تهیه و گرد آوری:

زهرا منوچهری سمیه حسینی

چکیده

همان‌طور که نیوتون می‌گوید: "اگر فاصله دورتری را دیده‌ام با ایستادن بر شانه‌های غول‌ها بوده است."

یکی از نیازهای اصلی و قدیمی انسان که این روزها به شدت به آن احساس نیاز می‌کند، اعتماد است.فکر می‌کنید؛ این نیاز چند سال است که حس می‌شود؟ ۱ سال؟ ۱۰ سال؟ ۱۰۰ سال؟ فراتر از این‌ها.

از زمانی که انسان‌ها داد و ستد کالا را کنار گذاشتند و از وسیله‌ای به نام پول یا همان سکه استفاده کردند، نیاز به اعتماد واقعی حس شد. از آن زمان تاکنون بشر مجبور بوده تا چشم بسته اعتماد کند. ابتدا سوالات بشر در حد سوالات زیر بود:

«آیا پادشاه پول را به درستی بین مردم تقسیم می کند؟»

«آیا مالیاتی که من می دهم عادلانه است؟»

«آیا اگر پولم را به اون بدهم تا تجارت کند، به من سود می رسد؟» و ...

با آمدن اینترنت، رشد فناوری و گسترش جوامع بشری سوالات بیشتر و بیشتر شد:

«فساد در سیستم مالی چقدر است؟»

«آیا حقوقی که می‌گیرم با زحمتی که می‌کشم تناسب دارد؟»

«آیا اطلاعات من که در آن سرور نگهداری می‌شود، امن است؟» و ...

و سوالاتی که با اندکی تأمل واقعاً نیاز به اعتماد در آن‌ها حس می‌شود. این‌ها همه سوالاتی هستند که شما راهی جز دادن جواب مثبت به خود ندارید.

انسان‌ها همیشه در اعتماد بهم دچار شک و تردید هستند. هیچ گزارشی کاملاً شفاف نیست و انسان به این نیاز همیشه فکر کرده.

خلاصه کلام، انسان نیاز به یک قاضی عادل را حس می‌کند که اشتباه نداشته باشد (یا حداقل اشتباهش عمدی نباشد) و به نفع جامعه کار کند.

سال‌هاست که دولت ها پول را توزیع می‌کنند؛ دولت‌های سراسر جهان پول چاپ می‌کنند و به اندازه نیازشان از آن بر می‌دارند. این پول در رده‌های پایین‌تر بین سرمایه‌داران و شاید افراد فاسد تقسیم می‌شود و وقتی پول به قشر متوسط یا ضعیف جامعه می‌رسد، قطره‌ای از دریای بیکرانی بوده که در شکم نهنگان است. حتی کسانی که تلاش کرده و به جایگاه بالایی رسیده‌اند، از منشا قدرت مافوقشان بی‌اعتماد هستند؛ این هم بر می‌گردد به اعتماد.

مردم به این که پول عادلانه تقسیم می‌شود اعتماد ندارند و قطعاً هم اگر حتی دولت‌مردان فرشته باشند و قصد این کار را داشته باشند، با سیستم‌های متمرکز این کار غیرممکن است.

در تمام این سال‌ها همه به جهانی اعتمادسازی شده فکر می‌کردند اما ابزار تحقق آن رویا فراهم نبود.

اکنون ما به ابزاری رسیده‌ایم تا نیازی به بانک مرکزی برای کنترل اقتصادمان نداشته باشیم. امروز ما به این توانایی رسیده‌ایم که هر کس نسبت به استعداد و توانایی‌اش بتواند با اعتماد کامل پولی را که لایقش است به دست آورد.

فرایند استخراج با تمام ضعف‌ها و مشکلاتش، یک ذات جالب دارد. به اندازه تلاشت پول می‌گیری. البته این فرایند فعلی استخراج اصلاً جالب نیست زیرا باز هم کسانی که سرمایه بیشتری دارند، دستگاه بیشتر و در نتیجه سود بیشتری به دست می‌آورند اما نوید یک نظام عادلانه را به ما می‌دهد که در آن به جز استخراج در سیستم‌های غیرمتمرکز هر کس به اندازه کاری که می‌کند پول به دست بیاورد نه به دلیل رنگ و نژاد و ژن خوبش!!!!

حالا انسان تلاش را برای رفع این نیاز بزرگ آغاز کرده قطعاً در این راه موانعی وجود خواهد داشت و تاریخ این حقیقت را اثبات می‌کند.

اولین قدم را ساتوشی ناکاموتو بنیان‌گذار ارز دیجیتالی (بیت‌کوین) برداشت. اصلاً چه اهمیتی دارد که بیت‌کوین را چه کسی ساخته است. فقط کافی‌ست به ذات نامحدود انسان در رفع نیازها حس کنیم. بیت‌کوین یا تیت‌کوین یا هر اسم دیگری یک روز به وجود می‌آمد چون نیاز به یک ارز جهانی و بدون واسطه حس می‌شد. برای استفاده از این ارز جهانی انسان به عدم تمرکز نیاز دارد که آن را نیز با هر اسمی می‌سازد بلاک‌چین یا ... .

بلاک‌چین‌ها سیستمی بدون تقلب و تمام رمزنگاری شده را در جهان پیاده خواهند کرد و تمام واسطه‌های متمرکز حذف می‌شوند. شرکت‌های آلفابت، اپل یا گوگل دیگر کنترل داده‌های کاربران را در اختیار نخواهند داشت. هیچ دولت یا نهادی قادر به مسدودسازی سایت‌ها و خدمات نخواهد بود و هیچ شخصی نمی‌تواند هویت دیگران را کنترل کند.

فناوری بلاک‌چین، یک دستاورد عمومی بشری است که تحت مالکیت هیچ کشور یا نهادی نبوده و مالکیت آن متعلق به نسل بشر است.

مقدمه

مردم از اصطلاح فن‌آوری بلاک‌چین چیزهای متفاوتی را مد نظر دارند و این می‌تواند گیج‌کننده باشد. گاهی از بلاک‌چین بیت‌کوین صحبت می‌شود، گاهی از ارزهای دیجیتالی دیگر یا ژتون‌های دیجیتالی،

گاهی از قراردادهای هوشمند. اما اغلب اوقات منظورشان دفاتر توزیعی است یعنی فهرستی از نقل و انتقالات مالی که به جای ذخیره در یک سرور مرکزی در شماری از کامپیوترها تکثیر می‌شود.

بلاک‌چین نوعی دیتابیس یا پایگاه داده است که روی یک یا چند سرور خاص قرار ندارد بلکه روی تمام کامپیوترهایی که به شبکه متصل می‌شوند، توزیع شده است و در حقیقت یک دفتر کل برای ثبت رکوردها و گزارشات است و به دلیل نوع رمزنگاری و ثبت آن در همه کامپیوترهای شبکه، گزارشات ثبت شده قابل هک یا حذف نیستند.

بیت‌کوین اولین کاربرد این فناوری بود اما از این سیستم انقلابی برای هر سیستمی که نیاز به ثبت گزارش داشته باشد می‌توان بهره برد.

فن‌آوری بلاک‌چین به مثابه مجموعه‌ای از فن‌آوری‌ها و موضوعات مشترک ذخیره اطلاعات و داده‌ها است که معمولاً شامل نقل و انتقالات مالی است، تقریباً هم‌زمان در شماری از سیستم‌ها تکثیر می‌شود، معمولاً روی یک شبکه همتا به همتا وجود دارد.

از رمزنگاری و امضاهای دیجیتالی برای اثبات هویت، اعتبار و حفظ حقوق دسترسی برای خواندن و نوشتن داده‌ها استفاده می‌شود.

می‌تواند توسط مشارکین مشخصی و احتمالاً مخاطبین گسترده‌تر از کسانی که می‌توانند بنویسند، خوانده شود.

مکانیزمی دارد که تغییر تاریخچه نقل و انتقالات را دشوار سازد یا دست کم آسان بتوان فهمید که چه کسی در تلاش برای دستکاری است.

یک بلاک‌چین فقط یک فایل است. یک بلاک‌چین به خودی خود تنها ساختاری از داده‌هاست. یعنی صرفاً نحوه کنار هم قرار گرفتن و ذخیره داده‌هاست. دیگر ساختارهای داده، پایگاه داده‌ها (ردیف‌ها، ستون‌ها، جداول)، فایل‌های متنی، رشته‌های مقادیر ارزشی (که با ویرگول از هم جدا شده‌اند)، تصاویر، فهرست‌ها و مانند این است. می‌توانید بلاک‌چین را دقیقاً مانند یک پایگاه داده در نظر بگیرید.

تاریخچه بلاک‌چین

اولین کار روی زنجیره بلاک‌چین در سال ۱۹۹۱ توسط استوارت هابر و اسکات استورنتا توصیف شد؛ اولین زنجیره بلوک توسط یک فرد ناشناس یا گروهی شناخته شده به نام ساتوشی ناکاموتو در سال ۲۰۰۸ معرفی شد. یک سال بعد به عنوان یک جزء اصلی از بیت‌کوین اجرا شد. زنجیره بلوکی معاملات آنلاین امن را تسهیل می‌کند. زنجیره بلوکی یک کتاب‌خانه دیجیتالی غیرمتمرکز و توزیع شده است که برای ضبط معاملات در میان رایانه‌های بسیاری استفاده می‌شود.

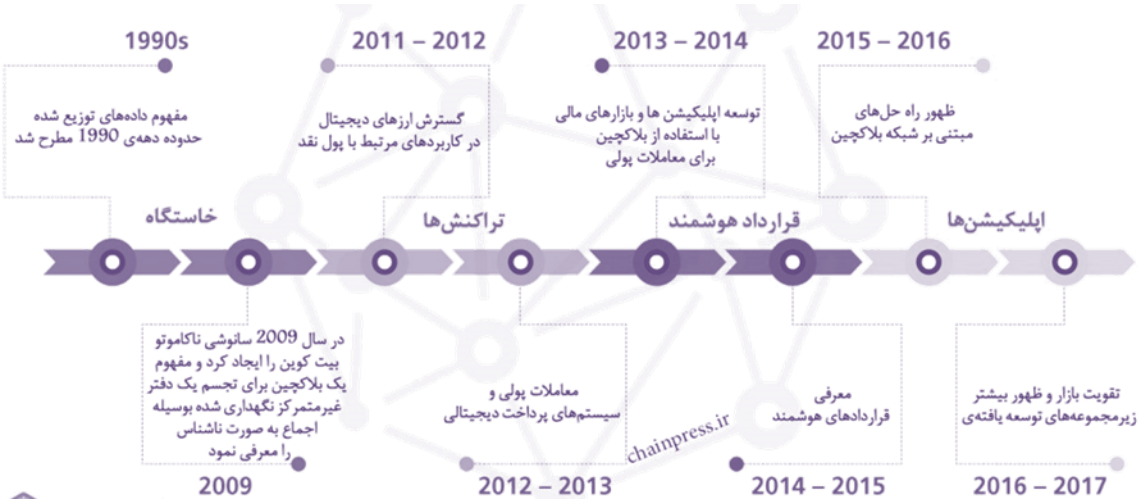
در سال ۲۰۰۹ الگوریتمی طراحی شد که اساس اولین پول دیجیتال تاریخ به نام بیت‌کوین شد. این پول بدون نیاز به تضمین هیچ بانک مرکزی در دنیا امکان انجام تراکنش (Peer to Peer) (تراکنش بدون

واسطه) را برای همه فراهم کرد. (مطابق نظر اقتصاد دانان، بیت‌کوین در واقع یک پول به معنایی کـه در علـم اقتصاد آمده نیست، بلکه بیشتر یک کالا است که می‌تواند به جای پول مورد استفاده قرار گیرد.).

آن چه بیت‌کوین بر اساس آن طراحی شده است مفهومی به نام بلاک‌چین است. در ساده‌ترین بیـان ممکن، بلاک‌چین در واقع یک دفتر دیجیتالی است که بر اساس سه اصل **باز بودن دفترچه، عدم تمرکـز** و **غیر قابل هک بودن** طراحی شده است. باید دقت داشت که بلاک‌چین و بیت‌کوین به هیچ عنوان حائز یـک معنا نیستند بلکه رابطه بلاک‌چین و بیت‌کوین مانند رابطه اینترنت و یوتیوب است. در واقع پخش ویدیو یکی از هزاران کاری است که می‌توان روی بستر اینترنت انجام داد.

بلاک‌چین چیست؟

بلاک‌چین اختراعی برجسته و مبتکرانه است؛ زاییـده فکـر یـک فـرد یـا گروهـی از افـراد. بلاکچـین



(Blockchain) از دو کلمه Block (بلوک) و Chain (زنجیره) ایجـاد شـده اسـت. ایـن فنـاوری در حقیقـت زنجیره‌ای از بلوک‌هاست. به‌طور کلی یک نوع سیستم ثبت اطلاعات و گزارش است و تفاوت آن با سیستم‌های دیگر این است که اطلاعات ذخیره شده روی این نوع سیستم، میان همه اعضای شبکه بـه اشـتراک گذاشـته می‌شوند و با استفاده از رمزنگاری امکان حذف و دست‌کاری اطلاعات ثبت شده تقریباً غیرممکن است.

فناوری بلاک‌چین در ابتدا برای پول دیجیتال بیت‌کـوین طراحـی شـد، امـا در حـال حاضـر جامعـه فناوری در حال پیدا کردن دیگر کاربردهای بالقوه برای این فناوری است. بلاک‌چین یک دفترکـل دیجیتـالی غیرقابل تخریب از معاملات اقتصادی است که می‌تواند نه تنها برای ضبط معاملات مالی بلکه تقریباً برای ثبت هر دارایی ارزش‌مندی استفاده شود.

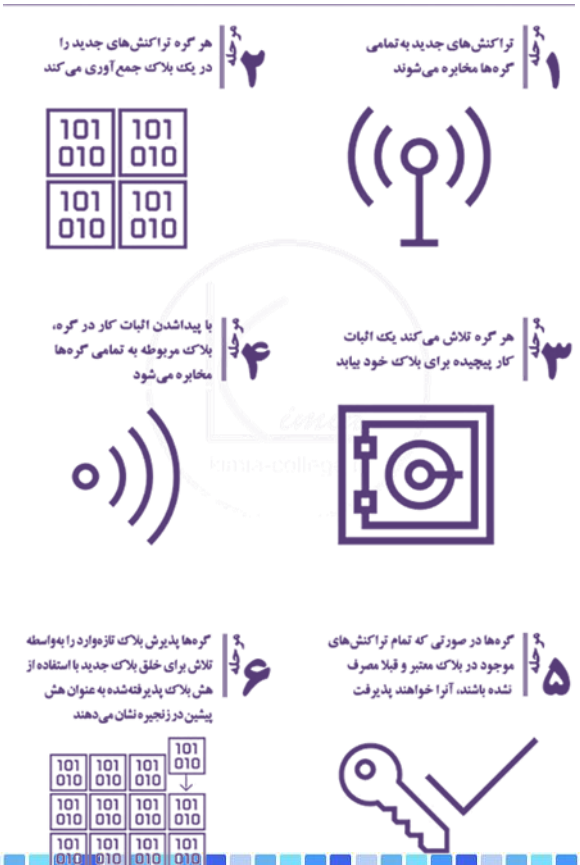
بلاک‌چین چگونه کار می‌کند؟

برای درک مفهوم بلاک‌چین باید شبکه عظیمی را در نظر بگیرید که از تعداد زیادی نود باتوان محاسبات کامپیوتری بسیار بالا تشکیل شده است. هر یک از اعضای شبکه که بخواهد تراکنشی انجام دهد، ابتدا باید درخواست آن را در شبکه صادر کند. سایر نودهای موجود در شبکه در برخورد با هر درخواست تراکنش دو فعالیت اساسی انجام می‌دهند.

اول؛ این که معتبر بودن آن تراکنش را از لحاظ (Business Role) در مورد بیت‌کوین کافی بودن موجودی فرد درخواست‌دهنده بررسی و تأیید کنند.

دوم؛ فعالیت اساسی در واقع پیدا کردن رمز پیچیده و تصادفی مورد نیاز بر اساس الگوریتم بلاک‌چین است که این رمز برای اضافه کردن آن تراکنش به دفتر دیجیتال مورد نیاز است.

نخستین نودی از شبکه که بتواند این دو فعالیت را با موفقیت به پایان برساند، آن را به دفتر دیجیتال اضافه کرده و سپس برای اطلاع سایر نودها آن را اعلام می‌نماید تا آن‌ها نیز بتوانند خود را بروز کنند. سایر نودها نیز از ادامه کار بروی آن تراکنش دست کشیده و پس از بروزرسانی دفتر دیجیتال به دنبال تراکنش بعدی می‌گردند. نودی که در بررسی معتبر بودن و هم‌چنین کشف رمز هر تراکنش قبل از همه موفق شود، جایزه‌ای دریافت می‌کند که از جنس پول دیجیتال است.



در هر ده دقیقه مجموعه تراکنش‌های صورت گرفته در شبکه، در قالب یک Block از اطلاعات ایجاد و منتشر می‌شود که آن Block به Blockقبل از خود لینک و در واقع در هم تنیده می‌شوند. بر همین منوال همه بلوک‌های بعدی به قبلی‌ها لینک شده و شما برای این که بتوانید یک رکورد (یک سطر از دفتر یادداشت) را تغییر دهید باید بتوانید همه بلاک‌ها را هک کرده و در واقع همه تراکنش‌های صورت گرفته را روی میلیون‌ها کامپیوتر به صورت هم‌زمان هک کنید. این کار تحقیقاً محال است و در نتیجه ما به عنوان بشر امروزی می‌توانیم از مواهب این دستاورد بزرگ استفاده کنیم.

متوجه هستید که: سه اصل باز بودن، عدم تمرکز و غیر قابل هک بودن به خوبی توسط این

نوآوری کم نظیر که با اختراع ماشین چاپ، اختراع موتور بخار و یا حتی اینترنت در یک طراز اهمیت قرار دارد پوشش داده می‌شود.

هش در بلاک‌چین چیست؟

هش به این مفهموم اشاره دارد که مقدار نامشخصی از داده ورودی، توسط یک الگوریتم، به یک داده خروجی که هش نام دارد تبدیل می‌شود. این داده خروجی طول ثابت و مشخصی دارد. داده ورودی نیز می‌تواند یک کارکتر باشد یا حتی یک فایل صوتی یا تمام اینترنت! نکته این است که داده ورودی می‌تواند بسیار بزرگ باشد. الگوریتم هش می‌تواند بر اساس نیاز ما انتخاب شود. الگوریتم هش، یک مقدار نامحدود از بیت‌ها را به عنوان ورودی می‌گیرد و بعد از انجام یکسری محاسبات روی آن، یک خروجی با طول مشخص را تولید می‌کند.

هش‌ها در بلاک‌چین برای نشان دادن حالت فعلی جهان به کار گرفته می‌شوند. یعنی ورودی کل حالت فعلی بلاک‌چین است؛ تمام تراکنش‌هایی که از ابتدا تاکنون صورت گرفته، به عنوان ورودی هش می‌شوند و در نتیجه هش، حالت فعلی بلاک‌چین را نشان خواهد داد. این هش برای توافق بین تمام بخش‌ها در دنیا بر سر این‌که حالت فعلی، تنها حالت فعلی و واقعی است به‌کار می‌رود.

اما در حقیقت چگونه این هش‌ها محاسبه می‌شوند؟

هش اول برای بلاک اول یا بلاک ریشه‌ای محاسبه می‌شود که حاوی تراکنش‌های درون بلاک است. دنباله‌ی تراکنش‌های اولیه برای محاسبه هشِ بلاکِ ریشه مورد استفاده قرار می‌گیرد. برای هر بلاکی که بعد از آن تولید می‌شود، هشِ بلاک قبلی نیز مانند تراکنش‌های همان بلاک بعنوان ورودی مورد استفاده قرار می‌گیرد تا هش این بلاک مشخص شود. این نحوه شکل گیری زنجیره‌ای از بلاک‌ها است.

هشِ هر بلاک جدید به هشِ بلاک قبل از آن اشاره می‌کند. این سیستم از هش‌ها تضمین می‌کند که هیچ تراکنشی در گذشته قابل تغییر نباشد؛ چون اگر یک قسمت از تراکنش تغییر کند، هش همان بلاک

نیز تغییر می‌کند و در نتیجه هش‌های بلاک‌های بعد از آن نیز تغییر خواهند کرد. در نهایت تشخیص تراکنش‌های دست‌کاری شده، بسیار ساده خواهد بود. زیرا برای این‌کار تنها نیاز دارید تا هش‌ها را با یک‌دیگر مقایسه کنید. نتیجه این کار بسیار جالب است.

ایده‌ی غیرمتمرکزسازی

بلاک‌چین یک فناوری غیرمتمرکز است. هر چیزی که روی آن اتفاق می‌افتد، حاصل از عملکرد شبکه به عنوان یک کل است. از این ویژگی بسیار استفاده می‌شود. با ایجاد یک روش جدید برای بررسی معاملات، برخی جنبه‌های تجارت سنتی ضرورت خود را از دست خواهند داد. برای مثال، معاملات بورس سهام می‌توانند به طور هم‌زمان در بلاک‌چین قرار گیرند؛ یا می‌توان انواع حسابرسی‌ها مانند ثبت زمین را کاملاً عمومی کرد. تمرکززدایی در حال حاضر یک واقعیت است.

مفهوم جامع تمرکززدایی (غیرمتمرکزسازی) از زبان ویتالیک بوترین:

ویتالیک بوترین، خالق اتریوم، درباره مفهوم به اشتباه تعبیر شده تمرکززدایی (Decentralization) و جوانب مختلف تمرکززایی (Centralization) صحبت می‌کند و با شکافتن این کلمه جنبه‌های مختلف آن را مورد بحث قرار می‌دهد. تا درک مفاهیم عنوان شده را آسان‌تر سازد.

غیرمتمرکزسازی یکی از واژه‌هایی است که در فضای ارزهای دیجیتال بسیار استفاده می‌شود و از سویی اغلب به عنوان تنها علت به وجود آمدن بلاک‌چین به آن نگاه می‌کنند. با این حال گویا این لغت یکی از ضعیف‌ترین کلمات تعریف شده به حساب می‌آید. هزاران ساعت مطالعه و میلیاردها دلار در قالب توان هش برای دستیابی به یگانه هدف تمرکززدایی و حفظ و بهبود آن صرف شده است؛ زمانی که بحث‌ها رقابتی می‌شود، به وفور دیده می‌شود که یکی از پروتکل‌ها ضربه آخر را با متهم کردن طرف مقابل به متمرکز بودن به آن‌ها می‌زند.

سه دلیل تمرکززدایی:

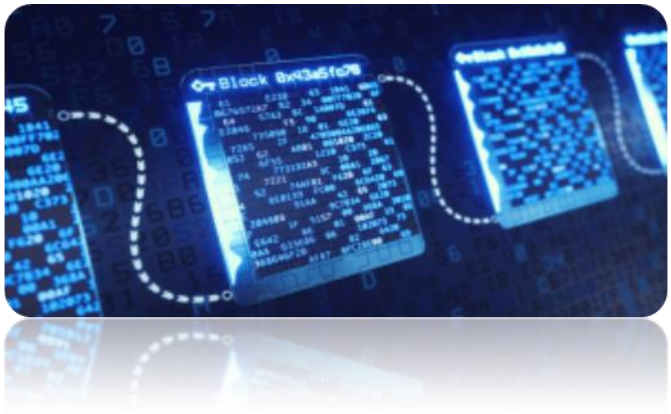
تحمل خطا: سیستم‌های غیرمتمرکز احتمال شکست تصادفی کم‌تری دارند چرا که به اجزای مختلفی تکیه دارند که شبیه هم نیستند.

مقاومت در برابر حملات: هزینه زیادی برای حمله، تخریب یا دستکاری سیستم‌های غیرمتمرکز باید صرف شود، چرا که نقاط حساس مرکزی در آن‌ها وجود ندارد که با هزینه‌های کم‌تری نسبت به حجم اقتصادی سیستم پیرامون به آن‌ها حمله کرد.

مقاومت در برابر توطئه: برای شرکت‌کنندگان در سیستم‌های غیرمتمرکز بسیار دشوارتر است که با یک‌دیگر توطئه کنند، به طوری که خود به سود برسند و هزینه‌اش را دیگر شرکت‌کنندگان بپردازند؛ چرا که سردمداران شرکت‌ها و دولت‌ها به طریقی ساخت‌وپاخت می‌کنند که سود آن به خودشان برسد و زیان آن بین شهروندان، مشتریان، کارمندان و عموم مردم هماهنگ‌شده در زمان مشابه پخش شود.

نظم و ترتیب بلاک‌ها در یک بلاک‌چین

صفحه به صفحه: در کتاب، شماره صفحه‌ها باعث می‌شود که نظم صفحات را به آسانی بدانیم. اگر ورق‌های یک کتاب را پاره کنید و آن‌ها را بُر بزنید، دوباره به آسانی می‌توان آن‌ها را منظم کرد.



بلاک به بلاک: در بلاک‌چین، هر بلاک به بلاک قبلی ارجاع دارد اما نه با شماره بلاک بلکه با اثرانگشت یا هش بلاک که هوشمندانه‌تر از شماره صفحه است زیرا اثرانگشت یک بلاک توسط محتوای آن بلاک تعیین می‌شود.

سازگاری درونی: با استفاده از اثرانگشت به جای توالی عددی، یک روش عالی نیز برای ارزش‌گذاری اطلاعات خواهید داشت. در هر بلاک‌چین با استفاده از چند الگوریتم می‌توانید اثرانگشت‌های بلاک را خودتان ایجاد کنید. اگر اثرانگشت‌ها با اطلاعات سازگار باشند و اثرانگشت‌ها در یک زنجیره به هم ملحق شوند، پس می‌توانید مطمئن باشید که بلاک چین درون‌سازگار است. اگر کسی بخواهد در داده‌ها دست ببرد، باید اثر انگشت‌ها را از آن نقطه به بعد دوباره ایجاد کند و بنابراین بلاک‌چین متفاوت خواهد بود.

این بدان معناست که اگر ایجاد اثرانگشت دشوار یا آهسته باشد پس به دشواری و آهستگی نیز می‌توان آن‌را در بلاک‌چین بازنویسی کرد.

انواع بلاک‌چین

- بلاک‌چین عمومی غیر انحصاری: مانند بیت‌کوین، اتریوم و ...
- بلاک‌چین عمومی انحصاری: مانند چند شرکت در آمریکا
- بلاک‌چین خصوصی انحصاری: مانند سیستم‌های پرداخت حقوق با بلاک‌چین

مزایای بلاک‌چین

- ارز خود را در چند دقیقه می‌توانید انتقال دهید.
- هزینه انتقال نسبت به بانک‌ها و مسیرهای سنتی بسیار کم می‌باشد.
- کنترل کامل روی دارایی خود و مانند بانک‌ها و مؤسسات کسی نمی‌تواند دسترسی شما را محدود سازد و... .
- به سادگی، یک بلاک‌چین می‌تواند برای ردگیری مسیر کالا، مبدا، کاهش هزینه‌ها و غیره استفاده شود.
- اگرنقصی در جایی از زنجیره تامین شناسایی شود، یک سیستم بلاک‌چین می تواند شما را به همه مسیرهای اصلی منتهی به نقص هدایت کند. این امر کسب و کار را برای انجام تحقیقات واقدامات لازم به موقع، آسان‌تر می‌کند.
- تراکنش‌های ثبت شده از طریق بلاک‌چین عملاً خطاهای انسانی را حذف و اطلاعات را از دست-کاری احتمالی محافظت می‌کند. در نظر داشته باشید که همه سوابق، هر بار که از یک گره بلاک‌چین به گره بعدی منتقل شود، حتما باید تأیید شوند. علاوه بر دقت، تضمین سوابق شما، مانند یک پروسه دنبال‌دار حسابرسی درسطح بالا قابل ردیابی خواهد بود.
- کل فرایند حسابداری سطح پایه نیز بسیار کارآمدتر می‌شود. به جای نگه‌داشتن سوابق جداگانه، کسب و کارها می‌توانند تنها یک ثبت واحد مشترک داشته باشد. یک‌پارچگی اطلاعات مالی شرکت نیز تضمین شده خواهد بود.

معایب و فناوری بلاک‌چین

- چون تراکنش‌ها به صورت ناشناس است امکان کارهای غیر قانونی هم بیشتر می‌شود.
- در حال حاضر فعلاً معامله کالا و خدمات با این فناوری رواج نیافته و آسان نیست.
- نوسان قیمت در بین ارزهای دیجیتال زیاد است.

- یکی دیگر از معایب سیستم‌های بلاک‌چین این است که پس از اضافه شدن اطلاعات در بلاک‌چین، اصلاح آن‌ها بسیار دشوار می‌شود. اگرچه ثبات یکی از مزایای بلاک‌چین است اما این ثبات همواره خوب نیست. تغییر کد یا اطلاعات بلاک‌چین معمولاً بسیار سخت است و اغلب به هاردفورک نیاز دارد.
- افرادی که به بیت‌کوین به چشم یک ارز تأثیرگذار نگاه می‌کنند وقتی درمی‌یابند که در سیستم بلاک‌چین در هر ثانیه تنها هفت تراکنش انجام می‌شود، ناامید می‌شوند.
- انجام یک تراکنش می‌تواند ساعت‌ها به طول بیانجامد. اگر می‌خواهید که تراکنش شما با سرعت انجام شود، باید بیشتر هزینه کنید.
- در شبکه‌های جدید تعداد گره‌های عضو شبکه محدود است، این کمبود منابع دو مشکل به وجود می‌آورد: ۱. هزینه بیشتر: گره‌های عضو شبکه پاداش بیشتری می‌خواهند. ۲. کاهش سرعت تراکنش‌ها: گره‌های عضو شبکه می‌خواهند تراکنش‌ها با پاداش بیشتر را اول انجام بدهند که این امر باعث مسدودی می‌شود.
- باوجود این که اطلاعات در بلاک‌چین عمومی به صورت رمزنگاری شده و ناشناس قرار می‌گیرد اما همه گره‌های عضو سیستم به آن دسترسی دارند. امکان دارد که هویت فرد را از طریق الگوهای تراکنشی ردیابی کنند. این امر ثابت می‌کند که حریم خصوصی بلاک‌چین در حدی که فکر می‌کردیم خصوصی نیست.
- از یک سو پروتکل‌های بلاک‌چین فرصتی برای دیجیتال‌سازی مدل‌های دولتی فراهم کرده است و از سوی دیگر ماینرها انگیزه تشکیل مدلی دیگر از حکومت را در سر دارند. این مسائل باعث به وجود آمدن اختلافاتی بین بخش‌های مختلف جامعه شده است.
- نقص امنیتی مشهود در بلاک‌چین این است که کامپیوترها به عنوان گره در این سامانه کار می‌کنند بنابراین اگر بیش از نیمی از آن‌ها دروغی بگویند، این دروغ به واقعیت تبدیل می‌شود. این پدیده «حمله ۵۱ درصدی» نام دارد. (اگر یک نهاد بتواند کنترل بیش از ۵۰٪ توان هشینگ شبکه را در اختیار بگیرد این حمله رخ می‌دهد که سرانجام به حمله‌کننده امکان می‌دهد تا با حذف یا تغییر تعمدی ترتیب تراکنش‌ها در عملکرد شبکه اخلال ایجاد کند.)
- اگر از بلاک‌چین به عنوان یک پایگاه اطلاعاتی استفاده شود، اطلاعات وارد شده به پایگاه باید از کیفیت بالایی برخوردار باشند. نمی‌توان به داده‌های ذخیره‌شده در بلاک‌چین اعتماد کرد بنابراین رویدادها باید از ابتدای کار با دقت ثبت شوند. اصطلاح «ورودی زباله، خروجی زباله» خیلی واضح سیستم ثبت بلاک‌چین را به عنوان یک پایگاه اطلاعاتی متمرکز توصیف می‌کند.
- تکنولوژی بلاک‌چین شامل لغات جدیدی می‌شود که نیاز به فرهنگ لغت مجزایی است.

تفاوت یک بلاک‌چین و یک پایگاه‌داده معمولی چیست؟

یک سیستم بلاک‌چین بسته‌ای است شامل یک پایگاه داده معمولی به علاوه چند نرم‌افزار که ردیف‌های جدید در پایگاه داده ایجاد می‌کند و با قواعد از پیش تأیید شده این ردیف‌های جدید را درست کرده و آن‌ها را به همتایان در یک شبکه می‌فرستد و تضمین می‌کند که تمامی هماتایان داده‌های یکسانی در پایگاه داده خود داشته باشند.

پایگاه داده توزیع شده چیست؟ صفحه گسترده‌ای را تصور کنید که هزاران بار در شبکه کامپیوتری کپی شده است. سپس تصور کنید که این شبکه طراحی شده تا به‌طور منظم به روزرسانی شود.

اطلاعاتی که در بلوک نگهداری می‌شود به عنوان پایگاه داده به اشتراک گذاشته شده و به‌طور پیوسته در حال تطبیق است. این روش استفاده از شبکه دارای مزایای آشکاری است. پایگاه داده بلاک‌چین در یک مکان خاص ذخیره نمی‌شود، به این معنی که پرونده‌هایی که نگهداری می‌کنند، واقعاً عمومی هستند و به راحتی قابل تأییدند. نسخه متمرکزی از این اطلاعات وجود ندارد تا یک هکر بتواند آن را تخریب کند. با میزبانی داده‌ها توسط میلیون‌ها کامپیوتر به‌طور هم‌زمان، داده‌های آن برای هر کسی در اینترنت قابل دسترسی است.

دوام و استحکام بلاک‌چین

فناوری بلاک‌چین مانند اینترنت است که دارای یک استحکام داخلی است. با ذخیره بلوک‌های اطلاعاتی‌ای که در سراسر شبکه آن یکسان هستند، بلاک چین نمی‌تواند:

۱. توسط یک نهاد واحد کنترل شود.

۲. هیچ نقطه‌ی شکست واحدی ندارد.

بلاک چین واقعاً مکانیزمی انقلابی است که همه را به بالاترین سطح پاسخگویی می‌رساند. دیگر معاملات نادرست، خطاهای انسانی و ماشینی یا حتی یک مبادله که با رضایت طرفین انجام نشده است، وجود نخواهد داشت. بالاتر از هر چیز دیگری، مهم‌ترین حوزه‌ای که بلاک‌چین به آن کمک می‌کند، ضمانت اعتبار یک معامله از طریق ثبت آن نه تنها در یک محل ثبت اصلی و متمرکز بلکه در یک سیستم توزیع شده است که از طریق مکانیزم اعتبارسنجی امن متصل هستند.

بلاک‌چین‌های همگانی و خصوصی

یک تفاوت مهم میان بلاک‌چین‌های همگانی و خصوصی این است که آیا شما اجازه می‌دهید که هرکسی در بلاک‌چین شما بنویسد یا فقط مشارکین مورد تأیید قادر به نوشتن باشند.

بلاک‌چین‌های همگانی: دفاتر ثبت می‌توانند به دو معنا همگانی باشند:

- هر کسی بدون اجازه از سوی یک مقام دیگر، می‌تواند داده‌ها را بنویسد.

- هرکسی بدون اجازه از سوی یک مقام دیگر می تواند داده‌ها را بخواند.

معمولاً وقتی مردم از بلاک‌چین همگانی یا عمومی صحبت می‌کنند، منظورشان این است که هرکسی می‌تواند روی آن بنویسد. چون بلاک‌چین طراحی شده به صورتی است که هر کسی می‌تواند روی آن بنویسد، مشارکین حسابدار معتمد نیستند و می‌توانند در دفتر بدون نیاز به تأیید صلاحیت‌شان چیزی بنویسند، پس لازم است در مورد اختلاف و ناهمگونی‌ها قضاوت شود (چون رییسی نیست که تصمیم گیرنده باشد) و مکانیزم دفاعی در مقابل حملات وجود داشته باشد (اگر انگیزه مالی وجود داشته باشد، پس هرکسی می‌تواند در یک امنیت نسبی سوءاستفاده کند). این باعث هزینه و پیچیدگی در اجرای بلاک‌چین می‌شود.

بلاک‌چین‌های خصوصی: برعکس، در یک شبکه بلاک‌چین خصوصی، مشارکین شبکه شناخته شده و قابل اعتماد هستند، برای مثال یک گروه صنعتی یا گروهی از شرکت‌ها تحت پوشش یک شرکت جمعی هستند. دیگر نیازی به خیلی از مکانیزم‌ها نیست یا این مکانیزم‌ها با قراردادهای حقوقی جایگزین می‌شوند. یعنی شما باید به گونه مشخصی رفتار کنید زیرا یک تکه کاغذ را امضا کرده‌اید. این امر در تصمیمات فنی تغییر ایجاد می‌کند.

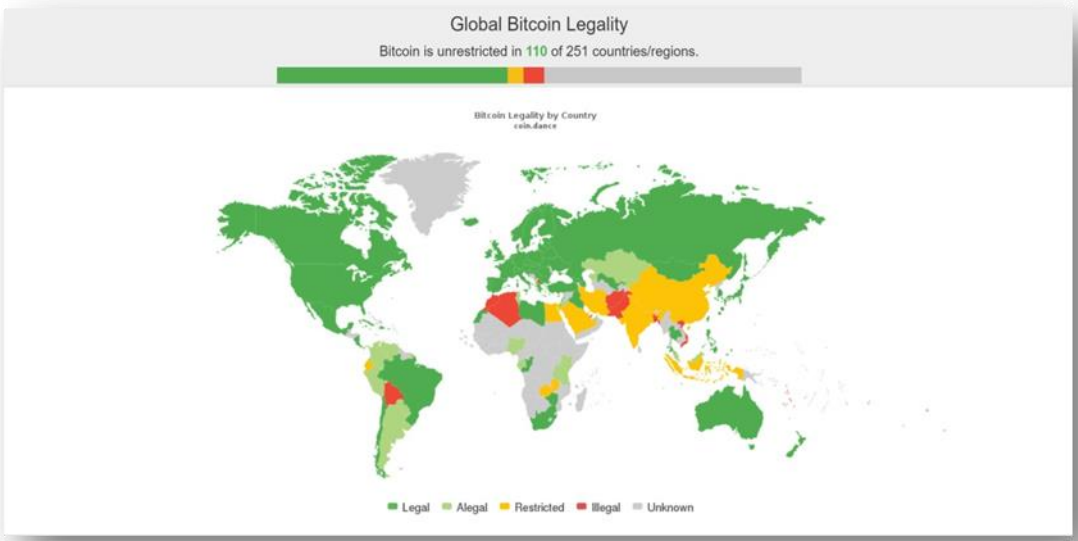
وضعیت بلاک‌چین در دنیا

با وجود این همه فعالیت‌های تجاری که در حول و حوش ارزهای دیجیتال وجود دارد هنوز هم یک قانون بین‌المللی واحد برای تنظیم این صنعت وجود ندارد. ارزهای دیجیتال به کاربران اجازه می‌دهند که در حال اجرای تراکنش‌ها ناشناس باقی بمانند.

در شکل زیر وضعیت قانون‌گذاری در کشورهای مختلف دنیا را می‌توانید مشاهده کنید.

- رنگ سبز نشان‌دهنده کشورهایی است که استفاده ارزهای دیجیتالی در آن‌ها مجاز است.
- رنگ قرمز نشان‌دهنده کشورهایی است که استفاده از ارزهای دیجیتالی ممنوع است.
- رنگ زرد نشان‌دهنده کشورهایی است که استفاده از ارزهای دیجیتالی با محدودیت‌هایی همراه است.

رنگ خاکستری نشان‌دهنده کشورهایی است که هنوز هیچ تصمیمی در این رابطه نگرفته‌اند.



نگاهی اجمالی به وضعیت قانونی بلاک‌چین در کشورها

ایالات متحده:

ایالات متحده رویکرد مثبتی به نسبت بیت‌کوین اتخاذ کرده است. هم‌زمان چندین آژانس حکومتی در حال کار برای جلوگیری و یا تقلیل استفاده از بیت‌کوین برای تراکنش‌های غیر قانونی هستند. خزانه این پول را به عنوان ارز تعریف نکرده است بلکه آن را به عنوان یک کسب و کار خدمات پولی تعریف کرده است.

چین:

چین هم‌چنان یکی از بزرگ‌ترین بازارهای بیت‌کوین در جهان می‌باشد. همه بانک‌ها و مؤسسات مالی دیگر مانند تصفیه‌کنندگان پرداختی‌ها از انجام تراکنش و معامله با بیت‌کوین منع شده‌اند. اما فرهنگ بیت-کوین در این کشور در حال شکوفایی است و افراد آزادند که به معامله بیت‌کوین در بین خود بپردازند.

روسیه:

مسئله قانونی بودن بیت‌کوین در روسیه مورد مناقشه است. وزارت امور مالی روسیه امیدوار است که قانونی برای تحریم بیت‌کوین تصویب کند.

کانادا:

به‌طور کلی رویکردی دوستانه را به نسبت بیت‌کوین اتخاذ کرده است، در حالی که هم‌چنین مراقب است که این ارز دیجیتال برای پول‌شویی و دیگر فعالیت‌های مجرمانه مورد استفاده قرار نگیرد. همچنین

وضع مالیات بستگی به این دارد که آیا فرد یک کسب و کار خرید و فروش دارد یا فقط در ارز دیجیتال سرمایه‌گذاری‌هایی کرده است.

استرالیا:

استرالیا به موجودیت‌ها اجازه معامله، استخراج و یا خرید بیت‌کوین را می‌دهد. اداره مالیات استرالیا تراکنش‌های بیت‌کوینی را مانند داد و ستد کالا تلقی می‌کند که با توجه به استفاده و کاربر شامل قوانین خاصی می‌شود.

اتحادیه اروپا:

اتحادیه اروپا پیشرفت‌ها در ارز دیجیتال را دنبال کرده اما هنوز تصمیمی رسمی در ارتباط با قانونی بودن، پذیرش و یا قانون گذاری نگرفته است. تعداد معدودی از کشورها در این اتحادیه بیت‌کوین را مجاز کرده‌اند در حالی که اکثراً یا در این مورد تصمیم‌گیری نکرده‌اند و یا در حال صادر کردن هشدارهایی در این زمینه هستند.

- فنلاند، هیأت مرکزی مالیات‌ها به بیت‌کوین وضعیت معاف از مالیات بر ارزش افزوده داده و آن را به عنوان یک سرویس مالی طبقه‌بندی کرده است. بیت کوین در فنلاند به عنوان کالا تلقی می‌شود نه ارز.
- بلژیک، اداره مالی سرویس عمومی فدرال این کشور هم‌چنین بیت‌کوین را معاف از مالیات بر ارزش افزوده دانسته است.
- قبرس، بیت‌کوین کنترل و یا قانون‌گذاری نشده است اما غیر قانونی نیز نمی‌باشد.
- بریتانیا، نوعی موضع‌گیری طرفدارانه از بیت‌کوین دیده می‌شود و طرفداران می‌خواهند که محیط قانونی حامی ارز دیجیتال باشد. بیت‌کوین در بریتانیا تحت مقررات مالیاتی خاصی است.
- بلغارستان، سازمان درآمد ملی این کشور نیز بیت‌کوین را تحت سلطه قوانین موجود درآورده است.
- آلمان، رویکرد بازی نسبت به بیت‌کوین دارد و آن را قانونی تلقی می‌کند اما مالیات بندی متفاوتی دارد و بستگی به برخورد مقامات با صرافی‌ها، ماینرها، سازمان‌ها و یا کاربران دارد. آلمان بیت‌کوین را به عنوان پول قانونی به حساب می‌آورد.

ایسلند:

ایسلند کنترل سرمایه را به عنوان بخشی از سیاست‌های مالی خود بعد از بحران اقتصادی جهانی ۲۰۰۸ پذیرفته است. ایسلند سعی می‌کند که از بیرون رفتن ارز خود از کشورش جلوگیری کند. معامله بیت-کوین در ایسلند ممنوع است زیرا ارز دیجیتال با قانون مبادلات مالی کشور سازگار نیست.

ویتنام:

این کشور ارز دیجیتال را مرتبط با فعالیت‌های مجرمانه‌ای مانند پول‌شویی می‌داند. حکومت و بانک مرکزی آن بیت‌کوین را به عنوان یک روش پرداخت قانونی به رسمیت نمی‌شناسند. حکومت ویتنام معاملات بیت‌کوین را برای مؤسسات مالی و شهروندان غیر قانونی اعلام کرده است.

بولیوی:

حکومت و بانک مرکزی آن استفاده از بیت‌کوین و دیگر ارزهای دیجیتال را ممنوع کرده است.

قرقیزستان:

حکومت و بانک مرکزی این کشور بیت‌کوین و آلت‌کوین‌ها را به عنوان روش پرداخت به رسمیت نمی‌شناسند و آن‌ها را غیر قانونی اعلام کرده‌اند.

اکوادور:

اکوادور برنامه‌هایی برای ایجاد ارز دیجیتال خود در آینده دارد اما بیت‌کوین و دیگر آلت‌کوین‌ها در اکوادور با رأی اکثریت در مجلس ملی ممنوع شده‌اند.

وضعیت بلاک چین در خاورمیانه

کشورهای حوزه خاورمیانه ثابت کرده‌اند که این منطقه، برای ورود ارزهای دیجیتالی و کاربردی کردن آن با مشکلات بسیاری دست‌وپنجه نرم می‌کنند؛ تا جایی که بسیاری از این کشورها استفاده و بهره‌گیری از ارزهای مجازی و بلاک‌چین را ممنوع اعلام نموده‌اند. اما اخبار جدید حاکی از آن است که خاورمیانه در حال بدل شدن به قطب جدید بلاک‌چین آسیا است. از دبی گرفته تا تل‌آویو، این فناوری استفاده‌های خود را ثابت کرده است.

بحرین:

چهارچوب قانونی: طرح‌ریزی شده

تمایل به استفاده از بلاک‌چین در سطوح داخلی: بله

تا پیش‌ازاین، دولت و مقامات بحرین هیچ اشاره مستقیمی به بلاک‌چین و بخش‌های مرتبط با آن نکرده بودند و بیشتر با مفهوم کلی فناوری‌های نوین اقتصادی از آن‌ها یاد می‌کردند. بحرین رویکردهای مثبتی را در قبال بلاک‌چین در پیش‌گرفته است. سپتامبر ۲۰۱۷، بانک مرکزی بحرین اعلام کرد که فضای آزاد قانون‌گذاری را ایجاد خواهد کرد. این فضا به‌منظور استفاده بهینه از تکنولوژی‌های نوین اقتصادی ایجاد شده بود که شامل بیت‌کوین و کسب‌وکارهای مبتنی بر بلاک‌چین می‌باشد.

ترکیه:

چهارچوب قانونی: طرح‌ریزی شده

تمایل به استفاده از بلاک‌چین در سطوح داخلی: بله

بر اساس آمارهایی که توسط بانک ING منتشرشده است، ارزهای دیجیتالی در کشور ترکیه با استقبال مناسبی روبه‌رو شده‌اند تا جایی که هجده درصد از مردم ترکیه ارزهای دیجیتالی خریداری کرده‌اند که در مقایسه با آمار هشت درصدی مردم آمریکا، نشان از محبوبیت این فناوری جدید در میان ترک‌هاست.

در سال ۲۰۱۷، قانون‌گذاران ترکیه اعلام کردند از آن جهت که بیت‌کوین قابل‌کنترل توسط دولت نیست، با قوانین اسلام سازگار نیست. بنا بر گفته‌های آن‌ها، ذات قمار گونه بیت‌کوین باعث شده تا معامله این ارز برای مسلمانان مناسب نباشد.

قطر:

چهارچوب قانونی: بدون چهارچوب، غیرقانونی

تمایل به استفاده از بلاک‌چین در سطوح داخلی: بله

ارزهای دیجیتالی در کشور قطر ممنوع هستند. در فوریه سال ۲۰۱۸، بانک مرکزی قطر آیین‌نامه جدیدی را به بانک‌های سراسر کشور ارسال کرد و از ممنوعیت خرید و فروش بیت‌کوین در این کشور خبر داد. در این آیین‌نامه آمده بود که سر باز زدن از پیروی این آیین‌نامه، جریمه شدن بانک‌های مذکور را به همراه خواهد داشت. بی‌ثباتی قیمت و استفاده از این ارز در حملات سایبری و فعالیت‌های غیرقانونی، نبود تعهدات لازم از جانب بانک‌های مرکزی، شفاف نبود در تبدیل بیت‌کوین به پول یا طلا، دلایل مخالفت بانک مرکزی قطر می‌باشد.

اما با وجود ممنوعیت این کشور میزبان کنفرانس بلاک‌چین در شهر دوحه بود. به‌علاوه استارت‌آپ‌های بسیاری نیز در قطر شروع به‌کار کرده‌اند. پس از قطع ارتباط کشورهای همسایه با عنوان حمایت این کشور از تروریست، قطر نیز به فکر بهره‌مندی از این تکنولوژی افتاد.

عربستان سعودی:

چهارچوب قانونی: بدون چهارچوب، غیرقانونی

تمایل به استفاده از بلاک‌چین در سطوح داخلی: بله

ارزهای دیجیتالی در این کشور با ممنوعیت‌هایی روبه‌رو هستند. مقامات مالی این کشور به‌صورت رسمی هشدار دادند که شهروندان این کشور حق استفاده و تبادل ارزهای دیجیتالی را ندارند.

درست به مانند قطر، ممنوعیت‌های استفاده از ارزهای دیجیتالی در عربستان نیز مانع از آزمایش این فناوری در پی دورنمای سعودی تا سال ۲۰۳۰ نشده است. این برنامه به‌منظور توسعه‌های اقتصادی بلندمدت در عربستان سعودی تدوین شده است.

عراق:

چهارچوب قانونی: بدون چهارچوب، غیرقانونی

تمایل به استفاده از بلاک‌چین در سطوح داخلی: خیر

استفاده از بیت‌کوین در عراق غیرقانونی است. در دسامبر سال ۲۰۱۷، «ایسر جبار»، مدیر بانک مرکزی عراق، اعلام کرد که ریسک‌های پیرامون بیت‌کوین بالاست و مشکلات مرتبط با دزدی اطلاعات و کلاه‌برداری در آن به وفور یافت می‌شود؛ از طرف دیگر این ارز در عراق هیچ محبوبیتی ندارد.

بنا بر اظهارات متخصصین تکنولوژی و اقتصادی عراق، مشکلات گفته شده پیرامون بیت‌کوین را می‌توان به‌وسیله یک ساز وکار ضد پول‌شویی قابل پیگیری نمود.

کویت:

چهارچوب قانونی: بدون چهارچوب، غیرقانونی

تمایل به استفاده از بلاک‌چین در سطوح داخلی: خیر

ارزهای مجازی از جمله بیت‌کوین در کویت ممنوع اعلام شده‌اند. دسامبر سال ۲۰۱۷، وزارت اقتصاد کویت اعلام کرد که ارزهای دیجیتالی را به رسمیت نمی‌شناسد و بانک و مؤسسات مالی نیز حق استفاده از این ارزها را ندارند.

با این حال به نقل از خبرگزاری «عرب تایمز» و بنا بر اظهارات منابعی این خبرگزاری در وزارت اقتصادی کویت، بانک‌ها و مؤسسات و دولت کویت توانایی قانون‌گذاری در حوزه ارزهای دیجیتالی را ندارند چرا که این امر از کنترل آن‌ها خارج است. به‌علاوه ارزهایی که از خارج از کویت، وارد این کشور می‌شوند به‌عنوان پول‌های غیرقانونی شناخته خواهند شد، چرا که قانون کویت این مبالغ را به‌عنوان ارز قبول نمی‌کند.

امارات متحده عربی:

چهارچوب قانونی: طرح‌ریزی شده

تمایل به استفاده از بلاک‌چین در سطوح داخلی: بله

موضع‌گیری مقامات امارات متحده عربی در قبال ارزهای دیجیتالی و بیت‌کوین متفاوت بوده است. در اوایل اکتبر سال ۲۰۱۷، این کشور اولین آیین‌نامه‌های مرتبط با ارزهای دیجیتالی و ICOها را منتشر نمود و آن‌ها را به‌عنوان اوراق بهادار و ابزار داد و ستد به رسمیت شناخت.

امارات متحده عربی در حال استفاده گسترده از بلاک‌چین است. در سال ۲۰۱۶، دبی اقدام به عرضه «بلاک‌چین استراتژی» کرد. هدف از ایجاد چنین نقشه راهی تبدیل‌شدن به اولین شهر بلاک‌چینی دنیا تا سال ۲۰۲۰ عنوان‌شده بود.

مصر:

چهارچوب قانونی: خیر

تمایل به استفاده از بلاک چین در سطوح داخلی: بله

در ماه ژانویه ۲۰۱۸، مفتی اعظم مصر اعلام کرد که بنا بر شریعت، استفاده از بیت‌کوین ممنوع است. وی با صدور فتوایی اعلام نمود که خرید و فروش ارزهای دیجیتالی باعث خواهد شد تا خریدار و فروشنده هر دو گرفتار کلاه‌برداری، جهل و خیانت در امانت شوند. دولت مصر نیز از ارزهای دیجیتالی حمایت نمی‌کند، اما با وجود این، هنوز تبادل و استفاده از این ارزها را ممنوع اعلام نکرده است.

در ماه آوریل سال ۲۰۱۸، اولین مرکز رشد بلاک چین در مصر راه‌اندازی شد و NU TechSace نام گرفت. این مرکز رشد تحت حمایت آکادمی علوم مصر نیز قرار دارد و در نظر دارد تا به دولت این کشور کمک کند که به فهم درستی از بلاک چین برسد.

اردن:

چهارچوب قانونی: غیرقانونی

تمایل به استفاده از بلاک چین در سطوح داخلی: بله

تبادل و خرید و فروش بیت‌کوین در اردن ممنوع است. در سال ۲۰۱۴، بانک مرکزی این کشور تمامی بانک‌ها و مؤسسات مالی اردن را از خرید و فروش ارزهای مجازی منع کرد و به شهروندان این کشور هشدار داد که این ارزها قانونی نیستند. در بیانیه این بانک آمده بود که ارزهای دیجیتالی در هیچ بانک مرکزی‌ای قابلیت به رسمیت شناخته‌شدن به‌عنوان یک ارزش را ندارند و هیچ طلا یا ارز رسمی بین‌المللی‌ای از آنها پشتیبانی نمی‌کند.

به کمک برنامه‌هایی نظیر Building Blocks، که در اوایل سال ۲۰۱۷ پایه‌ریزی شده اردن مهد بسیاری از پروژه‌هایی که حول محور بلاک‌چین به‌منظور تسهیل کمک‌رسانی به آوارگان و پناهندگان فعالیت می‌کنند قرار گرفته است. این برنامه ، به سازمان جهانی غذا و دارو کمک می‌کند که در کشور سوریه بالغ بر صد هزار کوپن مخصوص غذا را توزیع نماید. چنین استفاده‌هایی از بلاک‌چین را می‌توان نوید بخش توصیف نمود.

عمان:

چهارچوب قانونی: غیرقانونی

تمایل به استفاده از بلاک چین در سطوح داخلی: بله

به نظر می‌رسد که استفاده از ارزهای دیجیتالی در عمان نه ممنوع است و نه آزاد! در دسامبر سال ۲۰۱۷، بانک مرکزی این کشور اعلام کرد که این بانک هیچ‌گونه مسئولیتی در قبال ضررهایی که شهروندان این کشور در تبادل و سرمایه‌گذاری درزمینهٔ ارزهای دیجیتالی متحمل می‌شوند، ندارد. در این بیانیه

همچنین اعلام شد که در این کشور چهار چوب‌های قانونی و سازوکارهای هدایتی وجود ندارد و سیاستی نیـز تدوین‌نشده است. عمان در سال‌های اخیر به استفاده از بلاک‌چین علاقه نشان داده است.

فلسطین:

چهارچوب قانونی: غیرقانونی

تمایل به استفاده از بلاک چین در سطوح داخلی: بله

در ماه می سال ۲۰۱۷، مسئول سیاست‌گذاری مالی فلسطین، «اعظم شاوا»، در گفتگویی با خبرگزاری رویترز اعلام کرد که این کشور قصد دارد تا ارز دیجیتال مخصوص به خود را پنج سال آینده تدوین و عرضه نماید. او از این ارز با عنوان «پوند فلسطینی» (alestinian ound) نام برد.

این ارز قرار است تا به‌عنوان سپری در مقابل نفوذ اسرائیل و تجاوز بالقوه آن مورد استفاده قرار گیرد؛ چرا که اقتصادی فلسطین در حال حاضر مبتنی بر ارز بومی خاصی نیست و این کشور معاملات خود را به‌وسیله دلار، یورو، دینار اردن یا واحد پول اسرائیل انجام می‌دهد.

لبنان:

چهارچوب قانونی: خیر

تمایل به استفاده از بلاک چین در سطوح داخلی: خیر

در سال ۲۰۱۳، لبنان اولین کشوری در خاورمیانه بود که در ارتباط با تبادل و سرمایه‌گذاری در حوزه ارزهای مجازی به شهروندان خود هشدار داد. این کشور از بی‌ثباتی در قیمت، نبود سیاست‌های شناخت مشتری و مشکلات این چنینی، برای توجیه هشدار خود استفاده نمود بود. در اکتبر سال ۲۰۱۷، بانک مرکزی لبنان، اعلام کرد که ارزهای دیجیتالی و بیت‌کوین، در چهار چوب‌های قانونی کار نمی‌کنند و می‌بایست آن‌ها را در کشور ممنوع نمود. «ریاض سلامه» در ارتباط با بیت‌کوین اذعان داشت که، این ارز قابل‌اتکا نیست و از آن به‌عنوان یک کالا یاد نمود.

در مورد فعالیت‌های مرتبط با بلاک‌چین در کشور لبنان اطلاعات زیادی در دست نیست. با این حال، ConsenSys، یکی از استارت‌آپ‌های آمریکایی در حوزه بلاک‌چین اعلام کرد که لبنان میزبان یک نشست پنج روزه بلاک‌چین خواهد بود.

وضعیت بلاک چین در ایران

چهارچوب قانونی: طرح‌ریزی شده

تمایل به استفاده از بلاک چین در سطوح داخلی: بله

ایران باوجود تحریم‌های وضع‌شده از جانب دونالد ترامپ و دولت ایالات‌متحده، رفته‌رفته توجه خود را به سمت ارزهای دیجیتالی و استفاده از این ارزها متمرکز می‌کند. درحالی‌که ویزا و مستر کارت در این کشور فعالیتی ندارند و ارزش ریال به سبب وجود تورم بالا در حال کاهش است، محبوبیت بیت‌کوین در میان مردم بیشتر و بیشتر می‌شود. بنا بر گزارش‌ها، بیش از دو و نیم میلیارد دلار برای خرید ارزهای دیجیتالی در ایران صرف شده است.

در حال حاضر استفاده و خرید و فروش این ارزها در ایران با مشکلات قانونی مواجه است. بانک مرکزی اعلام کرد که ارزهای دیجیتالی به‌منظور پشتیبانی از تروریسم، پول‌شویی و اعمال غیرقانونی مورد استفاده قرار می‌گیرند و با استناد به این دلایل خرید و فروش و استفاده از ارزهای دیجیتالی را برای شهروندان، صرافی‌ها و بانک‌های ایران ممنوع اعلام نمود.

درست به مانند ونزوئلا، ایران نیز برای مقابله با تحریم‌های آمریکا به دنبال ایجاد ارز دیجیتالی مخصوص به خود است.

ما در حال ایجاد زمینه‌های لازم برای ساخت ارز دیجیتال بومی خود هستیم. این ارز می‌بایست قابلیت انتقال و ایجاد ارزش (پول) را در هرکجای دنیا داشته باشد. به‌علاوه این ارز می‌تواند ما را در دور زدن تحریم‌ها یاری کند.

ما نسبت به ارزهای دیجیتالی و تکنولوژی پشت این ارزها نگاهی سرسختانه از خود به نمایش گذاشته‌ایم. به عنوان مثال وزارت ارتباطات و فناوری یادداشت تفاهمی را به‌منظور استفاده بلاک‌چین برای دیجیتالی کردن بایگانی‌های این کشور به امضا رساند.

کشور ما با وجود این‌که شفافیت‌های لازم را در زمینه قانون‌گذاری ندارد؛ اما سعی بر پیشرو بودن در حوزه ارزهای دیجیتال و بلاک‌چین دارد. نسخه پیش‌نویسی از سند قانونی برای ارزهای دیجیتال توسط بانک مرکزی منتشر شده است و صنعت استخراج نیز توسط دولت قانونی اعلام شده است. ایران به دلیل مسائل تحریم و فضای گسترده و مناسبی که در ارزهای دیجیتال مانند بیت‌کوین و تکنولوژی زیرساخت آن یعنی بلاک‌چین وجود دارد می‌تواند؛ استفاده بهینه‌ای از این موقعیت بکند.

علت علاقه ایرانی‌ها به بلاک‌چین چیست؟

اصلی‌ترین دلیل علاقه و گرایش مردم ایران به بلاک‌چین و ارزهای دیجیتال را می‌توان نـا امیـدی از سیستم بانکی فعلی دانست. سیستم مالی تقریباً سنتی که ما اکنون در کشور خود داریم، نمی‌توانـد انتظـارات مردم را برآورده سازد. عدم وجود یک مکانیزم مدرن در چرخه اقتصاد، باعث بروز پیچیدگی‌های مالی می‌گردد که در نتیجه دل‌زدگی مردم را به همراه دارد که اتفاقاتی مانند جریان مؤسسات مـالی غیرمجـاز و بلاتکلیفـی طولانی مدت مال‌باختگان بر آن افزود.

هم‌چنین در دنیای پرسرعت امروز، سیستم بانکی کشور، از کندی و محدودیت‌های زیادی برخـوردار است که به عدم اطمینان مردم به آینده این سیستم دامن زده است.

دلیل دیگری که می‌تواند مردم را به سمت ارزهای دیجیتال سوق دهد، امکـان دور زدن تحـریم‌هـا و انجام تجارت با این ارزها است. سیستم‌های جامع بین‌المللی مانند مسـتر و ویـزا در کشـورهای زیـادی فعـال هستند و تجارت الکترونیک را با سراسر جهان امکان‌پذیر می‌سازدند اما در چند کشور از جمله ایران به دلیـل تحریم‌های بین‌المللی افراد ساکن در ایران امکان استفاده مستقیم از ایـن سیسـتم‌هـا را ندارنـد و مجبـور بـه استفاده از واسطه‌هایی هستند که هزینه‌ی تمام شده را به طرز چشمگیری افزایش می‌دهد. همه ایـن عوامـل باعث محدود شدن چرخه تجارت و در نتیجه رکورد اقتصادی می‌گردد. اما از آن‌جایی که ارزهای دیجیتال بـه شرکت یا سازمان خاصی وابسته نیستند، اغلب شرایط لازم را برای تجارت مستقیم و بدون واسطه بـا سراسـر جهان را دارند.

بخش دوم

مطالعه موردی بیت کوین

برای بهتر درک شدن موضوع بلاک‌چین معمول‌ترین نوع رمز ارز یعنی بیت‌کوین را مورد بررسی قرار می‌دهیم.

بیت‌کوین چیست و چرا ارزشمند است؟

بیت‌کوین شبکه‌ای با هدف پرداخت‌های همتا به همتا است و ارز دیجیتال آن هم بیت‌کوین (BTC) نام دارد. درست مانند ارزهای رایج ملی مثل دلار، یورو، بیت‌کوین به خودی خود ارزشی ندارد. مانند یک دلار؛ ارزشمندی بیت‌کوین هم فقط به دلیل اعتبار آن در نزد کاربرانش است که باعث عرضه و تقاضا می‌شود. شاید این مسئله را ندانید اما از دهه ۱۹۷۰ به بعد، پول‌های رایج جهان هیچ پشتوانه‌ای ندارند و فقط اعتبار و اعتماد به پول یک کشور ارزش آن را تعیین می‌کند. در دهه ۱۹۷۰، دولت آمریکا قانون استاندارد طلا را لغو کرد و دلار رسماً بدون پشتوانه شد. یک دلار آمریکا و بیشتر ارزهای ملی دیگر اکنون ارزششان نسبت به اعتبار و کاربرد آن تعیین می‌شود. ارزش بیت‌کوین را هم کاربران و شبکه آن تعیین می‌کنند.

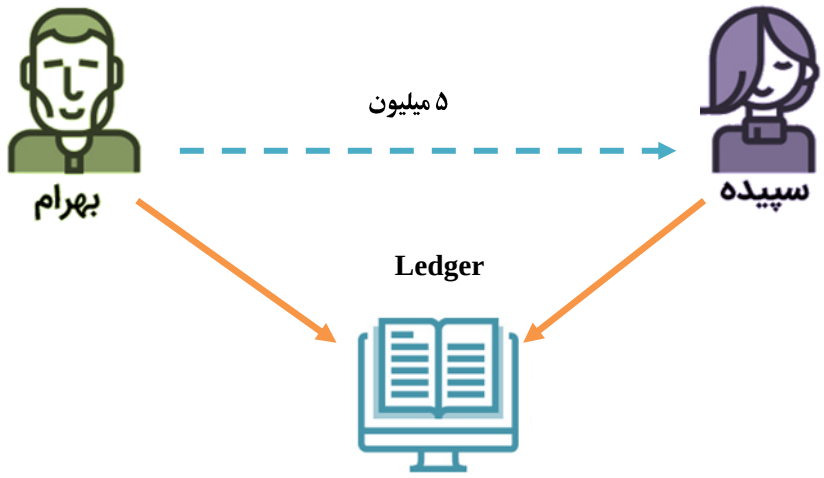
دقیقاً بیت‌کوین چیست؟

از اساسی‌ترین دیدگاه، بیت‌کوین فقط یک فایل دیجیتال شبیه به دفتر حساب وکتاب بوده که حساب‌ها و پول هر نفر را در خود ثبت می‌کند. یک کپی از این فایل در تمام کامپیوترهای متصل شده به شبکه بیت‌کوین نگهداری می‌شود. هنگام ارسال بیت‌کوین شما به شبکه اعلام می‌کنید که مقداری از حساب شما کسر شود و به حساب گیرنده واریز شود. نودها (Nodes) یا همان کامپیوترهای موجود در شبکه بیت‌کوین، تراکنش را در دفترهای خود اعمال می‌کنند و آن را به دیگر نودها پاس می‌دهند.

سیستمی که به گروهی از کامپیوترها اجازه می‌دهد تا از یک دفترکل (Ledger) نگهداری کنند.

در بانک‌ها هم همین‌گونه است. بانک‌ها یک دفترکل دیجیتال دارند که تراکنش‌ها و دارایی مشتریان در آن ثبت شده است.

مثلا بهرام ۱۰ میلیون تومان پول دارد و سپیده ۵ میلیون تومان. این اطلاعات روی دفترکل بانک‌ها ثبت می‌شوند. وقتی بهرام ۵ میلیون تومان به سپیده پول می‌فرستد، در دفتر کل موجود در بانک، ۵ میلیون تومان از حساب بهرام کسر می‌شود و به حساب سپیده واریز می‌شود. در هنگام انجام تراکنش بانکی، پول فیزیکی منتقل نمی‌شود بلکه فقط مالکیت پول تغییر می‌کند.



اما تفاوت دفترکل بلاک‌چین با دفتر کل بانک‌ها چیست؟

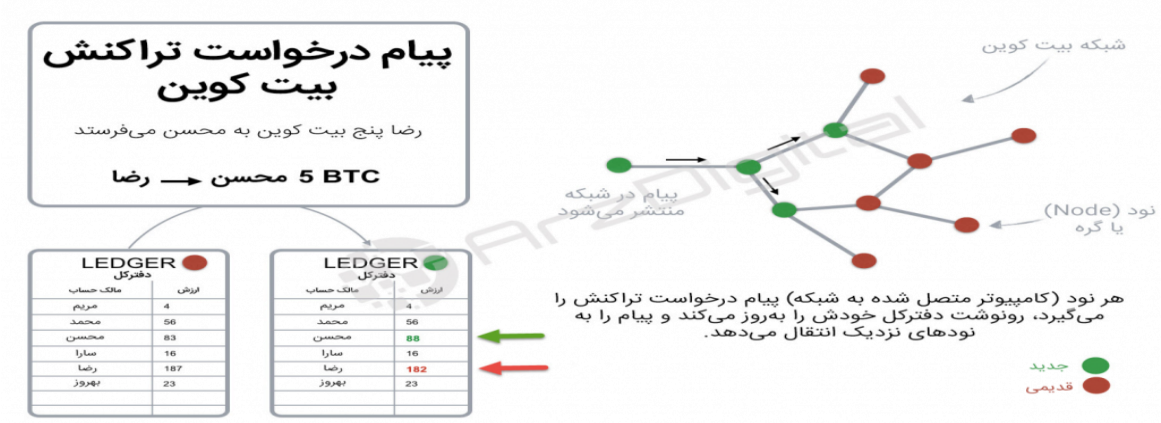
حقیقت این است که در بیت‌کوین به جای یک نهاد مرکزی، دفترکل به صورت گروهی نگهداری می‌شود و همین موضوع تفاوت‌های عمده‌ای را ایجاد می‌کند.

اول از همه، برخلاف بانک که شما فقط می‌توانید تراکنش‌های خود را ببینید، در بیت‌کوین همه می‌توانند تراکنش‌های هر فرد دیگری را ببینند.

در سیستم بانکی شما مجبور هستید به بانک، کورکورانه اعتماد کنید اما در بیت‌کوین شما با تعداد زیادی افراد غریبه سر و کار دارید که هیچ نیازی به اعتماد کردن ندارد.

سیستم بیت‌کوین به طرز شگفت‌انگیزی طراحی شده است و هیچ اعتمادی در شبکه آن نیاز نیست.

اگر رضا بخواهد برای محسن ۵ بیت کوین ارسال کند، باید درخواستش را به شبکه اعلام کند که ۵ بیت‌کوین از من کم کن و ۵ بیت‌کوین به محسن اضافه کن. هر نود در شبکه پیام را دریافت و کپی دفتر حساب و کتاب خود را طبق این درخواست به‌روز می‌کند. همه این فرایند به صورت دیجیتالی صورت می‌گیرد.



اما نودها چگونه مطمئن می‌شوند که این درخواست معتبر است؟ اگر کسی که این پیام را فرستاده، واقعاً بیت‌کوین نداشته باشد چه؟

به منظور انجام تراکنش در شبکه بیت‌کوین، شما به یک کیف پول دیجیتال (Wallet) نیاز دارید. کیف پول بیت‌کوین برنامه‌ای است که اجازه ذخیره و تبادل بیت‌کوین را به شما می‌دهد.

در بیت کوین، کیف پول شما بانک شخصی شماست. برای اینکه تضمین شود که فقط کیف پول مورد نظر بتواند بیت کوین های داخل خود را خرج کند، هر کیف پول با نوعی روش رمزنگاری محافظت می‌شود.

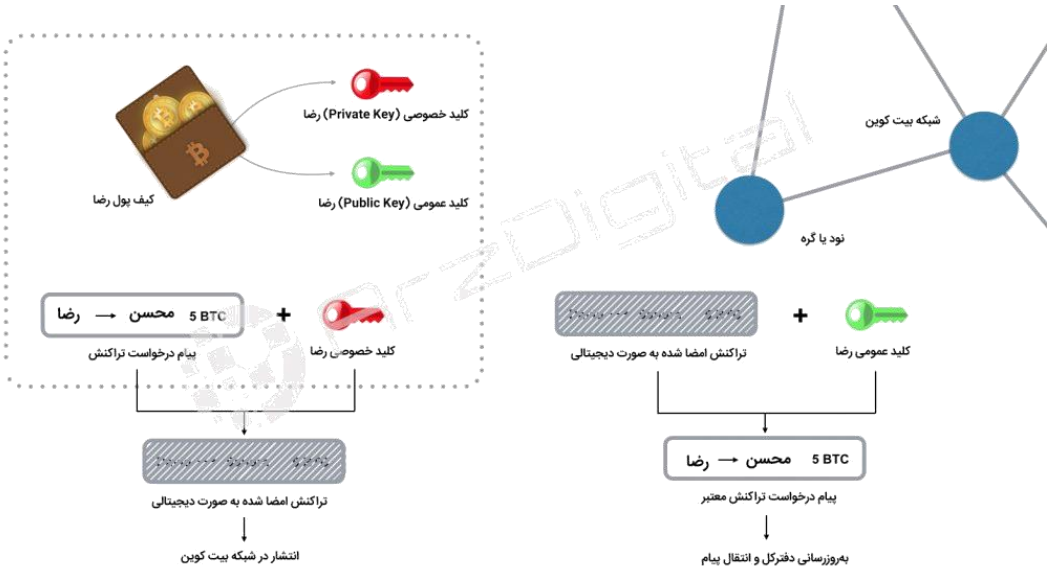
کلید عمومی و کلید خصوصی

دو رشته کلید رمزنگاری شده در هر کی پول بیت‌کوین وجود دارد که مجزا بوده اما باهم ارتباط مکمل دارند. این دو کلید: کلید عمومی (Public Key) و کلید خصوصی (private key) نام دارند. ارتباط این دو به این صورت است که وقتی یک پیام توسط یک کلید عمومی خاص رمزگذاری می‌شود، فقط کلید خصوصی جفت شده با آن می‌تواند پیام را باز کند و بخواند. برعکس این موضوع هم صدق می‌کند: وقتی شما یک پیام را با کلید خصوصی رمزگذاری می‌کنید، فقط کلید عمومی جفت شده با آن می‌تواند پیام را از حالت رمزنگاری خارج کند.

مثلاً، رضا برای ارسال بیت‌کوین باید پیامی را که با کلید خصوصی کیف پولش رمزنگاری شده، به شبکه ارسال کند. به این شکل مشخص می‌شود که بیت‌کوین‌ها دقیقاً از طریق کیف پول رضا ارسال شده‌اند و فرد دیگری به دروغ این پیام را به شبکه نفرستاده است.

هر نود (کامپیوتر متصل شده به شبکه به صورت مستقیم)، تراکنش ارسال شده از رضا را بررسی می‌کند تا مطمئن شود این پیام دقیقاً از کیف پول رضا ارسال شده است. برای این کار، نودها با استفاده از کلید عمومی کیف پول رضا، پیام ارسال شده را می‌خوانند.

هنگامی که کیف پول شما یک درخواست تراکنش را با استفاده از کلید خصوصی رمزنگاری می‌کند،



به نوعی یک **امضای دیجیتال** می‌سازد که نشان می‌دهد هر تراکنش متعلق به کدام کیف پول است.

این امضای دیجیتال یک رشته‌ی متنی است که از کلید خصوصی و پیام درخواست تراکنش تولید می‌شود.

با هرگونه تغییر در درخواست تراکنش، امضای دیجیتال به‌طور کامل تغییر می‌کند. این کار باعث می‌شود تا نتوان پیام‌های درخواست تراکنش را تغییر داد.

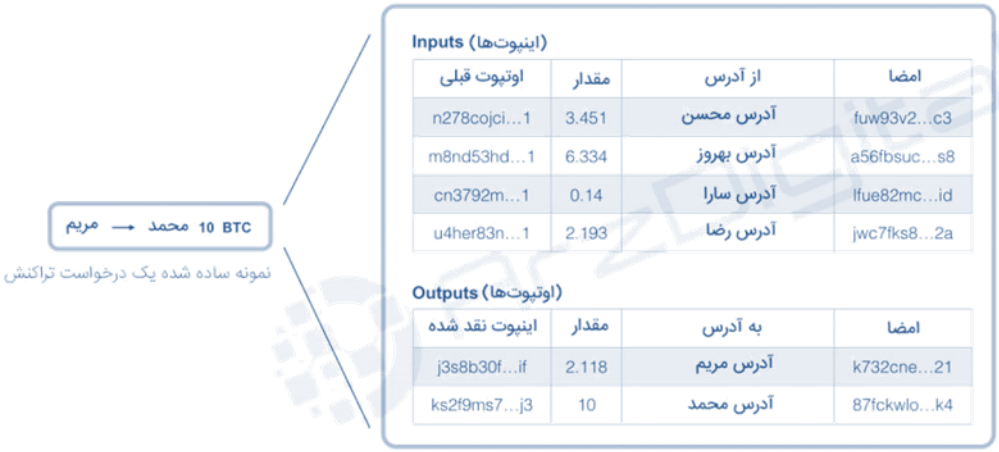
چگونه موجودی حساب‌ها مشخص می‌شود؟

سیستم بیت‌کوین میزان موجودی حساب‌ها را ذخیره نمی‌کند. در بیت‌کوین تنها چیزی که ثبت می‌شود تراکنش‌های تأیید شده هستند. به عبارت دیگر دفترکل بیت‌کوین فقط سوابق تراکنش‌های منتشر شده را ذخیره می‌کند.

به جای ذخیره موجودی حساب‌ها، مالکیت در بیت‌کوین بر اساس تراکنش‌های قبلی تعیین می‌شود.

مثال، اگر مریم قصد ارسال ۱۰ بیت‌کوین به محمد را داشته باشد، او درخواست تراکنشی را ایجاد می‌کند. درخواست تراکنش مریم دارای پیوندهایی به تراکنش‌های ورودی قبلی است و جمع میزان آن‌ها باید حداقل ۱۰ بیت‌کوین باشد تا تراکنش انجام شود. به این پیوندها اصطلاحاً انپوت (input) یا ورودی می‌گویند. در واقع هنگامی که مریم قصد ارسال بیت‌کوین را داشته باشد، باید تراکنش‌های ورودی قبلی خود را به عنوان مدرک به شبکه نشان دهد.

به عبارت دیگر و زبان ساده‌تر وقتی شما قصد ارسال بیت‌کوین دارید، به شبکه تراکنش‌های دریافتی قبلی خود را نشان می‌دهید و می‌گویید این‌ها مدارک دریافت بیت‌کوین هستند.



نمونه واقعی یک درخواست تراکنش

نودهای شبکه مقدار را بررسی کرده و مطمئن می‌شوند که این انپوت‌ها خرج نشده باشند. در حقیقت یک بار خود برنامه کیف پول مقدار موجودی شما را بررسی می‌کند و یک بار نودهای شبکه این کار را با استفاده از اطلاعات تراکنش‌های قبلی انجام می‌دهند. این فرایند موجب می‌شود که دوبار خرج کردن (خرج کردن دوباره بیت کوین) امکان پذیر نباشد.

داشتن بیت‌کوین بدان معناست که شما در شبکه بیت‌کوین تراکنش‌هایی دارید که خرج نشده‌اند. همان‌طور که می‌دانید بیت‌کوین کاملاً متن باز و مستقل از هر نهادی است. از این رو کلید خصوصی یک کیف پول به منزله کلید بیت‌کوین‌های شماست. همیشه از کیف پول خود نسخه پشتیبان تهیه کنید و هرگز کلید خصوصی خود را در اختیار کسی قرار ندهید.

بی‌نهایت آدرس

هر کس می‌تواند بدون نیاز به وارد کردن نام یا مشخصات خود به شبکه بیت‌کوین متصل شود. شبکه بیت‌کوین اجازه ساخت هر تعداد کیف پولی را به کاربران می‌دهد و هر کیف پول کلیدهای عمومی و خصوصی خاص خودش را دارد.

شاید فکر کنید که تولید یک کلید عمومی برای ساخت آدرس کیف پول، به معنای مشخص شدن هویت شخصی شما باشد. اما حتی این قدم هم ناشناس است و حتی می‌تواند بدون نیاز به اینترنت انجام شود.

شما می‌توانید به سادگی و با یک کلیک در کیف پول خود کلید عمومی و خصوصی جدید بسازید.

اما یک مسئله:

در هنگام ساخت کیف پول امکان بررسی داشتن یا نداشتن یک آدرس توسط فرد دیگر وجود ندارد.

برای این‌که جمله بالا را بهتر درک کنید، فرایند ساخت ایمیل را در نظر بگیرید. هنگامی که قصد ساخت ایمیل دارید، سرویس ایمیل دهی (مثل جیمیل) از شما می‌خواهد که یک آدرس ایمیل برای خود مشخص کنید. شما آدرس دلخواه خود را وارد می‌کنید اما سیستم به شما می‌گوید که این آدرس ثبت شده است و نمی‌توانید آن را برای خود بردارید. در بیت‌کوین این‌گونه نیست.

بنابراین اگر بتوانید کلید خصوصی یک نفر را حدس بزنید به دارایی‌های او دسترسی خواهید داشت اما حدس کلید خصوصی تقریبا محال است. چرا؟

حداکثر تعداد آدرس‌های احتمالی بیت کوین 2^{160} است یعنی

۱۴۶۱۵۰۱۶۳۷۳۳۰۹۰۲۹۱۸۲۰۳۶۸۴۸۳۲۷۱۶۲۸۳۰۱۹۶۵۵۹۳۲۵۴۲۹۷۶ احتمال برای آدرس‌های بیت کوین وجود دارد.

برای این‌که بزرگی این عدد را خوب درک کنید به این مثال توجه فرمایید:

تخمین زده می‌شود که 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، بازهم رقمی که به دست می‌آید خیلی پایین‌تر از احتمال آدرس‌های بیت‌کوین است. این موضوع باعث می‌شود تا هک یا حملات سایبری با استفاده از حدس زدن اعداد تقریباً غیرممکن شود.

مفهوم بلاک، بلاک‌چین و استخراج (ماینینگ) در بیت‌کوین

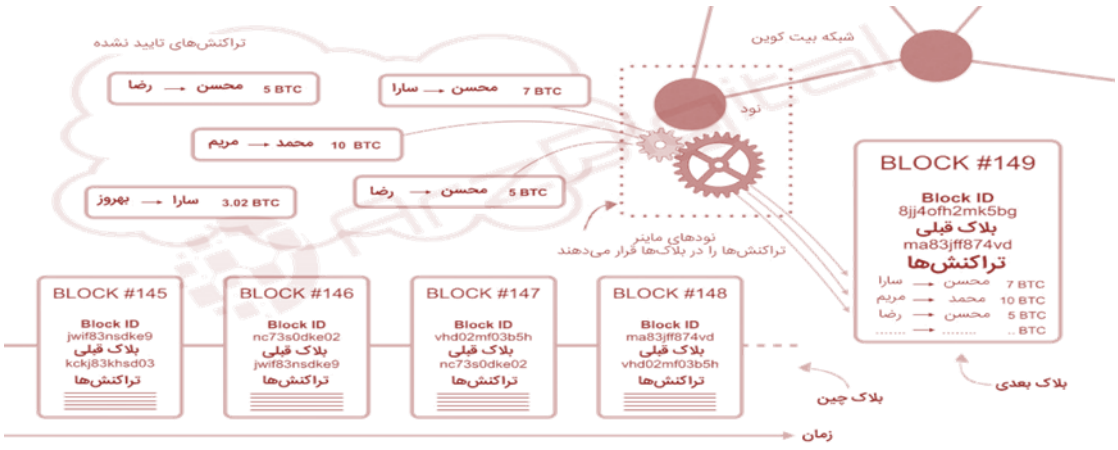
برای جلوگیری از دوبار خرج‌کردن بیت‌کوین‌ها، یک مفهوم دیگر در سیستم بیت‌کوین وجود دارد.

تراکنش‌ها از نودی به نود دیگر منتقل می‌شوند. بنابراین ترتیب رسیدن دو تراکنش مختلف به یک نود می‌تواند متفاوت باشد.

یک کاربر خراب کار می‌تواند به فرد دیگری بیت‌کوین بفرستد و بعد از این‌که آن فرد کالا یا پول بیت‌کوین را داد تراکنشی مخالف تراکنش قبلی بفرستد و در این صورت به دلیل عدم وجود ترتیب زمانی، نودها ممکن است تراکنش دوم را زودتر دریافت کنند و عملاً بیت‌کوین‌ها دوبار خرج شوند؛ بنابراین چگونه می‌توان فهمید که چه تراکنشی زودتر ارسال شده است؟

به همین دلیل سیستم بلاک‌چینی برای شبکه بیت‌کوین در نظر گرفته شده است. شبکه بیت‌کوین تراکنش‌ها را با گذاشتن آن‌ها در بلاک مرتب می‌کند.

هر بلاک دارای تعدادی تراکنش بوده و به بلاک قبلی خود متصل است. طبق این سیستم، در زمانی مشخص یک بلاک بعد از بلاک قبلی قرار می‌گیرد. به زنجیره‌ای از این بلاک‌ها زنجیره بلاکی یا همان بلاک-چین می‌گویند.



تمام تراکنش‌هایی که در یک بلاک خاص قرار دارند به عنوان تراکنش‌های ارسال شده در یک زمان در نظر گرفته می‌شوند و تراکنش‌هایی که هنوز در بلاک وارد نشده باشند به عنوان تأیید نشده یا آنکانفرم (unconfirm) در نظر گرفته می‌شوند. زمانی که تراکنش در بلاک ثبت شود و آن بلاک به شبکه ارسال شود، تراکنش یک تأیید (Confirm) می‌خورد. زمانی که بلاک‌های جدیدی روی بلاک تراکنش قبلی ثبت شوند، تعداد تأیید هم به همان میزان بالا می‌رود.

ماینینگ بیت‌کوین

هر نود می‌تواند تراکنش‌ها را در یک بلاک قرار دهد و آن‌ها را به دیگر نودها مخابره کند اما یک شرط دارد و آن این است که نود باید ماینر یا استخراج کننده باشد.

برای این‌که بلاک‌ها به بلاک‌چین اضافه شوند، هر بلاک باید دارای جواب یک معادله ریاضی پیچیده باشد. تنها راه حل کردن معادله، حدس زدن اعداد است. به عمل پیدا کردن معادله بلاک‌ها، ماینینگ می‌گویند.

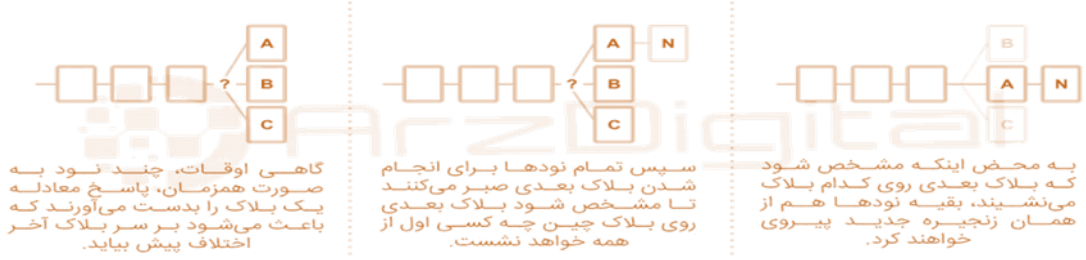
ماینرها این کار را انجام می‌دهند و اعداد را انقدر حدس می‌زنند تا جواب درست معادله را به دست آورند.

برای یک کامپیوتر عادی حل کردن این مسئله ریاضی و پیدا کردن جواب درست می‌تواند چندین سال طول بکشد. بنابراین کامپیوترهای قدرتمندی برای پیدا کردن جواب درست تلاش می‌کنند.

شبکه نسبت به جمع قدرت کامپیوترها، طوری تنظیم می‌کند که تقریباً هر ۱۰ دقیقه جواب درست توسط یکی از کامپیوترها پیدا شود. نودی (ماینری) که جواب درست را پیدا می‌کند، حق پخش آن بلاک به سایر نودها و در نتیجه اضافه کردن به بلاک‌چین را به‌دست می‌آورد.

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

در این مورد، هر دو بلاک به شبکه اعلام می‌شوند و هر نود، بلاکی 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 بلاک توافق حاصل نشود، به محض این‌که معادله آخرین بلاک حل شد، همه نودها بلندترین زنجیره خواهند پذیرفت.



با توجه به احتمال کم حل شدن بلاک‌ها در یک زمان، تقریباً غیرممکن است که به‌طور متوالی چند بلاک در یک زمان حل شوند.

عدم توافق بر سر آخرین بلاک در زنجیره می‌تواند باعث تقلب و دوبار خرج کردن شود. اگر یک تراکنش در بلاک زنجیره کوتاه‌تر باشد، زمانی که بلاک بعدی استخراج شود، این تراکنش و تمام تراکنش‌های آن بلاک دوباره به صورت تأیید نشده (آنکانفرم) در می‌آیند.

فرض کنید که مریم می‌خواهد از محمد با بیت‌کوین، یک فایل بخرد. مریم بیت‌کوین را به محمد می‌فرستد و محمد پس از دیدن اولین تأیید (کانفرم)، فایل را به مریم می‌دهد. حالا اگر مریم بتواند زنجیره‌ای طولانی‌تر بسازد که تراکنش برگشت با انپوت‌های یکسان داخل آن باشد، او می‌تواند پول خود را برگشت بزند و در عمل بیت‌کوین را دوبار خرج کند.

اما آیا مریم می‌تواند این کار را انجام دهد؟

او برای انجام این کار باید با کامپیوترهای زیادی که در حال رقابت برای یافتن جواب معامله کند، مسابقه دهد. حتی اگر به فرض محال او بتواند یک بلاک را پیش از بقیه حل کند، احتمال حل شدن بلاک‌های دوم، سوم، چهارم و ... به شدت پایین است و هر چه جلوتر می‌رویم پایین‌تر می‌آید.

مریم اگر بیش از ۵۰ درصد قدرت شبکه را در اختیار داشته باشد، شانس او برای حل کردن بلاک بیش از ۵۰ درصد خواهد بود اما برای حل کردن دو بلاک متوالی او فقط ۲۵ درصد شانس خواهد داشت و هر چه تعداد بلاک‌ها بیشتر می‌شوند شانس مریم کم‌تر و کم‌تر خواهد شد تا به صفر برسد.

به همین خاطر است که فروشندگان و صرافی‌ها برای تأیید تراکنش و ارایه خدمات، حداقل دو تا ۶ تأیید (کانفرم – Confirm) را ضروری می‌دانند. معمولاً ۶ کانفرم، امن‌ترین حالت ممکن برای تراکنش است و بعد از آن تراکنش دیگر مشکلی نخواهد داشت.

اما ماینرها چرا این کار را انجام می‌دهند؟

برای ایجاد انگیزه در ماینرها برای حفظ امنیت شبکه و هم‌چنین تولید واحدهای بیت‌کوین جدید به صورت غیرمتمرکز، برای پیدا کردن جواب معادله بلاک‌ها، پاداش در نظر گرفته شده است. پاداش بلاک بیت-کوین ابتدا ۵۰ واحد بیت‌کوین بود اما این پاداش پس از هر ۲۰۰،۰۰۰ بلاک نصف می‌شود. در حال حاضر

پاداش بلاک بیت کوین ۱۲,۵ واحد است. پس از گذشتن ۲۰۰،۰۰۰ بلاک این رقم به ۳,۲۵ نصف خواهد شد و همینطور ادامه خواهد یافت.

به دلیل بالا رفتن سختی شبکه بیت کوین و سخت بودن انجام عمل ماینینگ به صورت فردی، ماینرها به صورت گروهی در فضای‌های مجازی به نام استخر استخراج (mining pool) جمع می‌شوند تا از قدرت پردازش جمعی برای استخراج استفاده کنند. استخر استخراج محل مجازی است که استخراج کنندگان در آن جمع می شوند و همه برای استخراج یک بلاک تلاش می کنند. در این روش هر ماینر یا استخراج کننده معمولا بر اساس توان پردازشی خود سود می‌برد اما پاداش بلاک اصلی به استخر استخراج تعلق می‌گیرد. همان‌طور که گفتیم، سختی شبکه بیت‌کوین نسبت به قدرت پردازشی شبکه، طوری تنظیم می‌شود تا پاداش بلاک تقریباً هر ۱۰ دقیقه به دست بیاید.

هم‌چنین تراکنش‌های بیت‌کوین دارای کارمزد هستند. ماینرها اغلب تراکنش‌هایی را داخل بلاک قرار می‌دهند که کارمزد بهتری دارند و بنابراین تراکنش‌هایی که کارمزد بالاتر دارند زودتر تأیید خواهند شد. کاربر خودش حق دارد که کارمزد تراکنشش را مشخص کند اما اگر برای تراکنش خود کارمزد مناسب مشخص نکنید، تأیید تراکنش می‌تواند، چند روز یا تا ابد طول بکشد.

علاوه بر پاداش بلاک، میزان کل کارمزد تراکنش‌های یک بلاک هم به ماینر تعلق می‌گیرد.

بیت‌کوین شبکه‌ای غیرمتمرکز و همتا به همتا است که برای پرداخت‌های بدون واسطه طراحی شده است. سیستم بیت‌کوین از انواع و اقسام راه‌کارها برای حفظ امنیت استفاده می‌کند که مهم‌ترین آن‌ها رمزنگاری و بلاک چین است. به زبان ساده، بلاک‌چین یک دفترچه یادداشت دیجیتال است که اطلاعات می‌توانند روی آن به صورت توزیع شده و غیرقابل تغییر، ثبت شوند.

این اطلاعات هر چیزی می‌توانند باشند اما در بیت‌کوین، اطلاعاتی روی بلاک‌چین ثبت می‌شوند، تاریخچه تراکنش‌ها هستند.

تاریخچه تمام تراکنش‌های بیت‌کوین روی یک دفتر دیجیتال به نام بلاک‌چین ثبت می‌شود. هر کسی که به شبکه بیت‌کوین متصل می‌شود (که اصطلاحاً نود – node نام دارد) یک کپی کامل از بلاک‌چین را دریافت می‌کند. هر تراکنشی که به بیت‌کوین ارسال می‌شود توسط این کامپیوترهای متصل به شبکه بررسی می‌شود و هر کامپیوتر به آن تراکنش رأی می‌دهد. گروهی تراکنش را تأیید می‌کنند و گروهی آن را غیرمعتبر می‌دانند. در نهایت با رأی اکثریت مشخص خواهد شد که تراکنش معتبر است یا خیر.

اگر تراکنش توسط کامپیوترهای متصل به شبکه تأیید شود روی برگه‌ای به نام بلاک ثبت می‌شود و سپس بعد از گذشت یک زمان مشخص، این بلاک‌ها به هم متصل می‌شوند و از بهم پیوستگی بلاک‌ها، بلاک-چین (در معنای لغوی به معنای زنجیره‌ای از بلاک‌ها) پدید می‌آید. شاید زمانی که اصطلاح «استخراج بیت-کوین» را می‌شنوید، در ذهن خود سکه‌هایی را مجسم کنید که از دل زمین بیرون کشانده می‌شوند اما بیت-

کوین فیزیکی نیست. بنابراین چرا آن را استخراج یا ماینینگ می‌نامیم؟چون استخراج بیت‌کوین هم به نوعی از نظر فلسفی بی‌شباهت به استخراج طلا نیست. به این صورت که بیت‌کوین‌ها در طراحی پروتکل وجود دارند (مثل طلا که در معادن وجود دارد) اما هنوز قابل دسترسی نیستند (مثل طلاهایی که هنوز از دل خاک بیرون کشیده نشده‌اند). بر اساس پروتکل یا همان قوانین بیت کوین، فقط تعداد ۲۱ میلیون واحد از آن وجود خواهد داشت.

استخراج‌کنندگان بیت‌کوین یا ماینرها کاری انجام می‌دهند انجام می‌دهند که به وسیله آن می‌توانند به بیت‌کوین دست پیدا کنند. قبل از هر چیز باید درباره نودها صحبت کنیم. یک نود در شبکه بیت‌کوین، کامپیوتر قدرتمندی است که نرم‌افزار بیت‌کوین را اجرا و با مشارکت در انتقال اطلاعات به حفظ کار شبکه بیت‌کوین کمک می‌کند. هر کسی می‌تواند با دریافت رایگان نرم‌افزار بیت‌کوین و اختصاص برق و فضای ذخیره‌سازی کامپیوتر خود (در حال حاضر بیش از ۱۴۵ گیگابایت) یک نود را اجرا کند. نودها تراکنش‌ها در تمام شبکه پخش می‌کنند.

بعضی از نودها شرایطی ویژه دارند که به آن‌ها نود ماینینگ (همان ماینر) می‌گویند. در ابتدای کار بیت‌کوین همه نودها ماینر بودند اما امروزه نودهای ماینینگ با نودهای صرفاً اعتبارسنج کمی تفاوت دارند. نودهای ماینر، تراکنش‌ها را در بلاک‌ها جمع‌آوری و سپس آن‌ها را به بلاک‌چین اضافه می‌کنند. آن‌ها چگونه این کار را انجام می‌دهند؟

اضافه کردن بلاک به بلاک‌چین مستلزم حل کردن یک معادله ریاضی پیچیده است که فقط با حدس زدن اعداد امکان‌پذیر است.

نتیجه‌گیری

ذات انسان نامحدود است و هر چیزی را که به آن احساس نیاز کند و ابزار آن در دسترس باشد، خواهد ساخت. با افزایش آگاهی مردم و گسترش آنی اطلاعات در سراسر جهان به علاوه ابزارهایی که وجود دارند، قطعاض جهان آینده غیرمتمرکز خواهد بود و کسی نمی‌تواند در برابر این اتفاق ایستادگی کند.

البته علی‌رغم معایب موجود، فناوری بلاک‌چین مزایای منحصر به فردی ارایه می‌دهد و قطعاً برای حضور بلند مدت ایجاد شده است.

هم‌چنان مسیر طولانی درخصوص پذیرش گسترده بلاک‌چین پیش‌روی خود داریم اما بسیاری از صنایع در حال بررسی دقیق‌تر مزایا و معایب سیستم‌های بلاک‌چین می‌باشند. چند سال آتی احتمالاً شاهد این خواهیم بود که تجارت‌ها و دولت‌های مختلف در حال آزمایش کاربردهای جدید این فناوری می‌باشند تا متوجه شوند که فناوری بلاک‌چین در چه زمینه‌ای کاربرد و ارزش بیشتری دارد.

البته کشورها هنوز سیستم صریحی برای محدودیت، قانون‌گذاری و یا ممنوع کردن ارز دیجیتال ندارند. ماهیت ناشناس و غیر متمرکز بیت‌کوین بسیاری از حکومت‌ها را در مورد نحوه کاربرد قانونی این ارز همراه با جلوگیری از تراکنش‌های مجرمانه توسط آن با چالش جدی روبه‌رو کرده است. بسیاری از کشورها هنوز در حال تحلیل شیوه‌هایی برای قانون‌گذاری درست ارز دیجیتال هستند.

بیت‌کوین، بماند یا برود، ارزهای دیجیتال و بلاک‌چین باقی خواهند ماند چون نیاز برای مالکیت کامل و جلوگیری از فساد و تقلب، واقعاً در جوامع امروزی حس می شود و کشور ما هم برای پیشرفت نیازمند تعامل و تطابق با فناوری‌های بنیادی است.

این فناوری‌های نورآورانه با خصوصیات غیرمتمرکز خود می‌توانند چه به صورت مستقیم و چه غیرمستقیم با بهبود فرایندهای مالی و تسهیل روابط بین‌المللی از فشار تحریم‌ها تا حد زیادی کم کنند.

با این وجود برای رسیدن به این اهداف، نیازمند این هستیم که مسئولین، انفعال در این حوزه را کنار گذاشته و بسترهای لازم اما قانون‌مندی را فراهم نمایند تا با حذف معایب بتوانیم از کاربردهای مفید بلاک‌چین و ارزهای دیجیتال به عالی‌ترین شکل در نظام اقتصادی بهره ببریم.

اما پیشرفت تکنولوژی بهای خود را دارد. فناوری جایگزین بسیاری از فرصت های شغلی می شود.

پیوست ۱

اصطلاحات:

آلت‌کوین‌ها (Altcoins): به ارزهای دیجیتال بعد از بیت کوین مانند اتریوم، لایت کوین و ... اصطلاحا آلت‌کوین می‌گویند.

بیت (Bit): یکی از واحدهای کوچک بیت‌کوین هر بیت کوین = ۱،۰۰۰،۰۰۰ بیت

ساتوشی (Satoshi): یک ساتوشی کوچک‌ترین واحد بیت‌کوین است. این نام از ساتوشی ناکاموتو، خالق بیت‌کوین نام‌گذاری شده است. یک واحد ساتوشی برابر با ۱۰۰۰۰۰۰۰۰ بیت‌کوین است.

XBT و BTC: اختصارات معمولی برای بیت کوین؛ تفاوتی بین این دو اختصار وجود ندارد.

تایید (Confirmation): زمان انجام یک تراکنش، بلاک‌چین معتبر بودن آن را تایید می‌کند. تأیید توسط ماینرها انجام می‌شود.

استخراج (mining): فرایندی که در آن سخت افزار کامپیوتر برای تایید تراکنش ها یک سری محاسبات ریاضی را انجام می‌دهد. کاربرانی را که کامپیوترهای خود را برای این محسبات در اختیار شبکه قرار می‌دهند را ماینر می‌گویند.

کلمات بازیابی (Recovery phrase): کلمات تصادی ۱۲، ۱۸و یا ۲۴ کلمه‌ای که در زمان گرفتن بک آپ به شما داده می‌شود. با این کلمات خواهید توانست که در کیف پول دیگری، کیف پول خود را بازیابی کنید.

رمزنگاری (Cryptography): شاخه‌ای از ریاضیات و علوم رایانه‌ای است که فلسفه‌ی ایجاد ارزهای دیجیتال است.

کلید خصوصی (Private Key): کلید خصوصی رشته‌ای حروف و ارقام مختلف است که با آن تراکنش‌های ارزهای دیجیتال در شبکه امضا می‌شوند. داشتن کلید خصوصی از یک ارز به منزله دسترسی کامل به دارایی‌های آن کیف پول است.

کلید عمومی (Public Key): یک رشته‌ای حروف و ارقام مختلف است که نقش مکمل کلید خصوصی را در تایید تراکنش بازی می‌کند.

اطلاعات بیشتر

کیف پول (Wallet): نرم‌افزارهای آفلاین یا آنلاینی که در آن کلید خصوصی و کلید عمومی قابل استفاده هستند. از کیف پول‌ها برای ذخیره، انتقال و دریافت یک ارز دیجیتال استفاده می‌شود.

گزارش عملکرد – اوراق سفید (Whitepaper): گزارشی کامل از یک پروژه ارز دیجیتال که توسط توسعه‌دهندگان برای بیان تمام جزییات سیستم‌شان منتشر می‌شود.

شناسه تراکنش (Transaction ID): رشته‌ای حروف و ارقام مختلف است که از طریق آن شما می‌توانید جزییات کلی یک تراکنش را روی بلاک‌چین مشاهده کنید.

بلاک‌چین (Blockchain): دفترکلی که می‌تواند گزارشات را از قبیل گزارشات پرداخت یا هر نوع گزارش دیگری را در خود به صورت غیرمتمرکز ثبت کند.

ساتوشی ناکاموتو (Satoshi Nakamoto): خالق ناشناس بیت کوین

ذخیره‌سازی سرد (Cold storage): ذخیره‌سازی ارزها و کلیدهای خصوصی روی فضای آفلاین.

کیف پول سخت افزاری (Hardware Wallet): یک دستگاه سخت‌افزاری امن که به صورت آفلاین کلیدهای خصوصی را ذخیره می‌کند. کیف پول سخت‌افزاری از نوع سرد است.

کارمزدهای تراکنش (Transaction Fees): هزینه‌ای که کاربران برای تایید تراکنش پرداخت می‌کنند. حداقل این هزینه در زمان‌های مختلف و نسبت به شلوغی شبکه متفاوت است. هر چه کارمزد بیشتر باشد تراکنش ما زودتر تایید خواهد شد.

همتا به همتا – P2P: همتا به همتا به معنای ارتباط مستقیم و بدون واسطه‌ی دو شخص حقیقی یا حقوقی است.

بلاک (block): مجموعه‌ای از تراکنش‌ها که ماینرها آن را بررسی و تایید می‌کنند.

اثبات کار (Proof of work): فرایند استخراجی که با دستگاه‌های سخت‌افزاری برای انجام محاسبات انجام می‌شود.

اثبات سهام (Proof of Stake): فرایندی که هر کس نسبت به دارایی خودش ارز استخراج می‌کند.

پامپ و دامپ (Dump & Pump): به هر خبری که باعث افزایش یا کاهش قیمت در یک ارزدیجیتال شود، به ترتیب پامپ و دامپ می‌گویند.

هش (Hash): یک اثرانگشت دیجیتالی است که از یک داده طبق تابعی خواص و با مقداری ثابت تولید می‌شود. کوچک‌ترین تغییر در یک داده می‌تواند هش را به طور کلی تغییر دهد.

عرضه اولیه سکه (ICO) – آی سی او: در حوزه‌ی بلاک‌چین جمع‌سپاری و جذب سرمایه‌گذار بسیار مورد استفاده قرار می‌گیرد و مردم هم معمولاً علاقه زیادی به سرمایه‌گذاری در این پروژه‌ها از خود نشان می‌دهند. جذب سرمایه‌گذار در پروژه‌های غیرمتمرکز با استفاده از ICO انجام می‌شود.

هاردفورک (Hard Fork): یک هارد فورک(شاخه سخت) تغییری بزرگ در پروتکل ارز دیجیتال است. از آن‌جا که پروتکل‌های ارزهای دیجیتال اغلب متن باز هستند توسعه‌دهندگان می‌توانند با تغییرات کلی در آن یک هاردفورک انجام دهند. یک هارد فورک سازگار با قبل نیست. هارد فورک گاهی باعث تبدیل شدن به دو ارز می‌شود؛ مثلاً بیت‌کوین کش هارد فورکی از بیت‌کوین است یا اتریوم کلاسیک هارد فورکی از اتریوم است و این باعث می‌شود که دو ارز کاملاً جدا پدید آید و کسانی که مایل باشند می‌توانند در قبلی ادامه دهند یا به هارد فورک جدید نقل مکان کنند.

سافت فورک (Soft Fork): یک بروزرسانی جزیی در پروتکل ارز دیجیتال.

فاست (Faucet): سایت‌هایی که در قبال کارهایی مانند بخت‌آزمایی یا بازی کردن، به کاربران ارزدیجیتال می‌دهند که اغلب برداشت از این سایت‌ها بسیار سخت است.

فیات (Fiat): پول کاغذی تنظیم شده و متمرکز هر کشوری را فیات می‌گویند.

پاداش بلاک (Block Reward): در پروتکل‌های اثبات کار مثل بیت‌کوین یا اتریوم، با استخراج هر بلاک، مقداری از ارز بومی آن شبکه به استخراج‌کننده می‌رسد. در حال حاضر پاداش استخراج هر بلاک ۱۲٫۵ بیت‌کوین است که به مرور زمان کم‌تر می‌شود.

استخراج کننده ASIC: دستگاه ویژه‌ای با تراشه‌های قدرتمند برای استخراج به مقرون به صرفه بعضی ارزهای دیجیتال بزرگ استفاده می‌شود.

ارتفاع بلاک (Block Hight): بعد از اولین بلاک هر ارز دیجیتال، به آخرین بلاک استخراج شده آن ارتفاع بلاک می‌گویند.

نصف شدن (Halving): پس از هر ۲۱۰،۰۰۰ بلاک در بیت‌کوین، پاداش بلاک نصف می‌شود.

هش ریت (Hash Rate): هش ریت یا قدرت هش واحد اندازه‌گیری قدرت پردازش استخراج در یک ارز دیجیتال است.

صرافی ارزهای دیجیتال (Crypto Exchange): سایتی برای خرید و فروش ارزهای دیجیتال.

سفارشات Stop limit: این بخش در سایت‌های خرید و فروش ارزهای دیجیتال برای تریدرهای حرفه‌ای است. با این ویژگی می‌توانید مشخص کنید که وقتی قیمت به مقدار x رسید، سفارش خریدی یا فروشی با مقدار y برای شما ثبت کند. X: Stop Y: limit

(مثلا فرض می کنیم که شما یک تحلیل گر هستید و پیشبینی می کنید اگر قیمت یک ارز از خط مقاومت ۲۰ دلار عبور کند، قیمتش تا ۶۰ دلار صعود خواهد کرد. پس شما می توانید سفارشی با این ویژگی ایجاد کنید تا از ترید جا نمانید. در قسمت stop باید ۲۰ دلار رو وارد کنید و در قسمت limit باید مثلا ۲۲

دلار رو وارد کنید. برای فروش یا همان stop loss هم به همین گونه تعیین می کنید که در صورت کاهش قیمت یک ارز به مقداری x، سفارش فروشی با مقدار y ثبت شود تا از ضرر بیشتر شما جلوگیری کند.)

حمله ۵۱ درصد (Attack ۵۱٪): هنگامی که بیش از نیمی از توان محاسباتی یک شبکه ارزدیجیتال توسط یک نهاد یا گروه خاص کنترل می‌شود، این نهاد یا گروه خواهند توانست شبکه را نابود کنند. تنها راه نابودی شبکه‌های غیرمتمرکز همین راه است که به دلیل این‌که هر کسی می‌تواند ماینر باشد، تقریباً انجام آن غیرممکن است.

دوبار خرج کردن (Double Spending): دوبار خرج کردن زمانی اتفاق می‌افتد که یک به جای پول اصلی، یک کپی از پول ارسال شود. یکی از مشکلات ارسال پول به صورت دیجیتال در ابتداً این موضوع بود که سرورهای متمرکز و بعد از آن بلاک‌چین و شبکه‌های غیرمتمرکز این شکل را حل کردند.

سالیدیتی (solidity): سالیدیتی زبان برنامه‌نویسی اتریوم برای توسعه قراردادهای هوشمند است.

پیوست ۲

اصطلاحات عامیانه ارزهای دیجیتالی:

HODL: یک میم اینترنتی و اصطلاح عامیانه است که در جامعه بیت‌کوین و ارزهای دیجیتال برای تاکید بر نگهداری و عدم فروش آن‌ها، استفاده می‌شود.

(سال ۲۰۱۳ هنگام سقوط نسبتا بزرگ بیت کوین، در انجمن جهانی «بیت کوین تاک» در حالی که سرمایه گذاران نا امید مشغول بحث درباره نگه داری یا فروش بیت کوین هایشان بودند، کاربری با نام مستعار GameKyuubi، پستی با عنوان I AM HODLING (من نگه می‌دارم) درج می‌کند. او به جای I AM HOLDING، I AM HODLING را اشتباها نوشته بود. این کاربر که به نظردر زمان نگارش پست مست بوده است، قصد اعلام نگهداری بیت کوین ها و عدم فروش آن ها را داشته است. همین موضوع باعث شد تا اصطلاح HODL در فضای ارزهای دیجیتال و بیت کوین بسیار محبوب شود و برای توصیه به نگهداری ارزهای دیجیتال و عدم فروش آن ها استفاده شود. در حال حاضر یک ارز دیجیتال هم به نام HODL وجود دارد.)

ترس از دست دادن FOMO: مخفف «Fear of missing out»، که به معنای ترسِ از دست دادن است. از این اصطلاح در فضای ارزهای دیجیتال، زمانی استفاده می‌شود که فردی نگران از دست رفتن سود سرمایه گذاری یا تصمیمش باشد.

بالاترین قیمت تاریخ ATH: مخفف «All time high» به معنای بالاترین قیمت تاریخ. از این اصطلاح زمانی استفاده می‌شود که قیمت یک ارز، سهام یا چیزهایی شبیه این، به رکورد جدیدی برسد.

خرس BEAR: این اصطلاح از اشخاص فعال در وال استریت گرفته شده است. از واژه خرس در حوزه اقتصاد برای بیان موارد نزولی و کاهشی یک دارایی استفاده می‌شود. مثلا بازار خرسی به معنای بازار نزولی و رو به پایین است.

گاو BULL: این اصطلاح از اشخاص فعال در وال استریت گرفته شده است. از واژه گاو در حوزه اقتصاد برای بیان موارد صعودی و افزایشی یک دارایی استفاده می‌شود. مثلا بازار گاوی به معنای بازار صعودی و رو به بالا است.

نهنگ WHALE: این واژه در میان قماربازان کاربرد داشته است. نهنگ ها معامله گران سرمایه داری هستند که روی آینده یک ارز دیجیتال خوش بین و مبالغ سنگینی روی آن ها سرمایه گذاری می‌کنند. به آن ها نهنگ های گاوی (صعودی) نیز می‌گویند.

نهنگ خرسی BEARWHALE: نهنگ های خرسی معامله گران سرمایه داری هستند که مقدار زیادی از دارایی خود را می‌فروشند و باعث یک کاهش قیمت در بازار می‌شوند.

نگهداری غیر منطقی BAGHODLER: به سرمایه گذار و مخصوصا معامله گری که در نگهداری غیرمنطقی یک دارایی پافشاری می‌کند، اصطلاحا bag-holder یا از دیدگاه طنز BAGHODLER می‌گویند.

نابود شدن REKT: کلمه «REKT»، یک نگارش عمدا اشتباه از کلمه «wrecked» است که به معنای «نابود شده» است. از این اصطلاح برای اشاره به ورشکستی و یا نابودی افراد در بازارهای اقتصادی استفاده می‌شود.

به ماه TO THE MOON: این اصطلاح در بیان اخبار صعود بسیار بزرگ یک دارایی استفاده می‌شود.

آدرس ADDY:این اصطلاح به آدرس کیف پول یک ارزهای دیجیتال اختصاص دارد.

ترس، عدم قطعیت و شک FUD : مخفف کلمات متوالی «Fear, uncertainty, and doubt»، به معنای ترس، عدم قطعیت و شک است. از این اصطلاح معمولا برای اشاره به عدم اطمینان از یک موقعیت استفاده می‌شود.

ارسالی Shitcoin: ارز بی ارزش

چین CHOYNA: یک اصلاح رایج برای اشاره به چین. کشور چین علی رغم مخالفت دولت، در فضای بیت کوین بسیار فعال است. عمده استخراج و معاملات ارزهای دیجیتال در دست افراد چینی است.