حباب یا انقلاب؟

بلاک‌چین
حباب یا انقلاب؟

حال و آینده‌ی
بلاک‌چین و رمزارزها

نیل مهتا | آدیتیا آگاشه | پارت دتروجا

ترجمه‌ی **قاسم کیانی مقدم**

انتشارات مازیار

فهرست مطالب

مقدمه

بیت‌کوین ابزاری است برای رهایی بشر از بند خودکامگان و مستبدان که در ظاهر به‌عنوان روشی برای پولدار شدن سریع عرضه شده است.
ــ ناوال راویکانت، بنیان‌گذار اَنجِل‌لیست

بیت‌کوین احتمالاً مرگ موش به توان دو است.
ــ وارِن بافِت، مدیرعامل بِرکشایر هاتاوِی

سال۲۰۱۷، سازمان ملل با یک مشکل روبه‌رو بود. ده‌ها هزار پناهنده‌ی سوری به‌خاطر جنگ داخلی خونین در سوریه، به یک اردوگاه پناهندگان در کشور همسایه، اردن، گریخته بودند. برنامه‌ی جهانی غذای سازمان ملل (WFP) سوپرمارکت‌هایی را در اردوگاه بر پا کرده بود تا پناهندگان بتوانند اقلامی از قبیل روغن زیتون و عدس را خریداری کنند، و می‌بایست مبالغی پول را در اختیار پناهندگان بگذارد تا از آن برای خرید استفاده کنند.

مشکل این بود که صرفاً با دادن کارت اعتباری به پناهندگان این مسئله حل نمی‌شد. در گذشته WFP از این روش استفاده کرده بود و به علت کارمزد تراکنش‌ها و ضرورت قرارداد بستن با بانک‌های محلی، متحمل میلیون‌ها دلار خسارت شده بود ــ پولی که می‌توانست خرج تأمین غذای میلیون‌ها نفر شود. دادن کارت شناسایی به پناهندگان نیز برای دریافت کالا راه‌گشا نبود؛ در گذشته که WFP این روش را به کار گرفته بود، رهبران قبیله‌ای محلی کارت‌های پناهندگان را گرفته بودند و آن‌ها را مانند ارز بین خودشان خرید و فروش می‌کردند.

از این‌رو، WFP به سراغ فناوری نوپایی به نام بلاک‌چین [زنجیره‌ی بلوکی] رفت، که بیشتر به‌عنوان فناوری زیربنایی ارز دیجیتال بیت‌کوین شهرت داشت. به «حساب» هر پناهنده مقداری پول واریز می‌شد، و وقتی که پناهنده به فروشگاهی می‌رفت، هویت او را با اسکنر عنبیه تأیید می‌کردند و آن مبلغ را برای غذا و مایحتاج مورد نیاز او دریافت می‌کردند ــ بدون آن‌که لازم باشد پناهنده کیف پولش را باز کند. سپس مغازه‌ها کوپن‌های جمع‌آوری شده را

دوباره به سازمان ملل می‌فروختند.

این پروژه، که «قطعات سازنده» نام گرفته بود، با موفقیت چشم‌گیری روبه‌رو شد. این روش، کارمزد انتقال پول را به میزان ۹۸ درصد کمتر کرد، موارد کلاه‌برداری را کاهش داد، و فرایند کمک‌رسانی را، هم برای WFP و هم برای پناهندگان از اساس ساده‌تر کرد. سازمان ملل خیلی زود این برنامه را گسترش داد و ۱۰۰,۰۰۰ پناهنده را تحت پوشش آن قرار داد، و قصد دارد نهایتاً آن را به تمام پناهندگان مستقر در اردن توسعه دهد.

فواید این روش برای سازمان ملل فراتر از کمک‌رسانی است: این سازمان اعلام کرد که شاید روزی بتواند هویت و شرح زندگی پناهندگان را با استفاده از بلاک‌چین ردیابی کند، و به این طریق به پناهندگانی که گذرنامه یا سوابق تحصیلی آن‌ها از بین رفته است، کمک کند که در کشورهای جدید، کار پیدا کنند و وام بگیرند.

افراد در مناطق مختلف جهان درباره‌ی بلاک‌چین و فناوری دیگر مرتبط با آن، یعنی رمزارزها (مانند همان بیت‌کوین که در بالا به آن اشاره شد)، بسیار هیجان‌زده‌اند. مجله‌ی بازرگانی هاروارد این احتمال را مطرح کرده است که بلاک‌چین صنعت راکد بانکداری را متحول کند، سرمایه‌گذار مشهور مارک اندریسِن گفته است که بلاک‌چین «مهم‌ترین اختراع از زمان اینترنت است»، و تحلیلگران سراسر جهان بر این باور هستند که رمزارزها پول و فناوری شناخته شده را متحول خواهند کرد.

از سوی دیگر، این فناوری‌های اسرارآمیز جدید شهرت شومی نیز پیدا کرده‌اند. قاچاقچیان بزرگ از بیت‌کوین برای معامله‌ی مواد مخدر به‌صورت ناشناس استفاده می‌کنند، رمزارزها متهم شده‌اند که به گرمایش زمین دامن می‌زنند، و هکرها با استفاده از بیت‌کوین باج می‌گیرند تا برای نیروهای انتظامی امکان ردیابی آن‌ها وجود نداشته باشد. تازه حتی شهرت مثبت این فناوری‌ها نیز غالباً از حد معقول تجاوز می‌کند: یک شرکت چای یخ، به نام چای یخ لانگ آیلند کلمه‌ی «بلاک‌چین» را به نام خود اضافه کرد و قیمت سهام آن تقریباً چهار برابر شد.

پس حقیقت چیست؟ آیا بلاک‌چین و رمزارزها یک حباب پر شده از شایعات هستند، و هیچ‌گونه کاربرد مشروعی برای این فناوری‌ها وجود ندارد؟ یا این‌که

اختراعاتی تحول‌آفرین هستند که باعث تحول در ساختار حکومت‌ها، کسب‌وکارها، اقتصادها، و جوامع خواهند شد؟ به عبارت دیگر، حباب هستند یا انقلاب؟

هدف

همان‌گونه که از داستان‌های بالا برمی‌آید، بلاک‌چین و رمزارزها ــ که بر روی هم به آن‌ها کریپتو [یا رمزینه] گفته می‌شود ــ در میان تأثیرگذارترین و در عین حال، ناشناخته‌ترین فناوری‌های روزگار ما هستند. اکثر گفتمان‌های غالب درباره‌ی کریپتو به این صورت است که افراد مشتاق می‌گویند که کریپتو باعث نابودی بانک‌ها و حکومت‌ها خواهد شد، و صاحب‌نظران قدیمی می‌گویند که کریپتو چیزی جز کلاه‌برداری نیست. خیلی از افراد اصلاً نگاه نمی‌کنند ببینند این فناوری‌ها دقیقاً چه هستند و واقعاً چه پتانسیلی دارند.

در کتاب حباب یا انقلاب، می‌خواهیم این وضعیت را تغییر دهیم. می‌خواهیم با مثال‌هایی واقعی، توضیحاتی ساده‌فهم، و تحلیل‌هایی بدون سوگیری، به شما بیاموزیم که کریپتو چگونه کار می‌کند، در چه جاهایی سودمند است، و در چه جاهایی نیست. خواهیم گفت که نظر خودمان درباره‌ی حباب یا انقلاب بودن آن چیست، ولی ابزارهایی را نیز در اختیار شما قرار خواهیم داد تا خودتان بتوانید در این مورد تصمیم بگیرید.

درباره‌ی مطالب کتاب

در کتاب حباب یا انقلاب، درباره‌ی قطعات سازنده‌ی بلاک‌چین‌ها و رمزارزها چیزهایی یاد خواهید گرفت؛ نقاط قوت و ضعف آن‌ها را با استفاده از مطالعات موردی بررسی خواهید کرد؛ به عمق تبعات اجتماعی، سیاسی، اقتصادی، و فنی آن‌ها خواهید پرداخت؛ و بر اساس مصاحبه‌هایی انحصاری که با ده‌ها تن از رهبران صنعت و فناوری داشته‌ایم، بینش‌هایی درباره‌ی آینده‌ی آن‌ها به دست خواهید آورد.

فقط چند مورد از مطالبی را که بررسی خواهیم کرد، در این‌جا ذکر می‌کنیم:

- اقتصاد استخراج بیت‌کوین
- هک‌ها و نقایص مشهور رمزارزها
- بلاک‌چین ایکس‌باکس برای بازی‌های ویدئویی

- نظارت کمیسیون ارز و اوراق بهادار آمریکا بر شرکت‌های نوپای کریپتو
- توکن‌سازی ارزها و آینده‌ی پول
- رمزارزهای نوظهور فیس‌بوک

درباره‌ی ما

قبل از شروع بحث، بد نیست چند جمله در معرفیِ خودمان بگوییم.

نیل مهتا مدیر محصول در گوگل است و قبلاً برای مایکروسافت و دولت آمریکا کار کرده است، و در آن‌جا نخستین برنامه‌ی کارآموزی فناوری دولت آمریکا را ایجاد کرده است.

آدی آگاشه مدیر محصول در مایکروسافت است و قبلاً بنیان‌گذار و مدیرعامل بل اپلیکیشنز بوده است.

پارت دتروجا مدیر محصول در فیس‌بوک است و قبلاً موقعیت‌هایی در ارتباط با محصول و بازاریابی در مایکروسافت، آمازون، و IBM داشته است.

سپاسگزاریم ـ از کتاب لذت ببرید!

باز هم به‌خاطر انتخاب کتاب حباب یا انقلاب از شما متشکریم! امیدواریم این کتاب برای شما آموزنده، جالب، و شاید حتی سرگرم کننده باشد. همگی آرزومندیم که شما از خواندن این کتاب لذت ببرید!

نیل مهتا
namehta.com
linkedin.com/in/neelmehta18

آدیتیا آگاشه
adityaagashe.com
linkedin.com/in/adityaagashe
quora.com/profile/Adi_Agashe

پارت دتروجا
parthdetroja.com
linkedin.com/in/parthdetroja

۱
بیت‌کوین

طرف‌های ثالث مورد اعتماد، حفره‌های امنیتی هستند. امیدوارم همه‌ی کسانی که در فضای بلاک‌چین هستند، این را در ذهن داشته باشند. این اساساً کلید کلی طراحی بلاک‌چین است.

ـ نیک سابو، خالق بیت‌گولد (از پیش‌درآمدهای بیت‌کوین)

اگر بخواهید درباره‌ی دنیای بلاک‌چین‌ها و رمزارزها چیزی یاد بگیرید، اول باید از مشهورترین رمزارز و مشهورترین فناوری ساخته شده بر مبنای بلاک‌چین شروع کنید، که همانا فناوری بیت‌کوین است. و اگر بخواهید درباره‌ی بیت‌کوین چیزی یاد بگیرید، اول باید به یک چیز معمولی، یعنی کارت اعتباری، فکر کنید.

دردسر کارت‌های اعتباری

وقتی که می‌خواهید پول چیزی را با کارت اعتباری پرداخت کنید، روال انجام کار خیلی آسان است: مثلاً در پیتزا هات، کارت اعتباری ویزای بانک چیس خود را برای ۵ دلار می‌کشید، پیتزا به شما داده می‌شود، و در پایان ماه، بانک چیس صورتحسابی به مبلغ ۵ دلار برای شما می‌فرستد. کارت‌های اعتباری آسان و سریع هستند و همه جا پذیرفته می‌شوند.

ولی پشت صحنه اتفاقات زیادی در جریان است. وقتی که کارت خود را می‌کشید، پیتزا هات از بانک خود می‌خواهد که از بانک چیس بخواهد که تراکنش را تأیید کند. وقتی که تأیید شد، پیتزا هات از بانک خود تقاضای ۵ دلار می‌کند، بانک از ویزا ۵ دلار درخواست می‌کند، و ویزا از چیس درخواست ۵ دلار می‌نماید. چیس به ویزا ۵ دلار منهای مبلغی به نام کارمزد انتقال (حدود ۲ درصد) می‌دهد، که می‌شود حدود ۴/۹۰ دلار. ویزا به بانکِ پیتزا هات ۴/۹۰ دلار منهای یک کارمزد اندک ارزیابی به میزان ۰/۱ درصد می‌دهد، که حدود ۴/۸۹ دلار می‌شود. بانک پیتزا هات این مبلغ ۴/۸۹ دلار را به پیتزا هات می‌دهد. و در پایان ماه، چیس صورتحسابی به مبلغ ۵ دلار برای شما می‌فرستد.

ارزش این پیتزا برای پیتزا هات ۴/۸۹ دلار بود، ولی شما برای آن ۵ دلار پرداخت کردید. یازده سنت باقی‌مانده صرف پرداخت کارمزد برای چیس و ویزا شده است، که واسطه‌ی انجام پرداخت و بین شما و پیتزا هات بودند. شاید این ۱۱ سنت به نظر شما مبلغ زیادی نرسد، ولی به‌ازای هر یک میلیون دلار پیتزا که پیتزا هات می‌فروشد، ۲۰,۰۰۰ دلار برای کارمزد صرف می‌شود. و این کارمزدها نهایتاً از جیب شما، یعنی مصرف کننده، خرج می‌شود.

از طرف دیگر، اگر پول پیتزا هات را با یک اسکناس پنج‌دلاری پرداخت می‌کردید، دیگر بانک چیس یا شرکت ویزا در میانه‌ی پرداخت واقع نمی‌شدند و لذا هیچ‌گونه کارمزدی در کار نبود. (بدین خاطر است که بسیاری از مغازه‌های کوچک فقط پول نقد قبول می‌کنند، و یا این که بنزین غالباً اگر پول آن را به جای استفاده از کارت اعتباری، نقدی پرداخت کنید، ارزان‌تر است.)

درسی که از این بحث می‌گیریم، این است که هر کسی که بین خریدار و فروشنده واقع شده باشد ــ یعنی به‌اصطلاح واسطه ــ کارمزد می‌گیرد. و تازه فقط پول نیست که از طریق واسطه منتقل می‌شود؛ داده‌ها هم هست. بنابراین وقتی که از کارت اعتباری استفاده می‌کنید، در حقیقت باید به بانک‌هایی مانند بانک چیس و شبکه‌های کارت اعتباری مانند ویزا اعتماد کنید که داده‌های شما را ایمن نگه‌دارند. ولی بارها دیده شده که امنیت این واسطه‌ها نقض شده است: شرکت جی‌پی مورگان در سال ۲۰۱۴ هک شد، و در سال ۲۰۱۲، هکرها داده‌های هزاران مشتری ویزا و مسترکارت را سرقت کردند.

اما پول نقد کاملاً ناشناس است، چیزی برای هک شدن وجود ندارد، و هیچ‌کس نمی‌تواند پول شما را بدزدد، مگر آن‌که درست کنار شما باشد (که البته گهگاه اتفاق می‌افتد).

جز در صورتی که از پول نقد استفاده کنید، به‌سختی می‌توانید از دست واسطه‌ها رها شوید. سیستم اپل‌پی (apple pay) درست بر مبنای کارت اعتباری شما بنا شده است. پرداخت کَردن از طریق سرویس پرداخت موبایل وِنمو بدان معنا است که پول شما از بانک شما و شرکت پی‌پل، شرکت مالک وِنمو عبور می‌کند. چک کارمزد ندارد، ولی در اصل برای استفاده از آن باید حساب بانکی داشته باشید، که برای ۲ میلیارد نفر از مردم دنیا که حساب بانکی ندارند، یک مشکل محسوب می‌شود.

خلاصه این‌که اگر بخواهید از کارمزد، حفره‌های امنیتی، و محدودیت‌های دسترسی‌پذیری مرتبط با واسطه‌ها اجتناب کنید، باید از پول نقد استفاده کنید. ولی پول نقد هم مشکلات خاص خود را دارد: شمردن، ذخیره کردن، و انتقال دادن آن زحمت دارد، و برای پرداخت‌های راه دور یا دیجیتال قابل استفاده نیست. این به علت فیزیکی بودن یا مشهود بودن پول نقد است؛ در این دنیای دیجیتال و جهانی‌شده‌ی امروز، نمی‌توان پرداخت‌ها را به‌صورت مؤثری با اشیای فیزیکی که باید با خودتان راه ببرید، انجام داد. از سوی دیگر، کارت اعتباری و دیگر سیستم‌های پرداخت دارای واسطه برای پرداخت‌های دیجیتال و راه دور بسیار مناسب هستند.

پس می‌توانید یا مشکل مشهود بودن را حل کنید (اشیای فیزیکی در این دور و زمانه شکل‌های مناسبی از پول نیستند)، و یا مسئله‌ی واسطه را (واسطه‌ها کارمزد، حفره‌های امنیتی، و محدودیت‌های دسترسی‌پذیری دارند). نمی‌توانید هر دو را داشته باشید. درست است؟

ارز دیجیتال غیرمتمرکز

یک راه دیگر برای بیان این مطلب، به‌صورت بده‌بستان بین **غیرمتمرکزسازی** (یعنی نداشتن واسطه) و **دیجیتال‌سازی** (یعنی نامشهود بودن) است. **متمرکزسازی** اصطلاحی است که به معنای وجود واسطه‌ها است؛ در یک سیستم **غیرمتمرکز** مانند پول نقد، واسطه‌ای وجود ندارد، و پول مستقیم از خریدار به دست فروشنده می‌رسد، یعنی به‌صورت **همتابه‌همتا**. کارت‌های اعتباری (و سرویس‌های پرداخت مانند اپل‌پی و غیره) دیجیتال هستند ولی غیرمتمرکز نیستند؛ پول نقد غیرمتمرکز است ولی دیجیتال نیست.

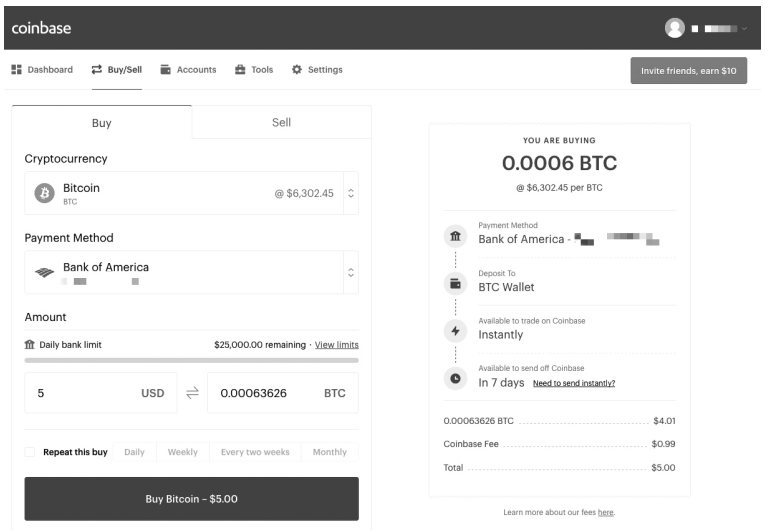
در سال ۲۰۰۸، یک دانشمند علوم کامپیوتر که نام خود را ساتوشی ناکاموتو گذاشته بود، اعلام کرد که یک سیستم پرداخت ایجاد کرده است که هم غیرمتمرکز است و هم دیجیتال. هیچ‌گونه بانکی یا شرکت کارت اعتباری بین خریدار و فروشنده واقع نمی‌شد، و لذا ادعا می‌کرد که کارمزدهای آن پایین‌تر است و نقطه‌ی حساسی برای اختلال یا حمله‌ی هکرها در آن وجود ندارد. و در عین حال، این سیستم برای پرداخت دیجیتال از راه دور نیز بسیار مناسب بود. در واقع، یک ارز کاملاً دیجیتال بود.

او نام آن را «بیت‌کوین» گذاشت.

تفاوت با اپلیکیشن‌های پرداخت بانکی

اولین سوآلی که درباره‌ی بیت‌کوین به ذهن می‌رسد، این است: حالا این چیز چگونه کار می‌کند؟

در نگاه اول، بیت‌کوین بسیار شبیه اپلیکیشن‌های ارسال پول، مانند ونمو [یا مثلاً همراه‌بانک یا اینترنت‌بانک در ایران]، به نظر می‌رسد. می‌توانید بیت‌کوین را خریداری کنید تا به حساب شما واریز شود، می‌توانید بیت‌کوین را برای دیگران بفرستید، می‌توانید از دیگران بیت‌کوین دریافت کنید، و یا این‌که می‌توانید بیت‌کوین‌هایتان را بفروشید تا پول آن دوباره به حساب بانکی شما واریز شود.

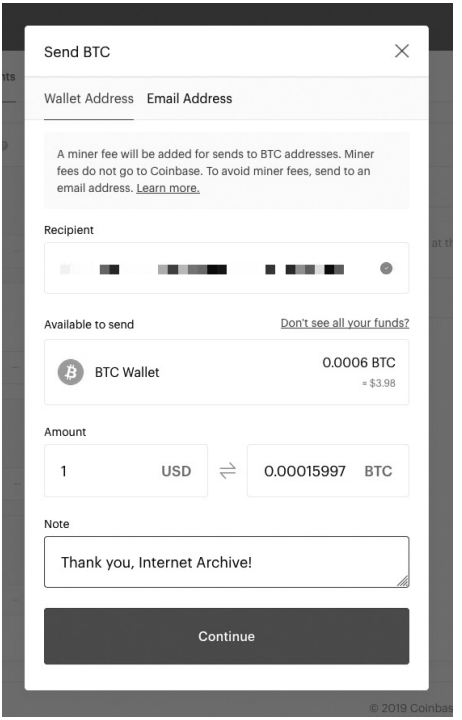


خریدن بیت‌کوین به ارزش ۵ دلار از صرافی بیت‌کوین کوین‌بیس و دریافت آن در حساب بیت‌کوین.

ولی اگر با دقت بیشتری نگاه کنید، متوجه تفاوت‌هایی می‌شوید:

نخست این‌که به‌جای این‌که دلار را به حساب خود واریز کنید، آن را با نرخ مشخص صرافی تبدیل به بیت‌کوین می‌کنید. (در انگلیسی، وقتی منظور مبلغ بیت‌کوین است، کلمه‌ی *bitcoin* با حرف کوچک شروع می‌شود، ولی وقتی منظور خود ارز بیت‌کوین است، به‌صورت *Bitcoin* با حرف بزرگ نوشته می‌شود.) این مانند تبدیل کردن دلار به یورو (یا ارزهای عادی دیگر یا به‌اصطلاح فیات) است.

این تبدیل در وب‌سایتی انجام می‌شود که به آن صرافی بیت‌کوین می‌گویند؛ ده‌ها وب‌سایت از این نوع در نقاط مختلف جهان وجود دارند، از قبیل Coinbase و Bittrex.



فرستادن بیت‌کوین با Coinbase. در این‌جا می‌خواهیم مقداری بیت‌کوین به ارزش ۱ دلار به‌عنوان هدیه برای آرشیو اینترنت بفرستیم.

علاوه بر این، پول شما به‌جای حساب، در یک کیف پول (*wallet*) نگهداری می‌شود. و بیت‌کوین به‌جای نام کاربری از آدرس (*address*) استفاده می‌کند. آدرس‌های بیت‌کوین به‌صورت رشته‌های بلند حروف و اعداد است که مانند حروف بی‌معنا به نظر می‌رسد. در تصویر نمونه‌ای که در بالا نشان دادیم، به آدرس *1Archive1n2C579dMsAu3iC6tWzuQJz8dN* بیت‌کوین فرستادیم، که متعلق به بنیاد غیرانتفاعی «آرشیو اینترنت» است، سایتی که نسخه‌های قبلی صفحات وب را ذخیره می‌کند تا در گذر زمان از بین نروند. ویکی‌لیکس هم آدرس بیت‌کوین نسبتاً مشهوری دارد: *1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v*.

از طرف دیگر، بیت‌کوین به‌جای گذرواژه از کلید خصوصی استفاده می‌کند. می‌توانید کلید خصوصی را به یک تابع ریاضی بدهید و آدرس را از آن به دست آورید، ولی عکس این کار امکان‌پذیر نیست (مانند این‌که اگر نام کامل کسی را بدانید، می‌توانید حروف اختصاری اول اسم او را بگویید، ولی اگر فقط حروف اختصاری اول اسم کسی را بدانید، نمی‌توانید نام کامل او را به دست آورید.) به این طریق، کاربران بیت‌کوین می‌توانند هویت خود را اثبات کنند، بدون این‌که لازم باشد که کلید خصوصی خود را در اختیار پایگاه داده‌ای یک شرکت بگذارند، در حالی که در سرویس‌های متعارف باید گذرواژه‌ی خود را در اختیار شرکت بگذارید.

پول فرستادن از طریق بیت‌کوین نیازی به پرداخت کارمزد کارت اعتباری ندارد، ولی نیاز به پرداخت کارمزد استخراج دارد. در مثال ما، مبلغ کارمزد استخراج معادل ۸۰ سنت بود (البته با توجه به این‌که تمام مبلغی که می‌خواستیم بفرستیم، ۱ دلار بود، مبلغ هنگفتی به نظر می‌رسد!). منظور از کارمزد استخراج را در فصل‌های بعد بررسی خواهیم کرد.

و سرانجام این‌که در مورد اپلیکیشن ونمو، هر یک دلار که در حسابتان دارید، همیشه ۱ دلار ارزش دارد ــ ولی در این‌جا، نرخ تبدیل بین دلار و بیت‌کوین، درست مانند قیمت سهام، نوسان دارد. یعنی می‌توانید بیت‌کوین بخرید، آن را نگه‌دارید، و وقتی که قیمت بالاتر رفت، بفروشید.

بنابراین، در این سطح، بیت‌کوین مانند ترکیب عجیبی از یک اپلیکیشن بانکی و یک اپلیکیشن دادوستد سهام به نظر می‌رسد: می‌توانید از آن برای فرستادن و دریافت کردن پول استفاده کنید، ولی در عین حال، می‌توانید از آن به‌عنوان روشی برای سرمایه‌گذاری بهره بگیرید. تقریباً مثل آن است که از طریق اپلیکیشن بانکی بتوانید برای دوستانتان سهام بورس بفرستید.

ولی علت اصلی تفاوت بیت‌کوین با سیستم‌های پولی معمولی این نیست، و به‌خاطر این قابلیت‌ها نیست که می‌خواهیم درباره‌ی بیت‌کوین چیزی یاد بگیریم. برای این منظور، باید فناوری خاصی را که بیت‌کوین بر پایه‌ی آن ساخته شده است، بشناسیم، و آن بلاک‌چین (*blockchain*) است.

فرهنگ اصطلاحات (انگلیسی- فارسی)

دنیای بلاک‌چین‌ها و رمزارزها مقدار زیادی اصطلاحات پیچیده‌ی فنی دارد. خیلی از آن‌ها در این کتاب مورد بحث قرار گرفت، ولی در این‌جا برخی از اصطلاحات کلیدی کریپتو را به‌طور خلاصه توضیح داده شده، که بعضی از آن‌ها در کتاب به‌صورت مفصلی بررسی نشده‌اند. هم‌چنین، خلاصه‌ی کوتاهی از مشهورترین و مهم‌ترین رمزارزها آورده شده است.

اصطلاحات

در این قسمت، برخی از عبارت‌ها و اصطلاحات شایعی را که در بحث‌های مربوط به بلاک‌چین‌ها و رمزارزها زیاد به آن‌ها اشاره شده، بیان می‌شود.

حمله‌ی ۵۱ درصد **51% attack**

حمله‌ی ۵۱ درصد زمانی روی می‌دهد که یک ماینر یا گروهی از ماینرها توان رایانشی بیشتر از مجموع تمام ماینرهای دیگر برای یک رمزارز خاص را در اختیار داشته باشند. (به عبارت دیگر، آن ماینر یا گروه ماینرها لااقل ۵۱ درصد تمام توان رایانشی شبکه را در دست داشته باشند.) در یک حمله‌ی ۵۱ درصد، ماینر یا گروه غالب می‌توانند بلاک‌چین را به دلخواه خود بازنویسی کنند، به خودشان هر چقدر بخواهند پول بدهند، تراکنش‌های گذشته را لغو کنند، و غیره.

آدرس **Address**

یک نام مستعار عمومی برای یک کاربر رمزارز. برای این‌که برای کسی سکه بفرستید، باید آدرس او را بدانید.

AML **AML**

قوانین ضدپول‌شویی. به قوانین و مقرراتی اطلاق می‌شود که صرافی‌های رمزارزی باید رعایت کنند تا افراد نتوانند از آن صرافی‌ها برای پول‌شویی استفاده کنند. هم‌چنین، رک. KYC.

گره بایگانی **Archival node**

نوعی گره کامل که نه فقط حاوی تمام زنجیره‌ی بلوکی است، بلکه حاوی بایگانی‌های لحظه‌ای از وضعیت رمزارز نیز هست، مثلاً این‌که در هر زمان هر آدرس چند سکه داشته است. گره‌های کامل نمونه‌های فشرده‌ای از گره‌های بایگانی هستند؛ اینها هم تمام اطلاعات را دارند، ولی انجام محاسبات و پرس‌وجوهای پیشرفته دشوار است، مگر این‌که گره کامل را به‌صورت یک گره بایگانی بسط دهید.

ASIC **ASIC**

نوعی تراشه‌ی تخصصی کامپیوتر که برای اجرای نوع خاصی از الگوریتم ماینینگ کاملاً بهینه‌سازی شده است. استخراج‌کنندگان حرفه‌ای بیت‌کوین باید از ASICها استفاده کنند، زیرا کامپیوترهای همه‌منظوره (مانند یک لپ‌تاپ) اصولاً به‌گونه‌ای بهینه‌سازی نشده‌اند که بتوانند الگوریتم استخراج رمزارز را با سرعت اجرا کنند. مخفف عبارت «مدار مجتمع با کاربرد خاص» است.

مقاومت به ASIC **ASIC-resistance**

نوعی ویژگی الگوریتم ماینینگ، مثلاً در مورد اتریوم، که سبب می‌شود که ASICها هیچ برتری بر کامپیوترهای همه‌منظوره نداشته باشند. در الگوریتم‌های معمولی استخراج رمزارز، استخراج‌کنندگان باید محاسبات یکسانی را مکرراً انجام دهند؛ از این‌رو، ماینرها از ASICهایی استفاده می‌کنند که برای آن نوع محاسبات بسیار سریع هستند. ولی الگوریتم‌های ماینینگ مقاوم به ASIC به‌گونه‌ای هستند که استخراج‌کنندگان باید محاسبات مختلفی را انجام دهند، به‌طوری که یک کامپیوتر همه‌منظوره (که برای انجام محاسبات مختلف استفاده می‌شود) بهتر از یک تراشه‌ی تخصصی عمل می‌کند. در مقاله‌ی اتریوم آمده است: «اگر بخواهیم برای اتریوم ASIC بسازیم، اساساً باید تراشه‌ای برای محاسبات عمومی باشد ــ یعنی یک CPUی بهتر.» مقاومت به ASIC چیز خوبی است، زیرا سبب می‌شود که افراد عادی و آماتور نیز امکان استخراج داشته باشند.

دارایی **Asset**

هر گونه منبعی که دارای ارزش اقتصادی باشد. دارایی‌های مالی انواع مختلفی دارند: دلار، سهام، رمزارزها، اوراق قرضه، و غیره. ولی خیلی چیزهای دیگر نیز دارایی محسوب می‌شوند: خودرو، کتاب، سند املاک، مالکیت معنوی، علایم تجاری، و غیره. بلاک‌چین‌ها یک راه غیرمتمرکز برای ثبت جابه‌جایی هر گونه دارایی ارائه می‌کنند.

بیس۵۸ **Base58**

فرمتی که برای آدرس‌های بیت‌کوین استفاده می‌شود. این فرمت شامل حروف بزرگ و کوچک انگلیسی و اعداد است، ولی نویسه‌های صفر، I بزرگ، O بزرگ، و l کوچک را که به‌راحتی ممکن است اشتباه شوند، حذف کرده است.

بایننس **Binance**

یک صرافی رمزارزی پرطرفدار.

بیت‌کوین (با حروف کوچک) **bitcoin (lowercase)**

به واحدهای ارز بیت‌کوین گفته می‌شود. مثلاً: «ثروت او شامل ده‌ها بیت‌کوین است.» بر عکس، می‌گوییم: «دوستان من در بیت‌کوین [با حرف اول بزرگ] سرمایه‌گذاری می‌کنند.»

بیت‌کوین کُور **Bitcoin Core**

نسخه‌ی رسمی نرم‌افزار بیت‌کوین. شامل کیف پول، نرم‌افزار مربوط به گره کامل، و یک موتور اعتبارسنجی تراکنش است.

مسئله‌ی مقیاس بیت‌کوین **Bitcoin's scaling problem**

یکی از مسایل شناخته شده در بیت‌کوین است، به این صورت که بیت‌کوین فقط توانایی پردازش ۷ تراکنش در ثانیه دارد، در حالی که سیستم‌های پرداخت متداول مانند ویزا می‌توانند ده‌ها هزار

تراکنش را در ثانیه پردازش کنند.هر گاه کاربران بیت‌کوین بخواهند بیشتر از ۷ تراکنش در ثانیه بفرستند، موجب تراکم شبکه می‌شود؛ این منجر به زمان انتظار طولانی و نرخ بالای تراکنش می‌شود.

بیت‌فینکس **Bitfinex**

یک صرافی رمزارزی پرطرفدار.

بلوک **Block**

دسته‌ای از تراکنش‌های رمزارزی. استخراج‌کنندگان با یکدیگر برای ایجاد بلوک‌ها رقابت می‌کنند؛ ماینر برنده موفق می‌شود بلوک را به انتهای زنجیره‌ی بلوکی اضافه کند و به‌عنوان پاداش، تعدادی سکه دریافت می‌کند.

بلاک‌چین [زنجیره‌ی بلوکی] **Blockchain**

یک دفترکل غیرمتمرکز که سابقه‌ی تغییرناپذیر تراکنش‌های قبلی را ذخیره می‌کند. رمزارزها همگی بر پایه‌ی بلاک‌چین [زنجیره‌ی بلوکی] ساخته شده‌اند، ولی می‌توانید جابه‌جایی هر گونه دارایی، اعم از دیجیتال یا فیزیکی، را روی بلاک‌چین ردیابی نمایید. «گذاشتن چیزی روی بلاک‌چین» صرفاً به‌معنای ثبت جابه‌جایی‌های آن در یک بلاک‌چین است.

کاوشگر بلوک **Block explorer**

ابزاری که به شما امکان می‌دهد که اطلاعات مربوط به بلوک‌ها، آدرس‌ها، و تراکنش‌ها را روی یک بلاک‌چین ببینید. به‌خصوص، کاوشگرهای بلوک به شما امکان می‌دهند که تراکنش‌های گذشته‌ی هر کسی و طرف‌های معامله‌ی او و مانده‌ی کنونی او را ببینید، البته به شرطی که آدرس او را بدانید.

ارتفاع بلوک **Block height**

تعداد کل بلوک‌ها در بلاک‌چین.

پاداش بلوک **Block reward**

تعداد سکه‌های کریپتو که یک ماینر به‌خاطر استخراج موفقیت‌آمیز یک بلوک دریافت می‌کند. در چندین رمزارز، از جمله بیت‌کوین، پاداش بلوک هر چند سال نصف می‌شود.

اندازه‌ی بلوک **Block size**

حداکثر اندازه‌ی فایل یک بلوک (مثلاً ۱ مگابایت)، که مشخص می‌کند که در هر بلوک، چند تراکنش جا می‌شود. از آن‌جا که بلوک‌ها در فواصل زمانی ثابت استخراج می‌شوند، لذا اندازه‌ی بلوک یکی از عواملی است که حداکثر ممکن تعداد تراکنش‌ها بر ثانیه را برای رمزارز مورد نظر تعیین می‌کند.

زمان بلوک **Block time**

مدت زمانی که طول می‌کشد تا هر بلوک استخراج شود. مثلاً در بیت‌کوین، به‌طور متوسط هر ۱۰ دقیقه یک بلوک استخراج می‌شود.

حباب **Bubble**

زمانی که قیمت یک دارایی (رمزارز، لاله، خانه، و غیره) از ارزش واقعی آن بالاتر رود. معمولاً حباب‌ها زمانی تشکیل می‌شود که دلالی و سفته‌بازی از کنترل خارج شود، و مردم مرتب دارایی مورد نظر را با قیمت‌های بسیار بالا خریداری کنند، به امید آن‌که قیمت هم‌چنان به بالا رفتن خود ادامه خواهد داد. حباب‌ها ناگزیر زمانی که چرخه‌ی دلالی شکسته شود، می‌ترکند.