رمزارزها

پادکست دایجست | قسمت ۴۰
تیرمـــاه ۱۴۰۰
فرشـــاد محمـــودی
ویرایش و تنظیم: شادی حسین‌نیا

مقدمه

مدتی است که دوباره بازار رمز-ارزها رونق گرفته است. اگر به یاد داشته باشید، ما حدوداً ۳ سال پیش، در سومین قسمت از پادکست دایجست، به رمز-ارزها پرداختیم. اپیزود سوم دایجست با عنوان «بیت‌کوین» زمانی ساخته شد که قیمت این رمز-ارز اوج گرفته و به حدود ۱۶-۱۷ هزار دلار رسیده بود. همان‌طور که می‌دانید قیمت بیت‌کوین تا ۶۴ هزار دلار هم رسید و امروز که دوباره از آن نام می‌بریم، با ریزشی که داشته، هر بیت‌کوین ۳۵ هزار دلار خرید و فروش می‌شود.

چرا دوباره به این موضوع بازگشته‌ایم؟ طبیعتاً از آن زمان تاکنون اتفاقات زیادی در جریان بوده‌اند و احتمالاً کار به‌جایی رسیده که این روزها دست‌کم یکی از اطرافیان شما درگیر رمز-ارزهاست. بازار رمز-ارزها بسیار بزرگ‌تر شده و مفاهیم جدیدی وارد آن شده که بازار را بسیار پیچیده‌تر کرده‌اند. به همین دلیل دایجست تصمیم گرفت که داستان رمز-ارزها را به زبان ساده برای شما توضیح دهد.

اگر این مبحث برای شما جدید است و قسمت سوم دایجست با عنوان بیت‌کوین را نیز نشنیده‌اید، پیش از آغاز مباحث این قسمت، پیشنهاد می‌کنم که یک ساعت وقت بگذارید و قسمت سوم را به‌عنوان مقدمه گوش کنید. این کار باعث می‌شود که با برخی مفاهیم آشنا شوید؛ بدین ترتیب درک بهتری از این قسمت خواهید داشت. البته ما مقدمه‌ی مختصری در ابتدای قسمت جاری بیان می‌کنیم؛ بااین‌وجود شنیدن قسمت «بیت‌کوین» زیرساخت اطلاعاتی شما را قوی‌تر می‌کند.

در مبحث رمز-ارزها هرآنچه که از پول و فایننس و کامپیوتر نمی‌دانیم با هم ترکیب شده است. پیش از هر چیز برخی مفاهیم را مرور می‌کنیم.

مروری بر مبانی نظری و پایه‌ای رمز-ارزها

به طور خلاصه «رمز-ارز» یعنی پول دیجیتالی که رمزنگاری‌شده، مستقیم و نامتمرکز است.

- **رمزنگاری:** اکثر پول‌های دیجیتال بر اساس الگوریتم‌های رمزنگاری، کدنویسی و ساخته شده‌اند. این ویژگی باعث قابلیتی در پول‌های دیجیتال می‌شود که دارنده و انتقال‌دهنده‌ی پول را ناشناس نگه می‌دارد. آیا به یاد دارید که اپلیکیشن تلگرام ادعا می‌کرد که مکالمات شما در این پیام‌رسان رمزنگاری شده است؟ رمزنگاری پول‌های دیجیتالی نیز تقریباً به همین شکل است و این یک انقلاب است. اینکه دارنده‌ی پول، مراحل انتقال آن و دریافت‌کننده‌اش همگی ناشناس باشند، قابلیتی است که در سیستم مالی فعلی جهان بسیار سخت و تقریباً نشدنی است. این حد از محرمانگی چه اختیاراتی به شما می‌دهد؟ به آن فکر کنید.

کسی نمی‌تواند این پول‌ها را ردیابی کند. اینکه دارایی هر شخص چه‌قدر است و هرکس چرا و چه مقدار پول به چه کسی داده است، تماماً رمزنگاری شده است. همین ویژگی رمز-ارزها بود که در ابتدا به رایج شدن آن‌ها کمک کرد. گروه‌هایی هستند که نیاز دارند مبادلات مالی‌شان ردگیری نشود؛ از تروریست‌ها و قاچاقچی‌ها گرفته تا کسانی که با سلطه‌ی سیستم‌های مالی و دولت‌ها بر آزادی‌های فردی مشکل دارند و کشورهایی که نیاز داشتند تحریم‌ها را دور بزنند. البته رمزنگاری برای محرمانگی و آزادی فردی تنها یکی از اهداف بیت‌کوین بوده است. دلیل دیگر این رمزنگاری به‌خاطر مکانیزم سیستم این پول است. در واقع باید این رمزنگاری انجام شود تا جلوی تقلب را بگیرد. در ادامه چگونگی این فرایند را توضیح می‌دهیم.

توسعه‌دهندگان رمز-ارزها، این پروتکل‌ها را بر مبنای الگوریتم‌های ریاضی و اصول مهندسی کامپیوتری‌ای می‌نویسند که چنان پیچیده‌اند که عملاً شکاندنشان غیرممکن است. همان‌طور که گفتیم این عملیات پیچیده‌ی رمزنگاری علاوه بر ایجاد محرمانگی بسیار زیاد، برای رفع مشکلات دیگری نیز به وجود آمده است و مانع بروز تقلب در سیستم می‌شود. این موضوع را همراه با ویژگی دوم رمز-ارزها توضیح می‌دهیم.

- **مستقیم و نامتمرکز بودن:** برای توضیح مستقیم (Peer To Peer) بودن، ابتدا ببینیم روش غیرمستقیم چگونه است. در حال حاضر وقتی شما قصد انتقال پول به حساب کسی را دارید یا هنگامی‌که با کارت بانکی خود خرید می‌کنید، این اتفاق می‌افتد: ابتدا یک پیام از سوی شما به بانک می‌رسد که x تومان از حساب من کم کن. بعد پیام از بانک شما به بانک شخص موردنظر ارسال می‌شود که همان x تومان را به حساب آن شخص اضافه کن. پس این تبادل پول مستقیم نیست و بانک این کار را انجام می‌دهد. اگر سیستمی ادعای محرمانگی و ناشناسی

دارد، باید واسطه را از روند جابه‌جایی پول حذف کند؛ یعنی پول مستقیم به طرف مقابل برسد، بدون اینکه شخص سومی متوجه شود. این یکی دیگر از ویژگی‌های اصلی رمز-ارزهاست. فقط شما و شخص موردنظر از مبادله‌ی پول خبر دارید و کس دیگری در میان نیست.

تا اینجای کار رمز-ارزها به شما محرمانگی اطلاعات می‌دهند و می‌توانید مستقیم و بدون واسطه مبادلات مالی خود را انجام دهید. شاید با این تعریف خلاصه بتوانید حدس بزنید که چرا دولت‌ها و کشورها چندان با مفهوم رمز-ارز موافق نیستند. به یک دلیل ساده: اگر روزی برسد که رمز-ارزها بیشتر مبادلات مالی را کنترل کنند، آن روز روزَ افول مراکز قدرت مالی و در پی آن افول قدرت دولت‌هاست.

در اینجا ذکر این نکته لازم است که «رمز-ارز» با مفهومی به اسم «پول دیجیتال» متفاوت است. پول دیجیتال کانسپتی است که حتی پیش از پیدایش بیت‌کوین نیز وجود داشته است. در حال حاضر کشورها و دولت‌ها در تلاش‌اند که به‌سرعت پول‌های دیجیتال خود را در رقابت با رمز-ارزها وارد بازار کنند.

تفاوت پول دیجیتال و رمز-ارز: پول دیجیتال فقط دیجیتال است، ولی نامتمرکز نیست؛ یعنی همچنان تحت کنترل یک بانک یا مؤسسه‌ی مالی است. رمز-ارز هرگونه واسطه‌ای را نمی‌پذیرد و همین تفاوت اصلی این دو است.

برای آنکه رمز-ارزها بتوانند چنین انقلابی ایجاد و مبادلات را به شکل نامتمرکز و مستقیم مدیریت کنند و هیچ تقلبی در این سیستم صورت نگیرد، باید روی یک تکنولوژی سوار می‌شدند. این تکنولوژی «بلاک‌چین» نام دارد. در قسمت سوم با ذکر مثال و در قالب داستان توضیح دادیم که بلاک‌چین در بیت‌کوین چگونه کار می‌کند. اما به طور خلاصه می‌توان آن را این‌گونه تعریف کرد که اگر شما سیستم واسط (یعنی بانک) را حذف کنید، باید جایگزینی داشته باشید که بتواند همه‌ی این مبادلات پرحجم را درست و مرتب و بدون اشتباه و مصون از حمله‌ی هکرها و مسائلی ازاین‌قبیل، مدیریت کند. بلاک‌چین این کار را می‌کند.

در این قسمت جزئیاتِ نحوه‌ی عملکرد بلاک‌چین را توضیح نمی‌دهم؛ اما به طور خلاصه، تمام مبادلات مالی در بلاک‌هایی زنجیره‌وار ثبت می‌شوند و برای اینکه صحت هریک از این بلاک‌ها -که مبادلات در آن‌ها نوشته شده است- تأیید شود، لازم است که افرادی به‌صورت داوطلبانه، با انجام معادلات ریاضی پیچیده‌ای که با کامپیوتر انجام می‌شود، این کار را انجام دهند. این کار داوطلبانه است و اگر کسی این کار را انجام ندهد، سیستم از کار می‌افتد. ولی تقریباً غیرممکن است که این اتفاق پیش بیاید؛ چراکه سیستم در ازای این کار داوطلبانه به فرد جایزه‌ای می‌دهد که ارزشش را دارد. مثلاً اگر شما از کامپیوتر و برق خانه‌ی خود استفاده کنید تا محاسبات بلاک‌های [مثلاً] بیت‌کوین را تأیید کنید، به‌ازای هر بار که موفق شوید، سیستم به شما چند بیت‌کوین می‌دهد. این بیت‌کوین از دارایی کسی کسر نمی‌شود؛ بلکه خلق می‌شود. اصطلاحاً به این کار «استخراج یا Mining» می‌گویند. پس چاپ پول یا به عبارت بهتر خلق رمز-ارز در رمز-ارزها طی این فرایند رخ می‌دهد و به کسانی که این کار را انجم می‌دهند «معدنچی یا Miner» می‌گویند؛ زیرا کار آن‌ها باعث می‌شوند که پول جدید از دل معادن دیجیتالی خلق شود.

میزان مصرف انرژی در رمز-ارزها و تأثیرات زیست‌محیطی

این‌جاست که مصرف برق و انرژی افزایش می‌یابد. احتمالاً شما نیز شنیده‌اید که قطعی‌های گسترده‌ی برق در چند وقت اخیر، به‌خاطر استخراج رمز-ارزهاست. در ادامه چگونگی این اتفاق را توضیح می‌دهیم.

پیش‌تر که هنوز رمز-ارزها پا نگرفته بودند و استخراج رمز-ارز فراگیر نشده بود، کسی که می‌خواست معدنچی باشد و معاملات سیستم‌های رمز-ارزی را محاسبه کند (تا هم به سیستم کمک کرده باشد و هم کسب درآمد کند) می‌توانست این کار را با یک لپ‌تاپ عادی انجام دهد و فشار زیادی وارد نمی‌شد.

اما این سیستم به‌گونه‌ای تعبیه شده که هرچه افراد بیشتری درگیر Mining شوند، محاسبات به‌صورت اتوماتیک پیچیده‌تر می‌شود. چون اگر این پیچیدگی وجود نداشته باشد، همه به‌راحتی از پس این کار برمی‌آیند و موازنه به هم می‌ریزد. این‌طور تصور کنید که می‌خواهید قفل یک گاوصندوق دیجیتالی را باز کنید و به یک دستگاه کدشکن وصلش می‌کنید؛ کار ماینرها هم همین است.

هرچه افراد بیشتری در دنیا روی بازکردن این قفل کار کنند، سیستم افزایش تعداد را تشخیص می‌دهد و قفل را سخت‌تر و سخت‌تر می‌کند. اما اگر یک روز همه این کار را کنار بگذارند، سیستم آن‌قدر آسان می‌شود که دوباره با یک لپ‌تاپ هم می‌توان آن را باز کرد. به همین دلیل است که دست‌کشیدن از این کار تقریباً محال است. هرچه بگذرد تعداد ماینرها بیشتر می‌شود و کمتر نمی‌شود.

اکنون‌که تعداد ماینرها بسیار زیاد شده است، دستگاه کدشکن ما باید پیچیده‌تر باشد. هرچه پیچیده‌تر باشد، انرژی بیشتری مصرف می‌کند. شاید لازم باشد دو دستگاه کدشکن وصل کنیم، شاید سه تا، چهار تا و... . احتمالاً اسم مزارع استخراج رمز-ارز را شنیده‌اید. این مزرعه‌ها درواقع مکانی هستند (مثلاً یک سوله) که با دستگاه‌های کدشکن (ماینرها) پر شده‌اند. ماینرها همه با هم و با قدرت خیلی زیاد شروع به کار می‌کنند تا بتوانند بلاک‌های آن رمز-ارز را کدشکنی کرده و در عمل به درست کارکردن سیستمَ Peer to Peer کمک کنند و در ازای این کار جایزه بگیرند.

این تعداد بالای دستگاه ماینر، برق زیادی مصرف می‌کند. به همین دلیل کشورهایی که برق ارزانی دارند، می‌توانند بهشت مزارع استخراج رمز-ارزها باشند. سردمدار همه‌ی این کشورها چین است؛ همچنین ایسلند، گرجستان، کانادا، آمریکا، روسیه، ونزوئلا و ایران. برخی از این کشورها مازاد انرژی دارند و برخی دیگر استخراج رمز-ارزها را سوبسید می‌کنند؛ چراکه به‌صورت یک استراتژی کلان کشوری سودمند است. در حال حاضر جایزه‌ی ماین شدن هر بلاک بیت‌کوین، ۶.۲۵ عدد بیت‌کوین است؛ یعنی با قیمت امروزی نزدیک به ۲۲۰ هزار دلار. با احتساب دلار ۲۲ هزار تومانی، درآمد حاصل از تنها یک بلاک (بدون درنظرگرفتن مخارج) حدود چهار میلیارد و هشتصد میلیون تومان است. این محاسبات برای رمز-ارز بیت‌کوین است. رمز-ارزهای دیگری نیز وجود دارند که هنوز به آن‌ها نپرداخته‌ایم. بد نیست بدانید که اوایل کار جایزه‌ی استخراج بیت‌کوین حدود ۵۰ عدد بود. تقریباً هر چهار سال یک‌بار مقدار جایزه‌ای که بیت‌کوین می‌دهد، نصف می‌شود. البته این تغییر وابسته به «سال» نیست و در اصل «بعد از هر ۲۱۰ هزار بلاک» میزان جایزه نصف می‌شود که تاکنون به طور تقریبی هر چهار سال یک‌بار بوده است. این قانون در رمز-ارزهای دیگر متفاوت است.

آمار میزان برق مصرفی برای استخراج فقط بیت‌کوین را به ما نشان می‌دهد. طبق گزارش مرکز کمبریج کل میزان برقی که در دنیا برای بیت‌کوین استفاده می‌شود، چیزی حدود ۱۱۰ تا ۱۱۵ تترا وات ساعت در سال است که حدود نیم درصد از کل تولید برق جهان است. برای

درک بهتر این ارقام می‌توانیم این‌طور به آن نگاه کنیم که این مقدار برق از کل برق مصرفی برخی کشورها (مثل مالزی یا سوئد) بیشتر است. مثلاً مصرف برق ایران حدود ۲۵۵ تترا وات ساعت است. یعنی برقی که در دنیا فقط برای ماینینگ بیت‌کوین مصرف می‌شود -صرف‌نظر از رمز-ارزهای دیگر- حدود نصف مصرف برق کل ایران است. با این مقایسه می‌توانید درک کنید که وقتی می‌گویند رمز-ارزها روی محیط‌زیست تأثیرگذارند یعنی چه. حال‌آنکه این میزان بیشتر نیز خواهد شد.

پس به طور خلاصه:

مبنای اصلی مبادله‌ی مالی رمز-ارزها این است که بتواند به‌صورت مستقیم و بی‌واسطه انجام شود. برای عملی شدن این ایده، رمز-ارز باید بتواند هم‌زمان جلوی تقلب و اشتباه سیستم را بگیرد. این کار با تکنولوژی بلاک‌چین صورت می‌گیرد. افرادی که ماینر یا معدنچی نامیده می‌شوند، پازل‌های سیستم را -که بر مبنای مباحث ریاضی است- حل می‌کنند. بدین ترتیب هم سیستم کار می‌کند و هم افراد -برای اینکه انگیزه‌ی کار داشته باشند- جایزه می‌گیرند و هم پول جدید به سیستم آن رمز-ارز اضافه می‌شود.

در برخی از رمز-ارزها میزان کوین یا رمز-ارزی که استخراج می‌شود محدود است و در برخی دیگر عرضه و اضافه‌شدن پول جدید به سیستم نامحدود است (یا محدودیت سالانه دارد، اما محدودیت کلی ندارد). بیت‌کوین از دسته‌ی اول است؛ یعنی از لحاظ ماهیت عرضه‌ای شبیه فلزات گران‌بهاست. همان‌طور که طلای موجود در کره‌ی زمین محدود است و از دل معادن استخراج می‌شود، بیت‌کوین نیز تعداد محدودی دارد. تعداد کل بیت‌کوین‌ها ۲۱ میلیون عدد است که تخمین زده می‌شود استخراج آخرین دانه‌ی آن حدوداً تا سال ۲۱۴۰ طول بکشد. به همین دلیل است که بیشتر تحلیل‌گرانی که با رمز-ارزها موافق‌اند، باور دارند که قیمت این رمز-ارز بسیار بیشتر از آنچه که اکنون است، خواهد شد. فارغ از مبحث مقبولیت، یکی از دلایل ارزشمند بودن بیت‌کوین همین محدودیت در عرضه‌ی آن است.

از سوی دیگر گفتیم که فرایند ماینینگ انرژی‌بر است و هر چه این افراد بیشتر می‌شوند، درجه‌ی سختی پازل‌های سیستم برای حل کردن بیشتر می‌شود. البته این سخت‌تر شدن هم تا حدی است که مسئله در مدت‌زمان موردنظر قابل حل‌شدن باشد. هرچند بعضی از رمز-ارزها زمان مشخص ندارند. برای مثال سیستم بیت‌کوین همیشه درجه‌ی سختی پازلش را به‌گونه‌ای طراحی می‌کند که در هر ۶۰۰ ثانیه (یعنی ۱۰ دقیقه) بلاک تأیید شود؛ یعنی این ۱۰ دقیقه ثابت است. فرقی نمی‌کند که افراد بیشتری درگیر باشند یا تنها یک کامپیوتر در دنیا ماین کند؛ به‌هرحال تأیید هر بلاک ۱۰ دقیقه به طول می‌انجامد. با افزایش تعداد ماینرها شانس هر یک کامپیوتر یا قدرت پردازشگر برای این کار، کمتر و کمتر می‌شود.

از زمانی که در چند وقت اخیر پدیده‌ی رمز-ارزها رایج شده، افراد زیادی در مورد مضرات رمز-ارزها روی محیط‌زیست و رد پای کربنی‌اش صحبت کرده‌اند. اما یک مقاله‌ای از هاروارد بیزینس در همین راستا می‌خواندم که با اینکه مصرف زیاد انرژی را در مورد استخراج رمز-ارزها رد نکرده، اما نکات جالب دیگری مطرح کرده است.

- اولین موضوعی که به آن پرداخته این است که بین میزان مصرف انرژی یک سیستم و تولید کربنش تفاوت بسیار مهمی وجود دارد. این مقاله می‌گوید درست است که به‌راحتی می‌توان میزان مصرف انرژی یک سیستم را محاسبه کرد، اما بدون آن‌که بدانیم آمیخته‌ی انرژی (Energy mix) سیستم چیست، نمی‌توان مصرف انرژی را به میزان تولید کربن بسط داد. یعنی باید بدانیم که منابع انرژی آن سیستم از کجا تأمین می‌شود. سوخت‌های فسیلی، انرژی‌های تجدیدپذیر مثل انرژی‌های آبی، بادی، خورشیدی و... یا منابع دیگر؟ دلیل اهمیت این موضوع آن است که یک واحد انرژی تجدیدپذیر به نسبت یک واحد انرژی سوخت‌های فسیلی، تأثیر منفی کمتری دارد.

تخمین میزان مصرف انرژی بیت‌کوین تقریباً کار آسانی است. فقط کافی است به میزان هش‌ریت (یعنی قدرت رایانشی که برای استخراج بیت‌کوین‌های جدید ایجاد شده) نگاه کرد و تخمین زد که چه‌قدر انرژی مصرف می‌شود. اما میزان تولید کربن به این سادگی‌ها قابل حدس زدن نیست. استخراج رمز-ارزها یک بیزینس بسیار رقابتی است و ماینرها معمولاً اطلاعات زیادی نمی‌دهند. تاکنون بهترین تحلیل در مورد مصرف انرژی منطقه‌ای که می‌توان به‌وسیله‌ی آن آمیخته‌ی انرژی را حدس زد، توسط مرکز کمبریج و در مورد فایننس مطرح شده و به آن CCAF می‌گویند. این مرکز با بزرگ‌ترین مزارع استخراجی رمز-ارزها کار کرده و اطلاعاتی را به‌صورت ناشناس جمع‌آوری کرده است.

بر اساس این اطلاعات، این مرکز می‌تواند منابع انرژی‌ای که این مزارع استفاده کرده‌اند را بر اساس کشور و گاه استان حدس بزند. البته این اطلاعات شامل تمام مزارع نمی‌شود و به‌روز نیست؛ در نتیجه تصویر درستی از آمیخته‌ی انرژی بیت‌کوین نمی‌دهد.

از سوی دیگر بسیاری از تحلیل‌های پیشرفته در مورد آمیخته‌ی انرژی نیز کلی و در سطح کشوری هستند که معمولاً تصویر غلطی از برخی کشورها ارائه می‌کنند. مثل لندسکیپ انرژی چین بسیار متنوع است. در نتیجه تحلیل‌ها و تخمین‌ها در مورد اینکه انرژی استخراج بیت‌کوین در این کشور چه‌قدر از منابع تجدیدپذیر تأمین می‌شود، بسیار متفاوت‌اند. برای مثال در دسامبر ۲۰۱۹ تحلیلی منتشر شد که می‌گفت ۷۳٪ از انرژی مصرفی بیت‌کوین از منابع کربنی نیست؛ چراکه بزرگ‌ترین مزارع استخراجی بیت‌کوین که در چین و کشورهای اسکاندیناوی قرار دارند، از فراوانی انرژی‌های آبی استفاده می‌کنند، نه کربنی. از طرف دیگر چندی بعد CCAF تحلیلی منتشر کرد که این عدد را حدود ۳۹٪ نشان می‌داد. حتی اگر عدد درست ۳۹٪ باشد، بازهم این میزان دوبرابر گرید انرژی آمریکاست. به همین دلیل در واقعیت نمی‌توان فقط به مصرف انرژی بیت‌کوین نگاه و تأثیر منفی کربنی این سیستم روی محیط‌زیست را محاسبه کرد.

- عامل دیگری که به آن اشاره شده این است که مصرف انرژی بیت‌کوین با دیگر صنایع متفاوت است. به این شکل که استخراج بیت‌کوین یا هر رمز-ارز دیگری می‌تواند در هر مکانی اتفاق بیافتد. این موضوع به این دلیل اهمیت دارد: تقریباً تمام انرژی مصرفی جهان معمولاً در جایی تولید می‌شود که به مصرف‌کنندگان نهایی نزدیک باشد؛ اما بیت‌کوین چنین محدودیتی ندارد. این باعث می‌شود که ماینرها بتوانند از منابع انرژی‌ای استفاده کنند که برای کاربری‌های دیگر بلااستفاده است.

انرژی‌های هایدرو یا آبی یکی از بهترین مثال‌هاست. برای مثال در فصل بارش در استان‌های سیچوان و یونان چین، هرساله مقادیر بسیار زیادی از انرژی‌های تجدیدپذیر آبی هدر می‌رود. در این مناطق ظرفیت تولید انرژی به شدت از میزان تقاضا در آن مناطق بیشتر است. از طرفی تکنولوژی‌های باتری‌ها نیز به‌اندازه‌ای پیشرفته نیستند که بتوانند این حجم از انرژی را ذخیره کنند و آن را برای استفاده از مناطق روستایی به شهرها انتقال دهند. این مناطق از بزرگ‌ترین مناطق کره‌ی زمین در زمینه‌ی هدررفت انرژی هستند. در نتیجه متمرکز شدن بزرگ‌ترین مزارع استخراج رمز-ارزها در این مناطق چندان تصادفی نیست. این مناطق قلب چین در استخراج رمز-ارزها هستند؛ به‌طوری‌که در فصول خشک ۱۰٪ و در فصول بارانی ۵۰٪ کل ماینینگ بیت‌کوین جهان در اینجا انجام می‌شود.

انرژی دومی که می‌تواند مورداستفاده‌ی بیت‌کوین قرار بگیرد، گاز طبیعی است. برای اینکه نفت از چاه‌های نفت استخراج شود، باید گاز طبیعی سوزانده شود. در حال حاضر این گاز بدون مصرف خاصی می‌سوزد و به هوا می‌رود و محیط‌زیست را آلوده می‌کند. استارت‌آپ‌هایی به وجود آمده‌اند که از این گاز -که بی‌مصرف هدر می‌رفت- استفاده می‌کنند تا انرژی لازم برای ماینینگ را تأمین کنند. شاید بپرسید که چرا از گاز طبیعی در صنایع دیگر استفاده نمی‌کنند؟ همان‌طور که گفتیم بیشتر انرژی مصرفی صنایع در نزدیکی همان محل تولید می‌شود و از آن‌جایی که گاز طبیعی در مناطق دور و خارج از دسترس سوزانده می‌شود، بیشتر صنایع سنتی نمی‌توانند به‌درستی از آن استفاده کنند. از آن‌جایی که استخراج بیت‌کوین محدود به لوکیشن نیست، می‌تواند به‌خوبی از چنین هدررفت‌هایی استفاده کند.

البته این کار هنوز باعث تولید کربن در محیط‌زیست می‌شود و عده‌ای معتقدند که این کار باعث تشویق تولیدکنندگان نفت می‌شود. اما وقتی در مقیاس کلان سنجیده شود، باتوجه‌به این‌که استخراج نفت در زمین تا آینده‌ی نه‌چندان نزدیک ادامه خواهد داشت، این کار در کل و از لحاظ اقتصادی و محیط‌زیستی اثر مثبتی دارد.

این مقاله در سومین ایده‌اش در مورد تأثیرات محیط‌زیستی می‌گوید که انرژی موردنیاز برای بیت‌کوین بیشتر در زمان استخراج آن مصرف می‌شود و استفاده کردن از آن انرژی بسیار اندکی می‌طلبد. در حقیقت این‌که انرژی چگونه تولید می‌شود فقط یک طرف معادله است. بسیاری به‌اشتباه تصویر غلطی از نوع مصرف انرژی بیت‌کوین یا رمز-ارزهای مشابهش دارند.

معمولاً خبرنگارها و افراد آکادمیک از واحد سنجشی با عنوان «نرخ هزینه‌ی انرژی در هر مبادله» استفاده می‌کنند و می‌گویند این نرخ در مورد ارزی مثل بیت‌کوین بسیار بالاست. در صورتی که بیشتر مصرف انرژی در رمز-ارزها در زمان استخراج آن‌ها اتفاق می‌افتد. انرژی‌ای که پس از استخراج و برای تأیید مبادلات استفاده می‌شود، بسیار کمتر و ناچیز است.

کیف‌های پول و کلیدها

چگونه باید رمز-ارزها را نگه‌داری کنیم؟ پرداخت این پول‌ها چگونه است؟ ما که مثلاً ۲ میلیون تومان پول داریم، چه رمز-ارزی می‌توانیم بخریم وقتی قیمت هرکدام این‌قدر بالاست؟

از بابت میزان خرید نگران نباشید. باهر مقدار پولی که دارید، می‌توانید این کار را بکنید. فکر نکنید که اگر یک عدد بیت‌کوین ۳۵ هزار دلار است، پس شما قدرت خرید ندارید. واحد شمارش بیت‌کوین یا رمز-ارزها کمتر از ۱ است. برای مثال خود بیت‌کوین تا ۸ رقم اعشار قابل خرد شدن است. اگر میانگین نرخ هر مبادله کاهش پیدا کند، پروتکل‌های بیت‌کوین در آینده می‌توانند بیشتر هم خرد شوند. پس نگران این بخش نباشید.

پس از خرید رمز-ارزها باید از آن‌ها نگه‌داری کنید. در حقیقت شما باید اول یک کیف پول دیجیتال داشته باشید که رمز-ارزها در آن نگه‌داشته می‌شوند. کیف پول دیجیتال در اصل یک اپلیکیشن است که شما با داشتن آن عملاً یک حساب بانکی دارید.

هر کیف پول یک آدرس خاص دارد که از ترکیب یک سری حروف بزرگ و کوچک الفبای انگلیسی به همراه اعداد تشکیل شده است. این آدرس مثل شماره‌حساب شماست که می‌توانید در اختیار دیگران قرار دهید. البته بسیاری از کیف پول‌ها در هر تراکنش آدرس جدیدی تولید می‌کنند.

علاوه بر این، همان‌طور که برای ورود به حساب‌های بانکی در اپلیکیشن‌ها و اینترنت به یوزرنیم و پسورد نیاز دارید، کیف پول دیجیتال شما نیز یک کلید عمومی و یک کلید خصوصی دارد. اگر به یاد داشته باشید گفتیم که یکی از ویژگی‌های رمز-ارزها ناشناس بودن صاحبان آن‌هاست. در حقیقت وقتی شما یک کیف پول دیجیتال باز می‌کنید، کسی از شما مشخصات هویتی نمی‌پرسد. در بانک از شما کارت ملی می‌خواهند تا تشخیص دهند صاحب کدام حساب هستید. در رمز-ارزها یک «کلید خصوصی» به شما داده می‌شود که از توابع رمزنگاری شده‌ی ریاضی به دست می‌آید. یک کد عجیب‌وغریب عریض‌وطویل است که اگر گم شود، به این معنی است که عملاً راه دسترسی به همه‌ی ارزها قطع می‌شود و اگر هک شود یا شخص دیگری به هر طریق از آن اطلاع پیدا کند، عملاً آن شخص صاحب تمام دارایی‌های شماست. به همین دلیل پیشنهاد می‌شود که از این کلید خصوصی در جاهای مختلف بک‌آپ بگیرید. مثلاً آن را روی یک تکه کاغذ بنویسید یا در هارد، فلش، صندوق امانات و... نگهداری کنید.

علاوه بر این شما یک کلید عمومی دارید که می‌توانید با دیگران به اشتراک بگذارید. این کلید عمومی با آدرس شما متفاوت است. البته خیلی از کیف پول‌ها هستند که کلید عمومی و آدرس را به یک شکل نمایش می‌دهند، ولی در اصل با هم تفاوت دارند. در علم رمزنگاری وقتی کلید عمومی با کلید خصوصی ترکیب شوند، با هم هماهنگ می‌شوند و نشان می‌دهد که شما صاحب حساب هستید. کلید عمومی بر اساس الگوریتم‌های خاص و از روی کلید خصوصی به وجود می‌آید، ولی برعکسش امکان ندارد. یعنی شما نمی‌توانید از روی کلید عمومی کسی بتوانید کلید خصوصی‌اش را حدس بزنید.

این سیستم رمزنگاری بسیار پیشرفته تقریباً امکان تقلب را به صفر رسانده است. اما هم‌زمان که این سیستم رمزنگاری بسیار پیشرفته است و خیال شما را راحت می‌کند، شما باید از اطلاعات شخصی خود بیشتر مراقبت کنید؛ چراکه دیگر سیستمی مانند بانک وجود ندارد که مراقب شما باشد و امکان شکایت از سیستم به یک مرجع دیگر وجود ندارد. اگر اطلاعات خود را گم کنید، همه چیز تمام می‌شود. اگر به‌خوبی از کلید خصوصی خود نگهداری نکنید یا هکرها به سیستم شما دسترسی پیدا کنند، تمام رمز-ارزهای خود را از دست می‌دهید. به همین دلیل توصیه می‌شود که آن را در جایی ذخیره کنید که مثلاً به کامپیوتر متصل نباشد تا دسترسی به آن به‌راحتی میسر نباشد.

کیف پول‌های مختلفی وجود دارد که می‌توانید از هرکدام استفاده کنید. پس از آن‌که کیف پول دیجیتال خود را باز کردید، زمان آن رسیده که از یک صرافی رمز-ارز بخرید. ناگفته نماند که معمولاً کیف پول‌هایی که متعلق به صرافی هستند، مستعد هک شدن توسط هکرها هستند. برای مثال «ماونت گاکس» (غول ژاپنی صرافی‌های رمز-ارزی) به‌خاطر هک شدن بخشی از رمز-ارزهایش به ارزش ۴۵۰ میلیون دلار، بسته شد.

تاریخچه‌ی توسعه‌ی رمز-ارزها

قبل از پیدایش بیت‌کوین مبانی نظری رمز-ارز از مدت‌ها قبل وجود داشت. در دهه‌ی ۸۰ «دیوید چاوم» الگوریتمی ابداع کرد که مبنای

رمزنگاری اینترنتی مدرن شد؛ همان مبنایی که بعدها مورداستفاده‌ی رمز-ارزها قرار گرفت.

۱۵ سال بعد شخصی به نام «Wei Dei» یک white paper منتشر کرد که یک پول را در آن معرفی کرده بود: B-Money. بیشتر مفاهیم پایه‌ای رمز-ارزهای مدرن در این مقاله آمده بود؛ اما این پول هیچ‌وقت فراگیر نشد، چون نتوانست ابزار مبادله شود. یک پول برای ارزش یافت باید ویژگی‌هایی داشته باشد. مثلاً شما همین‌الان می‌توانید یک تکه کاغذ چاپ کنید و بگویید این «پول» است. هیچ‌کس مانع شما نمی‌شود. اما برای اینکه پول شما ارزش بیابد، باید یک سری ویژگی داشته باشد. مهم‌ترین خاصیت پول این است که بتوانید با آن چیزی را معامله کنید؛ یعنی باید بتوانید کاغذی که چاپ کرده‌اید را به میوه‌فروشی ببرید و بگویید «این پوله. حالا باهاش دو کیلو خیار بده.» اگر میوه‌فروش توانست این پول را قبول کند، شما یکی از ویژگی‌های اصلی پول را تیک زده‌اید. قبول کردن پول نباید ازسرلطف باشد؛ بلکه میوه‌فروش به این باور رسیده باشد که خود او نیز می‌تواند با این پول خرید کند. اولین باری که بیت‌کوین توانست ابزار معامله قرار بگیرد زمانی بود که یک نفر در ازای خرید دو پیتزا، ۱۰ هزار بیت‌کوین داد. پول ویژگی‌های دیگری نیز دارد که در قسمت‌های قبلی (مثل تاریخ پول) گفته‌ایم.

در ادامه‌ی مسیر توسعه‌ی رمز-ارزها به دهه‌ی ۹۰ و ۲۰۰۰ می‌رسیم که دوره‌ی پا گرفتن واسطه‌های مالی دیجیتالی بود؛ از جمله پی‌پال (PayPal) که «ایلان ماسک» یکی از بنیان‌گذاران آن است. ولی تا زمانی که بیت‌کوین در سال ۲۰۰۸ به وجود نیامده بود، در واقع هیچ رمز-ارزی وجود نداشت.

در سال ۲۰۰۸ یک شخص یا گروه ناشناس با اسم مستعار ساتوشی ناکاموتو white paper بیت‌کوین را ارائه کردند. White paper یکی از اصطلاحاتی است که در این حوزه زیاد می‌شنوید. White paper در حقیقت شبیه یک تز یا مقاله است که در آن فلسفه‌ی وجودی آن رمز-ارز معرفی می‌شود و با خواندنش می‌توانید به ویژگی‌های رمز-ارز مربوطه پی ببرید.

سال ۲۰۰۹ که بیت‌کوین معرفی شد، گروه‌هایی از افراد استفاده از این رمز-ارز را شروع کردند. در قسمت سوم به‌تفصیل درباره‌ی این گروه‌ها و دلایل استفاده‌شان از بیت‌کوین توضیح داده‌ایم.

یک سال بعد رمز-ارزهای دیگری به بازار سرازیر شدند. به تمامی این رمز-ارزهای بعدی «آلت‌کوین» می‌گویند که از ترکیب واژه‌های «آلترناتیو» و «کوین» ساخته شده است؛ یعنی رمز-ارزهای جایگزین بیت‌کوین که همگی مشتقی از بیت‌کوین‌اند. یکی از اولین آلت‌کوین‌ها که در سال ۲۰۱۰ به بازار آمدند، «نیم‌کوین» و «لایت‌کوین» بودند. در همین زمان بود که صرافی‌های رمز-ارزی به وجود آمدند.

در سال ۲۰۱۲ پلتفرم wordpress -که یکی از بزرگ‌ترین پلتفرم‌های ساخت وبسایت است- اولین جایی بود که بیت‌کوین را به‌عنوان پول قبول می‌کرد. پس از آن شرکت‌های بزرگی مانند newegg.com، آژانس مسافرتی اکسپدیا، مایکروسافت و تسلا نیز اضافه شدند.

جالب است بدانید که بالغ‌بر ۱۰ هزار آلت‌کوین وجود دارد و امروزه حدود ۶۰٪ از کل بازار رمز-ارزها را در دست دارند. چند وقت پیش که بازار رمز-ارزها در اوج خودش بود، ارزش کل رمز-ارزها به ۲ تریلیون و ۴۰۰ میلیارد دلار رسید. الان و پس از افتی که این بازار تجربه کرد، به بازهٔ ۱ تریلیون و ۵۰۰ میلیارد دلار رسیده است.

همان‌طور که می‌شود حدس زد، بزرگ‌ترین رمز-ارز بیت‌کوین است که حدود ۴۳٪ بازار را به خودش اختصاص داده. اما نکته‌ی جالب این است که بدانید سهم بیت‌کوین از بازار کل رمز-ارزها در حال کوچک‌تر شدن است. در ابتدای سال ۲۰۲۱ سهم بیت‌کوین از بازار کل رمز-ارزها چیزی حدود ۷۰٪ بود و این نشان‌دهنده‌ی اقبال عمومی در قبال آلت‌کوین‌هاست.

بعد از بیت‌کوین، اتریوم با حدود ۱۸٪ سهم بازار، تتر با حدود ۴٪ ، بایننس‌کوین با حدود ۳.۵٪، کاردانو با حدود ۳٪ و دوج‌کوین با حدود ۲.۵٪ از بزرگ‌ترین‌های بازار رمز-ارز هستند که در ادامه به طور خلاصه آن‌ها را معرفی می‌کنیم.

معرفی آلت‌کوین‌ها

اگر بخواهیم به‌صورت دسته‌بندی‌شده نگاهی به بازار رمز-ارزها کنیم، باید بگوییم که همه چیز با بیت‌کوین شروع شد، اما در ادامه متوجه شدند که بیت‌کوین هم ایراداتی دارد. در نتیجه رمز-ارزهایی مشابه بیت‌کوین به وجود آمدند که سعی کرده بودند مشکلات بیت‌کوین را رفع کنند. البته ما این‌ها را در دستهٔ رمز-ارزهایی که صرفاً برای پرداخت استفاده می‌شوند تقسیم‌بندی می‌کنیم که خود نیز زیرشاخه‌های متفاوتی دارند.

برخی از این رمز-ارزها مثل لایت‌کوین، بیت‌کوین‌کش و دوج‌کوین، در واقع همان بیت‌کوین‌اند که سعی کرده‌اند کمی بهتر باشند. مثلاً سرعت مبادلات یکی از نکته‌هایی هست که بیشتر آلت‌کوین‌ها در صدد بهبود آن بوده‌اند. گفتیم سرعت مبادلات در هر بلاک بیت‌کوین ۱۰ دقیقه است. این آلت‌کوین‌ها این سرعت را کمتر کرده‌اند.

وقتی شما یک مبادله‌ی بیت‌کوینی انجام می‌دهید، آن مبادله در لحظه ثبت و انجام نمی‌شود. هر مبادله باید در یک بلاک انجام شود که ۱۰ دقیقه طول می‌کشد تا این بلاک به بلاک بعدی برود. این ۱۰ دقیقه همان مدت‌زمانی است که طول می‌کشد تا تمام کامپیوترهای در حال ماینینگ جهان تلاش می‌کنند تا آن مسئله‌ی ریاضی را حل کنند. از طرفی هر بلاک (مثل هر سیستم ذخیره اطلاعات دیگری) ظرفیت محدودی برای ذخیره‌ی اطلاعات دارد. ظرفیت هر بلاک بیت‌کوین حدود ۱ مگابایت است. یعنی هر بلاک می‌تواند حدود ۲۷۰۰ مبادله را در خود جا دهد. ۲۷۰۰ مبادله در ۱۰ دقیقه می‌شود حدود ۴.۵ مبادله در هر ثانیه. اگر این مقدار را با تعداد مبادله در ثانیه‌ی (مثلاً) سیستم «ویزا» مقایسه کنید، متوجه می‌شوید که مشکل کجاست. ویزا همان سیستم مالی ویزاست که احتمالاً credit cardهایش را دیده‌اید. ویزا در هر ثانیه ۱۷۰۰ مبادله را مدیریت می‌کند. این مشکل به این معناست که وقتی تعداد مبادلات در بیت‌کوین زیاد می‌شود، صف‌های طولانی به وجود می‌آید. یعنی مبادله‌ی شما برای ثبت شدن در صف انتظار قرار می‌گیرد و این یکی از ایراداتی است که به بیت‌کوین وارد می‌شود. گفته می‌شود که بیت‌کوین به‌خاطر این مشکل به رمز-ارزی تبدیل نمی‌شود که برای مبادلات روزمره مورد علاقه‌ی مردم باشد و بیشتر به آن به‌عنوان کالای سرمایه‌ای می‌نگرند. در نتیجه آلت‌کوین‌های دیگر آمدند که هرکدام به روشی سعی کردند این مشکل را حل کنند. مثلاً بیت‌کوین‌کش آن ظرفیت را از ۱ مگابایت به ۸ مگابایت ارتقا داده و بدین ترتیب سرعت مبادلات را بیشتر کرده است. در دوج‌کوین ۱ دقیقه طول می‌کشد تا هر بلاک تأیید شود. این زمان در لایت‌کوین -بسته به فشاری که به سیستم وارد می‌شود- بین ۲ تا ۸ دقیقه است. پس سرعت مبادلات یکی از تفاوت‌های آلت‌کوین‌هاست.

تفاوت دیگر در محدودیت عرضه‌ی رمز-ارز است. گفتیم که بیت‌کوین مثل طلاست و در نهایت میزان عرضه‌ی آن محدود است. تمام

بیت‌کوینی که وجود دارد ۲۱ میلیون است. این قضیه در برخی از رمز-ارزها متفاوت است. مثلاً عرضه‌ی لایت‌کوین نیز مانند بیت‌کوین محدود است، ولی تعدادش چهار برابر بیت‌کوین است. یعنی استخراج لایت‌کوین هم روزی به پایان می‌رسد، ولی به‌جای ۲۱ میلیون، ۸۴ میلیون عدد است. در مقابل دوج‌کوین محدودیت عرضه ندارد و قرار نیست که روزی به پایان برسد. از طرفی مثلاً رمز-ارزهایی مثل اتر در اتریوم محدودیت عرضه در سقف ندارد، ولی محدودیت ماین کردن سالانه دارد.

به‌صورت کلی نکته‌ای که باید در مورد میزان عرضه دانست این است که اگر عرضه محدود باشد (و البته با درنظرگرفتن عوامل دیگر، مانند اقبال عمومی آن رمز-ارز) هرچه جلوتر می‌رویم ارزش آن رمز-ارز در آینده بیشتر می‌شود. مثل بیت‌کوین و البته مثل طلا. به روند ارزش طلا در مرور زمان نگاه کنید؛ طلا همیشه کالای سرمایه‌ای بوده است. البته این به این معنا نیست که رمز-ارزهایی که سقف عرضه‌ای محدود ندارند، در آینده ارزشمندتر نخواهند شد.

از میان رمز-ارزها دسته‌ی دیگری به وجود آمدند که در پی افزایش میزان محرمانگی بودند. به این‌ها Privacy Coins می‌گویند. به‌صورت خلاصه در این رمز-ارزها، به‌غیراز دو نفری که در یک مبادله شرکت می‌کنند، هیچ‌کس دیگری از آن مبادله خبردار نخواهد شد و آن مبادله به‌هیچ‌وجه قابل ردیابی نیست. محرمانگی در رمز-ارزهای دیگر هم بالاست، ولی مبادلات در لجر کلی قابل‌رؤیت‌اند. در Privacy Coinها هیچ ردی از مبادلات دیده نمی‌شود. مثلاً رمز-ارزهای دش (DASH)، مونرو (Monero) و زد کش (Zcash) از این دسته‌اند.

دسته‌ی دیگری از رمز-ارزها به وجود آمدند که جلوی نوسانات قیمتی را بگیرند. به این دسته از رمز-ارزها stable coins می‌گویند. stable یعنی ثبات. سیستم این رمز-ارزها به‌گونه‌ای است که ارزششان به یک چیز باثبات دیگر بستگی دارد؛ مثل ارزش دلار. یعنی ارزش این رمز-ارزها با ارزش دلار تغییر می‌کند.

مهم‌ترین این رمز-ارزها تتر Tether است که با حروف اختصاری USDT در صرافی‌ها شناخته می‌شود. دلیل پیدایش این رمز-ارزها این بود که اگر قرار باشد از رمز-ارز برای مبادلات روزمره استفاده شود، این پول باید ثبات داشته باشد. پولی که ارزش آن مدام متغیر باشد، به‌سختی می‌تواند در پرداخت‌های عادی روزمره‌ی مردم و در سطح وسیع مورداستفاده قرار بگیرد. یکی از دلایل این نوسانات بالا این است که «مارکت کپ» این پول‌ها (یعنی کل ارزش در چرخه‌ی این پول‌ها) فعلاً کوچک است و هرقدر این کل کوچک‌تر باشد، بیشتر تحت تأثیر جریانات بازار قرار می‌گیرد و دچار نوسان می‌شود.

در نتیجه این رمز-ارزها به وجود آمدند که هم ثبات پول‌هایی مثل دلار را داشته باشند و هم از فواید سهولت رمز-ارزی نفع ببرند. اما نکته این است که فعلاً جاهای بسیار محدودی رمز-ارزها و در لایه بعدی این نوع رمز-ارزها را به‌عنوان پول قبول می‌کنند؛ پس همچنان نمی‌شود در مبادلات روزمره از آن‌ها استفاده کرد. در حال حاضر تاجران از این رمز-ارزها در مبادلات رمز-ارزی استفاده می‌کنند. همان‌طور که گفتیم ارزش رمز-ارزی مانند تتر وابسته به دلار و ثابت است. در نتیجه وقتی تجار رمز-ارزی بخواهند ریسک پرتفوی خود را کم کنند، می‌توانند رمز-ارزهای پرنوسان را به تتر تبدیل کرده و اگر خواستند دوباره به یک رمز-ارز دیگر برگردانند.

فرض کنید الان در دوره‌ای هستیم که ارزش بیت‌کوین تا ۶۰ هزار دلار بالا رفته بود و شما حدس می‌زنید که ریسک ریزش دارد. به همین دلیل بیت‌کوین خود را به تتر تبدیل می‌کنید (چون ارزش تتر تقریباً همیشه ثابت است و تغییر چندانی نمی‌کند). با این کار گویی شما پول خود را به دلار تبدیل کرده‌اید. پس از اینکه بیت‌کوین ریزش کرد، می‌توانید دوباره تتر را به بیت‌کوین برگردانید، ولی این بار با همان پول، بیت‌کوین بیشتری می‌خرید. این یکی از استفاده‌هایی است که در حال حاضر از stable coinها می‌شود؛ اما فلسفه‌ی وجودی‌شان چیزی است که در ابتدا گفتیم.

از این‌ها که بگذریم، به پلتفرم‌ها می‌رسیم. پلتفرم‌ها چیزی فراتر از یک ارز یا پول هستند. یک‌بار دیگر مرور کنیم که ایدهٔ بیت‌کوین چه بود: ایده این است که پولی به وجود بیاید که نامتمرکز باشد؛ یعنی واسطه‌ای در کار نیست که سامانه توسط او کنترل شود و خود سیستم با تکنولوژی بلاک‌چین این کار را انجام می‌دهد. بدین ترتیب واسطه‌ها (دولت‌ها، بانک‌های مرکزی و مؤسسات مالی) را دور می‌زند. اگر بخواهیم تمام این ساختار را بدون مشکل دور بزنیم، باید زیرساخت قوی‌ای داشته باشیم که بلاک‌چین این کار را انجام می‌دهد. تمام پروتکل‌های محاسبات ریاضی و برق و... نیز برای این است که این سیستم بتواند کار کند.

وقتی بیت‌کوین بلاک‌چین را معرفی کرد، انسان‌ها به‌تدریج به این فکر افتادند که اگر می‌توان واسطه‌های بزرگ پولی را دور زد و سیستم را غیرمتمرکز کرد، پس چرا همه چیز را غیرمتمرکز نکنیم؟ مثلاً خود اینترنت را غیرمتمرکز کنیم. چند لحظه به عظمت ایده فکر کنید ... اما مگر اینترنت متمرکز است؟ تقریباً بله. در ادامه با چند مثال می‌بینیم که بلاک‌چین چه قابلیت‌هایی دارد.

فرض کنید که می‌خواهید اسنپ یا تپسی بگیرید. اتفاقی که می‌افتد این است: شما برنامه‌ی اسنپ را باز می‌کنید. درخواست ماشین را ارسال می‌کنید. درخواست شما ابتدا به سیستم اسنپ وارد می‌شود و از آن‌جا به راننده منتقل می‌شود. راننده درخواست را تأیید کرده و به سمت آدرس شما حرکت می‌کند. پس از آن‌که به مقصد می‌رسید، آنلاین و از طریق کیف پول برنامه، کرایه را پرداخت می‌کنید. این پول به حساب اسنپ می‌رود و پس از اینکه اسنپ کمیسیون خود را برداشت، باقی‌مانده را به حساب راننده منتقل می‌کند. پس الان بین شما و راننده شرکتی به نام تپسی و اسنپ قرار دارند که این فرایند را مدیریت می‌کنند. حالا فرض کنید که این شرکت را از وسط بردارید و حذفش کنید. یعنی درخواست شما مستقیم به راننده می‌رسد و یک سیستم (یک سیستم، نه یک شرکت) واسطه‌ی شماست و فرایند را مدیریت می‌کند. این سیستم همان بلاک‌چین است. با این کار آن کمیسیون می‌تواند هم از کرایه‌ی شما کم شود و هم درآمد راننده را بیشتر کند. کار بلاک‌چین همین بود. اگر شما توانستید بانک مرکزی را دور بزنید و برای کل مبادلات مالی جهان راه‌حل پیدا کردید، انجام‌دادن این کارها هم شدنی است.

در حال حاضر شما یک جنس را برای فروش در دیوار و شیپور می‌گذارید و ظاهراً مستقیم به خریدار متصل می‌شوید؛ ولی در حقیقت یک واسطه به نام همین شرکت‌ها در میان است که این کارها را انجام می‌دهد. بلاک‌چین می‌تواند این واسطه را حذف کند.

شما با این کار عملاً می‌توانید مراکز قدرت را کلاً از بین ببرید. در انتخابات ریاست‌جمهوری یا هر چیز دیگری هم می‌شود از این سیستم استفاده کرد. وقتی شما پای صندوق‌های رأی حاضر می‌شوید، در اصل به سیستمی اعتماد می‌کنید که رأی‌های شما را همان‌طور که هست، بشمارد و کاندیدای موردنظر را انتخاب کند؛ پس رأی را در صندوق می‌ریزید. اما بلاک‌چین می‌گوید اصلاً نیازی به اعتماد نیست؛ چون من می‌توانم سیستمی ایجاد کنم که همه‌ی رأی‌ها را مستقیم و بدون حضور هیچ قدرت متمرکزی بشمارد و کسی که بیشترین رأی را اخذ می‌کند،

انتخاب خواهد شد. این واقعاً یک انقلاب است!

یکی دیگر از کانسپت‌هایی که در حال حرکت به این سمت است، فایننس است. امروزه مفهومی به نام DeFi به وجود آمده که مخفف «Decentralized Finance» و به معنی «امور مالی غیرمتمرکز» است. ایده این است که در مباحث مالی نیز می‌توان تمرکززدایی کرد. مثلاً بورس و بیمه و... را می‌توان با بلاک‌چین غیرمتمرکز کرد.

این کار با استفاده از قراردادهای هوشمند (Smart contracts) شدنی است. یک قرارداد مجموعه‌ای از اگرها و نتیجه‌ها و سپس‌ها است. مثلاً قرارداد خرید خانه به این شکل است که اگر خریدار ۲ میلیارد پول به حساب فروشنده واریز کرد، سپس خانه از تملک فروشنده درآمده و به خریدار می‌رسد. یک قرارداد هوشمند این شروط و نتیجه را می‌فهمد و زمانی که شرط اتفاق افتاد، نتیجه را حاصل می‌کند. این مبنای فلسفه وجودی چیزی به نام «اتریوم» است. اتریوم در سال ۲۰۱۳ به‌عنوان یک پلتفرم -که فراتر از تنها یک رمز-ارز است- به وجود آمد. در حقیقت اتریوم پلتفرمی است که از برنامه‌نویس‌ها دعوت می‌کند که برنامه‌های غیرمتمرکز بنویسند و البته زبان برنامه‌نویسی مخصوص خودش را دارد که solidity نامیده می‌شود. درواقع اتریوم دیگر تنها یک پول نیست؛ بلکه به‌طورکلی یک زیرساخت برای اجرای آن ایده‌ی بلاک‌چینی است.

اگر شما بخواهید هریک از این ایده‌های بلاک‌چینی را که مثال زدیم (مثل اسنپ و انتخابات و...)، به آن شکل انقلابی پیش ببرید، لازم است که آن سیستم بلاک‌چین توسط تعداد زیادی کامپیوتر غیرمتمرکز کار کند. این سیستم چگونه تأمین می‌شود؟ اتریوم این سیستم جهانی را راه انداخته و برای اینکه افراد را در سراسر دنیا تشویق به همکاری کند، رمز-ارز اِتر (Ether) را نیز به وجود آورده است. پس اتریوم رمز-ارز نیست؛ این اِتر است که رمز-ارز بوده و برای سیستم اتریوم در حکم سوخت است. درواقع افراد برای انجام محاسبات اتریوم و تأیید مبادلات در این سیستم -که اصطلاحاً ماین کردن یا فورج کردن گفته می‌شود- اتر جایزه می‌گیرند. به برنامه‌هایی که بر بستر مثلاً اتریوم شکل می‌گیرند، dApps یا decentralized Applications (برنامه‌های غیرمتمرکز) می‌گویند.

به‌عبارت‌دیگر اگر فرض کنیم که مثلاً بیت‌کوین یک اپلیکیشن است، اتریوم در حقیقت یک اپ‌استور یا پلی‌استور است که برنامه‌های مختلفی روی آن سوار می‌شوند. ارزی نیز در این اکوسیستم استفاده می‌شود که اِتر است.

«اتریوم» و رقیب چینی‌اش «نِئو» دو پلتفرم بزرگی هستند که سبک و سیاقشان با رمز-ارزهایی که تنها برای پرداخت استفاده می‌شوند فرق دارد و به همین دلیل «پلتفرم» نامیده می‌شوند.

وقتی چنین پلتفرم‌هایی به وجود آمدند، رمز-ارزهای دیگری نیز بر اساس آن‌ها شکل گرفتن که به آن‌ها Token می‌گویند. Tokenها در اصل رمز-ارزهایی‌اند که سیستم بلاک‌چین مستقلی مانند بیت‌کوین ندارند و روی یک سیستم سوار می‌شوند. بیشتر توکن‌ها بر بستر اتریوم قرار دارند؛ یعنی از آن زیرساخت استفاده می‌کنند و همین امر مقبولیت اِتر را بالاتر می‌برد. توکن‌ها در حقیقت کوین نیستند. چیزی هستند که چیز دیگری را نمایندگی می‌کند. احتمالاً بازی Clash of Clans را در موبایل‌ها دیده‌اید. در این بازی شما یک دهکده دارید که برای توسعه‌ی آن تلاش می‌کنید و با دوستان خود به دهکده و شهرهای دیگر حمله می‌کنید. برای اینکه در این بازی مدت زیادی در صف نمانید یا ساخت‌وساز یک آبجکت زیاد طول نکشد، می‌توانید Token بخرید و Tokenها را به‌عنوان پول بازی خرج کنید. طبیعتاً پول فیزیکی مانند ریال را نمی‌توان وارد بازی کرد! این کار مانند ژتون خریدن است. مثلاً برای وارد شدن به برخی شهربازی‌ها باید اول ژتون بخرید یا یک کارت را شارژ کنید تا بتونید از دستگاه‌ها استفاده کنید.

Tokenها نیز در رمز-ارزها چنین نقشی را برای برنامه‌های dApps (غیرمتمرکز) ایفا می‌کنند. مثلاً اگر بخواهید برنامه‌ای برای خریدوفروش خانه بدون حضور بنگاه داشته باشید، باید یک Smart Contract وجود داشته باشد. این قرارداد هوشمند متوجه می‌شود که مثلاً اگر ۲ میلیارد پول از حساب خریدار خارج شد، باید این خانه به نام او شود. بدیهی است که نمی‌توانیم خانه را به شکل فیزیکی وارد قرارداد کنیم و باید یک چیزی نماد آن باشد. این‌جاست که یک Token به خریدار منتقل می‌شود و گویای آن است این خانه به او تعلق دارد.

برای مثال توکنی به نام Wepower (با حروف اختصاری WPR) وجود دارد که یک چیز فیزیکی را نمایندگی می‌کند. با این token و با استفاده smart contractها برق خریدوفروش می‌کنند. در حقیقت هر واحد WPR میزانی از انرژی را نمایندگی می‌کند.

به‌تازگی دسته‌ی دیگری از Tokenها که باب شده‌اند که به آن‌ها NFT یا Non Fungible Tokens می‌گویند. برای توضیح این دسته باید اول بدانیم خاصیت Fungibility در دنیای مالی و پول به چه معناست. پولی که در دست من و شماست قابل تبدیل و تعویض است. من اگر به شما یک ده‌هزار تومانی بدم، با ده‌هزار تومانی‌ای که خودتان دارید، برابر است. یا اگر شما به من ده تومان بدهید و پول خرد بخواهید، من می‌توانم به شما دو تا ۵ تومانی یا مثلاً ده تا هزارتومانی بدهم که این با ده تومانِ اولیه‌ی شما برابر است. اما همه چیز این خاصیت fungible بودن را ندارند. مثلاً نمی‌توان تابلوی «مونالیزا» اثر داوینچی را داد و یک اثر پیکاسو گرفت. این دو با هم یکی نیستند؛ چون از هرکدام فقط یک عدد وجود دارد. اثر انگشت شما با اثر انگشت شخصی دیگر مساوی نیست. نمی‌توان آن را تعویض کرد و همان چیز را دریافت کرد. در واقع بعضی چیزها منحصر به فردند.

بر اساس همین تفکر روشی ایجاد کرده‌اند که شما می‌توانید این آثار منحصربه‌فرد را بفروشید. مثلاً چند وقت پیش یک ایرانی نزدیک به ۳ میلیون دلار پول داد و اولین توییت آقای جک دورسی (مؤسس توییتر) را خرید! اما «خریدن اولین توییت یک نفر» یعنی چه؟

در حقیقت NFT یک سند دیجیتال است که نشان می‌دهد شما مالک یک چیز دیجیتال هستید. مثلاً من اولین عکسی که شما ۴ سال پیش در اینستاگرام گذاشتید را می‌خرم. عکس همچنان در صفحه‌ی شماست و به من منتقل نمی‌شود، ولی متعلق به من است و صاحب‌اختیار آن عکس منم!

سینا استوی که مؤسس «کریپتولند» بود و چندی پیش دستگیر شد، همان کسی بود که این اولین توییت جک دورسی را خرید. برای اینکه این‌جور خریدها را درک کنید، باید کلکسیونرها را بشناسید. این خرید نیز مانند خریدن یک اثر هنری است.

فکر کنید که من بسیار معروف شوم و در دنیا ۴۰۰ میلیون نفر شنونده داشته باشم. حالا یک جمله‌ی ۵ ثانیه‌ای می‌گویم؛ مثلاً «سلام. من فرشاد محمودی‌ام و دوستون دارم.» و این چند ثانیه صدا را به‌صورت NFT به حراج بگذارم. یک نفر این صدا را از من می‌خرد و من در متادیتای فایل می‌نویسم و امضا می‌کنم که فلانی صاحب این صداست. صدسال بعد و پس از مرگ من که قیمت فایل چندبرابر شده است، نوه‌های کسی که صدا را خریده، صدا را به کس دیگری می‌فروشند.

با این روش خرید و فروش‌های بسیار عجیب‌وغریبی صورت گرفته است؛ از یک کلیپ گرفته تا ایموجی و توییت و نقاشی آنلاین و هر

چیزی که فکر کنید. می‌توانید در سایت Valuables توییت‌هایی که برای فروش گذاشته‌اند را ببینید. گران‌ترین NFTای که فروش رفته یک کلاژ دیجیتال به اسم The first ۵۰۰۰ days بوده که در آن فردی به اسم مایکل وینکلمن ۵۰۰۰ تا تصویر روزمره را کنار هم چیده است. برای خرید NFT این کلاژ در حراجی معروف کریستی لندن، یک برنامه‌نویس از سنگاپور حدود ۴۲ هزار و ۳۲۹ اِتر رمز-ارز پرداخت کرده که معادل ۶۹ میلیون دلار است. جالب است بدانید که با پرداخت این مقدار تنها حق به نمایش درآوردن اثر را خریده، نه حق کپی‌رایت کلاژ را. سازنده‌ی کلاژ نیز تصویر فول‌رزولوشن را در یک موزه‌ی دیجیتال به اسم متاورس به نمایش گذاشته است.

حالا متوجه شدیم که Tokenها چگونه روی پلتفرم‌ها می‌نشینند و چه‌کارهایی می‌توان با آن‌ها کرد.

این مختصری بود از آپدیت دنیای رمز-ارزها. مشخص نیست که چه پیشامدهایی در آینده منتظر ما هستند، اما بسیاری از تحلیل‌ها باور دارند که این جنبش دیگر از حرکت نمی‌ایستد و این انقلاب به بلوغ خواهد رسید. ارزش این رمز-ارزها در آینده بسیار بیشتر خواهد بود. چند روز پیش السالوادور اولین کشوری بود که بیت‌کوین را به‌صورت رسمی به‌عنوان یک پول پذیرفت و بناست که از انرژی آتشفشان برای ماینینگ استفاده کند.

فراموش نکنید که باید مراقب شِت‌کوین‌ها (رمز-ارزهای بی‌ارزش) نیز باشید. هرگاه پدیده‌ای توجه‌ها را به خود جلب می‌کند، افرادی پیدا می‌شوند که به فکر سودجویی از آن طریق هستند و این قضیه در مورد رمز-ارزها نیز صادق است. کلاهبردارانی هستند که شت‌کوین‌هایی را به وجود می‌آورند؛ تبلیغات وسیع و کمپین PR در اینترنت ایجاد می‌کنند، صف‌های سوری خرید شکل می‌دهند، قیمت رمز-ارز سوری را بالا می‌برند و پس از ملت آنکه مردم خرید کردند و همه‌ی ارزها به فروش رفتند، ناپدید می‌شوند و شما می‌مانید و تعدادی رمز-ارز بی‌ارزش که صاحب اول و آخرش خود شمایید. پس بی‌گدار به آب نزنید و سعی کنید با آگاهی کافی اقدام کنید.

موفق باشید.

منابع

https://www.moneycrashers.com/cryptocurrency-history-bitcoin-alternatives/
https://www.thebalance.com/how-much-power-does-the-bitcoin-network-use۳۹۱۲۸۰-
https://cbeci.org/cbeci/comparisons
https://cbeci.org/
https://www.theguardian.com/technology/۲۰۲۱/feb/۲۷/bitcoin-mining-electricity-use-environmental-impact
https://hbr.org/۰۵/۲۰۲۱/how-much-energy-does-bitcoin-actually-consume
https://www.arabnews.com/node/۱۸۵۹۴۲۶/business-economy
https://arzdigital.com/crypto-private-key/
https://arzdigital.com/difference-between-public-key-private-key-and-wallet-address/
https://coinmarketcap.com/charts/
https://www.bitdegree.org/crypto/tutorials/token-vs-coin