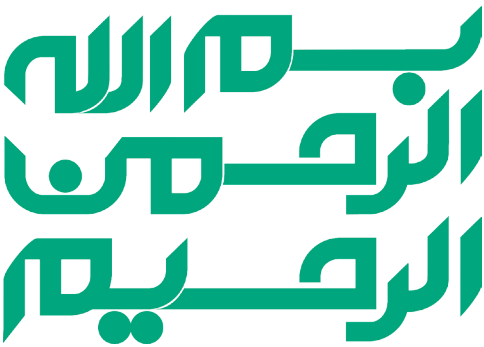
آشنایی با دفتر کل توزیع شده، توکن و رمزارز و ارز دیجیتال بانک مرکزی

دارایی دیجیتال

گروه بلاکچین مرکز نوآوری پل وینو با همکاری ققنوس

۱


بسم الله
الرحمن
الرحيم

The mark of responsible forestry
FSC™ C009732

سرشناسه: نواب‌پور، علیرضا، ۱۳۷۰-
عنوان و نام پدیدآور: دارایی دیجیتال: آشنایی با دفتر کل توزیع شده، توکن و رمز ارز و ارز دیجیتال بانک مرکزی/
نویسنده: علیرضا نواب‌پور
ویراستار ارشد: مینا والی
ویراستار محتوایی: قاسم سرافرازی
ویراستار فنی: یلدا شایسته‌فر
مشخصات نشر: تهران: راه پرداخت، ۱۴۰۰.
مشخصات ظاهری: ۲۰۰ ص.؛ ۵/۱۴×۵/۲۱ س‌م.
شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۰-۱
وضعیت فهرست نویسی: فیپا
موضوع: شبکه‌ققنوس
موضوع: رمزارز
موضوع: Cryptocurrencies
موضوع: بلاک‌چین (پایگاه‌های اطلاعاتی)
موضوع: Blockchains (Databases)
موضوع: ارز مجازی
شناسه افزوده: والی، مینا، ۱۳۶۳ -، ویراستار
شناسه افزوده: سرافرازی، قاسم، ۱۳۶۶-، ویراستار
رده بندی کنگره: HG۱۷۱۰
رده بندی دیویی: ۱۷۸/۳۳۲
شماره کتابشناسی ملی: ۸۵۰۶۷۶۱

آشنایی با دفتر کل توزیع شده، توکن و رمزارز و ارز دیجیتال بانک مرکزی

دارایی دیجیتال

گروه بلاکچین مرکز نوآوری پل وینو با همکاری ققنوس

۱

انتشارات
راه‌پرداخت

عنوان : دارایی دیجیتال؛ آشنایی با دفترکل توزیع شده، توکن و رمزارز و ارز دیجیتال بانک مرکزی

ناشر : راه پرداخت

نویسنده: گروه بلاکچین مرکز نوآوری پل و اینو

ویراستار ارشد : علیرضا نواب‌پور

ویراستار محتوایی : بهنام خاکباز

ویراستار فنی: فاطمه کاوندی، فرناز نکویی

بازبینی نهایی متن: بهار سرلک

صفحه‌آرا: علیرضا کیوان

ناظر چاپ : قادر شهبازی

نوبت چاپ: اول ۱۴۰۰

شمارگان : ۱۰۰۰ نسخه

شابک: ۱-۱۰-۷۷۰۲-۶۲۲-۹۷۸

تلفن : ۴۴۴۴۳۹۶۶-۰۲۱

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل : info@way2pay.press

وب‌سایت : way2pay.press

لیتوگرافی: هنر اشکان

چاپ و صحافی: واژه

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

@Way2Pay_Network Way2Pay.press @Way2Pay press

فهرست

[پیشگفتار]

پیش‌بینی دقیق آینده و اتفاقاتی که رخ خواهد داد امکان‌پذیر نیست؛ اما باید برای آنچه احتمالاً پیش خواهد آمد آمادگی لازم را داشته باشیم. تجارب چند دهه اخیر نشان می‌دهد که فناوری‌های برهم‌زننده، مسیر حرکت و اثرگذاری خود را پیدا می‌کنند تا جایی که پذیرش آن برای کسب‌وکارها یک الزام می‌شود نه یک انتخاب و مقاومت در مقابل آنها ادامه حیات کسب‌وکار را دچار چالشی جدی می‌سازد.

بنا بر پیش‌بینی بسیاری از متخصصان و آینده‌پژوهان، فناوری بلاکچین طی ۱۰ سال آتی به اوج شکوفایی خود می‌رسد و کاربردهای اصلی آن پدیدار خواهد شد. آن زمان، میان شرکت‌هایی که هم اکنون روی فناوری بلاکچین سرمایه‌گذاری می‌کنند و آنهایی که توجهی به این روند جهانی ندارند، شکاف معناداری پدیدار می‌شود. بسیاری از پلتفرم‌های متمرکز جای خود را به پلتفرم‌های غیرمتمرکز و توزیع‌شده خواهند داد. شاید برخی از روابط مالی بر پایه رمزارزها انجام شود، شاید زیرساخت تسویه بین بانکی یا بازار بورس به سمت دفاتر کل توزیع‌شده برود، شاید مرورگرها و رسانه‌های غیرمتمرکز ایجاد شوند، شاید نظام وام‌دهی به مدل همتا به همتا تغییر یابد و بسیاری از شایدهای دیگر... که به‌هیچ‌وجه دور از ذهن نیستند.

واقعیت این است که صنعت مالی و بانکداری بیشترین تأثیر را از بلاکچین خواهد داشت؛ بنابراین اگر بانک‌ها دقت و آمادگی لازم را در این زمینه نداشته باشند ممکن است

تازه‌واردانی را که با شیوه‌ها و خدمات جدید مورد استقبال عموم قرار می‌گیرند، رقبای جدی خود ببینند.

گروه بهســـازان فردا به نیابت از مجموعه بانک ملت از بیش از سه سال پیش اقدامات مختلفی را در این زمینه آغاز کرده که یکی از آنها مشارکت در کنسرسیوم ققنوس به‌عنوان یک شرکت تخصصی در این زمینه است. اما آمادگی برای شرایط پیش رو و متأثر از این فناوری نیازمند آگاهی و اشراف کارشناسان و مدیران حوزه کسب‌وکار است. بنابراین مرکز نوآوری پل‌وینو در سال ۱۳۹۹ بر آن شد در این راستا گامی مؤثر بردارد. بیان روان و ساده مفاهیم نهفته در فناوری بلاکچین به‌عنوان یک ضرورت به فرهنگ‌سازی درمیان ذینفعان کمک می‌کند که هدف از گردآوری این کتاب نیز همین امر است.

این کار ماحصل پژوهـــش جمعی از همکاران در مرکز نـــوآوری پل‌وینو و با هدایت همکاران گرامی آقایان علیرضا نواب‌پور و بهنام خاکباز و خانم فرناز نکویی است.

ضمن تشکر از زحمات ایشـــان، مطالعه این کتاب به همه کارشناسان و مدیران حوزه بانکی توصیه می‌شود. همچنین از شرکت ققنوس که حمایت از این کتاب را متقبل شد و در این زمینه در فصل شش به معرفی این شرکت پرداخته است سپاسگزارم. امیدواریم بعد از مطالعه کتاب، تصویر روشن‌تری از آینده حاصل شود.

محمدهادی شالباف
رئیس مرکز نوآوری گروه فن‌آوران هوشمند بهسازان فردا «پل‌وینو»

[مقدمه]

به دنبال اختراع اینترنت و تحقق رؤیای انتقال آزادانـــه «داده‌ها و اطلاعات» که ســـالیان متمادی، متخصصان فناوری اطلاعات روی آن کار می‌کردند، دانشمندان مطرحی همچون هایـــک[1]، برنده جایزه نوبـــل اقتصاد در ســـال ۱۹۷٤، مفهومی تحت‌عنوان غیرمتمرکزکردن ارزش[2] را در مجامع علمی مطرح کردند. دغدغه اصلی پیروان این تفکر، آزادی فردی، حفظ حریم شخصی و عدم اعتقاد و اعتماد به نهاد واسط و مرکزی بود. آنها معتقد بودند اساســاً چه دلیلی دارد نهاد ثالثی از اطلاعات دارایی و مالی مردم مطلع باشد و توان بلوکه و آزاد کردن آن را داشته باشد؟ این نهادها چگونه صلاحیت خود را برای اینکه امین مردم در نگهداری «ارزش» آنان باشـــند به‌دست آوردند؟

تفاوت «داده اطلاعاتی» با «داده ارزشی» در این است که داده ارزشی خلاف داده اطلاعاتی نباید امکان جعل یا کپی‌شـــدن داشته باشـــد و اگر این اتفاق بیفتد آن داده بی‌ارزش خواهد شد. از اواخر دهه ۱۹۹۰ متخصصان فناوری اطلاعات در پی توسعه فناوری‌ای بودند که بتواند داده ارزشی را بدون حضور نهاد مرکزی، غیرقابل‌جعل و کپی‌شدن سازد. در سیستم سنتی، همه به نهاد ثالثی اعتماد می‌کردند که ضامن و امین

1. Hayek
2. Value

آنها بود و یقین داشتند داده‌های ثبت شده در یک «دفتر کل» که نزد او قرار داشت کپی و جعل نخواهد شد.

حاصل این تلاش‌ها در سال ۲۰۰۹ با معرفی بلاکچین به ثمر نشست و فناوری‌ای به دنیا معرفی شد که با توزیع‌کردن دفترکل میان همه اعضا و در نتیجه حذف نهاد واسط می‌توانست هر داده‌ای را غیرقابل‌جعل و غیرقابل‌کپی‌شدن سازد و در نتیجه به آن داده ارزش بخشد. به عبارتی دیگر به‌وسیله فناوری یاد شده این امکان فراهم شد که هر داده ارزشی که در آن ثبت شود، بدون وجود نهاد مرکزی در خطر جعل یا کپی‌شدن قرار نگیرد و این پدیده می‌تواند بنیان تمام سیستم‌های متمرکز با نهاد مرکزی را به لرزه درآورد. این مکانیزم ثبتی غیرمتمرکز به‌طور کلی «فناوری دفاترکل توزیع‌شده»[1] نام گرفت. اولین نمونه این فناوری، بلاکچین و اولین محصول آن بیت‌کوین بود.

اگر چه این فناوری با محصولی به دنیا معرفی شد که قصد داشت جایگزین سیستم پولی فعلی شود؛ اما رفته‌رفته کاربردهای متعددی برای این فناوری تعریف شد؛ چراکه فناوری دفاترکل توزیع‌شده، نوعی فناوری نوین جهت «ثبت» است که به میزان مصادیق ثبت در کسب‌وکارها می‌توان برای آن کاربرد تعریف کرد. فناوری دفاترکلِ توزیع‌شده سه ویژگی محوری دارد که آن را منحصر به فرد و کاربردهای آن را در ثبت ارزش‌ها افزایش می‌دهد: غیرقابل‌جعل بودن بدون نیاز به نهاد مرکزی، شفاف‌بودن تمامی تراکنش‌ها و ناشناس‌بودن افراد در شبکه.

به مرور در دهه ۲۰۱۰ پس از افزایش قیمت بیت‌کوین، مطالب متعددی درباره سایر کاربردهای فناوری دفاترکل توزیع‌شده به‌طور خاص در صنعت مالی و بانکداری منتشر شد. همراه با این روند جهانی، یک سؤال و ابهام جدی میان فعالان فعلی صنعت مالی و بانکداری مطرح شد که آیا براساس فلسفه ایجاد بلاکچین، این فناوری یک چالش و تهدید جدی برای نهادهای متمرکز این صنعت است یا می‌تواند ابزاری در دستان آنها باشد؟ آیا همانگونه که وجود نهادها و فرایندهای متمرکز دارای ایراداتی هستند، دنیای مالی غیرمتمرکز به‌دلیل نبود نهادهای ناظر و رگولاتور، چالش‌های

1. Distributed Ledger Technology (DLT)

بزرگ‌تری را برای جامعه به همراه نخواهد داشت؟

به دنبال پاسخ به این سؤالات، متخصصان فناوری اطلاعات تغییراتی را در فناوری بلاکچین اعمال کردند و با ایجاد بلاکچین‌های «خصوصی» و «مجوزدار» که در عین داشتن مزایای سیستم‌های غیرمتمرکز، چالش‌های عدم‌حضور نهاد ناظر را نداشت، این فناوری به‌تدریج به مرز تعادل میان دنیای متمرکز و غیرمتمرکز نزدیک شد. همگام با این تعادل نسبی، شاهد روند روبه‌رشد به‌کارگیری این فناوری توسط دولت‌ها و بانک‌ها در جهان بوده‌ایم.

طبق گزارش WEF در سال ۲۰۱۶، تا آن زمان ۲۴ کشور در این فناوری معادل ۱,۴ میلیارد دلار سرمایه‌گذاری کرده‌اند، بیش از ۲۵۰۰ اختراع در این زمینه ثبت شده، بیش از ۹۰ شرکت بزرگ کنسرسیوم بلاکچینی تشکیل داده‌اند و بیش از ۹۰ بانک مرکزی وارد بحث بلاکچین شده‌اند؛ تا جایی که در سال ۲۰۱۷ پروژه ارز دیجیتال بانک مرکزی[1] را رسماً چند کشور کلید زدند. براساس این گزارش بیش از ۸۰ درصد بانک‌ها پیش‌بینی کرده‌اند که به زودی از پروژه‌های مبتنی بر فناوری دفاترکل توزیع‌شده خود رونمایی خواهند کرد.

از مهم‌ترین کاربردهای این فناوری که در ابتدا شناسایی شد می‌توان به افزایش کارایی «تسویه و پایاپای»[2] مخصوصاً در سطح بین‌المللی و تسهیل فرایندهای تأمین مالی تجارت[3] اشاره کرد. به مرور زمان این کاربردها به صنایع پرداخت، بیمه، قرض‌دهی، تأمین‌مالی جمعی و غیره نیز گسترش پیدا کرد.

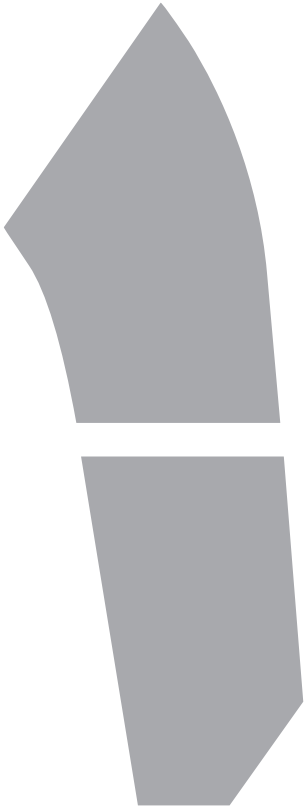
به‌دنبال سرعت روزافزون گسترش کاربردهای فناوری دفاترکل توزیع‌شده که نمود آن در صنعت مالی و بانکداری کاملاً مشهود شده است، مرکز نوآوری بانک ملت بر آن شد مطالعه جامعی روی فناوری دفاترکل توزیع‌شده و انواع محصولات توسعه‌داده‌شده از آن به منظور آشنایی خوانندگان با مفاهیم اولیه این فناوری، انجام دهد که متن حاضر به همین منظور تدوین شده است.

---

1. CBDC
2. Clearing and Settlement
3. Trade Finance

در این کتاب ابتدا فناوری دفاترکل‌توزیع‌شده و انواع آن معرفی می‌شوند، سپس به انواع توکن‌های موجود و مباحث رگولاتوری مرتبط با آن پرداخته خواهد شد. از مهم‌ترین توکن‌های تعریف شده برای صنعت بانکداری، ارز دیجیتال بانک مرکزی است که در فصلی مجزا به آن پرداخته‌ام و در انتها در مورد چالش‌ها و فرصت‌های این فناوری برای کشور توضیحاتی می‌دهم.

علیرضا نواب‌پور
مرکز نوآوری پل‌وینو



فصل اول

مروری بر فناوری‌های غیرمتمرکز

مقدمه

از هزاران سال پیش بشر تمایل داشت با رویکرد تمرکزگرایی، مسائل و چالش‌های روابط بین‌انسانی را حل و فصل کند. در برخی جوامع به مرور هنجارهای سختگیرانه‌ای شکل گرفت که منجر به ایجاد طبقات مختلف اجتماعی و اقتصادی، نابرابری و نژادپرستی شد. به‌طور کلی ساختار جوامع را می‌توان به دو نوع متمرکز با کنترل و فرماندهی و غیرمتمرکز به‌طور همتابه‌همتا[1] تقسیم کرد.

اما ساختارهای متمرکز به مرور مشکلات زیادی به بار آوردند. انقلاب صنعتی به نوآوری‌های گسترده در فناوری نیاز داشت و انحصارطلبی مانعی برای رشد آن بود. با ورود اینترنت و گسترش آن، مفهوم تمرکززدایی[2] فناوری در روابط انسان‌ها منعکس شد. از طرف دیگر از دهه ۱۹۷۰ جنبش‌های وسیع تمرکززدایی برای کاهش قدرت دولت مرکزی و ایجاد دموکراسی در کشورهای اروپایی آغاز شده بود. در واقع تمرکززدایی راه دموکراتیک کردن جامعه است، زیرا امکان تصمیمات جمعی شهروندان را فراهم می‌کند.

عبارت تمرکززدایی اولین بار برای توصیف توزیع قدرت سیاسی در ایالات متحده فدرال به‌کار برده شد. اما مفهوم متمرکزسازی و تمرکززدایی نه تنها در سیاست، بلکه در حکومت‌داری، اقتصاد، فرهنگ، فناوری و شکل‌گیری جوامع می‌تواند مؤثر باشد.

در سیستم‌های امروزی، تمرکززدایی به معنی ایجاد امنیت و عدم‌نیاز به یک معتمد با توزیع داده‌ها بین اعضا، افراد و نهادهای متعدد است. این ویژگی با تقسیم قدرت، کنترل، دسترسی و مالکیت برای بازیگران مختلف شبکه، این احتمال را که یک نفر بتواند تأثیر منفی بر سیستم بگذارد کاهش می‌دهد. شبکه‌های غیرمتمرکز با حذف واسطه‌ها و نهاد مرکزی می‌توانند اعتماد را بین افراد و سازمان‌ها افزایش دهند. در این شبکه‌ها اعتماد نیز مانند اطلاعات بین بازیگران توزیع می‌شود. عدم‌تمرکز، شفافیت و اعتماد در این سیستم‌ها باعث شده است فناوری‌های غیرمتمرکز کاربردهای وسیعی در حوزه خدمات مالی بیابند.

---

1. Peer to Peer
2. Decentralization

مفهوم دفترکل توزیع شده

استفاده از دفترکل جهت ثبت تراکنش‌های مالی، پدیده جدیدی نیست و بشر از صدها سال پیش تاکنون از آن برای ثبت قراردادها، پرداخت‌ها، خریدوفروش، جابه‌جایی املاک و دارایی‌ها استفاده می‌کرده است. بشر ابتدا به نگارش آنها بر روی لوح‌های سنگی می‌پرداخت و بعدها از کاغذ استفاده کرد. با گسترش رایانه و اینترنت فرایند ثبت تراکنش‌ها در دفترکل متمرکز با سرعت و سادگی بیشتری انجام شد. مشکلات و چالش‌های دفاتر کل متمرکز که در مشکل «اعتماد» به شخص ثالث خلاصه می‌شود همراه با کشف و استفاده از الگوریتم‌های جدید، مفهومی به نام «دفترکل توزیع‌شده» را پدید آورد. در ادامه با بیان یک مثال مالی به تفاوت میان دفترکل توزیع‌شده و متمرکز پرداخته می‌شود.

برای مثال در بانک تمام تبادلات مالی مشتریان در یک دفترکل ثبت و ضبط می‌شود و بانک به‌عنوان دارنده دفتر کل، تنها نهادی است که به آن دسترسی دارد. چنانچه دیگران به دفترکل یک بانک دسترسی پیدا کنند، امکان برداشت یا سوءاستفاده از حساب مشتری بدون رضایت او وجود دارد که این موضوع می‌تواند باعث آسیب جدی به بانک و مشتریان شود. از دیگر سو، به دلیل وجود اختلال یا هر مشکل دیگری ممکن است سرویس آن بانک محدود یا از دسترس خارج شده باشد که در این صورت مشتری به موجودی حساب خود دسترسی ندارد و نمی‌تواند تراکنشی انجام دهد. همچنین بانک می‌تواند دسترسی مشتری را بدون رضایت یا اطلاع او به هر دلیلی از جمله قضایی یا غیر آن محدود یا مسدود سازد و حتی از آن برداشت کند.

اکنون فرض کنید چند بانک تصمیم بگیرند اطلاعات تراکنش‌های خود را به‌صورت اشتراکی داخل یک دفترکل، ثبت و هر یک نسخه‌ای از آن را نگهداری کنند. در این صورت نه تنها تمام بانک‌ها می‌توانند بر صحت تراکنش‌های ثبت شده توسط یکدیگر نظارت داشته باشند، بلکه در صورت اختلال یا قطع سرویس یک بانک، مشتری می‌تواند از طریق دیگر بانک‌ها به‌حساب خود دسترسی داشته باشد و در این شرایط از امنیت بالاتری برخوردار خواهد بود. ضمناً هر بانک نمی‌تواند به اختیار خود حسابی را مسدود یا دستکاری کند.

دفترکل توزیع‌شده نوعی دفترکل است که به‌صورت اشتراکی بین چند عضو شبکه (مثلاً چند بانک) اســـتفاده می‌شـــود که البته نگهداری و به‌روزرسانی آن به‌صورت مکتوب عملاً غیرممکن است و حتماً برای پیاده‌سازی آن باید از سامانه‌های پیشرفته استفاده شود. هر یک از اعضای شـــبکه که می‌خواهند تراکنشی را در این دفترکل به ثبت برسانند، باید ابتدا تراکنش خود را به سایر اعضا اعلام کنند. پس از کنترل صحت تراکنش توسط بیش از نیمی از اعضای شبکه، آن تراکنش توسط همه اعضا تأیید و در دفترکل ثبت می‌شود.

دفترکل توزیع‌شده، اجماعی از داده‌های دیجیتال تکثیرشده، اشتراک‌گذاری‌شده و همگام‌سازی‌شده اســـت که در موقعیت‌های جغرافیایی مختلف گسترده شده‌اند. در این فناوری هیچ مدیریت یا ذخیره‌ســـازی متمرکزی بر داده‌هـــا وجود ندارد و جایگزینی است برای ســـامانه‌هایی که مدیریت آنها با اســـتفاده از پایگاه‌های داده متمرکز و ســـرورهای مرکزی انجام می‌پذیرد. این دفتر براساس سازوکار اجماع[1] (که در بخش بعد توضیح داده می‌شـــود) و معماری داده مورد قبول اعضای شبکه، نگهداری و به‌روزرسانی می‌شـــود. به این معنی که هر فرد در شبکه، هر تراکنش را پردازش می‌کند و ســـپس درباره ثبت شدن یا نشـــدن اطلاعات رأی می‌دهد و در صورت تأیید اکثریت، آن اطلاعات ثبت می‌شوند.

هدف اصلی این فناوری حل مشکل اعتماد و همچنین کاهش هزینه‌های ناشی از نهاد مرکزی یا شخص سوم قابل‌اعتماد است. در این فناوری، دفترکل میان اعضای شبکه توزیع می‌شود و خود ایشان موظف هستند اعتبار معاملات و حساب‌ها را حفظ کنند. نتیجه این کار یک سیستم غیرمتمرکز ثبت داده است که در آن معاملات سریع، شفاف، قابل‌اطمینان و غیرقابل‌دست‌کاری انجام می‌شوند.

انواع فناوری‌های غیرمتمرکز

معمولاً دو اصطلاح بلاکچین[2] و فناوری دفترکل توزیع‌شده هم‌معنی تلقی می‌شوند،

1. Consensus mechanism
2. Blockchain

اما دفترکل توزیع‌شده یک اصطلاح وسیع‌تر است که لزوماً نباید از بلاکچین استفاده کند و انواع مختلفی دارد که بلاکچین محبوب‌ترین نوع آن است. از دیگر انواع این فناوری می‌توان به گراف جهت‌دار غیرمدور[1] نیز اشاره کرد که تفاوت اصلی و عمده در پیاده‌سازی آنها در مکانیزم اجماع‌شان خلاصه می‌شود. در ادامه به بررسی انواع مختلف این فناوری می‌پردازم.

بلاکچین

ساده‌ترین و رایج‌ترین شکل فناوری دفترکل توزیع‌شده، بلاکچین است. واژه بلاکچین از دو کلمه بلوک[2] و زنجیره[3]، به معنای زنجیره‌ای از بلوک‌ها تشکیل شده است. در سال ۱۹۹۱ استوارت هابر و اسکات استورنتا[4] اولین کسانی بودند که روی فناوری بلاکچین کار کردند. این فناوری تا سال ۲۰۰۹ که ساتوشی ناکاموتو[5] بیت‌کوین را اختراع کرد، کاربرد زیادی نداشت. او توانست با پیاده‌سازی بیت‌کوین بر بستر این فناوری، اولین پایگاه داده مبتنی بر بلاکچین را طراحی کند.

دلیل این نامگذاری، وابستگی بلوک‌ها به یکدیگر است که به‌صورت یک زنجیره، رکوردهای داخل یک پایگاه داده را در خود ثبت و ضبط کرده است. در واقع بلوک پیدایش[6] (اولین بلوک) همانند دفترکل اولیه است که مالکیت‌ها در آن ثبت شده و به ازای هر تغییری در آن، یک الحاقیه در قالب بلوک جدید به آن الصاق (زنجیر) می‌شود و به این ترتیب بلوک‌هایی زنجیروار و مرتبط با هم پدید می‌آید و همین مسئله حمله به آن را هزینه‌بر می‌کند چراکه برای تغییر آخرین بلوک باید تک‌تک الحاقیه‌ها تا بلوک پیدایش تغییر کنند.

برای اضافه کردن هر الحاقیه (بلوک) باید بیش از نیمی از اعضای شبکه بر روی آن

1. Directed Acyclic Graph (DAG)
2. Block
3. Chain
4. Stuart Haber & Scott Stornetta
5. Satoshi Nakamoto
6. Genesis Block

اجماع کنند که پس از آن اجماع، می‌بایست برای اتصال بلوک جدید به قبلی انرژی مصرف شود (وظیفه استخراج‌کنندگان) تا رمز اتصال (عدد نانس [1]) استخراج و به همه اعلام شود تا بتوانند بلوک جدید را به‌روزرسانی کنند.

هر بلوک شامل بخش سرآیند [2] و بخش بدنه [3] است. در بخش سرآیند، برچسب زمانی بلوک [4] (زمان ایجاد بلوک)، هش [5] آن بلوک و هش بلوک قبلی و سایر اطلاعات مربوط به شناسایی آن بلوک قرار می‌گیرند و در بخش بدنه، داده‌هایی که قرار است در آن بلوک ذخیره شوند، جای می‌گیرد.

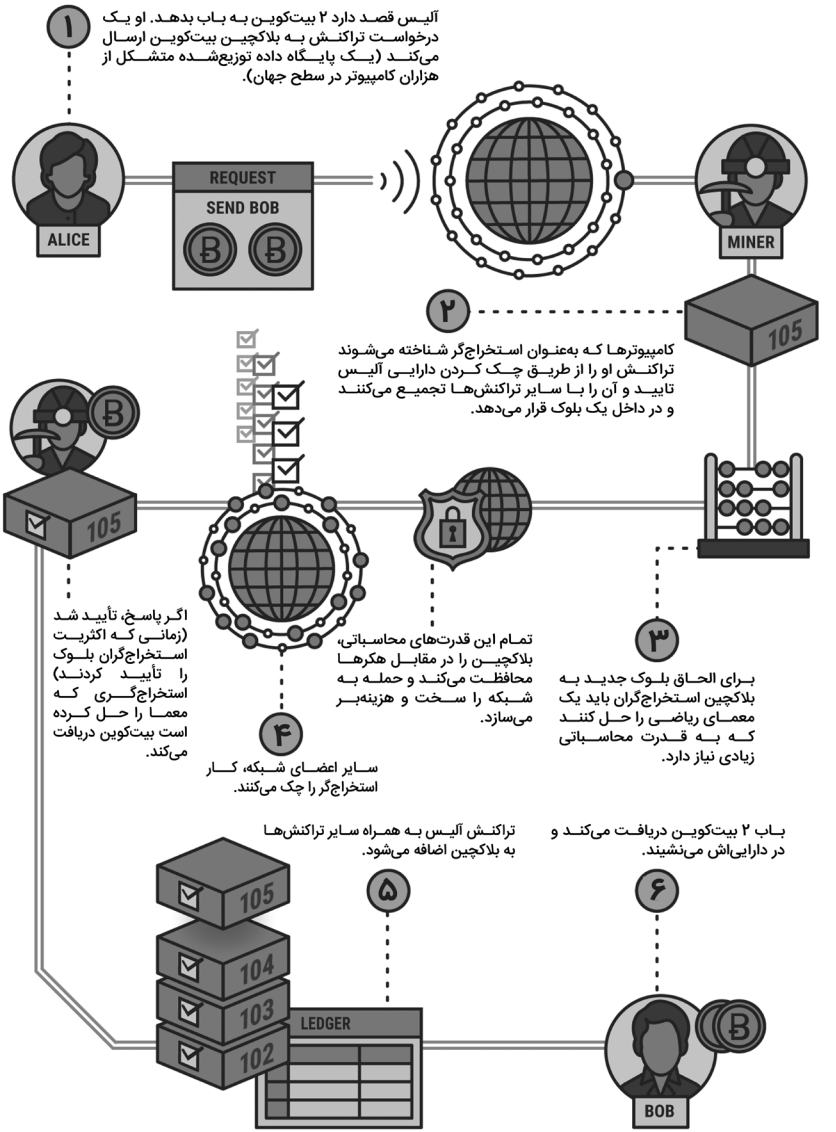
هش، مجموعه‌ای از اعداد و حروف تصادفی است که تأییدکنندگان تراکنش یا استخراج‌کنندگان [6] با کمک یک تابع ریاضی خاص به‌دست می‌آورند. هش هر بلوک مخصوص همان بلوک است و نقش اثر انگشت را برای آن دارد. اگر تغییری در اطلاعات بلوک به‌وجود آید، هش آن کاملاً عوض می‌شود و به دلیل وابستگی بلوک‌ها به یکدیگر، هش بلوک‌های بعدی نیز تغییر می‌کنند و بلوک‌ها نامعتبر می‌شوند و باعث به هم خوردن شبکه می‌شود. به همین دلیل، با بررسی هش یک بلوک به سادگی می‌توان اصالت یا عدم اصالت اطلاعات یک بلوک را تشخیص داد.

بنابراین، بلاکچین یک پایگاه داده تغییرناپذیر، غیرمتمرکز و مقاوم در برابر حمله‌های احتمالی است. از نظر امنیتی، بزرگ‌ترین تفاوت این شبکه با شبکه‌های دیگر این است که امکان حذف و دستکاری اطلاعات وجود ندارد، زیرا روی یک سرور خاص قرار نگرفته و تمامی سرورهای تأییدکننده متصل به شبکه بر یکپارچگی این اطلاعات نظارت می‌کنند. از سوی دیگر این اطلاعات توزیع شده است و در واقع یک کپی کامل از بلاکچین در اختیار اعضای شبکه قرار می‌گیرد که این مسئله نیز دستکاری اطلاعات را به مراتب سخت‌تر می‌کند.

شکل ۱ نحوه انجام تراکنش در یک شبکه بلاکچین را به‌خوبی نشان می‌دهد.

---

1. Nonce
2. Header
3. Body
4. Timestamp
5. Hash
6. Miners



شکل ۱: تراکنش در یک شبکه بلاکچین

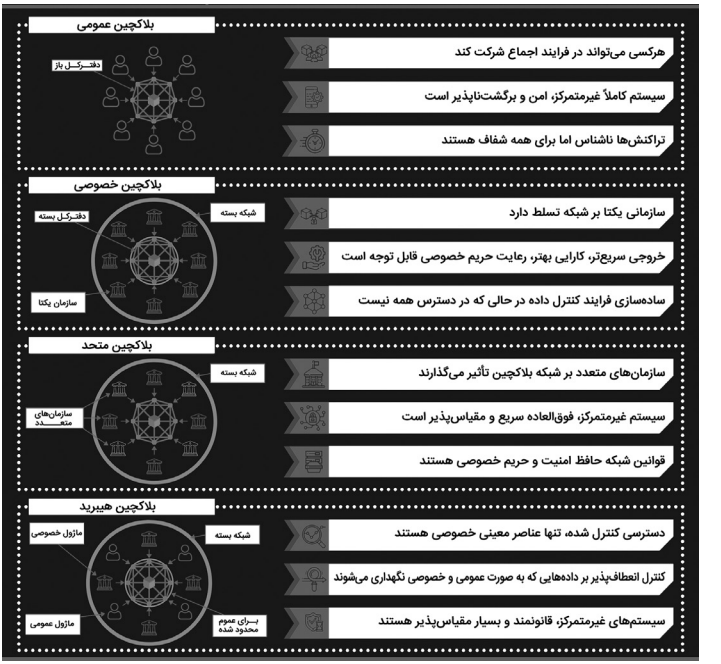
براساس دو معیار امکان مشاهده و تأیید تراکنش، بلاکچین‌ها به چند دسته تقسیم می‌شوند که هرکدام نشانگر این موضوع خواهند بود که چه کسانی قادر به مشاهده و تأیید تراکنش‌ها هستند. برای تفکیک براساس امکان مشاهده تراکنش‌ها، دو دسته کلی بلاکچین عمومی[1] و بلاکچین خصوصی[2] در این فناوری وجود دارد. در بلاکچین عمومی هر فرد می‌تواند با فراهم کردن امکانات فنی مورد نیاز به شبکه اضافه شود و ضمن مشاهده تراکنش‌ها، در تأیید آنها نیز مشارکت داشته باشد. هر فردی از هر نقطه‌ای در دنیا می‌تواند تراکنشی را به یک شبکه عمومی ارسال کند و در صورتی که این تراکنش تأیید و ثبت شود، می‌توان انتظار داشت که در داخل شبکه برای همه قابل رؤیت باشد. شفافیت مطلق از جمله ویژگی‌های بارز بلاکچین عمومی است که موجب افزایش اعتماد به شبکه می‌شود. ممکن است یک سازمان یا مجموعه‌ای از سازمان‌های همکار در راه‌اندازی یک بلاکچین خصوصی با یکدیگر مشارکت کنند که در این صورت تنها افراد خاصی قادر به مشاهده اطلاعات تراکنش‌ها هستند. بلاکچین خصوصی در واقع راهی برای استفاده از امتیاز بلاکچین و تعیین گروهی از مشارکت‌کنندگان برای تأیید تراکنش‌ها به شکل داخلی است. این قابلیت ممکن است میزان اعتماد کمتری نسبت به شبکه عمومی ایجاد کند اما هنگامی که بحث مقیاس‌پذیری[3] و سایر مشکلات در بخش قانونگذاری در میان است، بلاکچین خصوصی مزایای خاص خود را دارد. روش دیگر تفکیک شبکه‌های بلاکچین، طبقه‌بندی آنها براساس امکان تأیید تراکنش‌هاست که از آنها به‌عنوان «بلاکچین با کسب مجوز دسترسی»[4] و «بلاکچین بدون نیاز به مجوز دسترسی»[5] یاد می‌شود. در نوع دوم، تمام افراد امکان مشارکت در تأیید تراکنش‌ها را دارند و هر شخص بدون آنکه به کسب مجوز از شبکه نیاز داشته باشد، می‌تواند در بررسی و تأیید تراکنش‌ها مشارکت کند و در ازای این مشارکت از شبکه پاداش بگیرد. اما در بلاکچین از نوع با کسب مجوز دسترسی، تنها افراد خاصی که پیش‌تر توسط سایر مشارکت‌کنندگان شبکه تأیید شده باشند قادر به تأیید تراکنش‌ها هستند که در این روش، به دلیل کمتر بودن پیچیدگی فرایند تأیید، تراکنش‌ها با سرعت بیشتری

1. Public blockchain
2. Private blockchain
3. Scalability
4. Permissioned blockchain
5. Permissionless blockchain

پردازش و تأیید می‌شوند. براساس دو معیار فوق، معمولاً شبکه‌های بلاکچین یکی از چهار نوع زیر هستند که ویژگی‌های هریک را به اختصار ذکر می‌کنم:

۱. بلاکچین کنسرسیوم و متحد[1]: محدودکنندگی بیشتر، دسترسی محدود، مقیاس‌پذیری بسیار مناسب، شفافیت و حفظ حریم خصوصی بالا (به‌عنوان مثال کنسرسیوم R3).

۲. بلاکچین خصوصی و نیازمند مجوز[2]: در این نوع از بلاکچین‌ها دسترسی می‌تواند به‌صورت عمومی یا خصوصی تعریف شـــود. اما اجازه تأییـــد تراکنش‌ها، انجام توافق و تغییر داده‌ها فقط برای افراد معین و محدودی فراهم می‌شـــود. بانک‌چین[3] نمونه‌ای از این بلاکچین است.



شکل ۲: انواع فناوری بلاکچین

1. Federated blockchain
2. Permissioned/Private blockchain
3. Bankchain

۳. بلاکچین عمومی و بدون نیاز به مجوز[1]: این فناوری یک شبکه عمومی متن‌باز و شفاف است که همه امکان رؤیت تراکنش‌ها و مشارکت در تأیید آنها را دارند. این نوع بلاکچین با حداقل هزینه قابل راه‌اندازی است و نیازی به نگهداری ندارد. با این حال عمومیت‌اش باعث می‌شود روند پردازش آن آهسته باشد. بیت‌کوین و اتریوم[2] بهترین نمونه‌های عمومی بودنش، این نوع بلاکچین‌ها هستند. مشکل اصلی این نوع بلاکچین، محدودیت تراکنش در ثانیه (TPS[3]) و عدم مقیاس‌پذیری است. با وجود این، برای تأیید تراکنش‌ها می‌توان از سازوکارهای مختلف اجماع استفاده کرد.

٤. بلاکچین هیبریدی[4]: این نوع بلاکچین‌ها ترکیبی از شبکه‌های عمومی و خصوصی هستند. بلاکچین‌های هیبریدی از انعطاف‌پذیری خاصی در خصوص تعیین داده‌های خصوصی و همچنین داده‌های قابل ذخیره‌سازی در دفترکل عمومی برخوردارند. این شبکه‌های دوگانه مقیاس‌پذیری بهتری دارند و اجماع در آنها نیازمند مشارکت تمامی گره‌های شبکه نیست. هایپرلجر[5] یک نمونه از این شبکه‌های بلاکچین هیبریدی است.

هش‌گراف[6]

هش‌گراف در تلاش است محدودیت‌های بلاکچین را برطرف کند. هش‌گراف برای تأیید تراکنش‌های موجود روی شبکه فقط به مکانیزم اجماع و توافق متکی است. این اجماع از طریق روش‌هایی چون رأی‌گیری مجازی و همچنین تکنیک‌های شایعه[7] حاصل می‌شود.

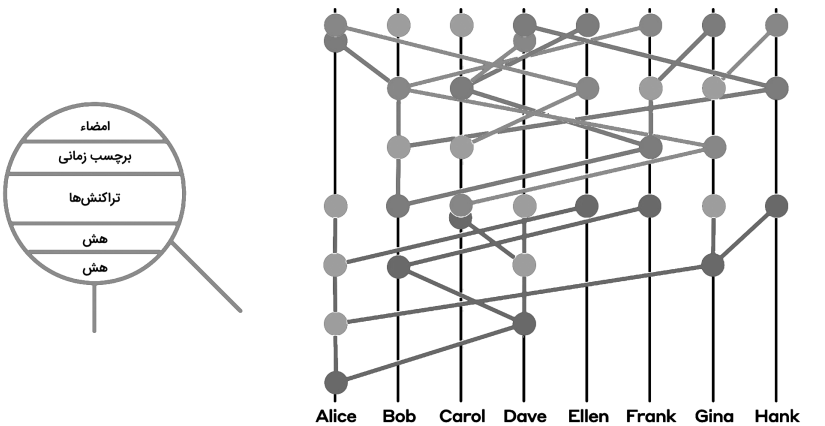
در این حالت فناوری هش‌گراف قادر است مقیاس‌پذیری بالاتر و نیاز به ذخیره‌سازی

1. Permissionless/Public blockchain
2. Ethereum
3. Transactions Per Second
4. Hybrid
5. Hyperledger
6. Hashgraph
7. Gossip techniques

پروتکل شایعه به‌منظور برقراری ارتباط بین ماشین‌های در حال سرویس‌دهی در خوشه‌های مختلف به‌کار می‌رود. با استفاده از این روش سرویس‌دهنده‌ها می‌توانند آخرین وضعیت خود را به دیگران اطلاع دهند و همچنین از آخرین وضعیت دیگر سرورها با خبر باشند.

پایین‌تری را نسبت به بلاکچین ارائه دهد. برخلاف فناوری بلاکچین، دفترکل هش‌گراف این امکان را فراهم می‌کند که چندین تراکنش به‌صورت همزمان و موازی ذخیره شوند. این تراکنش‌ها در یک برچسب زمانی با عنوان «رویداد[1]» ذخیره می‌شوند. تفاوت اصلی و عمده در پیاده‌سازی این دو فناوری دفترکل توزیع‌شده، در مکانیزم اجماع آنها خلاصه می‌شود.

در بلاکچین استخراج‌کنندگان قدرت انتخاب تراکنش را دارند اما در هش‌گراف تراکنش‌ها به ترتیب دریافت آنها تأیید می‌شوند و به‌این طریق به‌طور قابل‌توجهی مدت زمان لازم برای تأیید هر تراکنش کاهش می‌یابد. در این فناوری هنگامی که یک رویداد آغاز می‌شود، هر یک از گره‌های شبکه به‌صورت تصادفی و با استفاده از پروتکل شایعه از بین همسایگان خود، گره‌های دیگری برای انتقال اطلاعات انتخاب می‌کنند. در این حالت فقط در عرض چند دقیقه، تراکنش در سرتاسر شبکه پخش می‌شود و کل گره‌ها از آن اطلاع می‌یابند. در نهایت پیش از اضافه شدن تراکنش به دفترکل، هر گره از طریق رأی‌گیری مجازی آن را تأیید می‌کند.



شکل ۳: عملکرد اجماع هش‌گراف

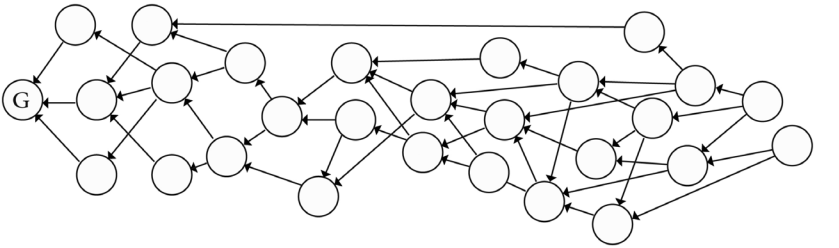
1. Event

از این رو هش‌گراف از لحاظ محاسباتی بسیار ساده‌تر و سریع‌تر عمل می‌کند. در این مکانیزم مطابق شکل۳ تمامی گره‌ها از هر تراکنشی اطلاع دارند و می‌توانند پس از تغییرات لازم، تراکنش مذکور را رها کنند. به‌این معنا که در دفترکل هش‌گراف نیازی به ذخیره‌سازی دائمی تراکنش‌ها در شبکه وجود ندارد و از همین رو نیاز به ذخیره‌سازی به‌شدت کاهش می‌یابد. فناوری هش‌گراف توسط لیمون برد[1]، هم‌بنیان‌گذار و معاون ارشد بخش فناوری سوئیرلدز[2] ابداع شده و از اوت سال ۲۰۱۸ برای استفاده در دسترس عموم قرار گرفته است. هش‌گراف مشتقات قابل‌توجهی نیز ایجاد کرد. یکی از انواع مهم آن، پلتفرم هش‌گراف هدرا[3] نام دارد. این پلتفرم امکان مقیاس‌پذیری و امنیت بسیار بالا را به ارمغان می‌آورد. در سپیدنامه هدرا ادعا شده سرعت آن بین ۲۰۰ هزار تراکنش در ثانیه تا ۵۰۰ هزار تراکنش در ثانیه است. برنامه‌هایی کاربردی روی این پلتفرم ایجاد شده که این ادعا را تأیید می‌کنند.

گراف جهت‌دار غیرمدور (DAG)

گراف جهت‌دار غیرمدور یا همان DAG، نوع دیگری از فناوری دفاترکل توزیع‌شده با قابلیت مقیاس‌پذیری بالاست. در این فناوری برای دست‌یابی به یک مکانیزم اجماع کارآمد از ساختار داده متفاوتی استفاده می‌شود. هرچه تعداد تراکنش‌های یک شبکه بیشتر شود، سرعت آن نیز افزایش خواهد یافت. در فناوری DAG تمامی گره‌ها دارای عملکرد دوگانه هستند. این گره‌ها علاوه بر تأیید یک تراکنش، قادر به نمایندگی از طرف یک تراکنش تأیید شده نیز هستند. در این فناوری هر گره می‌تواند آغازگر یک تراکنش باشد. اما برای تأیید شدن این تراکنش، هر گره باید دو تراکنش قبلی در دفترکل را نیز تأیید کند. در نتیجه طبق شکل ٤ دنباله‌ای از تراکنش‌ها به‌وجود می‌آیند که به اصطلاح یک انشعاب[4] نامیده می‌شود.

1. Leemon Baird
2. Swirlds
3. Hedera
4. Fork



شکل ٤: تصویر کلی از اجماع DAG

اولین پلتفرمی که برای استفاده در DAG منتشر شد، NXT نام داشت. این پلتفرم در نوامبر ۲۰۱۵ به‌صورت رسمی راه‌اندازی شد. علاوه بر این پلتفرم، تنگل آیوتا[1] و بایت‌بال[2] دو نمونه مهم و قابل توجه دیگر از مشتقات این مدل از فناوریِ دفترکل توزیع‌شده هستند.

به جز موارد ذکر شده، DAG مزایای دیگری نیز دارد که عبارتند از:

۱. طرح امضای یک‌بارمصرف مقاوم در برابر محاسبات کوانتومی که به‌عنوان یک محافظ در برابر تلاش کامپیوترهای کوانتومی برای شکستن شبکه عمل می‌کند.

۲. پیام احراز شده مخفی[3] که امکان ارتباط امن و رمزگذاری شده را میان گره‌ها فراهم می‌کند.

۳. مناسب برای نمایش انواع مختلف جریان‌ها مانند جریان پردازش داده. جریان پردازش داده ممکن است شامل مسیرهای متعددی باشد. گراف جهت‌دار غیرمدور می‌تواند داده‌ها را در چند مسیر پردازش کند تا خروجی‌های متفاوت به‌دست آورد. برای درک بهتر پردازش دسته‌ای[4]، فرض کنید پایگاه داده‌ای از میزان فروش جهانی دارید و گزارشی از فروش به دلار آمریکا به تفکیک مناطق لازم است. با به‌کارگیری گراف جهت‌دار غیرمدور می‌توانید همه داده‌ها را در موتور پردازش بارگذاری کنید، ارزهای مختلف را جدا سازید، ارقام مالی را به

1. IOTA Tangle
2. ByteBall
3. Masked Authenticated Messaging

یک پروتکل ارتباط داده لایه دوم است (لایه اول IOTA است) که امکان انتشار یا دسترسی به یک جریان داده رمزنگاری شده را فراهم می‌کند.

4. Batch processing

دلار آمریکا تبدیل کنید، داده‌ها را برای هر منطقه خلاصه کنید و در نهایت همه داده‌ها را با هم در گزارش نهایی بیاورید.

٤. پردازش سریع داده‌های تراکنشی که امکان پیشنهادهای در لحظه (آنی) به مشتریان را فراهم می‌کند. چرخه عمر داده شامل مراحل مختلفی مانند اصلاح داده‌های نامعتبر و غلط، تجمیع (محاسبه مجموع)، غنی‌سازی[1] (شناسایی ارتباط با داده‌های مرتبط) و انتقال (ثبت داده در فرمت جدید) است.

۵. داده‌ها را سریع‌تر و ارزان‌تر انتقال می‌دهد به همین دلیل برای تراکنش‌های خرد با ارزش پایین و مقیاس بالا مناسب است.

هولوچین

محسوس‌ترین تغییری که هولوچین در میان سایر فناوری‌های مشابه خود ایجاد کرده، حرکت از داده‌محوری[2] به سمت یک رویکرد عامل‌محوری[3] است.

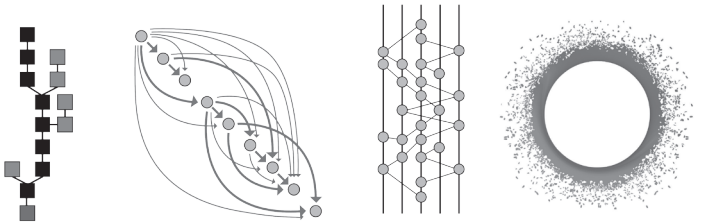
اجتناب از یک پروتکل اجماع جهان‌شمول[4] باعث شده فناوری دفترکل هولوچین مقیاس‌پذیری بالایی داشته باشد. درحالی‌که بلاکچین به دنبال غیرمتمرکزسازی تراکنش‌های موجود روی شبکه است، هولوچین قصد دارد تراکنش‌های بین دو گره مجزا را غیرمتمرکز کند. هر گره مجزا در این شبکه زنجیره مربوط به خود را اجرا می‌کند. این زنجیره در شبکه خود عملکرد مستقلی دارد و درعین‌حال بخشی از یک شبکه بزرگ‌تر متشکل از هزاران گره مشابه دیگر را شامل می‌شود. کاربران هولوچین می‌توانند داده‌ها را در مکانی با عنوان جدول هش توزیع‌شده[5] ذخیره کنند. این کار مستلزم استفاده از کلید خصوصی است. این داده‌ها به‌صورت توزیع‌یافته در سرتاسر نقاط جهان ذخیره می‌شوند.

غیرمتمرکزسازی واقعی در هر یک از سطوح شبکه باعث می‌شود هولوچین قادر به پردازش میلیون‌ها تراکنش در هر ثانیه باشد. اعتبارسنجی در سطح میکرو و انفرادی باعث می‌شود بار

1. Enrichment
2. Data-centric
3. Agent-centric
4. Global consensus
5. Distributed hash table

شبکه کاهش چشمگیری داشته باشد. با توجه به این که هر گره دارای دفترکل مخصوص به خود است، هر یک از دفترکل‌های موجود در شبکه با یک شناسه خاص به نام دی‌ان‌ای (DNA) شناخته می‌شوند. در صورتی که گره‌ها پیامی را با دی‌ان‌ای خاص یک گره دریافت کرده باشند، آن پیام را به سایر قسمت‌های شبکه نیز انتقال می‌دهند.

اما اگر پیام دریافت‌شده حاصل یک تلاش مخرب جهت افزودن اطلاعات غلط و جعلی به شبکه باشد، دی‌ان‌ای آن پیام توسط دیگر گره‌ها شناسایی نمی‌شود و تراکنش با شکست مواجه خواهد شد. در این حالت گره‌ها اطلاعات این پیام مخرب را برای سایر گره‌های دیگر در شبکه نیز ارسال می‌کنند تا از تلاش دوباره آن برای ورود به سیستم جلوگیری شود. این یک ویژگی و مزیت بزرگ برای فناوری هولوچین است تا از گزند حملات مخرب در امان باشد. درحالی‌که در فناوری بلاکچین با افزوده شدن بلوک‌های جدید بار محاسباتی شبکه افزایش می‌یابد، رویکرد متفاوت هولوچین باعث شده این روال کاملاً برعکس شود و افزوده شدن هر گره به افزایش فضای محاسباتی و در نتیجه کاهش مجموع بار شبکه منجر شود. همچنین عدم‌نیاز به وجود استخراج‌کننده‌ها در این گونه فناوری باعث شده تراکنش‌ها هیچ هزینه خاصی در بر نداشته باشند. این ویژگی هولوچین نیز موجب شده در کنار به‌صرفه بودن آن از لحاظ مصرف انرژی، هیچ گونه تجهیزات سخت‌افزاری جهت مدیریت آن مورد نیاز نباشد. گره‌های مجزا در هولوچین علاوه بر پردازش تراکنش‌ها، باعث ایجاد فضایی نامحدود جهت توسعه برنامه‌های غیرمتمرکز[1] نیز می‌شوند.



شکل ۵: مقایسه ساختار انواع فناوری‌های غیرمتمرکز

1. Decentralized applications (Dapps)

مقایسه انواع فناوری‌های دفترکل دیجیتالی مختلف حاکی از پیمودن مسیری طولانی در راه تحول این فناوری است. فناوری‌هایی چون هولوچین مفهوم غیرمتمرکزسازی را به سطح جدیدی رساندند. این امر به نوبه خود باعث ایجاد چنان پتانسیل جدیدی برای ساختارشکنی در این اکوسیستم می‌شود که پیش از این حتی تصور آن نیز ناممکن بود. با ظهور و ایجاد کاربردهای جدید برای فناوری دفترکل دیجیتالی در بخش‌ها و صنایع مختلف، این تحول سرعت بیشتری نیز به خود می‌گیرد.

دسته‌بندی‌ها	هولوچین	گراف مدور جهت‌دار	هش‌گراف	بلاکچین
استخراج	گره‌ها روی زنجیره‌های منفرد اجرا می‌شوند از این رو ماینرها مجبور نیستند که تراکنش‌ها را اعتبارسنجی کنند	تراکنش قبلی موفقیت در دستیابی به اجماع را تعیین می‌کند	گره‌ها از طریق رأی‌گیری مجازی به اجماع می‌رسند	شرکت‌کنندگان قادرند از طریق مکانیزم‌های اجماع مختلف توکن‌های جدید استخراج کنند
تراکنش‌ها در هر ثانیه	هر گره دفتر کل مخصوص به خود را پردازش می‌کند بنابراین مقیاس‌پذیری و TPS نامحدود است	ساختار داده منحصربه‌فرد از طریق گراف‌های غیرمدور جهت‌دار، مقیاس‌پذیری و TPS بالا را تضمین می‌کند	مکانیزم اجماع منحصربه‌فرد می تواند بار محاسباتی را کاهش دهد بنابراین مقیاس‌پذیری و TPS بالا ایجاد می‌کند	از نظر مقیاس‌پذیری و TPS بسیار محدود است
ساختار داده	داده‌ها روی گره‌های متعدد پلتفرم توزیع شده است بنابراین مشکل تراکم شبکه وجود ندارد	ساختار داده از مکانیزم گراف غیرمدور جهت‌دار پیروی می‌کند که درآن هر تراکنش مستقل است	رأی‌گیری مجازی و شایعه پشت شایعه تضمین می‌کند که تراکنش‌ها توسط اکثریت اعتبارسنجی شده‌اند	داده‌ها به ترتیب تراکنش‌هایی که توسط ماینرها در اکوسیستم اعتبارسنجی شده‌اند در بلوک‌ها طبقه‌بندی شده‌اند
اعتبارسنجی تراکنش‌ها	گره‌ها دفتر کل مخصوص به خود را پردازش می‌کنند از این رو نیازی به انجام این کار توسط ماینرها نیست	موفقیت تراکنش فعلی به توانایی آن در معتبر کردن دو تراکنش قبلی بستگی دارد	اعتبارسنجی تراکنش‌ها به آرای هر اجماع اتفاق میفتد	ماینرها این اختیار را دارند که تراکنشی را به تأخیر بیندازند یا به کلی کنسل کنند
زمان راه‌اندازی	محصول آلفا ۱ در می ۲۰۱۸ رونمایی شد	NXT اولین پلتفرمی است که DAG را در نوامبر ۲۰۱۵ به کار گرفت	از آگوست ۲۰۱۸ برای استفاده عموم آزاد شد	در سال ۲۰۰۸ عمومی شد
شبکه‌هایی که روی پلتفرم اجرا می‌شوند	شبکه هولوچین معروف‌ترین شبکه روی این پلتفرم است	Tangle ، NXT و ByteBall مشهورترین شبکه‌هایی هستند که از DAG استفاده می‌کنند	Swirlds و NOIA تنها شبکه‌های روی هش‌گراف هستند	بیت‌کوین و اتریوم مشهورترین شبکه‌های ساخته شده بر روی بلاکچین هستند

شکل ٦: ویژگی‌های عمومی انواع دفترکل توزیع‌شده

الگوریتم اجماع

همان‌طور که پیش از این اشاره شد، یکی از ویژگی‌های مهم بلاکچین و

انواع دیگر دفاتر کل توزیع شده، غیرمتمرکز بودن است. غیرمتمرکز بودن در دنیای کامپیوتر به زبان ساده به این معناست که هر نوع اطلاعات یا ارزشی در یک سرور مرکزی ذخیره و پردازش نمی‌شود، بلکه تمامی آنها در چندین کامپیوتر ذخیره و نگهداری می‌شوند. به سرورهایی که این اطلاعات را ذخیره می‌کنند و به نوعی سرویس‌دهنده شبکه هستند، گره یا نود[1] گفته می‌شود.

بزرگ‌ترین دلیل استفاده از انواع دفاتر کل توزیع‌شده مانند بلاکچین، بالا بردن امنیت و عدم‌دستکاری بدون وجود نهاد معتمد و مطمئن بودن از تغییرناپذیری و خرابی داده‌هاست.

اگر اطلاعات در یکی از سرورها (گره‌ها) به هر دلیلی از بین برود، چندین‌هزار و حتی میلیون‌ها سرور دیگر آن اطلاعات را در خود ذخیره کرده‌اند. اما هنگام استفاده از بلاکچین یا انواع دیگر دفاتر توزیع‌شده، یک مسئله حیاتی مطرح می‌شود. زمانی‌که قرار است اطلاعات به‌روزرسانی شوند، باید در سیستم همه گره‌ها این اتفاق بیفتد. برای حل این مسئله، از الگوریتم اجماع استفاده می‌شود.الگوریتم اجماع روشی است که از طریق آن، تمام افراد فعال در شبکه بلاکچین به یک توافق مشترک درباره وضعیت حال حاضر دفترکل توزیع شده، دست می‌یابند. به‌این ترتیب، الگوریتم‌های اجماع، اعتبار را در شبکه بلاکچین و اعتماد را بین نودها یا همتایان ناشناس در محیط محاسباتی توزیع شده، ایجاد می‌کنند. اساساً پروتکل اجماع اطمینان حاصل می‌کند هر بلوک جدید که به بلاکچین اضافه می‌شود، تنها نسخه واقعی است که توسط تمام نودها مورد توافق واقع شده است.

طبق این الگوریتم قبل از هر چیز فرض شده که برخی از گره‌ها در دسترس نباشند، که در حقیقت هم دسترسی به همه گره‌ها در یک زمان، احتمال خیلی کم و عجیبی است. الگوریتم‌های اجماع باید دارای یک «حداقل» برای تصویب یک تغییر باشند. برای مثال اگر ۵۱ درصد از گره‌های یک شبکه در الگوریتم اجماع بلاکچین به

1. Node

توافق برسند که اطلاعات را به‌روزرسانی کنند، این اتفاق خواهد افتاد.

به‌طور کلی الگوریتم‌های اجماع کاربردهای دیگری هم دارند، مانند:

- تصمیم‌گیری در مورد اینکه آیا یک تراکنش صلاحیت تأیید و ذخیره روی دفترکل توزیع‌شده را دارد یا خیر؛
- انتخاب گره‌ها برای مدیریت امور روی دفترکل توزیع‌شده؛
- تضمین یکدست‌سازی اطلاعات روی سیستم‌های سرویس‌دهنده به شبکه.

با استفاده از الگوریتم اجماع، به توافق رسیدن بین گره‌ها از طریق یک سیستم رأی‌گیری انجام خواهد شد. به این صورت که اگر یک کاربر تراکنشی (شامل هر نوع اطلاعاتی) را به شبکه ارسال کند، داده ارسالی توسط همه گره‌ها بررسی می‌شود، اگر با توجه به اطلاعات قبلی، تراکنش ارسال شده درست باشد، گره یک تأییدیه مبنی بر صحت آن به شبکه می‌فرستد. مجموعه‌ای از تراکنش‌ها یک بلوک را می‌سازند.

اگر بیش از ۵۱ درصد گره‌ها اضافه شدن این بلوک را به بلاکچین تأیید کنند، گره‌ها بلوک جدید را به سیستم خود اضافه خواهند کرد و تراکنش‌های داخل آن موفق و نهایی خواهد شد.

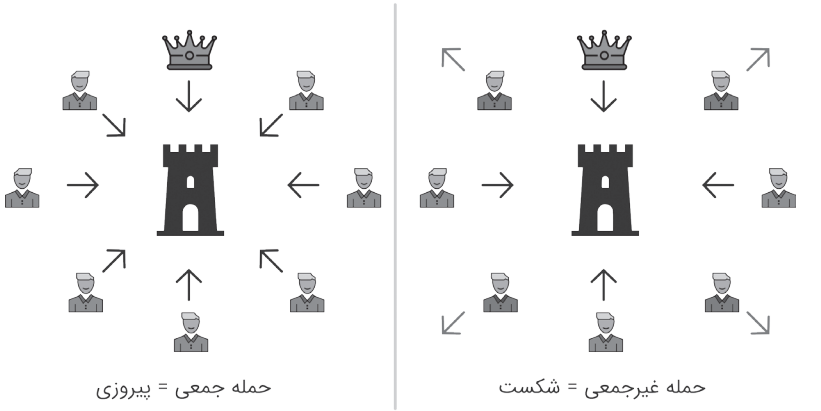
انواع الگوریتم اجماع

الگوریتم اجماع انواع مختلفی دارد اما چهار نوع پُرکاربرد آن در بلاکچین، الگوریتم تحمل خطای بیزانس[1]، الگوریتم گواه اثبات کار[2]، گواه اثبات سهام[3] و گواه اثبات سهام وکالتی[4] است. در حال حاضر اکثر ارزهای دیجیتال مانند بیت‌کوین از گواه اثبات کار استفاده می‌کنند و به دلیل اینکه این روش با بالا رفتن سختی شبکه مصرف انرژی را افزایش می‌دهد، این شبکه‌ها سعی دارند به سمت الگوریتم‌های دیگر مانند گواه اثبات سهام حرکت کنند. در ادامه به معرفی مهم‌ترین الگوریتم‌های اجماع پرداخته خواهد شد.

1. Byzantine Fault Tolerance
2. Proof-of-Work (PoW)
3. Proof-of-Stake (PoS)
4. Delegated Proof-of-Stake

الگوریتم تحمل خطای بیزانس کاربردی (PBFT[1])

ابتدا به وجه تسمیه این الگوریتم اجماع پرداخته می‌شود. هزاران سال پیش «مجموعه‌ای از ژنرال‌های بیزانس، شهری را برای حمله ناگهانی به آن محاصره کردند. اما زمان دقیق حمله، موضوع مهمی است که باید تمامی ژنرال‌ها در مورد آن به اجماع برسند. در صورتی که هماهنگی لازم در مورد زمان و نحوه حمله در میان ژنرال‌ها صورت نپذیرد، محاصره شکست خواهد خورد...»



شکل ۷: مشکل ژنرال‌های بیزانس

مشکل ژنرال‌های بیزانس[2]، معضلی کلاسیک است که نوعی از مکانیزم اجماع را برای سیستم‌های مبتنی بر رمزنگاری ارائه می‌کند. مکانیزمی محبوب تحت‌عنوان تحمل‌پذیری خطای بیزانس، که درست مانند مثال محاصره ژنرال‌های بیزانس، برای اعتبارسنجی و تأیید نهایی به عده‌ای خاص وابسته است؛ افرادی که همان ژنرال‌ها، یا در بستر دفترکل توزیع‌شده، اعتبارسنج‌ها[3] هستند.

1. Practical Byzantine Fault Tolerance
2. Byzantine Generals problem
3. Validators

اما یک مشکل بزرگ‌تر دیگر هم برای ژنرال‌های بیزانس وجود داشت: هریک از این ژنرال‌ها در بخشی از مرز دشمن ساکن می‌شدند و طبعاً در عصر بیزانس، وسیله ارتباطی الکترونیک وجود نداشت. ژنرال‌ها برای نهایی‌سازی و هماهنگی پایانی در مورد استراتژی‌های خود امکان ارتباط با یکدیگر را نداشتند. تنها راهکار ارتباطی موجود، پیام‌رسان‌هایی بودند که با صرف زمان و انرژی بسیاری، داده‌های مورد نظر را به ژنرال‌ها منتقل می‌کردند.

اکنون کافی است تصور کنید یکی از این پیام‌رسان‌ها لو می‌رفت و به دست دشمن می‌افتاد. اگر اطلاعات و نقشه‌های او را دستکاری می‌کردند چه اتفاقی می‌افتاد؟ بدیهی است اطمینان از اطلاعاتی که به این روش منتقل می‌شدند کار بسیار دشواری بود و می‌توانست کل نیروها را به کام مرگ بکشاند.

تحمل‌پذیری خطای بیزانس ویژگی شبکه توزیع‌شده برای دستیابی به اجماع است، حتی هنگامی که بعضی از نودهای شبکه نتوانند پاسخ دهند یا قادر نباشند با اطلاعات موثق پاسخ دهند. هدف مکانیزم محافظت در مقابل خطای سیستمی است و این کار را با اجرای تصمیم‌گیری جمعی محقق می‌سازد. هدف از تصمیم‌گیری جمعی، کاهش تأثیر نودهای ناکارآمد است. تحمل‌پذیری خطای بیزانس از مشکل ژنرال‌های بیزانس به‌دست آمده است.

علی‌رغم این‌که مقیاس‌پذیری و بهره‌وری ارائه شده توسط مکانیزم تحمل‌پذیری خطای بیزانس قابل‌ملاحظه است، اما این مکانیزم نیز جزو الگوریتم‌هایی است که برای شبکه‌های متمرکز و نیمه‌متمرکز طراحی و ساخته شده است.

تاکنون نسخه‌های بسیاری از این مکانیزم ارائه شده است که دو نسخه زیر رایج‌ترین آنها هستند:

۱ـ تحمل خطای بیزانس کاربردی[1]، یک الگوریتم اجماع است که در اواخر دهه ۱۹۹۰ توسط باربارا لیسکوف[2] و میگل کاسترو[3] معرفی شده است. تحمل خطای بیزانس

1. Practical Byzantine Fault Tolerance
2. Barbara Liskov
3. Miguel Castro

کاربردی برای اجرای کارآمد در سیستم‌های غیرهمزمان طراحی شده است. هدف این الگوریتم، حل کردن بسیاری از مشکلات موجود در راهکارهای تحمل خطای بیزانس است. کاربرد این الگوریتم در محاسبات توزیع‌شده و بلاکچین است و در هایپرلجرفابریک[1] نیز مورد استفاده قرار می‌گیرد. در این روش از کمتر از ۲۰ اعتبارسنج برای ارزیابی اجماع شبکه استفاده می‌شود.

۲ـ توافق بیزانسی یکپارچه[2] در شبکه‌های استلار و ریپل استفاده شده است و از هر کدام از ژنرال‌ها (گره‌ها) می‌خواهد اعتماد لازم را برای هر یک از زنجیره‌های مربوطه تأمین کنند.

از مزایای این الگوریتم می‌توان هزینه‌های پایین تراکنش، توان عملیاتی بالا، مقیاس‌پذیری شبکه و بهره‌وری بالا را نام برد. همچنین روش تحمل خطای بیزانس کاربردی می‌تواند بدون اجرای محاسبات پیچیده ریاضیاتی به اجماع توزیع شده دست یابد درنتیجه روش کم‌مصرفی است. از معایب این روش نیز می‌توان به متمرکز بودن و نیاز به کسب مجوز اشاره کرد.

الگوریتم اجماع گواه اثبات کار

پروتکل گواه اثبات کار، در حقیقت همان مکانیزم اجماع مورد استفاده در رمزارز بیت‌کوین است. اگرچه مفهوم گواه اثبات کار، قبل از ایجاد بیت‌کوین توسط ساتوشی ناکاموتو نیز وجود داشته است، اما پس از استفاده از آن در بیت‌کوین، تقریباً هرکسی حداقل یک‌بار نام این الگوریتم را شنیده است. گواه اثبات کار، الزامی برای حل یک محاسبه زمان‌بر و گران‌قیمت کامپیوتری یا همان استخراج است که برای ایجاد گروهی از تراکنش‌های جدید در بلاکچین صورت می‌گیرد.

در خلال این استخراج کردن، علاوه بر تأیید مشروعیت تراکنش‌ها و ایجاد رمزارز جدید، به اولین کاربر یابنده عدد تصادفی نانس[3] حل‌کننده مسئله نیز پاداشی تعلق

1. Hyperledger Fabric
2. Federated Byzantine Agreement
3. Nonce

می‌گیرد که می‌تواند کاربران بسیاری را تحت‌عنوان استخراج‌کننده به سمت بلاکچین جذب کند. در واقع این روش یک مکانیزم اجماع مبتنی بر قدرت محاسباتی کامپیوتر است که به نامتمرکز بودن قدرت در سیستم کمک می‌کند.

این روش عمدتاً برای محافظت در برابر خطاهای بیزانسی (به‌طور عمده در برابر خطای دو بار خرج کردن[1] توسط گره‌های مخرب) استفاده می‌شود؛ چراکه در این روش گره‌ای که به‌صورت مخرب عمل کند، فرصت کمی برای تحمیل بلوک مخرب در شبکه دارد؛ مگر اینکه حمله‌کننده بیش از ۵۰ درصد از منابع محاسباتی شبکه را تأمین کند (حمله ۵۱ درصد). بنابراین، الگوریتم اجماع گواه اثبات کار یک روش غیرقابل‌نفوذ ارائه می‌دهد، مگر اینکه مهاجم بتواند بیش از ۵۰ درصد منابع را جمع‌آوری کند.

فرایندهایی که در این مکانیزم صورت می‌گیرند به شرح زیر هستند:

- ورود تراکنش به دفترکل توزیع‌شده؛
- تأیید مشروعیت تراکنش توسط استخراج‌کنندگان؛
- حل مسئله ریاضی گواه اثبات کار توسط استخراج‌کنندگان؛
- اهدای جایزه به اولین استخراج‌کننده‌ای که عدد تصادفی مسئله را پیدا کرده است؛
- تأیید نهایی تراکنش و ثبت در بلاکچین عمومی توسط همه نودها.

گاهی‌اوقات، ممکن است بیش از یک گره راه‌حل را در یک زمان پیدا کند. وقتی این اتفاق می‌افتد، هر یک از این گره‌ها یک بلوک را پیشنهاد و به شبکه ارسال می‌کنند. این بلوک‌ها توسط بلوک‌های مجاور برداشت می‌شود و یک بلاکچین به‌صورت موقت شکل می‌گیرد و بلوک‌ها به زنجیره آنها اضافه می‌شود. در نهایت پروتکل شاخه‌ای را که طولانی‌تر از بقیه می‌شود به‌عنوان زنجیره رسمی انتخاب می‌کند و بقیه را از بین می‌برد. مهم‌ترین نقطه قوت این روش این است که برای مثال در بیت‌کوین گره‌ای که برای ایجاد یک بلوک جدید انتخاب شده است، بابت ثبت تراکنش‌ها، پاداش خود

1. Double spending

به‌صورت بیت‌کوین را دریافت می‌کند. به‌دلیل اینکه انجام محاسبات و استخراج پول کار بسیار پرتلاش و پرهزینه‌ای است، استخراج‌کنندگان تنها بر روی شاخه‌ای از بلاکچین تمرکز می‌کنند که به نظر می‌رسد زنجیره اصلی (یعنی بلاکچین با اکثریت بلوک‌ها) باشد.

در کنار مزایای این روش، چندین ضعف در الگوریتم اجماع گواه اثبات کار وجود دارد که مهم‌ترین آنها هزینه‌های انرژی قابل توجهی است که برای استخراج مصرف می‌شود و البته می‌توان به موارد زیر نیز اشاره کرد:

- **استخراج متمرکز**[1]: به‌دلیل اینکه اختلافات زیادی در قدرت CPU کامپیوترها وجود دارد، کاربرانی که پردازنده‌های کم‌قدرت دارند اغلب میدان را به ماشین‌های قدرتمند می‌بازند. بنابراین، گواه اثبات کار نمی‌تواند الزامات الگوریتم اجماع مبنی بر اینکه گره‌های تصادفی باید در میان وسیع‌ترین جمعیت ممکن از شرکت‌کنندگان انتخاب شوند را برآورده سازد. این ضعف خطر استخراج متمرکز را افزایش می‌دهد.
- **تأخیر زمانی زیاد**: بلوک‌های جدید تقریباً هر ۱۰ دقیقه تولید می‌شوند. در نتیجه انتظار برای تأیید نهایی تراکنش‌های یک بلوک تولید شده حدود ۳۰ دقیقه طول می‌کشد؛ چراکه باید از قرار گرفتن بلوک در شاخه اصلی اطمینان حاصل کرد.
- **نرخ پایین تراکنش**: حداکثر اندازه بلوک تأیید شده تحت الگوریتم اجماع در شبکه بیت‌کوین، هفت تراکنش در ثانیه[2] است که به نسبت تعداد کمی است.

الگوریتم اجماع گواه اثبات سهام

گواه اثبات سهام دومین الگوریتم اجماع معروف در بلاکچین است. در گواه اثبات سهام، بلوک‌های جدید به جای استخراج، «ساخته» می‌شوند. تحت شرایط گواه اثبات

1. Centralized mining
وقتی تعداد محدودی از شرکت‌ها تقریباً کنترل کامل را در قدرت هش‌کردن به دست می‌گیرند، فرایند استخراج متمرکزتر می‌شود.
2. TPS: Transaction per Second

سهام، گره انتخاب شـــده برای ایجاد بلوک بعدی، از طریق یک فرایند شبه‌تصادفی انتخاب می‌شود که این انتخاب به دارایی ذخیره شده در کیف پول (یا استخر سهام) مربوط به آن گره بســـتگی دارد. در این حالت، هیچ گره‌ای نمی‌تواند نوبت خود را پیش‌بینی کند. شمار مشخصی از کوین‌ها در استخر سهام نگهداری می‌شود تا شانس ایجاد بلوک را خریداری کنند.

خلاف گواه اثبات کار که در آن به اســـتخراج‌کنندگان برای حل معمای ریاضی با هدف تأیید تراکنش‌ها و ایجاد بلوک جدید جایزه داده می‌شود، در گواه اثبات سهام این خالق بلوک جدید اســـت که بسته به میزان ســـرمایه‌اش عایدی کسب می‌کند. قابل‌ذکر است که در الگوریتم اجماع گواه اثبات سهام برای نقش اعتبارسنج به‌عنوان تأییدکننده تراکنش‌ها از کلمه فورجر[1] به‌جای استخراج‌کننده استفاده می‌شود. در این مکانیزم، خلاف گواه اثبات کار، گره ایجادکننده بلوک بعدی به شکل کامل تصادفی نیست و کاربران (یا گره‌ها) می‌توانند با انجام برخی کارها و کسب برخی امتیازها، شانس خود را برای پیروزی در این رقابت افزایش دهند.

در حقیقت، در مکانیزم اجماع گواه اثبات سهام، هرچه میزان سهام یا پول کاربران در شبکه بیشتر باشد، شانس انتخاب شـــدن آنها برای یافتن پاسخ معمای شبکه نیز بیشتر است.

گواه اثبات سهام دارای مزایایی نســـبت به گواه اثبات کار است. گواه اثبات سهام قدرت محاسباتی زیادی مصرف نمی‌کند و با ممانعت از ایجاد استخرهای استخراج متمرکز[2]، خطر حملات مخرب را کاهش می‌دهد.

یکی از نقاط ضعف گواه اثبات سهام، در خطر نبودن منبع[3] است. به‌این معنا که یک اعتبارسنج در زمان ایجاد فورک انگیزه دارد با هر دو شاخه همراهی کند چراکه برای او هزینه‌ای ندارد و منطق حکم می‌کند با همه شاخه‌ها همراه باشد تا از بودن در شاخه اصلی و اخذ کارمزد یقین حاصل کند. این مسئله می‌تواند مانع شکل‌گیری اجماع بین

1. Forgers
2. Centralized mining pools
3. Nothing at stake

گره‌ها شود و خطر دو بار خرج‌کردن را افزایش دهد[۱].

گواه اثبات سهام چندین زیرگروه نیز دارد. گواه اثبات سهام وکالتی مشهورترین آنهاست که در ادامه مفصلاً بررسی‌اش می‌کنم. به غیر از آن می‌توان به گواه اثبات سهام تصادفی[۲]، گواه اثبات سهام استیجاری[۳] که پلتفرم Waves از آن استفاده می‌کند و گواه اثبات سهام هیبریدی[۴] که شبکه BTCA آن را به‌کار می‌برد، اشاره کرد.

الگوریتم اجماع گواه اثبات سهام وکالتی

گواه اثبات سهام وکالتی یا اعطایی، مدل تغییریافته و پیچیده‌تری از گواه اثبات سهام است که در آن، اعتبارسنجی تراکنش‌ها به گره خاص متکی است تا به نمایندگی از سوی کل گره‌های موجود در شبکه، بلوک‌ها را ارزیابی کنند.

تعداد این نمایندگان منتخب معمولاً بین ۲۱ الی ۱۰۰ گره است که سازمان‌دهی و کنترل شبکه را تسهیل می‌کنند و توزیع شرایط در خلال شبکه را ممکن می‌سازند.

این دقیقاً همان چیزی است که در مورد نمایندگان مجلس کشورها نیز جریان دارد. عده‌ای به‌عنوان نماینده انتخاب می‌شوند و در مورد صحت و تأثیرگذاری برخی از شرایط و قوانین تصمیم‌گیری می‌کنند، ضمن این‌که کنترل بخش‌های مهمی از شبکه در اختیار آنهاست. روندی دموکراتیک که می‌تواند علاوه بر ارتقای بهره‌وری در انرژی، هزینه‌ها و خطاهای سیستم را نیز بکاهد؛ هرچند این امر، قدرت را در حلقه‌ای از افراد خاص متمرکز می‌کند.

گواه اثبات سهام وکالتی یک الگوریتم اجماع است که برای ایمن‌سازی بلاکچین، توسعه یافته است. این الگوریتم به‌عنوان نسخه‌ای از دموکراسی مبتنی بر فناوری طراحی شده است و از فرایند رأی‌گیری و انتخاب برای محافظت از بلاکچین در مقابل متمرکزسازی و کاربردهای مخرب استفاده می‌کند.

---

۱. مباحث مربوط به الگوریتم‌های اجماع بسیار گسترده و فنی هستند که در متن حاضر سعی شده است صرفاً به کلیات آن اشاره شود تا علاقه‌مندان با موضوع آشنا شوند و در صورت تمایل به منابع تفصیلی در این زمینه مراجعه کنند.

2. Random Proof of Stake (RPoS)
3. Leased Proof of Stake (LPoS)
4. Hybrid Proof of Stake (HPoS)

گواه اثبات سهام وکالتی توسط دنیل لاریمر[1]، مؤسس بیت‌شیرز[2] و استیمیت[3] توسعه یافته است. لاریمر گواه اثبات سهام وکالتی را به‌عنوان جایگزینی برای اجماع گواه اثبات کار و گواه اثبات سهام طراحی کرده است که مصرف انرژی بسیار زیاد و محافظت ضعیفی در برابر اهداف مخرب دارند.

اولین پیاده‌سازی و نسخه گواه اثبات سهام وکالتی در بیت‌شیرز اجرا شد. علاوه بر این، گواه اثبات سهام وکالتی طوری برنامه‌ریزی شده است تا جایگزین مقیاس‌پذیرتری نسبت به الگوریتم‌های اجماع سنتی باشد. نمونه‌های معروف از ارزهای دیجیتال که از گواه اثبات سهام وکالتی استفاده می‌کنند شامل لیسک، استیم، ویکی‌چین، بیت‌شیرز و ای‌اواس[4] هستند.

این روش از مزایای زیر برخوردار است:

- کوین‌های گواه اثبات سهام وکالتی بسیار مقیاس‌پذیرتر از ارزهای دیجیتال مبتنی بر گواه اثبات کار هستند؛ زیرا این کوین‌ها به توان محاسباتی زیادی نیاز ندارند و معمولاً برای کاربرانی با تجهیزات ضعیف در دسترس هستند.
- بلاکچین‌های گواه اثبات سهام وکالتی سریع‌تر از بلاکچین‌های مبتنی بر گواه اثبات کار و گواه اثبات سهام هستند.
- کوین‌های گواه اثبات سهام وکالتی دموکراتیک‌تر و جامع‌تر از رقبای خود هستند؛ این الگوریتم در مقایسه با گواه اثبات سهام، قدرت نظارتی بیشتری به کاربران با سهم کمتر در استیکینگ[5] ارائه می‌دهد و در مقایسه با گواه اثبات کار به توان محاسباتی زیادی نیاز ندارد. بنابراین از لحاظ مالی به کاربر فشار نمی‌آورد.
- از آنجایی که الزامات ورود به گواه اثبات سهام وکالتی بسیار کم است، این

1. Daniel Larimer
2. BitShares
3. Steemit
4. Lisk, Steem, Bitshares, EOS
5. Staking

استیکینگ شامل نگهداری دارایی‌ها در کیف پول ارز رمزنگاری شده برای پشتیبانی از امنیت و عملکرد شبکه بلاکچین است. به زبان ساده،استیکینگ قفل کردن ارزهای دیجیتال برای دریافت پاداش است.

مکانیزم عمدتاً به‌عنوان غیرمتمرکزترین رویکرد به مکانیزم‌های اجماع در نظر گرفته می‌شود.

- گواه اثبات سهام وکالتی دوستدار محیط زیست و کم‌مصرف است.
- شبکه‌های گواه اثبات سهام وکالتی محافظت قوی در مقابل حمله دو بار خرج کردن ارائه می‌دهند.

در مقابل معایب آن به شرح زیر است:

- حضور موفقیت‌آمیز شبکه به مشارکت و همکاری جامعه علاقمند نیاز دارد تا شاهدان با رأی‌گیری بتوانند نظارت کارآمدی داشته باشند.
- سیستم‌های گواه اثبات سهام وکالتی نسبت به متمرکزسازی آسیب‌پذیر هستند؛ زیرا تعداد شاهدان بسیار محدود است و در واقع می‌توان آن را روشی نیمه‌متمرکز دانست.
- بلاکچین گواه اثبات سهام وکالتی در معرض نواقص و معایب رأی‌گیری‌های واقعی است. برای مثال، کاربران گواه اثبات سهام وکالتی با سهم کم در استیکینگ به این نتیجه می‌رسند که رأی آنها در مقایسه با رأی سهامداران بزرگ، کم‌اهمیت است.
- در انتها باید گفت در این بخش به مهم‌ترین الگوریتم‌های اجماع اشاره شد؛ اما واقعیت این است که روزانه و به سرعت بر انواع الگوریتم‌های اجماع افزوده می‌شود که توضیح آن از اهداف این کتاب نیست.

در شکل شماره ۸ عناوین کلی انواع الگوریتم‌های موجود تا به امروز آورده شده است. برای فهم و مقایسه بهتر انواع الگوریتم‌های اجماع می‌توان به شکل ۸ مراجعه کرد تا به درک بهتری از تناسب کاربری هر یک از آنان در کسب‌وکارهای مختلف رسید.

شکل ۸: انواع مختلف الگوریتم‌های اجماع

منابع:

[1] https://en.wikipedia.org
[2] https://hackernoon.com
[3] The futute is decentralized – the united nation development programme
[4] https://www.kuknos.org
[5] https://101blockchains.com
[6] https://way2pay.ir
[7] https://mihanblockchain.com
[8] https://hazelcast.com
[9] https://ico.li
[10] https://blocktelegraph.io/blockchain-before-bitcoin-history/
[11] https://ercwl.medium.com/hedera-hashgraph-time-for-some-fud-9e6653c11525

فصل دوم

مفهوم توکن و انواع آن

مقدمه

پس از آشنایی با مفهوم دفاترکل توزیع‌شده و انواع آن در بخش اول کتاب، در این فصل به انواع محصولاتی که در بستر این فناوری توسعه داده می‌شوند می‌پردازم. «توکن» واژه عامی است که برای تمامی محصولات بلاکچینی به‌کارمی‌رود و با خود مفاهیم امنیت و رمزنگاری را به همراه دارد. شاید این واژه یادآور توکن‌های امنیتی حساب‌های بانکی باشد؛ اما در دنیای بلاکچین، «توکن» مصادیق گسترده و متعددی دارد که با بهره‌گیری از کاربردهای آن می‌توان به دنیای اقتصاد غیرمتمرکز دست‌یافت. در ادامه، تعریف و ویژگی‌های توکن، انواع آن و کاربری‌هایش در اقتصاد حقیقی به‌صورت تفصیلی تبیین و مثال‌های موفق جهانی مرور خواهند شد.

توکن چیست؟

اصولاً توکن جایگزینی برای موجودیت دیگری است، که در هر دو حوزه «امنیت» رایانه و «رمزارزها» کاربرد دارد. در واقع توکن رشته‌ای از اعداد و حروف است که در رمزنگاری استفاده می‌شود. در امنیت رایانه این نوع توکن ممکن است چیزی شبیه به کد زیر باشد:

947153d332beaf39dec6ebae8883bfb84eda47abccccbc2d61436d8d1e81584d

در حالت فوق ماهیت رشته تولید شده فاقد هرگونه ارزشی است و فقط برای ایجاد امنیت در پرداخت یا عملیات دیگر استفاده می‌شود. چنانچه این رشته رمزنگاری‌شده جایگزین موجودیتی شود که دارای ارزش است؛ مانند پول یا دارایی دیجیتال، آنگاه اصطلاح توکن ارزشی[1] به‌کار می‌رود. توکن بیت‌کوین تلاشی برای جانشینی ارزش است درست مانند پول. به‌صورت خلاصه می‌توان گفت توکن همان مفهوم اوراق بهادار است که در بستر فناوری بلاکچین پیاده‌سازی شده و از ویژگی‌های این فناوری

1. Value token

برخوردار است.

توکن گاهی به‌عنوان مترادفی برای رمزارز استفاده می‌شود. البته غالباً این دو عبارت ترکیب‌شـــده و اصطلاح توکن رمزارز به‌کارمی‌رود. به‌عنوان‌مثال، واحد محاسبه در بلاکچین بیت‌کوین، توکن بیت‌کوین است و واحد محاسبه در بلاکچین اتریوم، توکن اتریوم است.

در رمزارزها یک توکن یا توکن رمزارز، داده توکنایزشـــده مرتبط با تراکنش‌هایی اســـت که از طریق اینترنت ارســـال و بدون بـــه خطر انداختن داده‌های حســـاس ذخیره می‌شود.

مفهوم توکنایز کردن[1]

توکنایز کردن در عمل برای ده‌ها ســـال به‌عنوان راهی جهت جداسازی داده‌ها در اکوسیستم‌هایی مانند بانک‌های اطلاعاتی بوده اســـت. در این سال‌ها رمزنگاری با کلیدهای رمزنگاری روش برتری برای محافظت از داده‌های حســـاس محســـوب می‌شده اســـت. رمزنگاری یعنی تبدیل داده‌ها به شـــکلی که توسط کسانی که کلید رمزگشایی را در اختیار ندارند، غیرقابل‌خواندن باشـــد. هدف آن اطمینان از حفظ حریم خصوصی با مخفی کردن اطلاعات از دیگران است. رمزنگاری موارد استفاده مختلفی دارد، از پنهان کردن پیام‌های خصوصی در برنامه‌های همتابه‌همتا گرفته تا انتقال اطلاعات حساس در یک محیط آسیب‌پذیر.

بنابراین به فرایند محافظت از داده‌های حساس به‌وسیله جایگزین کردن آنها با یک عدد که به‌صورت الگوریتمی تولید شده است، توکنایز کردن می‌گویند. اغلب اوقات از توکنایز کردن برای جلوگیری از کلاهبرداری در کارت اعتباری استفاده می‌شود. توکن‌های کارت اعتباری برای محافظت از داده‌های حساس مشتریان (مانند شماره کارت اعتباری، آدرس، شماره‌حساب و غیره) با جایگزین کردن آن با یک سری اعداد و حروف ایجاد شده است که توسط الگوریتم‌های ریاضی تولید می‌شوند. توکن‌ها

1. Tokenization

خارج از سیستمی که در آن تعریف شده‌اند هیچ معنا و ارزشی ندارند.

اما در زیســـت‌بوم بلاکچین توکنایز کردن به معنای خرد کردن دارایی‌هاســـت. هرچند در روش سنتی نیز می‌توان دارایی‌های با مقیاس بزرگ مانند ملک یا خودرو را به اوراق بهادار تبدیل کرد و به افراد این امکان را داد که با ســـرمایه کمتر در برخی دارایی‌ها و پروژه‌های عمرانی ســـرمایه‌گذاری کنند؛ اما در این روش بستر مناسب فناوری وجود ندارد که در آن معاملات شفاف باشد و قیمت‌گذاری به درستی انجام شود. در بســـتر بلاکچین می‌توان هر دارایی را که در مقیاس بزرگ تولید می‌شود یا حجم معاملات بالایی دارد، به اجزای کوچک‌تری (توکن) تقسیم کرد و توکن‌ها که امکان دسترسی به آنها آسان‌تر است، مورد معامله قرار گیرند. در این بستر هر توکن در واقع گواهی الکترونیک متناظر با بخشی از یک دارایی مشخص است.

دسته‌بندی توکن‌ها

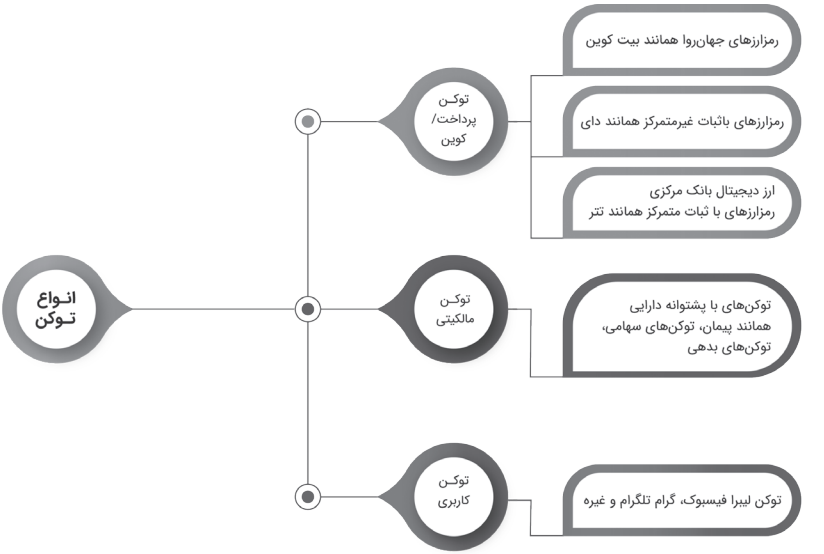
رویکردهای مختلفی برای دســـته‌بندی توکن‌ها وجود دارد که در ادامه براساس دسته‌بندی کاربردمحور این تفکیک انجام می‌شود.

این رویکرد بر مبنای گزارش پژوهشکده پولی و بانکی ایران و براساس مستندات نهاد نظارت بر بازارهای مالی انگلستان[1] و نهاد نظارت بر بازارهای مالی سوئیس[2] ارائه شده است. نهاد نظارتی آلمان[3] نیز بر برخی از جنبه‌های این موضوع تأکید کرده است. این تقسیم‌بندی به‌صورت شکل ۱ است:

براساس دسته‌بندی اشاره شـــده، توکن‌ها را می‌توان به سه دسته: پرداخت، بهادار و کاربری تقســـیم کرد که در ادامه به صورت تفصیلی توضیح داده می‌شوند. لازم به ذکر است که یکی از اشتباهات مصطلح در ادبیات عرفی این حوزه به مفاهیم توکن و رمزارز برمی‌گردد. باید توجه داشت که توکن، نماینده یک دارایی تأیید شده و دارای ارزش مانند ارز، حواله، آیتم‌های بازی‌های کامپیوتری و غیره است. براساس تعریف

1. UK Financial Conduct Authority, FCA
2. Swiss Financial Market Supervisory Authority, FINMA
3. German Federal Financial Services Supervisory Authority, BaFin

نهاد نظارت بر بازارهای مالی انگلستان، توکن موجودیتی رمزی است که یک ارزش واقعی یا مجازی را در بستر پلتفرم بلاکچین نمایندگی می‌کند. در واقع، می‌توان گفت معمولاً رمزارزها توکن هستند، ولی توکن‌ها لزوماً رمزارز نیستند.



شکل ۱: طبقه‌بندی توکن‌ها

۱. توکن پرداخت[1] (رمزارز، کوین)

همان‌طور که پیش‌تر اشـــاره شـــد، مفهوم توکن به‌طور کلی یک جایگزین برای موجودیت دیگر است. چنانچه آن موجودیت وسیله‌ای جهت انتقال پول در نظر گرفته شود، به آن توکن پرداخت می‌گویند.

یک توکن پول رایج (توکـــن ارزش یا توکن پول)[2] نماینـــده مقداری از یک پول است؛ چه یک دلار در شکل کاغذی یا دیجیتالی که نماینده یک دلار است و چه یک

1. Payment token
2. Currency tokens/value tokens/ money token

بیت‌کوین که نماینده یک واحد ارزش بیت‌کوین است. البته در خصوص بیت‌کوین تقریباً همه اقتصاددانان معتقدند در حال حاضر کارکرد پول را ندارد و به‌دلیل محدودیت‌هایی که دارد در آینده نیز امکان تبدیل شدن به ابزار پرداخت را نخواهد داشت؛ از جمله این محدودیت‌ها می‌توان به سرعت پایین تراکنش‌های قطعی‌شده (حداقل ۳۰ دقیقه) و کارمزد بالا اشاره کرد. اما توکن‌هایی همچون لایت‌کوین، تتر، دای، ریپل و غیره این امکان را دارند که روزی بتوانند به ابزاری برای پرداخت تبدیل شوند. اگر در زمان فعلی رمزارزی مثل بیت‌کوین جزو توکن پرداخت نام برده می‌شود، صرفاً یک عبارت عامیانه و غلط مصطلح است و ریشه علمی ندارد.

رمزارزها نوعی توکن ارزش هستند. آنها می‌توانند جای پول استفاده شوند ولی خودشان ذاتاً ارزشی ندارند. به عبارتی از توکن‌ها برای نشان دادن دارایی‌های دیجیتال که قابل تعویض و معامله هستند استفاده می‌شود.

بنابراین توکن‌های پرداخت همان رمزارزهایی هستند که نقش ابزار پرداخت یا پول را پیدا می‌کنند. این توکن ممکن است توسط هیچ نهاد متمرکزی منتشر نشود (مانند DAI) و ممکن است توسط بانک مرکزی منتشر شود. این توکن به‌عنوان وسیله مبادله، وسیله سنجش و ذخیره ارزش استفاده می‌شود که با توجه به نوع دسترسی به دفترکل توزیع‌شده می‌توان آن را در دو قالب طبقه‌بندی کرد:

الف) توکن پرداخت در بستر دفترکل توزیع شده عام: می‌توان گفت این نوع توکن همان رمزارزهای جهان‌روا همچون لایت‌کوین است که با استفاده از فناوری رمزنگاری شده طراحی شده و فراتر از مرزهای جغرافیایی در یک شبکه همتابه‌همتا و به‌صورت غیرمتمرکز فعالیت می‌کند.

ب) توکن پرداخت در بستر دفترکل توزیع‌شده خاص: ارز دیجیتال بانک مرکزی را می‌توان در این طبقه دسته‌بندی کرد. تفاوت اصلی این دسته با مورد قبلی نوع دسترسی دفترکل توزیع‌شده آن است. در واقع، مجوز دسترسی در این حالت تنها در اختیار افراد خاص قرار دارد. نمونه‌ای از این تلاش ها، پروژه جاسپر[1] کاناداست.

1. Jasper

پروژه جاسپر بانک مرکزی کانادا در حال مطالعه روی نوعی ارز دیجیتال بانک مرکزی[1] است که تناظر یک به یک با دلار کانادا دارد و در شـــبکه با دسترسی خاص آن، بانک مرکزی کانادا و تعدادی از بانک‌های تجاری این کشور حضور دارند. کدکوین برای تسویه بین بانکی و موازی با سامانه تسویه ناخالص آنی[2] عمل می‌کند (در فصول بعد درباره رمزارز بانک مرکزی توضیحات مفصل‌تری ارائه می‌کنم).

تاریخچه رمزارزها

در ســـال ۱۹۸۳، دیوید چاوم[3] نوعی پول دیجیتالی رمزنگاری شده اختراع کرد که ای‌کَش[4] نام داشت. دیوید چاوم بعدها، در ســـال ۱۹۹۵، پول دیجیتالی دیگری به نام دیجی‌کَش[5] ابداع کرد که روش رمزنـــگاری آن به‌گونه‌ای بود که نه بانک، نه دولت و نه هیچ شخص ثالثی قادر به رهگیری تراکنش‌های مالی آن نبودند. در سال ۱۹۹۶ و در موسسه فنی ماساچوست[6] مطالبی منتشر شد که در آن یک نظام رمزارز به تفصیل شرح داده شده بود. این سلسله مطالب در همان سال توسط آژانس امنیت ملی آمریکا در قالب یک گزارش با عنوان «چگونه یک ضرابخانه بســـازیم: رمزنگاری پول‌های الکترونیکی گمنام»[7] منتشـــر شـــد. تا حدود ســـال ۲۰۰۹ تمام رمزارزهای موجود به‌صورت متمرکز بودند و اولین رمزارز یا کوین که به‌صورت غیرمتمرکز کار می‌کرد، در سال ۲۰۰۹ به‌وجود آمد که همان بیت‌کوین اســـت. در بلوک پیدایش بیت‌کوین، ساتوشی پیامی نوشت که برای همیشه در تاریخ ثبت شده‌است. در پارامتر کوین‌بیس[8]، همراه با داده‌های معمول بلوک، پیام زیر که یکی از ســـرتیترهای نشریه تایمز است درج شد:

نشـــریه تایمز روز ۳ژانویه ۲۰۰۹: رئیس خزانه [ســـلطنتی انگلستان] در آستانه

1. Central Bank Digital Currency (CBDC)
2. Real-Time Gross Settlement (RTGS)
3. David Chaum
4. Electronic Cash
5. Digi Cash
6. Massachusetts Institute of Technology
7. How to Make A Mint: The Cryptography of Anonymous Electronic Cash
8. Coinbase

دومین کمک مالی به بانک‌ها. این پیام احتمالاً به‌عنوان یک برچسب زمانی[1] درج شده بود تا ثابت کند که بلوک پیش از سوم ژانویه ایجاد نشـــده بود. با این حال، سرتیتر انتخاب‌شده با علت و هدف اولیه از خلق بیت‌کوین نیز ارتباط محکمی دارد که طراح آن قصد دارد بیت‌کوین را جایگزین سیستم پولی و مالی فعلی در جهان کند.

توسعه‌دهندگان بیت‌کوین مبانی فلسفی شکل‌گیری این رمزارز را به مکتب اقتصاد اتریشی[2] و فلسفه آزادی‌خواهی[3] نسبت می‌دهند. مکتب اقتصاد اتریشی توسط افرادی مثل «کارل منگر»[4] و «لودویگ فن میزس»[5] پایه‌گذاری شد. به‌طور کلی اقتصاددانان پیرو این مکتب مخالف حضور بانک‌های مرکزی و مؤسسات دولتی در کنترل اقتصاد هســـتند. آنها همچنین معتقدند که منشـــأ تمام کنش‌های اقتصادی فرد (و نه جمع) است. از همین رو سنجه‌های اقتصادی نمی‌توانند روی تصمیم‌گیری شخصی افراد اثر بگذارند.

یکی دیگر از اصول اقتصاد اتریشی بحث نهایی‌گرایی[6] است که سعی می‌کند تفاوت در ارزش کالا و خدمات را با استفاده از میزان مطلوبیت نهایی آنها توضیح دهد. بر پایه این اصل و اصول قبلی پیروان مکتب اقتصاد اتریشی عامل زمان را در تصمیم‌گیری و انتخاب‌های اقتصادی افراد مؤثر می‌دانند.

فلسفه آزادی‌خواهی یا اختیارگرایی حول این باور شکل گرفته است که آزادی عمل باید در تمام شئونات زندگی به افراد داده شود. امروزه اندیشه‌های آزادی‌خواهانه با ایدئولوژی‌های سیاسی آمیخته شده و شاخه‌های مختلفی از آن شکل گرفته است.

مکاتب مذکور سیســـتم‌های غیرمتمرکز را ترویج می‌کنند و بیت‌کوین نمونه یک سیستم مالی غیرمتمرکز است که در آن نیازی به نقش‌آفرینی دولت‌ها و بانک‌ها نیست. به‌علاوه هم اقتصاد اتریشی و هم فلسفه آزادی‌فردی تأکید می‌کنند که بیت‌کوین هم می‌تواند یک آزادی مالی بی‌سابقه برای افراد به ارمغان آورد.

---

1. Timestamp
2. Austrian School of Thought
3. Libertarianism
4. Carl Menger
5. Ludwig Von Mises
6. Marginalism

انواع رمزارزها و کاربردهای آنها

رمزارزها از زمان بیت‌کوین تاکنون مسیری طولانی طی کرده‌اند. به‌عنوان یک سیستم پرداخت همتابه‌همتا شروع به کار و مجموعه‌ای از موارد کاربری را ایجاد کرده‌اند که بسیار فراتر از نقش اولیه رمزارز یعنی انتقال پول است. درحالی‌که عملکرد اصلی رمزارزها مانند اتریوم و بیت‌کوین بحث‌برانگیز است، بی‌شک رمزارزها اکنون می‌توانند برای اموری بیش از پرداخت هزینه کالا و خدمات استفاده شوند. اکوسیستم رمزارزها شامل راهکارهای منحصربه‌فردی در صنعت مالی است که میزان گستردگی این انقلاب فناوری مالی[1] را نشان می‌دهد.

رمزارزها همچنان در حال اثبات قابلیت‌های کاربردی خود هستند. در سال‌های آتی، رمزارزها در حال انجام کارهایی هستند که هنوز پیش‌بینی‌نشده است، چه برسد به اینکه طراحی شده باشند. در ادامه به برخی از کاربردهای رمزارزها اشاره می‌شود.

- **پرداخت‌ها:** با افزایش هزینه‌های شبکه، معامله‌گران بسیاری مجبور شدند حمایت خود از بیت‌کوین را متوقف کنند. شرایط نامناسب بیت‌کوین برای پرداخت‌های با هزینه پایین در اواسط سال ۲۰۱۷ باعث شد بیت‌کوین‌کش[2] به‌عنوان یک انشعاب از بیت‌کوین آغاز به کار کند. شبکه بیت‌کوین‌کش از آن زمان آرمان خود را برای تسهیل پرداخت سریع و کم‌هزینه، با کمک صدها کسب‌وکار که بیت‌کوین‌کش را در فروشگاه و به‌صورت آنلاین پذیرش می‌کردند، حفظ کرده است.
- **ذخیره ارزش:** ارزها و شبکه‌هایی که به‌عنوان شکل جدید ارز بومی کمیاب و همچنین وسیله تسویه‌حساب استفاده می‌شوند؛ مانند بیت‌کوین و لایت‌کوین.
- **پول برنامه‌پذیر**[3]: قراردادهای هوشمند[4] در واقع قدیمی‌تر از بیت‌کوین هستند. قرارداد هوشمند به زبان ساده کد اجرایی مبتنی بر بلاکچین است که در صورت

1. Fintech: Financial Technology
2. Bitcoin Cash
3. Programmable money
4. Smart contracts

برآورده شدن شرایطی خاص، خروجی مشخصی می‌دهد.

آراس‌کی[1] بستر قراردادی هوشمندی را ابداع کرده که بر روی امنیت بلاکچین بیت‌کوین و تأثیرات شبکه آن سرمایه‌گذاری کرده است. با افزایش تسلط بیت‌کوین[2] بر رمزارزهای دیگر یا همان آلت‌کوین‌ها، جذابیت ساخت رمزارز بر بستر بیت‌کوین در مقابل گزینه‌های کمتر غیرمتمرکز مانند ترون[3] نیز افزایش یافته است. در نتیجه، توسعه‌دهندگانی که قبلاً به سمت بلاکچین به‌اصطلاح «نسل دوم» رفته بودند، به بیت‌کوین نگاهی کاملاً جدید دارند. در مورد شبکه بیت‌کوین‌کش، پروتکل دفترکل ساده[4]، صدور توکن‌های فرعی را (با استفاده از کدهای رمزگذاری شده‌ای که از ابتدا در پروتکل بیت‌کوین ایجاد شده) تسهیل کرده است.

- **استیبل کوین‌ها:** رمزارزهایی که به ارزش یک منبع خارجی مانند دلار آمریکا یا طلا جهت پایداری گره‌خورده‌اند یا از طریق طراحی و ترکیب چند قرارداد ارزشش را در عددی خاص حفظ می‌کنند؛ مانند تتر و دای[5].
- **حریم خصوصی:** تراکنش‌های دیجیتالی خصوصی، مانند ویژگی ناشناس بودن که برخی رمزارزها ارائه می‌دهند؛ مانند مونرو، ورج و زی‌کش[6].
- **مالکیت دیجیتال:** روش نوینی در کنترل کردن، انبار کردن و کسب درآمد از اطلاعات را شکل می‌دهد؛ مانند سیا، بت و گلم[7].
- **کاربری‌های غیرمتمرکز:** شبکه‌ها، محصولات و خدمات فعال‌شده توسط رمزارزها با قابلیت تبادل بین دارایی‌های صادرشده روی شبکه (بازارهای پیش‌بینی‌کننده، تبادلات ارز، تسویه‌حساب)؛ مانند اینترنت غیرمتمرکز (اتریوم)، قراردادهای هوشمند یا قرارداهای سفارشی خودصادرشونده (نئو[8]) و دیگر خدمات رمزارزی (فاکتوم و نیم‌کوین[9]).

---

1. RSK: Rootstock
2. Bitcoin dominance
3. Tron
4. Simple Ledger Protocol
5. Dai
6. Monero, Verge, Zcash
7. Sia, BAT, Golem
8. NEO
9. Namecoin, Factom

دارایی دیجیتال مفهومی است که در سال‌های گذشته با رشد رمزارزهایی مانند بیت‌کوین مورد توجه قرارگرفته؛ حالا بسیاری از ما درکنار دارایی‌های فیزیکی، چیزهایی درباره دارایی دیجیتال شنیده‌ایم. زمانی دارایی خلاصه شده بود در ارز، زمین و ملک، کسب‌وکار و سهام، طلا و خودرو؛ ولی حالا شرایط تغییر کرده است. اکنون درکنار دارایی‌های فیزیکی، دارایی‌های دیجیتال نیز در دنیای کسب‌وکارها نقش‌آفرینی می‌کنند. همان‌گونه که در دنیای فیزیکی طلا داریم، در دنیای دیجیتال هم طلا داریم. در سال‌های گذشته برخی معتقد بودند که بیت‌کوین طلای دنیای دیجیتال است. امروز به این نتیجه رسیده‌ایم که دنیای دارایی‌های دیجیتال می‌تواند به فراتر از بیت‌کوین هم فکر کند.
این روزها مفاهیمی مانند دفترکل توزیع شده، توکن، رمزارز و ارز دیجیتال بانک مرکزی مصداق‌هایی از دارایی دیجیتال هستند.
آشنایی با مفاهیم مرتبط با دارایی دیجیتال برای شناخت این دنیای جدید، هدف اصلی این کتاب است. این کتاب تلاش می‌کند شما را با مفاهیم مرتبط با دارایی دیجیتال آشنا کند و یکی از کسب‌وکارهای پیشروی ایرانی در زمینه دارایی دیجیتال را نیز به شما بشناساند.
مهم‌ترین چالش پیش روی دارایی‌های دیجیتال رگولاتوری این حوزه جدید است. همان‌گونه که دارایی‌های فیزیکی را مدیریت و رگولاتوری می‌کردیم، نمی‌توانیم به سراغ دنیای دارایی‌های دیجیتال برویم. اولین قدم در راه رگولاتوری صحیح و اثربخش دارایی دیجیتال هم شناخت مفاهیم بنیادین این جهان جدید است. در صورتی می‌توانیم ابزارها و کسب‌وکارها و صنایع مرتبط با دارایی دیجیتال را رگولاتوری کنیم که مفاهیم پایه‌ای آن را بشناسیم.

پل وینو
Polwinno

کتاب دارایی دیجیتال در مرکز نوآوری پل وینو تولید و با حمایت ققنوس منتشر شده است

ققنوس
KUKNOS

انتشارات راه‌پرداخت
ناشر فناوری و نوآوری
way2pay.press

ISBN 978-622-7702-10-1
۱۱۰ هزار تومان