی که ادعای حل‌کردن مشکلات بیت‌کوین را داشتند، در حقیقت فضای نوپای ارزهای دیجیتال را فرصت مناسبی برای شهرت و کسب درآمد دیدند. بدیهی است که مانند هر صنعت آزاد دیگری، بیت‌کوین نمی‌توانست بدون رقیب بماند. همچنین از آنجایی که کد بیت‌کوین کاملاً متن‌باز و شبکه آن آزاد است، هر کسی که از قوانین و عملکرد آن رضایت ندارد، می‌تواند با استفاده از کد بیت‌کوین، شبکه و بلاکچین جدیدی بسازد.

دومین گروهی که درصدد عرضه ارزهای دیجیتال و بلاکچین‌های جدید برآمدند، معتقد بودند که کاربردهای بلاکچین می‌تواند فراتر از پول باشد که البته درست است. گروه دوم روی شبکه‌هایی کار می‌کنند که ضمن کاربرد به‌عنوان پول و روش پرداخت، می‌توان روی آن برنامه‌های غیرمتمرکز و «قرارداد هوشمند» ایجاد کرد. در ادامه بیشتر درباره قراردادهای هوشمند می‌خوانید، اما به بیان ساده قراردادهای هوشمند برنامه‌هایی هستند که روی بلاکچین پیاده‌سازی می‌شوند. این قراردادها در صورت رخدادن یک یا چند شرط، یک عملیات از پیش تعیین‌شده را اجرا می‌کنند. زمانی که قرارداد هوشمند ثبت می‌شود، به‌دلیل ذات غیرقابل تغییر بلاکچین، دیگر هیچ‌کس نمی‌تواند مانع از فعالیت و اجرای دستورات آن شود. این در جهانی با خطاهای عمدی و غیرعمدی ایده‌ای بی‌نظیر است. در شبکه‌های مبتنی بر قرارداد هوشمند، افراد می‌توانند بدون اینکه نیاز باشد بلاکچین جدیدی بسازند، ارز دیجیتال خود را روی همان شبکه ایجاد کنند که در اصطلاح به آن «توکن»[1] می‌گویند.

1. Token

توجه: در زمان نگارش کتاب، طرح‌های کلاهبرداری زیادی از جمله «کینگ‌مانی»، «بیکسبی کوین»، «بنک آو ترون» و... با سوءاستفاده از نام قراردادهای هوشمند و وعده سودهای نجومی، فعالیت می‌کنند. فراموش نکنید که قرارداد هوشمند یک نوآوری زیربنایی است و مانند یک وب‌سایت خالی از محتوا، اگر در قرارداد هوشمند فعالیت اقتصادی وجود نداشته باشد، کاملاً بی‌مصرف است.

بسیاری از ارزهای دیجیتال پس از بیت‌کوین که در میان جامعه ارزهای دیجیتال به آنها «آلت‌کوین»[1] گفته می‌شود، خیلی زود با ایده‌های بلندپروازانه و عجیب خود از دور رقابت حذف شدند و به رده‌های پایین بازار سقوط کردند. برخی دیگر اما همچنان در صدر قرار دارند و به تلاش‌های خود برای رسیدن به جریان اصلی در بین مردم و شاید پیشی گرفتن از بیت‌کوین ادامه می‌دهند. اکنون و در زمان نگارش این کتاب، بازار بیت‌کوین حدود ۴۰ درصد از کل بازار ارزهای دیجیتال را در اختیار دارد و به نظر نمی‌رسد که بیت‌کوین برای حفظ جایگاه نخست، رقیب جدی غیر از اتر داشته باشد. طبق یک معیار کلی، رتبه ارزهای دیجیتال بر اساس ارزش بازار یا همان «مارکت‌کپ» تعیین می‌شود. ارزش بازار برابر است با تعداد واحدهای یک سهام یا دارایی، ضرب در قیمت هر واحد از سهام یا دارایی.

به‌عنوان مثال، اگر قیمت هر واحد بیت‌کوین ۱۰,۰۰۰ دلار باشد و تعداد بیت‌کوین‌های در گردش (بیت‌کوین‌های استخراج‌شده) ۱۸,۰۰۰,۰۰۰ باشد، ارزش بازار بیت‌کوین برابر است با ۱۰,۰۰۰ ضرب در ۱۸,۰۰۰,۰۰۰ که مساوی است با ۱۸۰,۰۰۰,۰۰۰,۰۰۰ دلار یا همان ۱۸۰ میلیارد دلار. تاکنون هیچ ارز دیجیتالی نتوانسته از نظر ارزش بازار از بیت‌کوین پیشی بگیرد، اما در رده‌های دیگر مدام شاهد تغییر جایگاه ارزهای دیجیتال هستیم و هر روز یکی از دیگری پیشی می‌گیرد یا زیر پای ارزهای دیجیتال جدید له می‌شود. در اینجا چند مورد از بزرگ‌ترین و محبوب‌ترین ارزهای دیجیتال پس از بیت‌کوین را معرفی کنیم.

لایت‌کوین

لایت‌کوین جزء اولین ارزهای دیجیتال غیرمتمرکزی است که خیلی زود پس از بیت‌کوین عرضه شد. این ارز دیجیتال هم مانند بیت‌کوین مبتنی بر فناوری بلاکچین است و همانند

۱. (Altcoin) به معنای ارز دیجیتال جایگزین برای بیت‌کوین

پادشاه ارزهای دیجیتال، امنیت لایت‌کوین هم با رمزنگاری و فرایند اثبات کار (استخراج) تضمین می‌شود. تراکنش‌های لایت‌کوین تقریباً چهار برابر سریع‌تر از بیت‌کوین هستند، اما سازوکار شبکه و تراکنش‌های لایت‌کوین و بیت‌کوین کاملاً مشابه با یکدیگر است. از آنجایی که لایت‌کوین زمان ایجاد بلوک کمتری دارد (۲٫۵ دقیقه)، سرعت تراکنش‌های آن بالاتر از بیت‌کوین است. در حالی که هویت ساتوشی ناکاموتو، خالق بیت‌کوین مشخص نیست، خالق لایت‌کوین جوانی چینی‌الاصل به نام «چارلی لی» است. کارمند سابق گوگل و کوین‌بیس، در سال ۲۰۱۱ با تغییرات بزرگی در پروتکل بیت‌کوین، شبکه لایت‌کوین را معرفی کرد. فلسفه‌ای جالب برای تولد لایت‌کوین وجود دارد. اگر بیت‌کوین طلا باشد، لایت‌کوین مانند لوگویی که دارد، یادآور نقره است؛ به این معنی که هدف لایت‌کوین ایجاد ارزی برای مقاصد روزمره‌تر و ارزان‌تر نسبت به بیت‌کوین است که برای مقاصد کلان استفاده می‌شود. مانند بیت‌کوین، لایت‌کوین هم محدود است، با این تفاوت که بر خلاف بیت‌کوین که فقط ۲۱ میلیون از آن تولید خواهد شد، لایت‌کوین تا ۸۴ میلیون واحد استخراج می‌شود.

نماد معاملاتی لایت‌کوین LTC است. این ارز دیجیتال هم مانند بیت‌کوین از قیمتی در حدود یک سنت کارش را آغاز کرد و تا سال ۲۰۱۴ رشد قیمت خیلی خوبی داشت. بعد از آن با کاهش قیمت محسوسی مواجه شد و حدود سه سال در محدوده قیمت یک تا چهار دلار بالا و پایین می‌شد. سال ۲۰۱۷ دوران انفجار لایت‌کوین بود. در حالی که بیت‌کوین در سال ۲۰۱۷ حدود ۱,۷۰۰ درصد رشد کرد، لایت‌کوین با رسیدن به بالاترین قیمت تاریخش یعنی ۳۲۰ دلار، صعودی ۷,۰۰۰ درصدی را تجربه کرد. در سال‌های ۲۰۱۸ و ۲۰۱۹، لایت‌کوین هم مانند سایر ارزهای دیجیتال سقوط شدیدی داشت و تا ۲۰ دلار هم پایین آمد. از آنجایی که پاداش استخراج لایت‌کوین هم مانند بیت‌کوین، هر چهار سال یک بار نصف می‌شود، در سال ۲۰۱۹، چند ماه قبل از رویداد هاوینگ یا همان نصف‌شدن پاداش استخراج، قیمت لایت‌کوین صعود شدیدی را تجربه کرد و به حدود ۱۵۰ دلار رسید. با این حال پس از هاوینگ قیمت دوباره سقوط کرد و در محدوده ۵۰ دلار قرار گرفت. لایت‌کوین طی سال‌های ۲۰۲۰ و ۲۰۲۱ همگام با رشد بازار موفق شد که سقف تاریخی جدیدی رقم بزند و به محدوده ۴۰۰ دلار برسد.

اتریوم

در زمان نوشتن کتاب، اتریوم پس از بیت‌کوین دومین ارز دیجیتال بزرگ بازار است که به همین دلیل به آن «ملکه ارزهای دیجیتال» هم می‌گویند. اتریوم برای اولین‌بار توانست راهکاری برای تحقق یکی از رویاهای دیرینه علم کامپیوتر و برنامه‌نویسی ارائه کند؛ ساختن برنامه‌هایی که هیچ‌وقت متوقف نمی‌شوند و هیچ‌کس نمی‌تواند آنها را کنترل کند. دنیایی بدون واسطه را تصور کنید. دنیایی که مردم به‌صورت مستقیم و بدون اینکه نیاز باشد به یکدیگر اعتماد می‌کنند، به مبادله دارایی‌ها، عقد قرارداد و استفاده از خدمات می‌پردازند؛ برنامه‌هایی غیرمتمرکز که هیچ‌گاه متوقف نمی‌شوند و هیچ‌کس نمی‌تواند در کار آنها تداخل ایجاد کند. اتریوم اولین سیستمی بود که برای تحقق این آرمان پا به عرصه گذاشت.

در مقایسه با بیت‌کوین، اتریوم یک پروژه بسیار جوان است. «ویتالیک بوترین»، نابغه روسی - کانادایی و جوان ۱۹ساله‌ای که از سال ۲۰۱۱ با بیت‌کوین آشنا شده بود، اواخر سال ۲۰۱۳ از ایده اتریوم رونمایی کرد. اتریوم دنیای بدون واسطه‌ای است که مردم در آن بدون نیاز به اعتماد به یک فرد یا گروه، می‌توانند برنامه‌های کامپیوتری را اجرا کنند که هیچکس قادر به متوقف‌کردن آن نیست و قراردادهایی را تنظیم کنند که بدون نیاز به واسطه متمرکز، اجرا می‌شوند.

شکل ۱-۳: ویتالیک بوترین، خالق روسی-کانادایی اتریوم که در ۱۹سالگی کار روی اتریوم را آغاز کرد.

به عبارت دیگر، اتریوم تنها یک ارز نیست؛ بلکه یک بستر غیرمتمرکز مبتنی بر بلاکچین است که روی آن می‌شود هر چیزی ساخت. توسعه‌دهندگان به جای اینکه برای هر کاری بلاکچین بسازند، می‌توانند روی بلاکچین اتریوم ایده‌های خود را پیاده‌سازی کنند و برای خود ارزهای دیجیتال (توکن) بسازند. به همین دلایل، اتریوم خود را به‌عنوان یک «کامپیوتر جهانی» معرفی کرده است. در حال حاضر، شبکه اتریوم نیز با سازوکار اثبات کار یا همان ماینینگ پیش می‌رود و تأیید تراکنش‌ها، اجرای قراردادهای هوشمند و سایر فعالیت‌ها بر عهده استخراج‌کنندگان اتریوم است. ارز بومی شبکه اتریوم، اتر نام دارد و از آن به‌عنوان «سوخت شبکه اتریوم» یاد می‌شود. اتر در حقیقت علاوه بر روشی برای پرداخت، انگیزه‌ای برای فعالیت ماینرهاست.

حرکت به سمت اثبات سهام

توسعه‌دهندگان اتریوم از همان ابتدای عرضه اتریوم به‌دنبال پیاده‌سازی سازوکاری تحت عنوان «اثبات سهام» بودند تا این شبکه دیگر به دستگاه‌های استخراج و ماینرها نیاز نداشته باشد و در عوض تأیید تراکنش‌ها را سهام‌دارانی انجام دهند که خودشان مالک واحدهای اتر هستند. فاز ابتدایی (صفر) این به‌روزرسانی در سال ۲۰۲۰ اجرا شد و قرار است فاز بعدی (یک) آن در سال ۲۰۲۲ اجرایی و امکان انتقال بر روی شبکه جدید فعال شود. بهتر است بدانید که هر دو شبکه با سازوکارهای جدید در حال حاضر فعال هستند و این به‌روزرسانی به صورت یک گذار تدریجی به سمت سازوکار جدید در چند فاز مختلف برنامه‌ریزی شده است.

به بیان ساده، در الگوریتم اجماع اثبات سهام، افراد ارزهای دیجیتال شبکه را می‌خرند و به شبکه اختصاص می‌دهند. شبکه از آن دارایی‌ها برای اعتبارسنجی و حفظ امنیت خود استفاده می‌کند و به‌عنوان پاداش، سالانه مقداری سود به سرمایه‌گذاران پرداخت می‌کند. در واقع، در روش اثبات سهام سرمایه‌گذاران می‌توانند علاوه بر کسب سود از سرمایه‌گذاری، از اختصاص‌دادن ارزهای خود به شبکه هم کسب درآمد کنند. در سیستم اثبات سهام، به افرادی که در سهام‌گذاری و تأیید تراکنش‌ها مشارکت می‌کنند، اعتبارسنج گفته می‌شود. اعتبارسنج‌ها به‌نوعی همان کار ماینرها در شبکه‌های اثبات کار را انجام می‌دهند، ولی دیگر به سخت‌افزارهای استخراج نیازی نیست.

در روش اثبات سهام، سوءنیت اعتبارسنج‌ها برای فعالیت خرابکارانه به از دست‌دادن سکه‌هایشان منجر می‌شود و در طرف مقابل، عملکرد صحیح آنها پاداشی از سوی شبکه به همراه خواهد داشت، تا به این ترتیب با ایجاد انگیزه مادی، میل به خرابکاری از بین برود.

در بین اعضای جامعه ارزهای دیجیتال، به ارز دیجیتال شبکه اتریوم، همان اتریوم هم گفته می‌شود، اما در حقیقت نام آن اتر است. بنابراین اگر جایی «خرید اتریوم»، «تحلیل اتریوم» و... را دیدید، منظور همان اتر است. اتر برای پرداخت هزینه‌ها و به‌عنوان انگیزه‌ای برای مشارکت‌کنندگان در جهت ادامه فعالیت اتریوم ساخته شده است. اگر اتر، این ارز دیجیتالِ ارزشمند وجود نداشت، چه کسی حاضر می‌شد به‌عنوان ماینر یا مشارکت‌کننده در شبکه فعالیت کند؟ فراموش نکنید استفاده از خدمات شبکه اتریوم و ایجاد برنامه روی آن نیازمند پرداخت کارمزد است و این کارمزد باید به‌صورت اتر پرداخت شود. اترهایی که برای کارمزد پرداخت می‌شود، به ماینرهایی تعلق می‌گیرد که امنیت شبکه را حفظ می‌کنند. به همین دلیل، به اتر «سوخت شبکه اتریوم» هم می‌گویند. بر خلاف بیت‌کوین، برای تعداد کل سکه‌های اتریوم محدودیتی لحاظ نشده است، اما این بدان معنی نیست که اتریوم بدون هیچ محدودیتی عرضه می‌شود. اتر دارای نرخ تورم حدود چهار درصد است و قرار است در به‌روزرسانی‌های آینده، فقط متناسب با نیازهای شبکه، اتر جدید عرضه شود[۱].

قرارداد هوشمند

قرارداد به معنی توافقی بین دو یا چند شخص است که آنها را متعهد به انجام کاری در آینده می‌کند. برای مثال، قرارداد اجاره یک خانه، فرد مستأجر را به پرداخت اجاره در مدت‌زمان مشخصی ملزم می‌کند. ضمانت اجرای تعهدات یک قرارداد از سوی طرفین، به وسیله یک طرف سوم مورد اعتماد برقرار می‌شود؛ به این صورت که اگر یکی از دو طرف کوتاهی کند، باید به یک نهاد قضایی یا سازمان دولتی مراجعه شود تا روند اجرای قرارداد را پیگیری کند. قرارداد هوشمند ضمن حفظ ساختار یک قرارداد، نیاز به طرف سوم مورد

۱. در به‌روزرسانی «لندن» که تابستان سال ۲۰۲۱ بر روی شبکه اتریوم اجرا شد، بخشی از کارمزد تراکنش‌ها از عرضه شبکه خارج شده و به‌اصطلاح سوزانده می‌شد. طی این به‌روزرسانی نرخ تورم اتر کاهش قابل‌توجهی پیدا کرد.

اعتماد را از میان برداشته است.

یک قرارداد هوشمند، توافقی میان طرفین است که در قالب کدهای کامپیوتری نوشته شده و روی یک بلاکچین ثبت می‌شود تا ضمانت اجرایی پیدا کند. هوشمندبودن این نوع قراردادها به خاطر فعال‌شدن خودکار آنها در صورت برقرار شدن شرایط از پیش تعیین‌شده است. زمانی که یک قرارداد هوشمند روی یک بلاکچین باز مثل اتریوم اجرا شود، دیگر قابل توقف نیست و هیچ‌کس نمی‌تواند جلوی اجرای آن را بگیرد. با قراردادهای هوشمند می‌توان برنامه‌ها و پروژه‌هایی را ساخت که بدون هیچ‌گونه واسطه و ازکارافتادگی تا ابد به کار خود ادامه دهند. به این برنامه‌ها، برنامه‌های غیرمتمرکز هم می‌گویند. حتی خود برنامه‌نویس قرارداد هوشمند هم نمی‌تواند کد قرارداد هوشمند ثبت‌شده در بلاکچین را تغییر دهد. از قراردادهای هوشمند می‌توان در صنعت بیمه، مبادلات تجاری، انتخابات شفاف و بدون تقلب و جمع‌آوری سرمایه اولیه استفاده کرد. اتریوم اولین پلتفرمی بود که این نوع قابلیت را روی بلاکچین معرفی و نوشتن آنها را با زبان برنامه‌نویسی مخصوصی به نام «سالیدیتی» ممکن کرد. با این حال، هم‌اکنون تعداد دیگری از پلتفرم‌ها مانندسولانا[1]، تزوس[2]، کاردانو[3]، آولنچ[4] و... نیز میزبان قراردادهای هوشمند هستند.

برای درک بهتر قرارداد هوشمند به این مثال توجه کنید؛ فرض کنیم بهزاد خانه مجید را با ودیعه ۱۰۰ میلیون تومان و اجاره ماهانه دو میلیون تومان، برای یک سال اجاره می‌کند. بنابراین با کمک زبان‌های برنامه‌نویسی در کد قرارداد هوشمند شرط گذاشته می‌شود که بهزاد ابتدا ۱۰۰ میلیون تومان و هر ماه دو میلیون تومان به‌صورت ارز دیجیتال (مثلاً اتریوم) برای اجاره، به آدرس قرارداد هوشمند پرداخت کند. می‌توانیم قرارداد را طوری تنظیم کنیم که اگر اجاره عقب افتاد، از ودیعه کم کند تا زمانی که ودیعه به پایان برسد. سپس می‌توانیم در کد قرارداد هوشمند این شرط را تعیین کنیم که در صورتی که ودیعه تمام شد و بهزاد همچنان اجاره پرداخت نکرد، برای تخلیه خانه اطلاع داده شود.

---

1. Solana
2. Tezos
3. Cardano
4. Avalanche

در حال حاضر عمده کاربرد قراردادهای هوشمند در پلتفرم‌ها به‌طور عمده برای پیاده‌سازی برنامه‌های غیرمتمرکز مربوط به مبادله غیرمتمرکز است. مثال بارز این بخش به حوزه امور مالی غیرمتمرکز یا دیفای[1] مربوط است که وام‌دهی و تأمین نقدینگی برای صرافی‌های غیرمتمرکز به‌واسطه آن ممکن شده است.

اتریوم و اتریوم کلاسیک

تا سال ۲۰۱۶ فقط یک اتریوم وجود داشت، اما هک بزرگی که در ۱۷ ژوئن ۲۰۱۶ رخ داد، باعث شد اتریوم جدیدی خلق شود و اتریوم قبلی «اتریوم کلاسیک» نام بگیرد. در اینجا قصد داریم داستان شکل‌گیری اتریوم کلاسیک را خیلی مختصر توضیح دهیم تا در این بین با مفهوم «فورک» هم آشنا شوید.

تا سال ۲۰۱۶ همه‌چیز بر وفق مراد اتریوم پیش می‌رفت. این شبکه توانسته بود تمام برنامه‌های نقشه راه خود را در زمان مقرر انجام دهد. با اینکه کمتر از دو سال از راه‌اندازی رسمی شبکه گذشته بود، قیمت هر واحد اتر با رشد چندصد درصدی به بالای ۲۱ دلار رسیده و با اختلاف زیاد نسبت به لایت‌کوین در رده دوم بازار جای گرفته بود. در ماه مه ۲۰۱۶، یک طرح انقلابی به نام DAO برای اتریوم معرفی شد که امیدواری‌ها به آینده اتریوم را دوچندان کرد. این همان بلای اتریوم بود.

سازمان خودگردان غیرمتمرکز (DAO) چیست؟

شرکتی را تصور کنید که بدون وجود یک مدیر در رأس امور، تمام اجزای آن کار خود را به‌درستی انجام می‌دهند، بدون اینکه نیازی باشد وظایف‌شان را کسی به آنها گوش‌زد کند. «سازمان خودگردان غیرمتمرکز» یا DAO، در واقع نظام مدیریتی خودکار و غیرقابل کنترلی است که طبق قوانین از پیش تعیین‌شده، بدون اینکه نیازی به دخالت وجود داشته باشد، به راه خود ادامه می‌دهد. از نظر فنی، بیت‌کوین اولین DAO بود؛ چراکه خالق آن قوانینش را در کدهایش نوشته بود و به‌طور خودکار می‌توانست بر اساس آنها عمل کند. در اتریوم، با استفاده از قرارداد هوشمند امکان پیاده‌سازی شکل پیچیده‌تری از DAO وجود دارد و کاربردهای آن را به فراتر از پول ارتقا داده است. برای شکل‌گیری یک DAO، اول از همه قوانین آن باید در قالب کدهای قرارداد هوشمند نوشته شود و در دسترس عموم قرار

1. DeFi

گیرد. پس از توزیع توکن (ارز دیجیتالی داخلی) یک DAO که برای فعالیت‌های اقتصادی آن کاربرد دارد، سازمان خودگردان غیرمتمرکز کار خود را شروع می‌کند و پس از آن هیچ‌کس حتی سازنده آن نمی‌تواند آن را متوقف کند یا قوانینش را بدون نظر اکثریت تغییر دهد. برای همین، وجود یک خطا در کدهای قرارداد هوشمند DAO می‌تواند مشکلات بزرگی به وجود بیاورد؛ همان‌طور که این اتفاق در اتریوم نیز رخ داد.

در سال ۲۰۱۶ یک سازمان خودگردان غیرمتمرکز به نام دائو (DAO) (این یک نام است و با خود مفهوم DAO اشتباه نگیرید) روی بلاکچین اتریوم ساخته شد. به بیان ساده، دائو یک صندوق سرمایه‌گذاری بود که به‌صورت غیرمتمرکز توسط سرمایه‌گذارانش اداره می‌شد و هدف آن جذب سرمایه برای توسعه برنامه‌های غیرمتمرکز بود. روند کار دائو به این صورت بود که مردم می‌توانستند اتریوم بخرند و به دائو واریز کنند. در قبال اتریوم‌ها، دائو به سرمایه‌گذاران توکن‌هایی می‌داد که با آنها در صندوق حق رأی پیدا می‌کردند. برنامه‌نویسان می‌توانستند ایده‌های خود را ارسال کنند و سپس در میان دارندگان توکن‌های دائو رأی‌گیری انجام می‌شد. اگر ۲۰ درصد موافقت خود را با طرح اعلام می‌کردند، صندوق دائو به‌طور خودکار سرمایه مورد نیاز را در اختیار توسعه‌دهنده قرار می‌داد تا با آن بتواند برنامه خود را بسازد و بعد از ساختن برنامه، سود خوبی نصیب خودش و سرمایه‌گذاران شود. برنامه دائو اولین سازمان خودگردان غیرمتمرکز بود که به‌صورت گسترده شروع به کار کرد و همه فرایندها به‌صورت غیرمتمرکز و بدون واسطه انجام می‌شد؛ دموکراسی به معنای واقعی. طی کمتر از ۳۰ روز از معرفی، این صندوق معادل بیش از ۱۵۰میلیون دلار اتریوم جذب کرد و سرمایه‌گذاران زیادی برای خرید توکن‌های بیشتر لحظه‌شماری می‌کردند. ۱۵۰میلیون دلار اتریوم در آن زمان معادل ۱۴ درصد از کل اتریوم‌های استخراج‌شده بود.

ناگهان اتفاقی که نباید، رخ داد. در کد قرارداد هوشمند این سازمان غیرمتمرکز ایرادی وجود داشت و یک هکر به وسیله آن توانست هزاران واحد اتریوم را که در آن زمان معادل حدود ۵۰ میلیون دلار بود، به سرقت ببرد. فراموش نکنید ایراد یافت‌شده به کدهای برنامه‌نویس مربوط بود و ارتباطی با اتریوم نداشت؛ فرض کنید اتریوم اینترنت باشد و دائو وب‌سایتی روی اینترنت. بنابراین در خود شبکه اتریوم اتفاقی رخ نداده بود، اما از

دست‌رفتن ۵۰ میلیون دلار اتریوم برای شبکه‌ای که در ابتدای راه خودش قرار داشت، یک فاجعه محسوب می‌شد.

به‌طور کلی سه راه پیش روی جامعه اتریوم بود؛ ۱. هیچ‌کاری نمی‌کردند، به این معنا که طبق قوانین شبکه و این قاعده که «کد قانون است»، هکر ۵۰ میلیون دلار را برداشت می‌کرد که با ذات غیرمتمرکز بلاکچین یک موضوع طبیعی بود. ۲. انشعاب نرم یا همان سافت‌فورک برای بازگشت دارایی‌ها. ۳. انشعاب سخت یا همان هاردفورک برای بازگشت دارایی‌ها. اکثریت جامعه تصمیم گرفتند که نگذارند اعتبار اتریوم زیر سؤال برود و در ابتدا قرار بر این شد که با استفاده از سافت‌فورک، مبالغ را برگردانند.

سافت‌فورک چیست؟

همان‌طور که احتمالاً می‌دانید، یک بلاکچین را نمی‌توان تغییر داد. پس اگر لازم باشد تا روی آن به‌روزرسانی صورت بگیرد یا اگر عده‌ای از قوانین یک بلاکچین ناراضی باشند، راه‌حل چیست؟ برای بلاک چین‌های نسل قدیمی (بلاکچین‌های جدید این‌گونه نیستند) دو راه بیشتر وجود ندارد؛ سافت فورک، هارد فورک.

سافت‌فورک یک به‌روزرسانی در بلاکچین بوده که با نسخه‌های قدیمی سازگار است. سازگاری با نسخه‌های قدیمی مانند این است که یک فایل متنی را که با برنامه Word 2016 ساخته شده است، در برنامه قدیمی Word 2003 باز کنید. به زبان ساده، با سافت‌فورک یک به‌روزرسانی روی بلاکچین انجام می‌شود، اما کسانی هم که مایل به به‌روزرسانی نیستند، همچنان می‌توانند در اعتبارسنجی تراکنش‌ها نقش داشته باشند. در واقع توسعه‌دهندگان اتریوم می‌خواستند بدون تغییردادن قوانین بلاکچین اتریوم، جلوی تراکنش هکر DAO را بگیرند و ماینرها بلوک‌هایی را که مربوط به تراکنش‌های هکر است، نادیده بگیرند تا بتوان مبالغ را برگشت داد. در سافت‌فورک شاهد ارز دیجیتال و بلاکچین جدیدی نخواهیم بود.

همه‌چیز برای سافت‌فورک آماده بود، اما فقط چند روز مانده به فورک گروهی از توسعه‌دهندگان اتریوم در مقاله‌ای اثبات کردند در صورت اجرای سافت‌فورک، شبکه اتریوم تا مدتی در خطر حملات DDoS (حملاتی برای توقف کار یک شبکه یا سرویس) قرار خواهد گرفت. در این حملات با استفاده از تراکنش‌های بیش از اندازه و بدون

پرداخت کارمزد زیاد، مهاجمان می‌توانستند باعث شلوغی شبکه و توقف در آن شوند؛ بنابراین توسعه‌دهندگان اتریوم تصمیم گرفتند برای بازگرداندن پول سرمایه‌گذاران، گزینه بعدی یعنی هاردفورک را انتخاب کنند.

هاردفورک چیست؟

هاردفورک به زبان ساده، تغییر در قوانین بلاکچین است که سازگار با نسخه‌های قدیمی‌تر نیست، به‌طوری که نسخه‌های قدیمی‌تر نمی‌توانند در شبکه فعالیت کنند. بنابراین، برای مشارکت در شبکه مجبور خواهید بود که نسخه خود را ارتقا دهید. طبق همان مثال فایل ورد که به آن اشاره شد، فرض کنید نتوانید یک فایل متنی ساخته‌شده در برنامه Word 2016 را در برنامه Word 2003 اجرا کنید، زیرا ساختار این برنامه به‌طور کلی تغییر کرده است. هاردفورک‌ها همیشه باعث تولد یک ارز دیجیتال جدید نمی‌شوند؛ فقط در صورتی که اختلاف‌نظر وجود داشته باشد و عده کثیری از کاربران همچنان بخواهند روی نسخه قدیمی فعالیت کنند، شاهد یک بلاکچین و یک سکه جدید خواهیم بود.

انجام هاردفورک و تغییر قوانین اتریوم، در میان توسعه‌دهندگان اختلاف زیادی ایجاد کرد. مخالفان می‌گفتند: «کد قانون است» و تغییر قوانین خلاف آرمان‌های تمرکززدایی است. همان‌طور که گفتیم، در صورت وجود اختلاف گسترده، هاردفورک به بلاکچین و ارز دیجیتال جدید منجر می‌شود؛ به این صورت که جامعه مخالف همچنان نسخه قدیمی خودشان را اجرا می‌کنند و جامعه جدید هم نسخه جدید خودشان را.

هاردفورک بزرگ در بلوک ۱,۹۲۰,۰۰۰، یعنی یک بلوک قبل از رخ‌دادن هک دائو انجام شد تا پول سرمایه‌گذاران برگردد. با این اتفاق، یک بلاکچین و یک ارز دیجیتال جدید ساخته شد. البته به دارندگان ارز قدیمی، ارز جدید هم تعلق گرفت. به‌دلیل حمایت گسترده از هاردفورک جدید و پشتیبانی توسعه‌دهندگان اصلی از جمله ویتالیک بوترین، اتریومی که اول وجود داشت، در صرافی‌ها به اتریوم کلاسیک با نماد ETC تغییر نام داد و اتریوم جدید، همان اتریوم نام گرفت. این بر خلاف معمول بود؛ زیرا معمولاً اسم بلاکچین قبلی ثابت می‌ماند و یک اسم به بلاکچین جدید می‌دهند؛ مانند جریان بیت‌کوین و بیت‌کوین‌کش که بلاکچین جدید بیت‌کوین‌کش نام گرفت.

اکنون اتریوم کلاسیک یک پروژه تقریباً رهاشده است و با فاصله زیادی از اتریوم، با کاهش قیمت شدید در رده‌های پایین بازار ارزهای دیجیتال قرار دارد. همچنین به‌دلیل عدم فعالیت کافی استخراج‌کنندگان بر روی این شبکه، تاکنون به آن چند حمله با خسارت‌های چندمیلیون دلاری انجام شده است. با این حال، عده زیادی همچنان معتقدند اتریوم کلاسیک، اتریوم واقعی است و امیدوار هستند دوباره به اوج برسد.

قیمت اتر

پس از رشد استفاده از قراردادهای هوشمند و پلتفرم‌ها در سال‌های ۲۰۲۰ و ۲۰۲۱، سرمایه‌گذاران بلندمدت اتریوم جزو راضی‌ترین افراد بازار ارزهای دیجیتال بودند.

اتر در زمان فروش در عرضه اولیه حدود ۰/۳ دلار به ازای هر واحد قیمت داشت. زمانی که اتر در اواسط سال ۲۰۱۵ وارد صرافی‌ها شد، حدود ۱/۲ دلار معامله شد و برحسب ارزش بازار در جایگاه پایین‌تری نسبت به بیت‌کوین، ریپل و لایت‌کوین قرار گرفت. طی کمتر از یک سال، قیمت اتر با رشدی سرسام‌آور به حدود ۱۵ دلار رسید و رتبه دوم بازار را تصاحب کرد. پس از آن، به‌دلیل مسائل پیش‌آمده از هک دائو، کمی قیمت اصلاح شد تا اینکه سال ۲۰۱۷ فرا رسید. اتر سال ۲۰۱۷ را با قیمت ۸/۵ دلار به ازای هر واحد آغاز کرد و با قیمت ۸۰۰ دلار به پایان برد. در سال ۲۰۱۷ تقریباً همه ارزهای دیجیتال رشد شدیدی را تجربه کردند و قیمت بیت‌کوین هم به بالاترین رقم تاریخ خود یعنی حدود ۲۰ هزار دلار رسید، اما جهش اتر و ریپل بسیار چشم‌گیرتر بود. یکی از اصلی‌ترین علل صعود تاریخی اتر امکان ایجاد توکن روی این شبکه بود. در آن زمان برنامه‌های جذب سرمایه با پیش‌فروش توکن یا همان ICOها مانند قارچ رشد می‌کردند و هر کسی به اسم بلاکچین و با ایده‌های عجیب‌وغریب توکن خودش را می‌ساخت و می‌فروخت. در سال ۲۰۱۷ که به حباب ICO معروف است، با خرید هر توکن یا ارزی، سود چند صددرصدی نصیب‌تان می‌شد. رشد اتر تا ژانویه ۲۰۱۸ هم ادامه یافت و ملکه ارزهای دیجیتال در همان ماه به بالاترین قیمت تاریخ یعنی حدود ۱۴۰۰ دلار رسید. به این ترتیب، اتر از سال ۲۰۱۶ تا ۲۰۱۸ طی کمتر از دو سال حدود ۱۴۰ هزار درصد رشد کرد.

اتر پس از ثبت اوج قیمتی در سال ۲۰۱۸ بیش از ۹۰ درصد از ارزش خود را از دست داد و به کمتر از ۱۰۰ دلار به ازای هر واحد رسید. با این حال سال‌های ۲۰۲۰ و ۲۰۲۱ با مطرح‌شدن

برنامه‌های غیرمتمرکز مربوط به حوزه‌های دیفای، توکن‌های غیرمثلی و دائوها، کاربرد پلتفرم‌ها و قراردادهای هوشمند بیش از هر زمان دیگری آشکار شد. اولین نتیجه این اتفاق رشد ارزهای بومی پلتفرم‌ها بود و در میان آن‌ها اتریوم موفق شد با رشد تقریباً ۵۰۰۰ درصدی به محدوده ۴۸۰۰ دلار برسد. در زمان نگارش این کتاب، اتریوم در حدود ۳۰۰۰ دلار معامله می‌شود.

ریپل

ریپل هم با نماد معاملاتی XRP یکی از بالانشینان همیشگی بازار ارزهای دیجیتال است. ایده جذاب، همکاری‌های بزرگ با شرکت‌های مالی و رشد نجومی و چندهزار درصدی این ارز دیجیتال در سال ۲۰۱۷ باعث شد تا توجه زیادی به آن جلب شود، اما هدف ریپل با چیزی که در بیت‌کوین یا اتریوم می‌بینیم، از زمین تا آسمان متفاوت است.

سالانه بیش از ۱۵۵ تریلیون دلار پول در سراسر جهان جابه‌جا می‌شود، اما مشکلات انتقال پول با بانک‌ها و مؤسسات مالی سنتی سال‌هاست که حل‌نشده باقی مانده و با توجه به رشد فناوری، هنوز انتقال بین‌المللی پول‌های کلان بین سه تا هفت روز طول می‌کشد که نیازمند کارمزدهای بسیار بالا و انجام کاغذبازی‌های زیادی است. ریپل می‌خواهد برای همیشه به این مشکلات پایان داده و بخش بزرگی از انتقالات پول را انجام دهد.

می‌توان گفت که هدف ریپل کاملاً در تضاد با بیت‌کوین است. در حالی که بیت‌کوین با هدف تراکنش‌های همتابه‌همتا و حذف واسطه‌ها و بانک‌ها روی کار آمده است، شرکت ریپل عقیده دارد که بانک‌ها به خودی خود بد نیستند و فقط نحوه انجام کار است که باعث ایجاد مشکلات پرداختی و انتقال پول می‌شود. ریپل مدعی است که می‌تواند حجم زیادی از پول را در کمتر از چند ثانیه منتقل کند؛ چنانچه تراکنش‌های ریپل در عرض حدود چهار ثانیه تأیید می‌شوند و کارمزدهای آن به‌شدت پایین است.

قبل از توضیح بیشتر در مورد ریپل، باید ابهام‌زدایی انجام شود. وقتی مردم نام ریپل را می‌شنوند، بلافاصله فکرشان به سمت ارز دیجیتال آن یعنی XRP می‌رود، اما ریپل از این نظر با تقریباً تمام ارزهای دیجیتال تفاوت دارد. در حقیقت، وقتی ارز دیجیتال

اتریوم (ETH) می‌خرید، به این معنی است که روی شبکه اتریوم سرمایه‌گذاری می‌کنید. وقتی ارز دیجیتال بیت‌کوین (BTC) می‌خرید، یعنی روی شبکه بیت‌کوین سرمایه‌گذاری می‌کنید، اما وقتی ارز دیجیتال XRP می‌خرید، الزاماً روی ریپل سرمایه‌گذاری نکرده‌اید. البته در بین جامعه ارزهای دیجیتال وقتی نام ریپل به میان می‌آید، منظور همان ارز دیجیتال XRP است، اما لازم است بدانیم که این دو مفهوم در حقیقت با یکدیگر متفاوت هستند. اگر تاکنون کمی گیج شده‌اید، جای نگرانی نیست، در این مورد بیشتر توضیح خواهیم داد.

یادتان نرود، ریپل یک شرکت است و XRP یکی از محصولات این شرکت. ریپل یک شرکت بزرگ واقع در سان‌فرانسیسکو آمریکاست که برای بانک‌ها و نهادهای مالی، محصولات مالی غیرمتمرکز می‌سازد. این شرکت چند محصول گوناگون برای بانک‌ها و مؤسسات مالی طراحی کرده که فقط یکی از آنها با ارز دیجیتال XRP کار می‌کند. بنابراین وقتی XRP می‌خرید، روی یکی از محصولات شرکت ریپل سرمایه‌گذاری کرده‌اید، نه خود ریپل. در حال حاضر شرکت ریپل سه محصول اصلی برای بانک‌ها و مؤسسات مالی دارد که عبارت‌اند از: «ایکس‌کارنت»، «ایکس‌رپید» و «ایکس‌ویا». اینها در حال حاضر سه محصول اصلی شرکت ریپل هستند که با یک نام جامع تحت عنوان «ریپل‌نت» فعالیت می‌کنند.

ارز دیجیتال XRP فقط روی شبکه ایکس‌رپید با نام جدید (On demand liquidity) کاربرد دارد و در دیگر محصولات این شرکت، یعنی ایکس‌کارنت و ایکس‌ویا، این ارز دیجیتال کاربرد و جایگاه چندانی ندارد. لازم به ذکر است که این روزها بیشتر شرکت‌های تحت قرارداد ریپل از محصول ایکس‌کارنت آن استفاده می‌کنند. بنابراین وقتی خبر همکاری ریپل با یک شرکت بزرگ منتشر می‌شود، لزوماً به معنای کاربرد بیشتر XRP و احتمال افزایش قیمت آن نخواهد بود. پس فراموش نکنید ارز XRP، یک دارایی دیجیتال است که توسط شرکتی به نام ریپل ساخته و عرضه شده است. در زمان نگارش این کتاب، این ارز دیجیتال در رده چهارم بازار ارزهای دیجیتال قرار دارد.

ریپل یا به‌طور دقیق‌تر XRP استخراج نمی‌شود. تمام ۱۰۰ میلیارد واحد آن در سال ۲۰۱۳ توسط شرکت ریپل صادر شد. در آن زمان، حدود ۲۰ میلیارد واحد از تمام توکن‌ها

به بنیان‌گذاران این شرکت رسید و ۸۰ درصد باقی‌مانده توسط شرکت در یک سپرده غیرمتمرکز نگهداری شد تا آرام‌آرام به بازار تزریق شود. تقریباً هر ماه یک میلیارد واحد XRP به بازار تزریق می‌شود. ارز دیجیتال XRP روی یک دفتر کل توزیع‌شده به نام «ایکس‌آرپی لجر» منتقل می‌شود و تراکنش‌های این ارز دیجیتال توسط نودهایی که روی این دفتر کل قرار دارند و خود ریپل آنها را انتخاب می‌کند، تأیید می‌شوند. از مزایای XRP می‌توان به سرعت فوق‌العاده بالای تراکنش‌ها و کارمزدهای به‌شدت پایین اشاره کرد. همان‌طور که اشاره شد، در حال حاضر تکمیل‌شدن هر تراکنش ریپل فقط حدود چهار ثانیه طول می‌کشد و می‌توان میلیون‌ها دلار پول را فقط با چند دلار کارمزد انتقال داد. پروتکل ریپل به گونه‌ای است که برای نگهداری آن باید حداقل ۲۰ واحد XRP در کیف پول خود داشته باشید تا امکان انتقال مابقی واحدهای XRP وجود داشته باشد. نباید فراموش کنید که ۲۰ واحد XRP را نمی‌توانید از کیف پول خود خارج کنید.

از موضوعات مهم پیرامون شرکت ریپل و ارز XRP می‌توان به دعوی قانونی آن با کمیسیون بورس و اوراق بهادار[1] ایالات متحده اشاره کرد. شکایت رسمی این سازمان که ریپل را متهم به فروش ثبت‌نشده اوراق بهادار به صورت دارایی‌های دیجیتال می‌کند، در اواخر سال ۲۰۲۰ صورت گرفت و کشمکش دادگاه‌های ریپل از آن زمان همواره بر روی قیمت XRP تاثیر قابل توجهی داشته است.

ریپل در سال ۲۰۱۳ با قیمت هر واحد ۰٫۰۰۵ دلار به صرافی‌ها عرضه شد و در ژانویه ۲۰۱۸ به اوج قیمت خود یعنی ۳٫۸ دلار رسید که نشان‌دهنده بیش از ۷۰ هزار درصد افزایش قیمت است. پس از رسیدن به اوج، قیمت ریپل سقوط بسیار هولناکی داشت و هم‌اکنون، با قیمت هر واحد ۰٫۲۱ دلار معامله می‌شود. با این حال، این ارز دیجیتال همچنان حدود چهار هزار درصد نسبت به قیمت اولیه خود رشد داشته است.

صعود اصلی قیمت ریپل از سال ۲۰۱۷ آغاز شد. اگر در ابتدای ۲۰۱۷ که قیمت هر ریپل ۰٫۰۵ دلار بود، فقط معادل هزار دلار ریپل می‌خریدید، در ژانویه ۲۰۱۸ (با قیمت ۳٫۸ دلار)، یعنی یک سال بعد، سرمایه شما بیش از ۷۰۰ هزار دلار ارزش داشت. این اعداد و ارقام هر کسی را به وجد می‌آورند، اما باید بدانید که این فقط یک روی سکه بود. در روی

1. SEC

دیگر سکه سقوط شدید قیمت ریپل از ۳٫۸ دلار به کمتر از ۰٫۳ دلار قرار دارد که بسیاری از سرمایه‌گذاران تازه‌کار را به خاک سیاه نشاند؛ سرمایه‌گذارانی که به امید صددلاری شدن قیمت ریپل، بخش زیادی از پول‌هایشان را در اوج قیمت سرمایه‌گذاری کردند.

در سال ۲۰۲۱ ریپل برخلاف بسیاری از ارزهای دیجیتال دیگر که موفق به شکستن سقف تاریخی خود شدند، تنها تا محدوده ۲ دلار رشد کرد و به‌دلیل اخبار منفی و مثبت دادگاه‌های مربوط به دعوی قانونی‌اش، اعتماد بخش قابل‌توجهی از سرمایه‌گذارانش را از دست داد.

تتر

تتر با واحد اختصاری USDT، یک ارز دیجیتال باثبات (استیبل کوین[1]) دارای قیمتی همیشه ثابت است. ارزش هر واحد تتر همواره برابر با یک دلار ایالات متحده آمریکاست. این ارز دیجیتال برای معامله‌گران دو کاربرد اصلی دارد:

- در امان ماندن از نوسانات شدید بازار ارزهای دیجیتال؛
- انتقال آسان پول به صرافی‌ها و کیف پول‌ها به‌صورت دلاری.

فرض کنید یک بیت‌کوین با قیمت هشت هزار دلار خریده‌اید. کمی بعد قیمت به ۱۰ هزار دلار می‌رسد. خیلی سریع و آسان بیت‌کوین‌های خود را به تتر تبدیل می‌کنید و ده هزار تتر ذخیره می‌کنید. سپس قیمت بیت‌کوین سقوط می‌کند و به شش هزار دلار می‌رسد، اما ارزش سرمایه شما همچنان هشت هزار دلار است و می‌توانید با آن در قیمت‌های پایین بیت‌کوین بیشتری بخرید. تتر را به‌راحتی می‌توانید در کیف پول‌های دیجیتالی روی موبایل یا کامپیوتر خود یا کیف پول‌های موجود در صرافی‌ها ذخیره کنید و ارسال و دریافت تتر به‌سادگی و سرعت ارسال یک ایمیل است. در واقع همین ویژگی‌ها باعث شده این ارز دیجیتال برای معامله‌گران بسیار محبوب باشد.

شرکت «آیفینکس» مالک تشکیلات تتر و همچنین گرداننده صرافی ارز دیجیتال «بیتفینکس»[2] است. تتر ابتدا رسماً در سال ۲۰۱۴ با نام «رئال‌کوین» (Realcoin) عرضه

1. Stable coin
2. Bitfinex

شد و پس از مدت کوتاهی نام آن تغییر کرد. همچنین این شـرکت در سال ۲۰۱۹ یک ارز دیجیتال باثبات دیگر به نام «تترگولد» عرضه کرد که دارای پشتوانه طلاست.

علت ثابت‌بودن قیمت تتر یک چیز است؛ به ازای هر واحد USDT که تولید می‌شود یک دلار آمریکا در ذخایر بانکی نگهداری شـده که به‌عنوان پشـتوانه ایـن ارز دیجیتال عمل می‌کند. یعنی اگر چهار میلیون واحد USDT به بازار عرضه شده باشد، باید چهار میلیون دلار در خزانه بانک نگهداری شود تا قیمت آن همواره برابر یک دلار بماند. البته بر سر این موضوع در بین جامعه ارزهای دیجیتال شـک و تردید وجود دارد و برخی این ارز دیجیتال را به نداشتن پشتوانه کافی متهم می‌کنند؛ بنابراین بر خلاف اغلب ارزهای دیجیتال، عرضه تتر محدود نیسـت؛ بلکه نسـبت به تقاضای بـازار، واحدهای USDT جدید تولید و عرضه می‌شود.

ارز دیجیتال USDT در ابتدا روی لایه آمنی[1]، بستری روی بلاکچین بیت‌کوین، توزیع شـد، اما اکنون روی بلاکچین‌هایی از جملـه اتریوم، بیت‌کوین‌کش، تـرون و الگورند[2] هم عرضه می‌شود. این یعنی دسترسی به تتر بسیار آسان اسـت و می‌توان آن را روی کیف پول‌های رسمی اتریوم، بیت‌کوین‌کش، ترون و الگورند ذخیره کرد. واحدهای تتر نسبت به نیاز بـازار و در دوره‌های زمانی مختلف از سـوی شـرکت آیفینکس تولیـد و به صرافی بیتفینکـس وارد می‌شـوند و سـپس از آنجـا توسـط معامله‌گران بـه صرافی‌هـای دیگر می‌روند. بنابراین با اینکه تراکنش‌های USDT غیرمتمرکز است و روی بلاکچین‌های بزرگی انجام می‌شود، توزیع واحدهای آن کاملاً متمرکز است و نمی‌توان آن را یک ارز دیجیتال غیرمتمرکز نامید.

بیت‌کوین‌کش

از همان روزهای اول که بیت‌کوین پا به عرصه گذاشت تا همین امروز، سرعت و کارمزد تراکنش‌های آن یکی از چالش‌برانگیزترین بحث‌های این حوزه است. شبکه بیت‌کوین نمی‌تواند در هر ثانیه بیش از هفت تراکنش را پردازش کند و این موضوع کاربرد آن برای

1. Omni
2. Algorand

پرداخت‌های روزمره را تحت تأثیر قرار می‌دهد.

گروهی معتقد هستند که برای حل مشکل کند بودن تراکنش‌ها و کارمزدهای بالا لازم نیست تغییری در بیت‌کوین ایجاد شود و باید از راه‌حل‌های جایگزین (مثل لایتنینگ) استفاده کرد. گروه دیگری عقیده دارند که هدف اصلی بیت‌کوین کاربرد داشتن به‌عنوان پول است و برای رسیدن به این هدف، راه‌حل‌های جایگزین بی‌فایده هستند. بنابراین و طبق نظر گروه دوم، باید ضمن حفظ ذات غیرمتمرکز بیت‌کوین، یکسری از قوانین محدودکننده آن را تغییر داد تا مشکل سرعت و کارمزد تراکنش‌ها حل شود. برخی پیروان تفکر دوم، بیت‌کوین‌کش را از دل بیت‌کوین بیرون کشیدند.

همان‌طور که در صفحات پیشین اشاره کردیم، زمانی که بر سر قوانین یک بلاکچین اختلاف جدی وجود داشته باشد، راه‌حل مناسب هاردفورک است. یعنی گروه مخالف، بلاکچین و ارز دیجیتال جدید خود را می‌سازند و از آن استفاده می‌کنند. بیت‌کوین‌کش مهم‌ترین و بزرگ‌ترین فورک بیت‌کوین است و ارز دیجیتالی است که خودش را به‌عنوان «پول نقد الکترونیکی همتابه‌همتا» معرفی کرده است؛ درست همان چیزی که در عنوان مقاله ابتدایی (وایت‌پیپر) بیت‌کوین آمده بود. کلمه «Cash» در زبان انگلیسی به معنای پول نقد است. به عبارت دیگر بیت‌کوین‌کش می‌خواهد بیت‌کوینی باشد که با افزایش سرعت تراکنش‌ها، بتوان از آن به‌عنوان پول استفاده کرد.

در یکم آگوست ۲۰۱۷، پس از استخراج بلوک شماره ۴۷۸,۵۵۹ یک بلاکچین جدید از بلاکچین بیت‌کوین ایجاد شد و به این ترتیب رسماً بیت‌کوین‌کش متولد شد. در نهایت هر دو گروه تصمیم گرفتند راه خود را به‌صورت جدا از یکدیگر ادامه دهند. بیت‌کوین‌کش نماد جدید BCH را دریافت کرد و کسانی که از قبل بیت‌کوین داشتند، پس از انجام فورک به همان اندازه بیت‌کوین‌کش دریافت کردند. بیت‌کوین‌کش با افزایش سایز بلوک به ۳۲ مگابایت که در بیت‌کوین محدود به یک مگابایت است، امکان پردازش تراکنش‌های بیشتری را فراهم می‌کند.

البته به دور از اختلاف‌نظرات ایدئولوژیک و اندازه بلوک، شباهت‌های زیادی بین بیت‌کوین و بیت‌کوین‌کش وجود دارد. هر دوی این ارزها از مکانیسم اجماع اثبات کار

(PoW) یا همان استخراج (ماینینگ) برای تأیید تراکنش‌ها و تولید سکه‌های جدید استفاده می‌کنند و عرضه کل هر دوی آنها محدود به ۲۱ میلیون واحد است. علاوه بر این، هر دوی این ارزها از تابع هش SHA256 بهره می‌برند. خودِ بیت‌کوین‌کش در نوامبر ۲۰۱۸ به‌دلیل اختلافات بین اعضای اصلی جامعه، فورک شد و بیت‌کوین اس‌وی از آن به وجود آمد.

سولانا

در صورتی که تجربه تعامل با قراردادهای هوشمند را در اتریوم داشته باشید، احتمالا متوجه کارمزد بسیار بالای آن شده‌اید. برای مثال برای انتقال توکن تتر در شبکه اتریوم که با قرارداد هوشمند این توکن با استاندارد ERC-20[1] تعامل برقرار می‌کنید، کارمزد قابل‌توجهی در برداشت از صرافی‌ها یا انتقال به آدرسی دیگر داشته است. کارمزد بالای شبکه اتریوم و چالش‌های مقیاس‌پذیری آن موجب شد تا توسعه‌دهندگان و کاربران برای استفاده از قابلیت قراردادهای هوشمند به سمت پلتفرم‌های دیگری بروند که با وجود کمرنگ بودن جنبه تمرکززدایی در آن‌ها، مقیاس‌پذیری به‌صورت چشم‌گیری بهبود یافته باشد.

در این میان سولانا یکی از پلتفرم‌هایی بود که در سال ۲۰۲۱ با تمرکز روی سرعت بالا و کارمزد پایین تراکنش‌ها موفق شد نام خود را در میان پروژه‌ها و ارزهای دیجیتال مطرح بازار جا بیندازد. استراتژی موفق بازاریابی، حمایت‌های مالی و جذب سرمایه این پروژه نیز به گسترش اکوسیستم آن و پروژه‌های ساخته بر روی این شبکه کمک زیادی کرد.

شبکه سولانا امکان تایید تراکنش‌ها را در کمتر از یک ثانیه فراهم کرده و با پشتیبانی از قراردادهای هوشمند، میزبان توسعه‌دهندگان زیادی است. این شبکه برای امنیت خود از سازوکار اثبات سهام در کنار اثبات تاریخچه[2] استفاده می‌کند. شبکه سولانا بر روی کاغذ امکان انجام بیش از ۵۰ هزار تراکنش در ثانیه را دارد اما در سال ۲۰۲۱ و ابتدای ۲۰۲۲ اختلال در شبکه آن موجب قطعی شبکه به مدت چندین ساعت شد که به اعتبار آن لطمه وارد کرد. مقیاس‌پذیری در این شبکه از طریق بهبودها در لایه اصلی شبکه دنبال می‌شود؛ برخلاف اتریوم یا سایر پروژه‌ها که بر روی بهبود سرعت و کارمزدها در لایه دوم

---

۱. استاندارد ERC-20 امکان ایجاد توکن‌های سفارشی از یک نوع را بر روی شبکه اتریوم ممکن می‌کند.

2. Proof of history

حساب باز کرده‌اند.

ارز دیجیتال سولانا که SOL نام دارد، در سال ۲۰۲۱ از جمله شگفتی‌سازهای بازار بود که ابتدای سال میلادی در حدود ۱ دلار معامله می‌شد و در اواخر سال میلادی با رشد ۲۵ هزار درصدی به حدود ۲۵۰ دلار رسید. در زمان نگارش این کتاب، ارز دیجیتال SOL با کاهش بیش از ۵۰ درصدی نسبت به سقف تاریخی خود در حدود ۱۰۰ دلار معامله می‌شود.

هزاران توکن؛ تفاوت توکن و کوین چیست؟

همان‌طور که در صفحات قبل خواندید، پس از ظهور بیت‌کوین ارزهای دیجیتال دیگری پدید آمدند که یا از کدهای اولیه بیت‌کوین در آنها استفاده شده بود یا اینکه تنها مفهوم ارائه‌شده در بیت‌کوین را گرفته و از آن برای ساخت شبکه مخصوص خود استفاده کرده بودند. تکامل این عرصه با ورود مفاهیم جدیدی همچون قراردادهای هوشمند همراه بود که ارزهای دیجیتال را از فقط پول‌بودن خارج می‌کرد. چند سال پس از ظهور بیت‌کوین، پلتفرم‌هایی مانند اتریوم به وجود آمدند؛ بنابراین حوزه ارزهای دیجیتال به کاربردهایی فراتر از پول گسترش یافت.

واحدهای ارزی بیت‌کوین در شبکه که با نماد BTC شناخته می‌شود، در حوزه ارزهای دیجیتال یک سکه یا همان «کوین» نامیده می‌شوند. این موضوع برای سایر ارزهای دیجیتالی نیز که بلاکچین مخصوص خودشان را دارند، صدق می‌کند. برای نمونه، اتریوم، لایت‌کوین، ریپل و تقریباً تمامی ارزهای دیجیتال شناخته‌شده و مطرح دارای بلاکچین‌های مخصوص و مستقل خودشان هستند که به واحدهای ارزی آنها اصطلاحاً کوین گفته می‌شود. تفاوتی که در میان سکه‌های دیجیتال وجود دارد این است که برخی از آنها مانند لایت‌کوین و دوج‌کوین، از کد اولیه بیت‌کوین استفاده کرده‌اند یا به‌اصطلاح فورکی از بیت‌کوین هستند (مفهوم فورک را در صفحات قبل توضیح داده‌ایم) و برخی دیگر مانند اتریوم، ریپل و... بلاکچین مخصوص خود را با ساختاری کاملاً متفاوت ساخته‌اند. به ارزهای دیجیتال پس از بیت‌کوین، «آلت‌کوین» (به معنای سکه جایگزین) هم گفته می‌شود.

در طرف دیگر، ارزهای دیجیتالی وجود دارند که سکه نیستند و «توکن» نام دارند. این دارایی‌های دیجیتالی، بلاکچین یا همان شبکه مخصوص خود را ندارند و بر بستر یک بلاکچین دیگر ایجاد می‌شوند؛ البته کلمه توکن معنای گسترده‌ای دارد و می‌تواند به هر کالای قابل مبادله‌ای؛ چه در دنیای مجازی و چه واقعی اطلاق شود. توکن‌ها در دنیای ارزهای دیجیتال امکان دریافت کاربرد خاصی از یک پروژه را فراهم می‌کنند که تنها در اکوسیستم مربوط به آن قابل استفاده است.

برای مثال، اگر پروژه‌ای با این هدف کار خود را آغاز کند که بلیت اتوبوس‌های بین‌شهری را تنها با توکن‌های مخصوصی بتوان خریداری کرد، در این صورت کاربرد آن توکن تنها برای خرید بلیت‌ها خواهد بود و نمی‌توان از آن برای خرید غذا از رستوران استفاده کرد. همان‌طور که گفته شد، توکن‌ها بر بستر یک بلاکچین دیگر شکل می‌گیرند. برای نمونه، اتریوم، ترون، ویوز[1] و وی‌چین[2] از جمله پلتفرم‌هایی هستند که با استانداردهای مخصوص خودشان، اجازه ایجاد توکن را می‌دهند. ساخت توکن بسیار ساده‌تر از ایجاد یک پلتفرم است و به همین خاطر تعداد پلتفرم‌هایی که وجود دارند، از تعداد توکن‌ها بسیار کمتر است.

پروژه‌هایی که قصد توسعه یک بلاکچین را دارند، معمولاً ابتدا از یک بلاکچین واسطه برای خود توکن ایجاد کرده و اقدام به برگزاری پیش‌فروش می‌کنند. پس از جمع‌آوری سرمایه، به سرمایه‌گذاران‌شان تعداد توکن‌هایی که خریداری کرده‌اند را می‌دهند. ارزش این توکن‌ها رابطه مستقیمی با وضعیت پروژه و حرکت آن در راستای اهدافش خواهد داشت. همچنین، برخی توکن‌ها پس از اینکه به حد کافی توسعه پیدا کردند، به‌دنبال ایجاد بلاکچین اختصاصی خودشان می‌روند و به کوین تبدیل می‌شوند.

1. Waves
2. Vechain

فصل چهارم

بلاکچین

احتمالاً شما هم جزء کسانی هستید که بیشتر درباره بیت‌کوین شنیده‌اند تا بلاکچین. بسیاری از کسانی که کلمه بلاکچین به گوش‌شان خورده، برداشت غلطی از آن پیدا کرده‌اند. قبل از اینکه بگوییم بلاکچین چیست، باید بدانید که بیت‌کوین موفق‌ترین کاربرد این فناوری است، اما می‌تواند در زمینه‌های دیگر هم کاربردهای فوق‌العاده‌ای داشته باشد. بلاکچین مانند اینترنت یکی از فناوری‌های ساختارشکن و متحول‌کننده‌ای است که می‌تواند در آینده زندگی همه ما را تغییر دهد.

در این فصل به بلاکچین، دلیل اهمیت آن، چگونگی کارکرد آن و تأثیر این فناوری در آینده می‌پردازیم.

بلاکچین چیست و چگونه کار می‌کند؟

همان‌طور که در صفحات قبل هم اشاره شد، به‌طور کلی، بلاکچین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با سیستم‌های دیگر این است که اطلاعات ذخیره‌شده روی این نوع سیستم، میان همه اعضای شبکه به اشتراک گذاشته می‌شود و با توجه به تکنیک‌های رمزنگاری، امکان حذف و دست‌کاری اطلاعات ثبت‌شده روی بلاکچین عمومی تقریباً غیرممکن است. مفهوم بلاکچین اولین‌بار با پیدایش بیت‌کوین به وجود آمد و پادشاه ارزهای دیجیتال از این راهکار برای ذخیره اطلاعات مربوط به دارایی کاربران بهره برد. برای درک بهتر بلاکچین به مثال زیر توجه کنید:

در یک جمع یکصد نفری، برگه‌ای حاوی یکسری اطلاعات را بالا می‌گیریم و همه با تلفن همراه‌شان از آن برگه عکس می‌گیرند. حالا اگر آن اطلاعات را نابود کنیم یا تغییری در آن بدهیم، دیگر برای آن جمع قابل‌پذیرش نیست، چون آنها یک کپی از نسخه اصلی را دارند، مگر اینکه موبایل همه را بگیریم و آن عکس را حذف کنیم. این جمعی که از آن صحبت کردیم، می‌تواند چندین هزار نفر باشد که در بیت‌کوین، اتریوم و سایر ارزهای بلاکچینی شاهد آن هستیم، یا به‌صورت خصوصی در یک گروه خاص مورد استفاده قرار بگیرد.

علاوه بر بلاکچین‌های عمومی مانند بیت‌کوین و اتریوم، بلاکچین‌ها می‌توانند به‌صورت خصوصی و برای اهداف خاص در یک نهاد یا سازمان هم مورد استفاده قرار بگیرند که به

آن «بلاکچین سازمانی» می‌گویند. البته به عقیده بسیاری از صاحب‌نظران، بلاکچین‌های سازمانی نمی‌توانند هدف اصلی این فناوری، یعنی تمرکززدایی را محقق کنند.

بنابراین، بلاکچین به‌طور کلی نوعی پایگاه داده (دیتابیس) است که برای ثبت داده بدون امکان دست‌کاری یا تغییر، مورد استفاده قرار می‌گیرد. در واقع، بلاکچین یکی از بهترین راهکارهای موجود برای پیاده‌سازی «دفتر کل توزیع‌شده» است. قبل از پرداختن به جزئیات بیشتر، باید بدانید یک دفتر کل توزیع‌شده چیست.

در علم حسابداری، دفتر کل به محلی گفته می‌شود که در آن اطلاعات مالی از قبیل حساب‌ها، بدهی‌ها، اعتبارات و... مکتوب می‌شوند تا در زمان مشخص بتوان از آنها برای رسیدگی به امور استفاده کرد. در میان مردم به دفتر کل، دفتر حساب‌وکتاب هم گفته می‌شود. انسان‌ها هزاران هزار سال است که از دفتر کل‌ها به شکل‌های مختلف استفاده می‌کنند و مفهوم دفتر کل قدمتی به اندازه خود تاریخ دارد. خوب است بدانید یکی از دلایل اساسی اختراع خط، نوشتن حساب‌های مالی و معاملات افراد روی لوح‌های سنگی بود که نقش دفتر کل را ایفا می‌کردند. با توجه به حافظه نامناسب انسان‌ها در به‌یادسپاری طولانی‌مدت داده‌ها، دفتر کل‌ها به جزء جدایی‌ناپذیری از زندگی ما تبدیل شده‌اند. دولت‌ها، بانک‌ها، مراکز اداری و هر جا که فکرش را بکنید، به‌نوعی از دفتر کل‌ها استفاده می‌کنند.

پس از هزاران سال استفاده از لوح‌های گلی، پاپیروس و به‌خصوص کاغذ، در دهه‌های ۸۰ و ۹۰ میلادی با ظهور اینترنت و توسعه کامپیوترها، سندهای دیجیتال به‌تدریج به‌عنوان جایگزینی عالی برای پرونده‌های کاغذی مطرح شدند. در ابتدا پایگاه‌های داده اولیه، فهرست‌بندی و حسابداری دنیای کاغذی را تقلید می‌کردند و می‌توان گفت که دیجیتالی‌کردن آنها نیاز به وقت و انرژی بیشتری نسبت به نمونه‌های کاغذی داشت، اما با گسترش زیرساخت‌ها، دیگر استفاده از دفتر کل‌های کاغذی خیلی منطقی به نظر نمی‌رسد، اگرچه عناصر کاغذی ستون‌فقرات جامعه ما هستند؛ پول، مهر و موم، امضای کتبی، صورت‌حساب، گواهی‌نامه و حساب‌وکتاب‌های دفتری.

امروزه ذخیره دفتر کل روی فضاهای کامپیوتری بسیار مرسوم است و روزبه‌روز شاهد از بین رفتن دفترهای سنتی هستیم. صفحات اکسل و پایگاه‌های داده کامپیوتری، در عصر

اینترنت نقشی غیرقابل انکار در جامعه انسانی دارند.

در ابتدایی‌ترین سطح، پایگاه‌های داده در یک کامپیوتر مرکزی ذخیره می‌شدند و سایر افرادی که قصد داشتند داده‌ای به آن اضافه کنند، مجبور بودند به همین یک کامپیوتر یا سرور متصل شوند که از نظر امنیت و دسترسی به اطلاعات عملکرد بسیار نامناسبی داشت. یک نفر به کل پایگاه داده دسترسی داشت و می‌توانست آن را از بین ببرد یا اطلاعات ثبت‌شده در آن را تغییر دهد. همچنین، در صورت وقوع مشکل برای کامپیوتر مرکزی، تمام اطلاعات به خطر می‌افتاد. راه‌حل چه بود؟ استفاده از دفتر کل‌های توزیع‌شده.

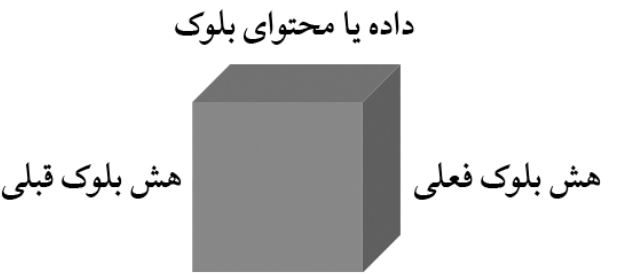
رشد قدرت محاسبات و توسعه رمزنگاری، همراه با کشف و استفاده از الگوریتم‌های جدید، پدید آمدن مفهومی به نام دفتر کل توزیع‌شده را رقم زد. در ساده‌ترین توضیح، یک دفتر کل توزیع‌شده، پایگاه داده‌ای است که اطلاعات ثبت‌شده روی آن، توسط چندین کامپیوتر یا نود نگهداری می‌شود که امنیت اطلاعات را تا حد زیادی افزایش می‌دهد. به این ترتیب، ویژگی متمایزکننده یک دفتر کل توزیع‌شده این است که نقطه شکست یکتا ندارد؛ یعنی اطلاعات روی چند کامپیوتر در مکان‌های مختلف ذخیره می‌شود و مهاجم تنها با حمله به یک کامپیوتر نمی‌تواند اطلاعات ذخیره‌شده را از بین ببرد. این معماری اجازه می‌دهد تا به‌عنوان یک سیستم تهیه گزارش، دفتر کل توزیع‌شده فراتر از یک پایگاه داده ساده باشد.

این جمله را خوب به یاد داشته باشید؛ بلاکچین نوعی دفتر کل توزیع‌شده است، اما هر دفتر کل توزیع‌شده‌ای بلاکچین نیست. در واقع در بلاکچین با مفهومی به نام «بلوک» سروکار داریم، اما به‌جز بلاکچین دفاتر کل توزیع‌شده زیادی وجود دارند که در آنها بلوکی تعریف نشده است.

در مفهوم بلاکچین، داده درون جعبه‌هایی مجازی به نام بلوک ثبت می‌شود. این بلوک به بلوک قبلی می‌پیوندد و جمع این بلوک‌ها، بلاکچین (زنجیره بلوکی) را تشکیل می‌دهند. بلاکچین باعث می‌شود که دفتر کل بتواند ضمن توزیع‌شده بودن، تا حد زیادی غیرمتمرکز و غیرقابل تغییر هم باشد. حالا که کمی با مفهوم اولیه بلاکچین آشنا شدید، از نظر فنی هم این فناوری را بررسی می‌کنیم.

در بلاکچین هر بلوک شامل سه جزء اساسی است:

- **داده:** هر چیزی می‌تواند باشد. برای مثال، در بیت‌کوین داده‌های یک بلوک شامل تاریخچه تراکنش‌های شبکه است؛ اطلاعاتی که آدرس گیرنده، فرستنده، تعداد سکه‌های ارسال‌شده و مواردی از این دست را دربر می‌گیرد.
- **هَش:** نمی‌خواهیم درباره ماهیت تابع هش و اینکه دقیقاً چگونه کار می‌کند، صحبت کنیم، اما به‌طور کلی، هش در بلاکچین چیزی مانند اثرانگشت یا یک امضای منحصربه‌فرد است که به‌تنهایی نماینده تمام محتویات بلوک است. اگر داده داخل بلوک کوچک‌ترین تغییری کند، هش بلوک هم کاملاً تغییر کرده و بلوک را کاملاً غیرمعتبر می‌کند.
- **هش بلوک قبلی:** این بخش در واقع موجب تشکیل یک زنجیره می‌شود و بلوک‌ها را به یکدیگر مرتبط می‌کند. از آنجایی که هر هش محتوای اطلاعات بلوک خود را حمل می‌کند، وجود هش بلوک قبلی، داده‌های قبلی را به داده‌های فعلی ربط می‌دهد و همین هم موجب می‌شود تغییر دادن اطلاعات گذشته غیرممکن شود. بنابراین، وجود هش بلوک قبلی باعث می‌شود تا اگر یک بلوک را تغییر دهیم، بلوک‌های دیگر نامعتبر شوند.



شکل ۱-۴: ساختار یک بلوک در بلاکچین

برای درک بهتر این مفاهیم، آن را با مثالی توضیح می‌دهیم. یک بلاکچین را در نظر

بگیرید که دارای سه بلوک است:

بلوک شماره ۱:

داده: عارف ۱۰ بیت‌کوین برای امیر فرستاده است.

هش: 11A

هش بلوک قبلی: 2R3

بلوک شماره ۲:

داده: امیر ۵ بیت‌کوین برای بهزاد فرستاده است.

هش: 4TD

هش بلوک قبلی: 11A

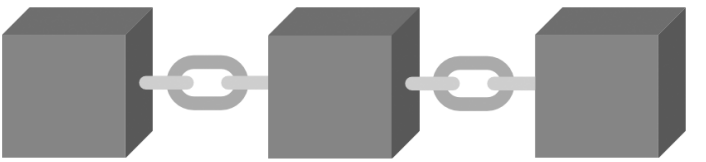
بلوک شماره ۳:

داده: بهزاد ۳ بیت‌کوین برای مجید فرستاده است.

هش: GBF

هش بلوک قبلی: 4TD

همان‌طور که در این مثال نیز مشاهده می‌کنید، هر بلوک شامل هش خود و هش بلوک قبلی است. پس بلوک ۳ به بلوک ۲ و همین‌طور بلوک ۲ به بلوک ۱ متصل می‌شود. شایان ذکر است اولین بلوک که آن را بلوک پیدایش می‌خوانیم، از جهتی ویژه است؛ چراکه به هیچ بلوک قبلی اشاره نمی‌کند.



شکل ۲-۴: ساختار یک بلاکچین بسیار ساده

اگرچه امنیت داده در بلاکچین به‌شدت بالاتر از سیستم‌های متمرکز است، اما از نظر

تئوری، اطلاعات یک بلاکچین هم می‌تواند دست‌کاری شود. به سراغ امنیت بلاکچین‌ها و نحوه در امان‌ماندن آنها از هک و دست‌کاری برویم.

امنیت بلاکچین

دست‌کاری یک بلاکچین عمومی و بزرگ مانند بیت‌کوین تقریباً محال است. بلاکچین‌ها در گام اول امنیت خود را از طریق رمزنگاری و هش تأمین می‌کنند. در صورتی که بخواهید اطلاعات بلوکی را در زنجیره تغییر دهید، اطلاعات بلوک بعدی اعتبار خود را از دست می‌دهد؛ چراکه در هر بلوک به اطلاعات بلوک قبل از خودش اشاره شده است. در واقع تغییر یک بلوک، تمامی بلوک‌های پس از خود را غیرمعتبر می‌کند.

اما باید به خاطر داشته باشید که هش‌کردن به‌تنهایی نمی‌تواند امنیت را تأمین کرده و بلاکچین را از دست‌کاری مصون نگه دارد. امروزه دستگاه‌های محاسباتی پیشرفت زیادی کرده‌اند و میلیون‌ها هش را در ثانیه محاسبه می‌کنند. از نظر فنی، یک مهاجم می‌تواند هش بلوک خاصی را تغییر داده و هش تمامی بلوک‌های پس از آن را نیز محاسبه کرده و بلاکچین را دست‌کاری کند. به همین دلیل، علاوه بر هش‌کردن، لایه امنیتی دیگری به نام «اجماع» در بلاکچین وجود دارد. اجماع یعنی اینکه هر کسی اجازه ندارد همین‌طور برای خودش بلوک ایجاد کند؛ بلکه برای ایجاد بلوک ابتدا باید حسن‌نیت خود را به بلاکچین اثبات کند. یکی از چندین نوع اجماع، اثبات کار یا همان ماینینگ است که در بیت‌کوین و بسیاری از ارزهای دیجیتال دیگر با آن سروکار داریم. همان‌گونه در فصل‌های پیشین گفتیم، اثبات کار سازوکاری است که افراد را ملزم می‌کند برای ایجاد بلوک‌های جدید و افزودن آنها به زنجیره، یک معمای ریاضی پیچیده را حل کنند. با این مکانیسم، امکان دست‌کاری بلاکچین دشوارتر از چیزی می‌شود که فکرش را می‌کنید.

همچنین همان‌طور که اشاره شد، بلاکچین یک فناوری توزیع‌شده است. به‌عنوان نمونه، در بیت‌کوین، هر کسی می‌تواند عضو شود. هر عضو شبکه یک اعتبارسنج یا نود نامیده می‌شود و یک کپی از کل بلاکچین و تمامی اطلاعات را در اختیار دارد. از این رو، یک نود می‌تواند درستی اطلاعاتی که بعداً دریافت می‌کند را تأیید یا رد کند.

زمانی که یک بلوک در شبکه ایجاد می‌شود، مراحل زیر به ترتیب انجام می‌شود:

۱. بلوک جدید به تمامی مشارکت‌کنندگان یا نودها در شبکه ارسال می‌شود.
۲. هر نود بلوک را تأیید کرده و از اشتباه‌نبودن آن اطمینان حاصل می‌کند.
۳. زمانی که همه این کار را انجام دادند، هر نود بلوک جدید را به زنجیره خود اضافه می‌کند.

پس در نتیجه باید بگوییم که اگر می‌خواهید اطلاعات بلاکچین را تغییر دهید، اولاً باید تمامی بلوک‌های پس از آن را در زنجیره تغییر دهید، اثبات کار را برای هر بلوک به‌طور جداگانه انجام دهید و کنترل شرکت‌کنندگان شبکه همتابه‌همتا را به دست بگیرید. این کار در بلاکچین‌های بزرگی مانند بیت‌کوین تقریباً غیرممکن است.

اما در مورد بلاکچین‌های خصوصی یا کوچک بااطمینان کامل نمی‌توان از غیرقابل دست‌کاری‌بودن بلاکچین سخن گفت. برای مثال، تاکنون چند ارز دیجیتال نه‌چندان مطرح تحت حملاتی موسوم به «حمله ۵۱ درصدی» قرار گرفته‌اند. در این نوع حملات، فرد مهاجم با در اختیار گرفتن بیش از ۵۰ درصد از حق رأی (مانند ۵۱ درصد قدرت پردازش در شبکه‌های مبتنی بر ماینینگ)، بلاکچین را بازنویسی و اطلاعات جدید را به‌دلخواه میان اعضای شبکه مخابره می‌کند.

برای درک بهتر، فرض کنیم فردی به نام سامان فایلی را در ازای مقداری ارز دیجیتال خریداری می‌کند. فروشنده تراکنش را بررسی می‌کند و می‌بینید که یک تأیید خورده است (در یک بلوک جای گرفته است). او فایل را به سامان می‌دهد، اما به‌دلیل اینکه تراکنش فعلاً فقط در یک بلوک ثبت شده است، اگر سامان بتواند بیش از ۵۰ درصد از قدرت پردازش شبکه را از آن خود کند، می‌تواند زنجیره بلاکچین را بازنویسی کند و ارز دیجیتال خود را برگرداند. البته باید تأکید کنیم در شبکه‌های بزرگی همچون بیت‌کوین و اتریوم، به‌دلیل قدرت پردازش بسیار زیاد، احتمال انجام حمله نزدیک به صفر است، اما در شبکه‌هایی مانند اتریوم کلاسیک و بیت‌کوین‌گولد بارها این اتفاق افتاده است.

چرا بلاکچین یک فناوری انقلابی است؟

به سه دلیل عمده بلاکچین یک فناوری انقلابی است.

بی‌نیاز کردن از اعتماد

فناوری منحصربه‌فرد بلاکچین موجب می‌شود در داده‌ها و اطلاعات اطمینان واقعی برقرار شود. با بلاکچین دیگر نیازی نیست کورکورانه به واسطه‌ها اعتماد کنیم.

به‌عنوان یک نمونه بارز، در بیت‌کوین قبل از اینکه یک بلوک به زنجیره اضافه شود، چند اتفاق مختلف باید به وقوع بپیوندد:

۱. دستگاه‌های محاسباتی که تحت اختیار عده‌ای از مشارکت‌کنندگان شبکه یا همان استخراج‌کنندگان هستند، باید یک معمای پیچیده ریاضی را حل کنند.

۲. استخراج‌کننده‌ای که زودتر از همه به جواب می‌رسد، پاسخ خود را با سایر استخراج‌کنندگان به اشتراک می‌گذارد. این مدل اثبات کار نام دارد که پیش‌تر در مورد آن توضیح دادیم.

۳. در نهایت، مشارکت‌کنندگان شبکه پاسخ به‌دست‌آمده را تأیید کرده و از آنجا که تأیید این پاسخ به معنی تأیید اطلاعات یک بلوک است، آن بلوک را به زنجیره و بلاکچین خود اضافه می‌کنند.

به‌دلیل اینکه هر مشارکت‌کننده در شبکه پاسخ را با زنجیره خود مقایسه می‌کند، آنها می‌توانند به هر بلوکی که به شبکه اضافه می‌شود، اعتماد کنند. اگر بخواهیم خیلی خلاصه بگوییم، فناوری بلاکچین سبب «اعتماد در فضای عاری از اعتماد» می‌شود.

صرفه‌جویی چشم‌گیر در وقت و هزینه

مشکلی که طرف‌های سوم و واسطه‌های متمرکز مانند وکلا و بانک‌ها دارند، این است که یک مرحله اضافه برای حل مشکل اضافه می‌کنند و در بسیاری از فرایندها خود به مشکل تبدیل می‌شوند. در واقع با ظهور بلاکچین آنها مانعی اضافه هستند که موجب صرف وقت، هزینه و همچنین اعتماد ما می‌شوند. این شیوه تبادل همتابه‌همتا و مورد اعتماد می‌تواند به انقلابی در میان مبادلات غریبه‌ها با یکدیگر منتهی شود.

شفافیت

شفافیت می‌تواند یکی از بزرگ‌ترین مزایای سیستم‌های بلاکچینی باشد. در

بیت‌کوین همه می‌توانند تاریخچه تراکنش‌های شبکه، وضعیت شبکه و میزان بیت‌کوین‌های استخراج‌شده را ببینند. در مقایسه با پول‌های رایج و دارایی‌های دیگر، این یک ویژگی انقلابی است. چقدر طلا در جهان وجود دارد؟ چقدر پول از سوی دولت‌ها چاپ شده است؟ هر کس چیزی می‌گوید و ما ناچاریم به ارقامی که بانک‌ها و نهادهای متمرکز (آن هم اگر مایل به انتشار ارقام باشند) اعتماد کنیم، اما در بیت‌کوین نیازی به اعتماد نیست. هر کسی که به شبکه بیت‌کوین متصل شود، خودش می‌تواند وضعیت شبکه را رصد کند.

خارج از فضای پول هم بلاکچین می‌تواند در شفافیت نقش اساسی داشته باشد. آیا این غذا سالم است؟ این محصول از مواد اولیه مرغوب تولید شده است؟ آیا این کالا اصالت دارد؟ اینها مسائلی هستند که با بلاکچین می‌توان به آنها پاسخ داد. از این فناوری می‌شود برای رهگیری و سنجش زنجیره تأمین بهره برد. مراحل برداشت و تولید محصول از ابتدا تا لحظه رسیدن به دست مشتری روی بلاکچین ثبت شده و مشتری می‌تواند با اسکن یک کد کیوآر از اصالت و کیفیت محصول مطمئن شود. امروزه شرکت‌های زیادی به‌خصوص در صنایع غذایی از بلاکچین برای رهگیری محصولات‌شان استفاده می‌کنند تا هم خیال خودشان و هم مشتریان‌شان از کیفیت محصول راحت باشد. همچنین، در حوزه سیاست مدت‌هاست که بحث برگزاری انتخابات با بلاکچین نقل محافل است. البته در بلاکچین‌های حریم‌خصوصی محوری مانند مونرو[1]، شفافیت برای حفظ حریم‌خصوصی تراکنش‌ها با تکنیک‌های رمزنگاری کاهش یافته و اطلاعاتی مانند مقادیر جابه‌جاشده یا گیرنده و فرستنده تراکنش‌ها مخفی باقی مانده است. در ادامه بیشتر در مورد کاربردهای بلاکچین می‌خوانید.

مشکلات بلاکچین

بلاکچینی که تا به اینجای کتاب برایتان توصیف کردیم، شگفت‌آور و دوست‌داشتنی بود، اما وجود برخی اشکالات باعث شده تا کاربردی‌شدن این فناوری و استفاده روزمره از آن به تأخیر بیفتد. در این قسمت برخی از موانعی که سد راه موفقیت فراگیر و پذیرش گسترده بلاکچین شده را توضیح می‌دهیم.

1. Monero

مقیاس‌پذیری

مشکل مقیاس‌پذیری، به معنای مشکل کندبودن و پرهزینه‌بودن تراکنش‌ها، احتمالاً یکی از اساسی‌ترین چالش‌هایی است که فناوری بلاکچین با آن روبه‌روست. تعریف ساده مقیاس‌پذیری عبارت است از توانایی سیستم برای پاسخگویی بدون مشکل به افزایش میزان بار کاری. برای مثال، یک خیابان گنجایش مقدار مشخصی از خودرو را دارد و در صورتی که تعداد خودرو در آن خیابان از این مقدار مشخص بیشتر باشد، ترافیک به وجود می‌آید. توانایی بلاکچین‌ها نیز اغلب با مقدار تراکنش‌هایی که در هر ثانیه می‌توانند پردازش کنند، نشان داده می‌شود.

در ابتدای فصل درباره چگونگی تأمین امنیت در بلاکچین و روش‌های مقابله آن با هکرها صحبت شد، اما این امنیت هزینه‌ای هم برای کاربران داشته است. تراکنش‌های بلاکچین کند و گاهی اوقات گران تمام می‌شود. به‌عنوان نمونه، شبکه بیت‌کوین حداکثر می‌تواند هفت تراکنش را در ثانیه انجام دهد. این نقطه‌ضعفی است که شبکه بیت‌کوین با آن مواجه است. البته همین ویژگی نیز باعث شده تا امنیت و تمرکززدایی بیت‌کوین به‌شدت بالا باشد. نمی‌توان تصور کرد که بیشتر مردم از بیت‌کوین استفاده کنند و با این شرایط شبکه بیت‌کوین قادر به پاسخگویی به همه آنها باشد.

خوشبختانه راهکارهایی برای حل مشکلات در دست توسعه است. اولین راه‌حلی که برای حل این مشکل می‌توان ارائه داد، افزایش ظرفیت بلوک‌های داده است تا تراکنش‌های بیشتری دریافت کنند.

گنجایش هر بلوک بیت‌کوین در شرایط فعلی یک مگابایت است که با دوبرابر کردن آن، میزان تراکنش‌های قابل پردازش نیز در هر ثانیه دوبرابر می‌شود، اما این راهکار به خودی خود می‌تواند مشکل جدیدی برای شبکه باشد. این کار با افزایش حجم بلاکچین و سخت‌کردن اجرای نود، می‌تواند موجب تمرکز بیشتر شود. این مسئله همچنین امکان مشارکت در شبکه را از بیشتر افراد می‌گیرد و شبکه را با خطر انحصار روبه‌رو می‌کند. راهکارهای دیگری نیز برای حل مشکل مقیاس‌پذیری بلاکچین‌ها ارائه شده که در ادامه به آنها می‌پردازیم.

شبکه صاعقه

شبکه صاعقه یا لایتنینگ یک لایه جدید روی شبکه اصلی بیت‌کوین ایجاد می‌کند که از طریق آن می‌توان تراکنش‌های آنی و تقریباً بدون کارمزد را با بیت‌کوین انجام داد. کاربران می‌توانند با ایجاد کانال‌هایی در شبکه صاعقه بین یکدیگر بیت‌کوین انتقال دهند، بدون آنکه لازم باشد هر تراکنش توسط استخراج‌کنندگان بیت‌کوین تأیید شود. به عبارت دیگر، با لایتنینگ افراد دیگر فقط برای تراکنش‌های سنگین (آنهایی که پرداخت کارمزد برایشان صرفه دارد) از شبکه اصلی بیت‌کوین استفاده می‌کنند. در این راه‌حل سعی شده که تا حد امکان تمرکززدایی حفظ شود.

شاردینگ

شاردینگ هم راهکار دیگری است که برای حل مشکلات مقیاس‌پذیری بلاکچین ارائه شده و قرار است در اتریوم پیاده‌سازی شود. به‌طور خلاصه، شاردینگ در ارزهای دیجیتال به این معناست که شبکه به بخش‌های کوچکی به نام «شارد» تقسیم می‌شود. در این ایده تراکنش‌های کاربران به جای تأییدشدن توسط کل شبکه، به دست یکسری نودهای تصادفی تأیید می‌شوند. نودهای کمتر در هر شارد می‌توانند اطلاعات را سریع‌تر پردازش کنند و توزیع تصادفی نودها امکان دست‌کاری را از بین می‌برد.

با نگاه به راهکارهای ارائه‌شده، سرمایه‌گذاران می‌توانند امید داشته باشند که مسئله مقیاس‌پذیری بلاکچین‌ها در آینده نزدیک حل خواهد شد.

مشکلات زیست‌محیطی

تأمین امنیت بلاکچین که پیش‌تر درباره آن صحبت شد، مشکلات دیگری نیز به همراه دارد؛ مصرف انرژی و آسیب به محیط زیست در ارزهای دیجیتال مبتنی بر ماینینگ.

در شبکه‌های مبتنی بر استخراج، با افزایش تعداد استخراج‌کنندگان، انرژی مصرفی شبکه هم افزایش می‌یابد. طبق برآوردها، انرژی مصرفی شبکه بیت‌کوین در حال حاضر با انرژی مصرفی کل کشور یونان برابری می‌کند. البته با تکامل دنیای ارزهای دیجیتال و بلاکچین، سخت‌افزارهای بهینه‌تری با مصرف انرژی کمتر معرفی خواهد

شد. از طرف دیگر، بیشتر صاحب‌نظران نه‌تنها ماینینگ را مشکلی برای محیط‌زیست نمی‌دانند؛ بلکه معتقدند که این فعالیت به گسترش استفاده از انرژی‌های تجدیدپذیر کمک می‌کند. در حال حاضر ۶۰ درصد برق مورد استفاده برای استخراج بیت‌کوین در جهان با استفاده از انرژی آبی تأمین می‌شود. استفاده از انرژی‌های تجدیدپذیر به جای سوخت‌های فسیلی و زغال‌سنگ فقط زمانی صرفه اقتصادی دارد که همراه با مصرف، ثروتی تولید شود که هزینه‌ها را جبران کند و ماینینگ بیت‌کوین این ثروت را تولید می‌کند.

معضل کلاهبرداری

صنعت بلاکچین و ارزهای دیجیتال، روندهای هیجانی زیادی به خود دیده است. برخی سودجویان نیز این فرصت را غنیمت شمرده‌اند تا از آن برای کلاهبرداری و سودجویی از دیگران بهره ببرند. امروزه پروژه‌های کلاهبرداری زیادی وجود دارد که با استفاده از واژه‌هایی مانند ارز دیجیتال، قرارداد هوشمند و بلاکچین، برای جیب‌های مردم کیسه دوخته‌اند. بازار این کلاهبرداری‌ها نیز زمانی که قیمت‌ها روند صعودی به خود می‌گیرند، بیش از پیش رونق پیدا می‌کند. طرح‌های پانزی[۱] و هرمی با وعده سودهای نجومی (برای مثال استفاده از واژه‌های سود قطعی یا مثلاً سود تضمینی پنج درصد ماهانه) و کلاهبرداری موسوم به «در رو»[۲] از مهم‌ترین کلاهبرداری‌هایی هستند که در حوزه ارزهای دیجیتال و بلاکچین شاهد آن هستیم.

کلاهبرداران معمولاً با استفاده از واژه‌های نامأنوس، ذهن مشتری را درگیر می‌کنند و با پیشنهادهای اغواکننده آنها را در دامی که برایشان پهن کرده‌اند می‌اندازند. مهمترین کاری که سرمایه‌گذاران باید انجام دهند، جست‌وجوی نام پروژه در منابع فارسی و انگلیسی، آشنایی با ویژگی طرح‌های پانزی و سوال‌کردن از دیگران در انجمن‌های معتبر است.

---

۱. طرح پانزی (Ponzi scheme) نوعی طرح کلاهبرداری است که در آن به سرمایه‌گذاران وعده سودهای نجومی داده می‌شود، اما در آن هیچ فعالیت اقتصادی انجام نمی‌شود. در حقیقت سود سرمایه‌گذاران قدیمی از سرمایه سرمایه‌گذاران جدید پرداخت می‌شود. زمانی که مقدار زیادی پول جمع‌آوری شد، طراح فرار می‌کند و طرح از هم می‌پاشد.

۲. Exit scam: دریافت پول و عدم تحویل کالا یا خدمات

مشکلات سیاسی و قانون‌گذاری

همان‌طور که در بحث‌های قبلی اشاره کردیم، بلاکچین و ارزهای دیجیتال در پی حذف واسطه‌ها هستند. با وجود اینکه حذف واسطه یک مزیت بوده و می‌تواند به کاهش هزینه‌ها و صرفه‌جویی در زمان منجر شود، اما همین واسطه‌ها می‌توانند موانع بزرگی بر سر راه پیشرفت بلاکچین و ارزهای دیجیتال ایجاد کنند. اگر نگاهی به بانک‌ها، کارگزاری‌ها و بسیاری از این واسطه‌ها بیندازیم، با غول‌های بزرگی در صنایع مختلف مواجه خواهیم شد که سروکله‌زدن با آنها جرئت و قدرت زیادی می‌طلبد. تمامی آنها از واسطه‌بودن سود زیادی به جیب می‌زنند و مختل‌کردن کسب‌وکارشان قطعاً آنها را عصبانی خواهد کرد. در بسیاری از کشورها مؤسسات مالی و بانک‌ها نقش قابل توجهی در تصمیم‌گیری دولت‌ها و قانون‌گذاران ایفا می‌کنند، اما قدرت مردم را هم نباید دست‌کم گرفت. از این جهت بسیاری ظهور فناوری بلاکچین و ارزهای دیجیتال را آغاز نبردی میان واسطه‌ها و مردم می‌دانند که با افزایش آگاهی افراد از این پدیده، کار بانک‌ها و مؤسسات مالی در این نبرد سخت‌تر خواهد شد.

کاربردهای بلاکچین

فناوری بلاکچین چند سال پس از پیدایش بیت‌کوین، توجه شرکت‌ها و سرمایه‌گذاران را به خود جلب کرد. موفقیت بیت‌کوین با بلاکچین باعث شد جریانی برای استفاده از این فناوری در سایر حوزه‌ها شکل بگیرد. اگر فرایند انتقال پول می‌تواند بدون واسطه انجام شود، پس می‌توان برای تمرکززدایی در سایر فرایندهایی هم که در آنها نیاز به اعتماد وجود دارد، تلاش کرد.

رأی‌گیری و انتخابات

یکی از مسائل اساسی جوامع انسانی، عدم شفافیت در رأی‌گیری‌ها و انتخابات است که خطر تقلب و پایمال‌شدن حقوق فردی را افزایش می‌دهد. رأی‌گیری و انتخابات یکی از حوزه‌های مهمی است که می‌تواند پذیرای بلاکچین باشد. یک فرایند رأی‌گیری با شفافیت کافی می‌تواند امکان تقلب و تغییر آرای مردمی را خنثی کرده و از بین ببرد.

پیاده‌سازی انتخابات بلاکچینی هرچند در حال حاضر با مشکلات و ابهامات بنیادینی روبه‌روست، اما در صورت وقوع می‌تواند نقطه‌عطفی برای آینده باشد.

نظارت بر زنجیره تأمین

تولیدکنندگان همیشه با چالش اعتماد مصرف‌کنندگان روبه‌رو هستند. آیا جنسی که می‌خرید، اصالت دارد؟ آیا از کشور برند می‌آید یا ساخت چین است؟ آیا می‌خواهید بدانید غذایی که در حال میل آن هستید، از کجا و به چه طریقی تهیه شده است؟ آیا این ماده غذایی ارگانیک بوده و اینکه حلال است یا خیر؟ با کمک فناوری بلاکچین می‌توان تمام فرایند تولید تا رسیدن کالا به دست مشتری را رهگیری کرد. استفاده از بلاکچین می‌تواند هم به نفع مشتریان باشد و هم با افزایش اعتماد مصرف‌کنندگان، به تولیدکنندگان در افزایش اعتبار و بهره‌وری کمک کند.

تأیید هویت

بلاکچین می‌تواند گام بزرگی در ایجاد هویت دیجیتالی و اعتبارسنجی اطلاعات هویتی افراد به‌صورت امن بردارد. مراکز اعتبارسنجی و شبکه‌های اجتماعی مانند فیس‌بوک و اینستاگرام در دنیای امروز، نگهبانان دروازه‌ای هستند که بر سر مسیر ارتباط هویت مجازی و فیزیکی ما قرار گرفته است. در همین حال، مصرف‌کنندگان نیز به‌دنبال سیستم‌های امنی هستند که اطلاعات خود را در اختیار آنها قرار دهند تا امکان استفاده از خدمات و سرویس‌های مختلف در دنیای مجازی را پیدا کنند. برای فائق آمدن بر این چالش، شرکت‌های بسیاری در حال استفاده از فناوری بلاکچین برای ساخت سیستم تأیید هویت دیجیتالی هستند.

حق مالکیت

ممکن است هنگام خرید زمین و خانه به مشکلات حقوقی زیادی برخورد کنید. تکه کاغذی که در آن مالکیت زمینی به نام شماست، ممکن است گم شود یا از بین برود. مدارک اثبات حق مالکیت بسیاری از دارایی‌های مردم در حال حاضر کاغذی هستند. همچنین،

ممکن است دولت دلش نخواهد که شما مالک یک زمین باشید و بخواهد آن را مصادره کند. بلاکچین می‌تواند راه‌حلی برای حذف تکه‌های کاغذ و واسطه‌های متصل‌شده به آنها باشد. پس اگر زمین، خانه یا اتومبیلی می‌خرید و می‌فروشید، می‌توانید اطلاعات آن را روی بلاکچین ذخیره کنید تا حق مالکیت آن برای همیشه محفوظ باقی بماند. این حق مالکیت می‌تواند معنوی هم باشد. مثلاً حق مالکیت یک عکس یا آهنگ می‌تواند در بلاکچین ذخیره شود تا استفاده غیرقانونی و بدون اجازه از این آثار هم قابل پیگیری باشد.

سلامت و تحقیق

در حوزه‌های پزشکی، سلامت و تحقیقات آزمایشگاهی با سه چالش اصلی مواجه هستیم؛ امنیت اطلاعات، امکان دست‌کاری اطلاعات و به‌اشتراک‌گذاری اطلاعات. ذخیره اطلاعات پزشکی و تحقیقاتی روی پایگاه‌های داده متمرکز امنیت آنها را به خطر می‌اندازد و هر لحظه امکان هک یا سرقت آنها وجود دارد. از طرف دیگر، یک نهاد مرکزی مثل دولت یا یک شرکت بانفوذ ممکن است بتواند اطلاعات حساس پزشکی یا تحقیقاتی را به نفع خودش دست‌کاری کند. بنابراین به‌اشتراک‌گذاری داده‌ها به خودی خود یک چالش جدی است. تیم‌های تحقیقاتی و پزشکی که روی موضوعات مشترک کار می‌کنند، همیشه در به‌اشتراک‌گذاری داده‌ها با چالش‌های زیادی مواجه بوده‌اند، اما از طرفی دیگر، اشتراک‌گذاری داده‌های پزشکی و تحقیقاتی می‌تواند به سرعت پیشرفت تحقیقات کمک زیادی کند. بلاکچین می‌تواند این مشکلات را حل کند. تمامی اطلاعات پزشکی و تحقیقاتی می‌تواند روی بلاکچین ذخیره شود. این شیوه باعث می‌شود تمامی سوابق دائمی، قابل انتقال و دسترس‌پذیر باشند.

تحصیل

آموزش‌وپرورش و تحصیل از حوزه‌هایی هستند که زیاد با کاغذ سروکار دارند و از همه مهم‌تر، مسئله مدارک جعلی امروزه به یک مشکل جدی تبدیل شده است. در صورت فراهم‌شدن بستر بلاکچین، امکان جعل مدارک و تقلب در آنها از بین می‌رود و سوابق تحصیلی یک فرد از ابتدا تا آخرین مدرک تحصیلی او در بلاکچین ذخیره می‌شود. این

می‌تواند موجب یکپارچگی اطلاعات شخصی افراد در شبکه‌ای امن شود و خطرات نگهداری این مدارک روی تکه کاغذهای نابودشدنی را از بین ببرد. کمااینکه حذف تمام سیستم‌های کاغذبازی خود کمک بزرگی به طبیعت و محیط زیست است.

اینترنت اشیا

اینترنت اشیا حوزه‌ای است که تلاش می‌کند با اتصال دستگاه‌ها و اشیای مورد استفاده در زندگی روزمره به اینترنت، به افزایش کیفیت زندگی کمک کند. برای مثال، با بهره‌مندی از فناوری اینترنت اشیا می‌توانیم همه‌چیز را، از دمای خانه گرفته تا روشنایی آن، روشن‌شدن اجاق گاز و بازوبسته شدن درها، با اینترنت کنترل کنیم. تحقیقات نشان می‌دهد که اینترنت اشیا در صورت ترکیب‌شدن با بلاکچین کامل می‌شود. به عبارتی بلاکچین می‌تواند در تأمین امنیت فرایندهای مختلف در اینترنت مفید واقع شود.

این موارد فقط برخی از کاربردهای اصلی بلاکچین هستند. همان‌طور که گفتیم، این فناوری زیرساختی می‌تواند هر حوزه‌ای را که در آن نیاز به از بین رفتن اعتماد و افزایش امنیت باشد، متحول کند.

هیچ‌کس هیچ‌چیز مدنظر نیست

کتاب حاضر تلاشی برای راهنمایی افرادی است که تنها در حد شنیدن واژه بیت‌کوین یا دنبال کردن قیمت ارزهای دیجیتال با این فناوری آشنا هستند و به‌دنبال شناخت جنبه‌های بیشتر و روش‌های سرمایه‌گذاری در آنها می‌گردند. ازکوچک‌ترین واحد پولی بیت‌کوین به پاس خدمات سازنده آن تحت عنوان «ساتوشی» یاد می‌شود. یک ساتوشی جزئی از صد میلیون واحد کوچک دیگر است که در کنار یکدیگر یک واحد بیت‌کوین را تشکیل می‌دهند. انقلاب پولی که بیش از یک دهه قبل شروع شد، هم‌اکنون به جایگاهی رسیده که رسانه‌ها؛ رویدادها و حوادث آن را از نزدیک دنبال می‌کنند و چشم‌های بسیاری به آینده آن دوخته شده است. یک ساتوشی نمادی برای سهیم‌شدن در این انقلاب است؛ مشارکتی که با کوچک‌ترین واحد پولی آغازگر این انقلاب انجام می‌شود. یک ساتوشی می‌تواند دارایی ارزشمندی در آینده باشد.

ISBN 978-622-7702-26-2
۱۰۸ هزار تومان
انتشارات راه‌پرداخت
ناشر فناوری و نوآوری
way2pay.press