

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

چاپ دوم





انتشارات راه پرداخت

برای دانلود نسخه کامل به وبسایت
فروشگاه انتشارات راه پرداخت مراجعه کنید
way2pay.shop

نسخه نمونه

بِسْمِ اللَّهِ
الرَّحْمَنِ
الرَّحِيمِ



The mark of
responsible forestry
FSC® C009732

سرشناسه: نواب‌پور، علیرضا، ۱۳۷۰-

عنوان و نام پدیدآور: آشنایی 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: ۵/۲۱×۵/۱۴، س.م.

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۰-۱

وضعیت فهرست نویسی: فیپا

موضوع: شبکه ققنوس

موضوع: رمزارز

Cryptocurrencies: موضوع

موضوع: بلاک‌چین (پایگاه‌های اطلاعاتی)

Blockchains (Databases): موضوع

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

چاپ دوم





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 وینو

ویراستار ارشد: علیرضا نواب پور

ویراستار محتوایی: بهنام خاکباز

ویراستار فنی: فاطمه کاوندی، فرناز نکویی

بازبینی نهایی متن: بهار سرلک

صفحه آرا: علیرضا کیوان

ناظر چاپ: قادر شهبازی

نوبت چاپ: دوم ۱۴۰۴

شمارگان: ۱۰۰ نسخه

شابک: ۹۷۸-۶۲۲-۷۷۰۲-۱۰-۱

تلفن: ۰۲۱-۴۴۴۳۹۶۶

دورنگار: ۸۹۷۸۴۹۰۲

ایمیل: info@way2pay.press

وبسایت: way2pay.press

لیتوگرافی: هنراشکان

چاپ و صحافی: واژه

همه حقوق چاپ و نشر این اثر برای «انتشارات راه پرداخت» محفوظ است. هرگونه تکثیر، انتشار و بازنویسی این اثر یا قسمتی از آن به هر شکل و شیوه (چاپی، صوتی، ویدئویی، دیجیتال و...) بدون اجازه کتبی ناشر ممنوع است.

نشانی فروشگاه انتشارات راه پرداخت: تهران، جنت آباد جنوبی، خیابان لاله غربی، روبه روی پاساژ سمرقند، خیابان حدیث، کوچه حدیث دوم، پلاک ۸

فهرست

فصل اول: مروری بر فناوری‌های غیر متمرکز

۱۷	انواع فناوری‌های غیر متمرکز
۲۰	بلاکچین
۲۱	هش گراف
۲۶	گراف جهت‌دار غیر مدور (DAG)
۲۸	هولوچین
۳۰	الگوریتم اجماع
۳۲	انواع الگوریتم اجماع
۳۴	الگوریتم تحمل خطای بیزانس کاربردی (PBFT)
۳۵	الگوریتم اجماع گواه اثبات کار
۳۷	الگوریتم اجماع گواه اثبات سهام
۳۹	الگوریتم اجماع گواه اثبات سهام وکالتی
۴۱	

فصل دوم: مفهوم توکن و انواع آن

۴۷	توکن چیست؟
۴۸	مفهوم توکنایز کردن
۴۹	دسته‌بندی توکن‌ها
۵۰	۱. توکن پرداخت
۵۱	تاریخچه رمزارزها
۵۳	انواع رمزارزها و کاربردهای آنها
۵۵	بررسی رپبل به عنوان توکن پرداخت
۵۸	۲. توکن اوراق بهادار
۶۱	اوراق استاندارد در مقایسه با اوراق توکنایز شده
۶۳	

۶۴	مزایای توکن بهادار
۶۶	چالش های توکنایز کردن اوراق بهادار
۶۷	ضوابط به کارگیری توکن های بهادار
۶۸	طبقه بندی توکن بهادار به عنوان ابزار بدهی یا ابزار مالکیت
۶۸	بازدهی برای سرمایه گذاران
۷۰	باز خرید نهایی توکن های بهادار
۷۱	نمونه ای از توکن بدهی
۷۳	نمونه ای از توکن سهامی
۷۵	۳. توکن کاربری
۷۶	توکن های کاربری خالص
۷۶	توکن های دسترسی و توکن های ترکیبی
۷۷	توکن وفاداری به عنوان نمونه ای از توکن های کاربری
۷۹	اپلیکیشن موبایلی وفاداری نت کوین
۸۱	توکن استیمیت و توکن ترون به عنوان نمونه توکن کاربری موفق
۸۱	تفاوت استیمیت با بقیه شبکه های اجتماعی
۸۳	توکن ترون
۸۴	عرضه اولیه سکه
۸۴	مزایا
۸۵	معایب
۸۵	بهترین و موفق ترین عرضه اولیه سکه

۸۹ فصل سوم: قوانین و مقررات رمزارزها

۹۰	مقدمه
۹۰	قوانین و مقررات کشورهای جهان
۹۱	رویکرد مثبت و تنظیم گرانه (قانونی)
۹۵	محدودیت و ممنوعیت برخی بخش ها
۹۶	رویکرد منفی و بازدارنده (ممنوعیت)
۹۸	رویکرد منفعلانه (عدم اتخاذ موضع دقیق در خصوص ممنوعیت یا عدم ممنوعیت)
۱۰۲	قوانین و مقررات ایران
۱۰۳	الزامات حوزه رمزارزهای جهان روا
۱۰۳	الزامات حوزه عرضه اولیه سکه/توکن
۱۰۵	الزامات حوزه رمزارز بانک مرکزی (ملی)

فصل چهارم: ارزش دیجیتال بانک مرکزی

۱۰۷

۱۰۸

ارزش دیجیتال بانک مرکزی چیست؟

۱۰۹

ارزش دیجیتال کلان بانک مرکزی

۱۱۰

ارزش دیجیتال خرد بانک مرکزی

۱۱۱

رویکرد بانک تسویه حساب‌های بین‌المللی (مفهوم گل پول)

۱۱۳

مزایای صدور پول دیجیتال توسط بانک مرکزی

۱۱۴

معایب صدور پول دیجیتال توسط بانک مرکزی

۱۱۵

ارزش افزوده پول دیجیتال بانک مرکزی برای کسب‌وکارهای آنلاین

۱۱۶

موارد کاربردی ارزش دیجیتال بانک مرکزی

۱۱۹

طراحی ارزش دیجیتال بانک مرکزی

۱۱۹

توکن محور یا حساب محور

۱۱۹

وضعیت بهره

۱۱۹

مدل تک‌لایه یا دولایه

۱۲۱

دفتر کل متمرکز در برابر فناوری‌های دفترکل غیر متمرکز

۱۲۱

بانک‌های مرکزی و چند منظوره برای ارزش‌های دیجیتال

۱۲۲

مدل پلتفرمی ارزش دیجیتال بانک مرکزی

۱۲۳

کشورهای پیشرو در حوزه پول دیجیتال بانک مرکزی

فصل پنجم: فرصت‌ها و چالش‌های رمزارزها

۱۳۳

۱۳۴

مزیت‌ها

۱۳۷

چالش‌ها و ریسک‌ها

فصل ششم: درباره ققنوس

۱۴۷

۱۴۸

تأسیس ققنوس

۱۵۲

تطابق مقرراتی

۱۵۳

توکن‌های مبتنی بر شبکه ققنوس

۱۵۵

محصولات مبتنی بر شبکه ققنوس

۱۵۸

سپیدنامه شبکه ققنوس و توکن پیمان

۱۵۹

مقدمه

۱۶۰

تعاریف

۱۶۵

بیان مسأله

۱۶۵	نبود سکوی فناوری چابک و منعطف برای عرضه انواع توکن‌ها
۱۶۶	عدم نقدشوندگی دارایی‌های منجمد
۱۶۶	عدم حفظ ارزش سرمایه‌های خرد
۱۶۶	عدم شفافیت، تغییرپذیری و در دسترس نبودن
۱۶۷	لزوم احراز هویت مشتری
۱۶۷	راه‌حل پیشنهادی
۱۶۸	اصول و ارزش‌های ققنوس
۱۷۰	زیرساخت فنی شبکه ققنوس
۱۷۱	معماری شبکه
۱۷۲	اجزای فنی شبکه ققنوس
۱۷۳	سرویس هسته
۱۷۴	سرویس واسط
۱۷۴	سرویس پل
۱۷۴	سرویس انطباق
۱۷۴	سرویس آدرس‌دهی
۱۷۵	سرویس تبادل
۱۷۵	سرویس بایگانی
۱۷۶	کیف توکن ققنوس
۱۷۶	داشبورد ققنوس
۱۷۶	آزمایشگاه ققنوس
۱۷۶	شبکه اصلی و آزمایشی ققنوس و استقرار میزبان‌ها
۱۷۸	نقش‌ها و ارکان ققنوس
۱۸۳	پیمان
۱۸۹	الگوی درآمدی میزبان‌ها
۱۹۰	رقابت میزبان‌ها
۱۹۰	نظام حقوقی ققنوس
۱۹۶	خروج میزبان
۱۹۷	حل و فصل اختلافات ققنوس
۱۹۸	پایان ققنوس
۱۹۸	لازم‌الاجرا شدن سپیدنامه

[پیشگفتار]

پیش بینی دقیق آینده و اتفاقاتی که رخ خواهد داد امکان پذیر نیست؛ اما باید برای آنچه احتمالاً پیش خواهد آمد آمادگی لازم را داشته باشیم. تجارب چند دهه اخیر نشان می دهد که فناوری های برهم زننده، مسیر حرکت و اثرگذاری خود را پیدا می کنند تا جایی که پذیرش آن برای کسب و کارها یک الزام می شود نه یک انتخاب و مقاومت در مقابل آنها ادامه حیات کسب و کار را دچار چالشی جدی می سازد.

بنا بر پیش بینی بسیاری از متخصصان و آینده پژوهان، فناوری بلاکچین طی ۱۰ سال آتی به اوج شکوفایی خود می رسد و کاربردهای اصلی آن پدیدار خواهد شد. آن زمان، میان شرکت هایی که هم اکنون روی فناوری بلاکچین سرمایه گذاری می کنند و آنهایی که توجهی به این روند جهانی ندارند، شکاف معناداری پدیدار می شود. بسیاری از پلتفرم های متمرکز جای خود را به پلتفرم های غیر متمرکز و توزیع شده خواهند داد. شاید برخی از روابط مالی بر پایه رمزارزها انجام شود، شاید زیرساخت تسویه بین بانکی یا بازار بورس به سمت دفاتر کل توزیع شده برود، شاید مرورگرها و رسانه های غیر متمرکز ایجاد شوند، شاید نظام وام دهی به مدل همتا به همتا تغییر یابد و بسیاری از شایدهای دیگر... که به هیچ وجه دور از ذهن نیستند.

واقعیت این است که صنعت مالی و بانکداری بیشترین تأثیر را از بلاکچین خواهد داشت؛ بنابراین اگر بانک ها 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 بهسازان 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 به عنوان 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 کسب و کار است. بنابراین مرکز نوآوری پل وینو در سال ۱۳۹۹ بر آن شد در این راستا گامی مؤثر بردارد. بیان روان و ساده مفاهیم نهفته در فناوری بلاکچین به عنوان یک ضرورت به فرهنگ سازی در میان ذینفعان کمک می‌کند که هدف از گردآوری این کتاب نیز همین امر است.

این کار ماحصل پژوهش جمعی از همکاران در مرکز نوآوری پل وینو و با هدایت همکاران گرامی آقایان علیرضا نواب پور و بهنام خاکباز و خانم فرناز نکویی است. ضمن تشکر از زحمات ایشان، 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 روشن تری از آینده حاصل شود.

محمدهادی شالباف

رئیس مرکز نوآوری گروه فن‌آوران هوشمند بهسازان فردا «پل وینو»

[مقدمه]

به دنبال اختراع اینترنت و تحقق رؤیای انتقال آزادانه «داده‌ها و اطلاعات» که سالیان متمادی، متخصصان فناوری اطلاعات روی آن کار می‌کردند، دانشمندان مطرحی همچون هایک^۱، برنده جایزه نوبل اقتصاد در سال ۱۹۷۴، مفهومی تحت عنوان غیر متمرکز کردن ارزش^۲ را در مجامع علمی مطرح کردند. دغدغه اصلی پیروان این تفکر، آزادی فردی، حفظ حریم شخصی و عدم اعتقاد و اعتماد به نهاد واسطه و مرکزی بود. آنها معتقد بودند اساساً 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 باشند به دست آورند؟

تفاوت «داده اطلاعاتی» با «داده ارزشی» در این است که داده ارزشی خلاف داده اطلاعاتی نباید امکان جعل یا کپی شدن داشته باشد و اگر این اتفاق بیفتد آن داده بی ارزش خواهد شد. از اواخر دهه ۱۹۹۰ متخصصان فناوری اطلاعات در پی توسعه فناوری ای بودند که بتواند داده ارزشی را بدون حضور نهاد مرکزی، غیر قابل جعل و کپی شدن 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 توزیع کردن دفتر کل میان همه اعضا و در نتیجه حذف نهاد واسط می‌توانست هر داده‌ای را غیرقابل جعل و غیرقابل کپی شدن سازد و در نتیجه به آن داده ارزش بخشد. به عبارتی دیگر به وسیله فناوری یاد شده این امکان فراهم شد که هر داده ارزشی که در آن ثبت شود، بدون وجود نهاد مرکزی در خطر جعل یا کپی شدن قرار نگیرد و این پدیده می‌تواند بنیان تمام سیستم‌های متمرکز با نهاد مرکزی را به لرزه درآورد. این مکانیزم ثبتی غیرمتمرکز به‌طور کلی «فناوری دفاتر کل توزیع شده»^۱ نام گرفت. اولین نمونه این فناوری، بلاکچین و اولین محصول آن بیت کوین بود.

اگرچه 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 دفاتر کل توزیع شده، نوعی فناوری نوین جهت «ثبت» است که به میزان مصادیق ثبت در کسب و کارها می‌توان برای آن کاربرد تعریف کرد. فناوری دفاتر کل توزیع شده سه ویژگی محوری دارد که آن را منحصر به فرد و کاربردهای آن را در ثبت ارزش‌ها افزایش می‌دهد: غیرقابل جعل بودن بدون نیاز به نهاد مرکزی، شفاف بودن تمامی تراکنش‌ها و ناشناس بودن افراد در شبکه.

به مرور در دهه ۲۰۱۰ پس از افزایش قیمت بیت کوین، مطالب متعددی درباره سایر کاربردهای فناوری دفاتر کل توزیع شده 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

بزرگ تری 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 عدم حضور نهاد ناظر را نداشت، این فناوری به تدریج به مرز تعادل میان دنیای متمرکز و غیرمتمرکز نزدیک شد. همگام با این تعادل نسبی، شاهد روند روبه‌رشد به کارگیری 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^۱ 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»^۲ مخصوصاً در سطح بین‌المللی و تسهیل فرایندهای تأمین مالی تجارت^۳ اشاره کرد. به مرور زمان این کاربردها به صنایع پرداخت، بیمه، قرض‌دهی، تأمین مالی جمعی و غیره نیز گسترش پیدا کرد.

به دنبال 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 توسعه داده‌شده 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 دفاتر کل توزیع شده و انواع آن معرفی می شوند، سپس به انواع توکن های موجود و مباحث رگولاتوری مرتبط با آن پرداخته خواهد شد. از مهم ترین توکن های تعریف شده برای صنعت بانکداری، ارز دیجیتال بانک مرکزی است که در فصلی مجزا به آن پرداخته ام و در انتها در مورد چالش ها و فرصت های این فناوری برای کشور توضیحاتی می دهم.

علیرضا نواب پور
مرکز نوآوری پل وینو



فصل اول
مروری بر فناوری های
غیر متمرکز



مقدمه

از هزاران سال پیش بشر تمایل داشت با رویکرد متمرکزگرایی، 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 هم‌تابه هم‌تأ^۱ 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^۲ 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 به کار 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 عدم نیاز 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. عدم تمرکز، 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، خرید و فروش، 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 دفاترکل متمرکز که در مشکل «اعتماد» به شخص ثالث خلاصه می‌شود همراه با کشف و استفاده از الگوریتم‌های جدید، مفهومی به نام «دفترکل توزیع شده» را پدید آورد. در ادامه با بیان یک مثال مالی به تفاوت میان دفترکل توزیع شده و متمرکز پرداخته می‌شود.

برای مثال در بانک تمام تبادلات مالی مشتریان در یک دفترکل ثبت و ضبط می‌شود و بانک به عنوان دارنده دفترکل، 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 به صورت 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 به حساب 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.

دفتر کل توزیع شده نوعی دفتر کل است که به صورت اشتراکی بین چند عضو شبکه (مثلاً چند بانک) استفاده می‌شود که البته نگهداری و به‌روزرسانی آن به صورت مکتوب عملاً غیرممکن است و حتماً برای پیاده‌سازی آن باید از سامانه‌های پیشرفته استفاده شود. هر یک از اعضای شبکه که می‌خواهند تراکنشی را در این دفتر کل 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 دفتر کل ثبت می‌شود.

دفتر کل توزیع شده، اجماعی از داده‌های دیجیتال تکثیر شده، اشتراک‌گذاری شده و همگام‌سازی شده است که در موقعیت‌های جغرافیایی مختلف گسترده شده‌اند. در این فناوری هیچ مدیریت یا ذخیره‌سازی متمرکزی بر داده‌ها وجود ندارد و جایگزینی است برای سامانه‌هایی که مدیریت آنها با استفاده از پایگاه‌های داده متمرکز و سرورهای مرکزی انجام می‌پذیرد. این دفتر بر اساس سازوکار اجماع^۱ (که در بخش بعد توضیح داده می‌شود) و معماری داده‌مورد قبول اعضای شبکه، نگهداری و به‌روزرسانی می‌شود. به این معنی که هر فرد در شبکه، هر تراکنش را پردازش می‌کند و سپس درباره ثبت شدن یا نشدن 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 قابل اعتماد است. در این فناوری، دفتر کل 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، قابل اطمینان و غیرقابل دست‌کاری انجام می‌شوند.

انواع فناوری‌های غیرمتمرکز

معمولاً دو اصطلاح بلاکچین^۲ و فناوری دفتر کل توزیع شده هم‌معنی تلقی می‌شوند،

1. Consensus mechanism
2. Blockchain

اما دفترکل توزیع شده یک اصطلاح وسیع تر است که لزوماً نباید از بلاکچین استفاده کند و انواع مختلفی دارد که بلاکچین محبوب ترین نوع آن است. از دیگر انواع این فناوری می توان به گراف جهت دار غیرمدور^۱ نیز اشاره کرد که تفاوت اصلی و عمده در پیاده سازی آنها در مکانیزم اجماع شان خلاصه می شود. در ادامه به بررسی انواع مختلف این فناوری می پردازم.

بلاکچین

ساده ترین و رایج ترین شکل فناوری دفترکل توزیع شده، بلاکچین است. واژه بلاکچین از دو کلمه بلوک^۲ و زنجیره^۳، به معنای زنجیره ای از بلوک ها تشکیل شده است. در سال ۱۹۹۱ استوارت هابر و اسکات استورنتا^۴ اولین کسانی بودند که روی فناوری بلاکچین کار کردند. این فناوری تا سال ۲۰۰۹ که ساتوشی ناکاموتو^۵ بیت کوین را اختراع کرد، کاربرد زیادی نداشت. او توانست با پیاده سازی بیت کوین بر بستر این فناوری، اولین پایگاه داده مبتنی بر بلاکچین را طراحی کند.

دلیل این نامگذاری، وابستگی بلوک ها به یکدیگر است که به صورت یک زنجیره، رکوردهای داخل یک پایگاه داده را در خود ثبت و ضبط کرده است. در واقع بلوک پیدایش^۶ (اولین بلوک) همانند دفترکل اولیه است که مالکیت ها در آن ثبت شده و به ازای هر تغییری در آن، یک الحاقیه در قالب بلوک جدید به آن الصاق (زنجیر) می شود و به این ترتیب بلوک هایی زنجیروار و مرتبط با هم پدید می آید و همین مسئله حمله به آن را هزینه بر می کند چرا که برای تغییر آخرین بلوک باید تک تک الحاقیه ها 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^۱) استخراج و به همه اعلام شود تا بتوانند بلوک جدید را به‌روزرسانی کنند.

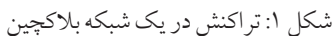
هر بلوک شامل بخش سرآیند^۲ و بخش بدنه^۳ است. در بخش سرآیند، برچسب زمانی بلوک^۴ (زمان ایجاد بلوک)، هش^۵ آن بلوک و هش بلوک قبلی و سایر اطلاعات مربوط به شناسایی آن بلوک قرار می‌گیرند و در بخش بدنه، داده‌هایی که قرار است در آن بلوک ذخیره شوند، جای می‌گیرد.

هش، مجموعه‌ای از اعداد و حروف تصادفی است که تأییدکنندگان تراکنش یا استخراج‌کنندگان^۶ 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 می‌کند 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 به خوبی نشان می‌دهد.

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



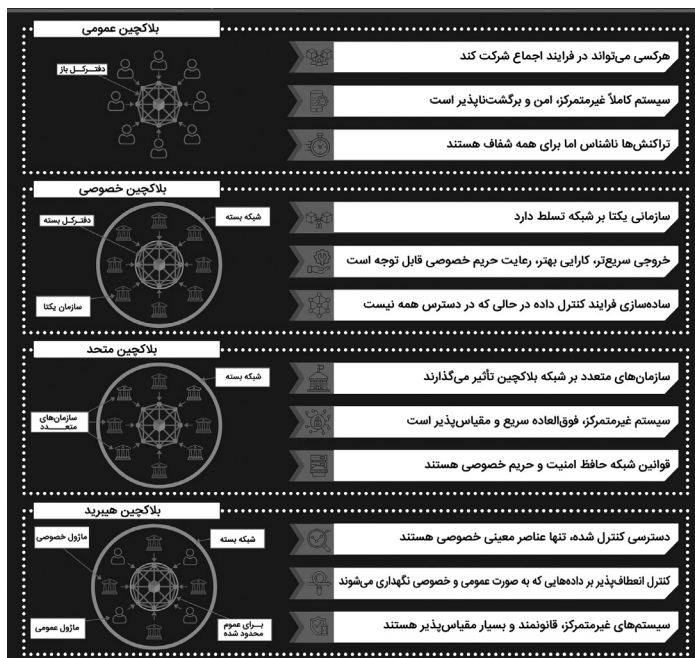
بر اساس دو معیار امکان مشاهده و تأیید تراکنش، بلاکچین‌ها به چند دسته تقسیم می‌شوند که هر کدام نشانگر این موضوع خواهند بود که چه کسانی قادر به مشاهده و تأیید تراکنش‌ها هستند. برای تفکیک بر اساس امکان مشاهده تراکنش‌ها، دو دسته کلی بلاکچین عمومی^۱ و بلاکچین خصوصی^۲ در این فناوری وجود دارد. در بلاکچین عمومی 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 دنیای 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 راه اندازی یک بلاکچین خصوصی بایکدیگر 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^۳ و سایر مشکلات در بخش قانونگذاری در میان است، بلاکچین خصوصی مزایای خاص خود را دارد. روش دیگر تفکیک شبکه‌های بلاکچین، طبقه‌بندی آنها بر اساس امکان تأیید تراکنش‌هاست که از آنها به عنوان «بلاکچین با کسب مجوز دسترسی»^۴ و «بلاکچین بدون نیاز به مجوز دسترسی»^۵ 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. بر اساس دو معیار فوق، معمولاً شبکه‌های بلاکچین یکی از چهار نوع زیر هستند که ویژگی‌های هر یک را به اختصار ذکر می‌کنم:

۱. **بلاکچین کنسرسیوم و متحد^۱**: محدودکنندگی بیشتر، دسترسی محدود، مقیاس پذیری بسیار مناسب، شفافیت و حفظ حریم خصوصی بالا (به عنوان مثال کنسرسیوم R3).

۲. **بلاکچین خصوصی و نیازمند مجوز^۲**: در این نوع از بلاکچین‌ها دسترسی می‌تواند به صورت عمومی یا خصوصی تعریف شود. اما اجازه تأیید تراکنش‌ها، انجام توافق و تغییر داده‌ها فقط برای افراد معین و محدودی فراهم می‌شود. بانک چین^۳ 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**^۱: این فناوری یک شبکه عمومی متن باز و شفاف است که همه امکان رؤیت تراکنش ها و مشارکت در تأیید آنها را دارند. این نوع بلاکچین با حداقل هزینه قابل راه اندازی است و نیازی به نگهداری ندارد. با این حال عمومیت اش باعث می شود روند پردازش آن آهسته باشد. بیت کوین و اتریوم^۲ بهترین نمونه های عمومی بودنش، این نوع بلاکچین ها هستند. مشکل اصلی این نوع بلاکچین، محدودیت تراکنش در ثانیه (TPS^۳) و عدم مقیاس پذیری است. با وجود این، برای تأیید تراکنش ها می توان از سازوکارهای مختلف اجماع استفاده کرد.

۴. **بلاکچین هیبریدی**^۴: این نوع بلاکچین ها ترکیبی از شبکه های عمومی و خصوصی هستند. بلاکچین های هیبریدی از انعطاف پذیری خاصی در خصوص تعیین داده های خصوصی و همچنین داده های قابل ذخیره سازی در دفترکل عمومی برخوردارند. این شبکه های دو گانه مقیاس پذیری بهتری دارند و اجماع در آنها نیازمند مشارکت تمامی گره های شبکه نیست. هایپر لجر^۵ یک نمونه از این شبکه های بلاکچین هیبریدی است.

هش گراف^۶

هش گراف در تلاش است محدودیت های بلاکچین را برطرف کند. هش گراف برای تأیید تراکنش های موجود روی شبکه فقط به مکانیزم اجماع و توافق متکی است. این اجماع از طریق روش هایی چون رأی گیری مجازی و همچنین تکنیک های شایعه^۷ حاصل می شود.

در این حالت فناوری هش گراف قادر است مقیاس پذیری بالاتر و نیاز به ذخیره سازی

1. Permissionless/Public blockchain

2. Ethereum

3. Transactions Per Second

4. Hybrid

5. Hyperledger

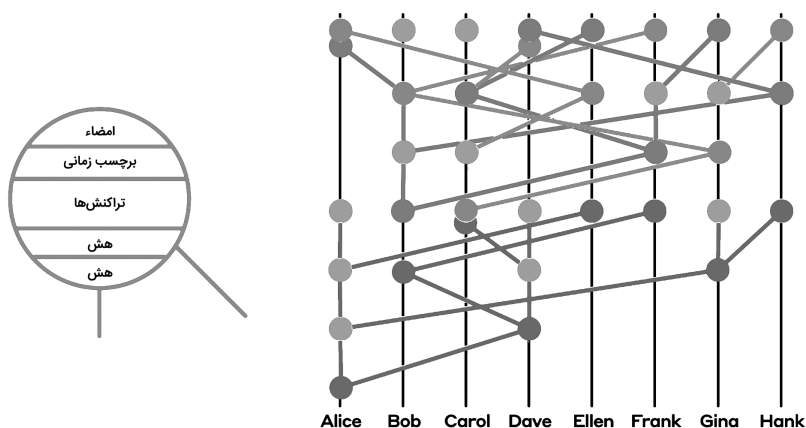
6. Hashgraph

7. Gossip techniques

پروتکل شایعه به منظور برقراری ارتباط بین ماشین های در حال سرویس دهی در خوشه های مختلف به کار می رود. با استفاده از این روش سرویس دهنده ها می توانند 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 هش گراف این امکان را فراهم می‌کند که چندین تراکنش به صورت همزمان و موازی ذخیره شوند. این تراکنش‌ها در یک برچسب زمانی با عنوان «رویداد»^۱ ذخیره می‌شوند. تفاوت اصلی و عمده در پیاده‌سازی این دو فناوری دفترکل توزیع شده، در مکانیزم اجماع آنها خلاصه می‌شود.

در بلاکچین استخراج کنندگان قدرت انتخاب تراکنش را دارند اما در هش گراف تراکنش‌ها به ترتیب دریافت آنها تأیید می‌شوند و به این طریق به طور قابل توجهی مدت زمان لازم برای تأیید هر تراکنش کاهش می‌یابد. در این فناوری هنگامی که یک رویداد آغاز می‌شود، هر یک از گره‌های شبکه به صورت 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 هش گراف

از این روش گراف از لحاظ محاسباتی بسیار ساده‌تر و سریع‌تر عمل می‌کند. در این مکانیزم مطابق شکل ۳ تمامی گره‌ها از هر تراکنشی اطلاع دارند و می‌توانند پس از تغییرات لازم، تراکنش مذکور را رها کنند. به این معنا که در دفترکل هاش گراف نیازی به ذخیره‌سازی دائمی تراکنش‌ها در شبکه وجود ندارد و از همین رو نیاز به ذخیره‌سازی به شدت کاهش می‌یابد. فناوری هاش گراف توسط لیمون برد^۱، هم‌بنیان‌گذار و معاون ارشد بخش فناوری سوئیرلدز^۲ ابداع شده و از اوت سال ۲۰۱۸ برای استفاده در دسترس عموم قرار گرفته است. هاش گراف مشتقات قابل توجهی نیز ایجاد کرد. یکی از انواع مهم آن، پلتفرم هاش گراف هدر^۳ نام دارد. این پلتفرم امکان مقیاس‌پذیری و امنیت بسیار بالا را به ارمغان می‌آورد. در سپیدنامه هدر 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)

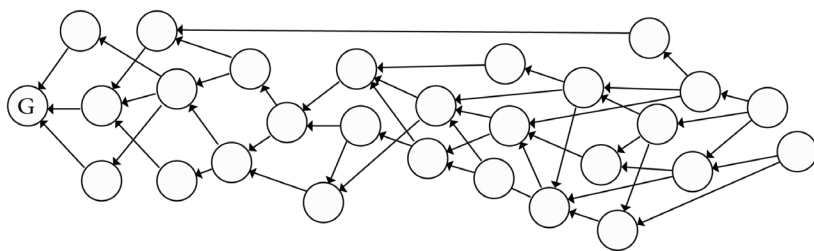
گراف جهت‌دار غیرمدور یا همان DAG، نوع دیگری از فناوری دفاترکل توزیع شده با قابلیت مقیاس‌پذیری بالاست. در این فناوری برای دستیابی به یک مکانیزم اجماع کارآمد از ساختار داده متفاوتی استفاده می‌شود. هرچه تعداد تراکنش‌های یک شبکه بیشتر شود، سرعت آن نیز افزایش خواهد یافت. در فناوری DAG تمامی گره‌ها دارای عملکرد 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 ۴ دنباله‌ای از تراکنش‌ها به وجود می‌آیند که به اصطلاح یک انشعاب^۴ نامیده می‌شود.

1. Leemon Baird

2. Swirls

3. Hedera

4. Fork



شکل ۴: تصویر کلی از اجماع DAG

اولین پلتفرمی که برای استفاده در DAG منتشر شد، NXT نام داشت. این پلتفرم در نوامبر ۲۰۱۵ به صورت رسمی راه اندازی شد. علاوه بر این پلتفرم، تنگل آیوتا^۱ و بایت بال^۲ دو نمونه مهم و قابل توجه دیگر از مشتقات این مدل از فناوری دفتر کل توزیع شده هستند.

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

۱. طرح امضای یک بار مصرف مقاوم در برابر محاسبات کوانتومی که به عنوان یک محافظ در برابر تلاش کامپیوترهای کوانتومی برای شکستن شبکه عمل می کند.
۲. پیام احراز شده مخفی^۳ که امکان ارتباط امن و رمز گذاری شده را میان گره ها فراهم می کند.
۳. مناسب برای نمایش انواع مختلف جریان ها مانند جریان پردازش داده. جریان پردازش داده ممکن است شامل مسیرهای متعددی باشد. گراف جهت دار غیر مدور می تواند داده ها را در چند مسیر پردازش کند تا خروجی های متفاوت به دست آورد. برای درک بهتر پردازش دسته ای^۴، فرض کنید پایگاه داده ای از میزان فروش جهانی دارید و گزارشی از فروش به دلار آمریکا به تفکیک مناطق لازم است. با به کار گیری گراف جهت دار غیر مدور می توانید همه داده ها را در موتور پردازش بار گذاری 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 رمز نگاری شده را فراهم می کند.

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.

۴. 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، جمع‌بندی (محاسبه مجموع)، غنی‌سازی^۱ (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^۲ به سمت یک رویکرد عامل‌محوری^۳ است.

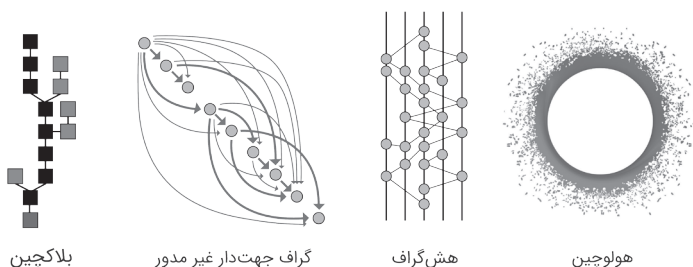
اجتناب از یک پروتکل اجماع جهان‌شمول^۴ باعث شده فناوری دفترکل هولوچین مقیاس‌پذیری بالایی داشته باشد. در حالی که بلاکچین به دنبال غیرمتمرکزسازی تراکنش‌های موجود روی شبکه است، هولوچین قصد دارد تراکنش‌های بین دو گره مجزا را غیرمتمرکز کند. هر گره مجزا در این شبکه زنجیره مربوط به خود را اجرا می‌کند. این زنجیره در شبکه خود عملکرد مستقلی دارد و در عین حال 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 توزیع شده^۵ ذخیره کنند. این کار مستلزم استفاده از کلید خصوصی است. این داده‌ها به صورت توزیع یافته 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 دفتر کل مخصوص به خود است، هر یک از دفتر کل‌های 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 دریافت شده 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 ویژگی و مزیت بزرگ برای فناوری هولوچین است تا از گزند حملات مخرب در امان باشد. در حالی که 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 عدم نیاز 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 به صرفه 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 غیر متمرکز^۱ نیز می‌شوند.



شکل ۵: مقایسه ساختار انواع فناوری‌های غیر متمرکز

مقایسه انواع فناوری های دفتر کل دیجیتالی مختلف حاکی از پیمودن مسیری طولانی در راه تحول این فناوری است. فناوری هایی چون هولوچین مفهوم غیر متمرکز سازی را به سطح جدیدی رساندند. این امر به نوبه خود باعث ایجاد چنان پتانسیل جدیدی برای ساختار شکنی در این اکوسیستم می شود که پیش از این حتی تصور آن نیز ناممکن بود. با ظهور و ایجاد کاربردهای جدید برای فناوری دفتر کل دیجیتالی در بخش ها و صنایع مختلف، این تحول سرعت بیشتری نیز به خود می گیرد.

دسته بندی ها	هولوچین	گراف مدور جهت دار	هش گراف	بلاکچین
استخراج	گره ها روی زنجیره های منفرد اجرا می شوند از این رو مانبرها مجبور نیستند که تراکنش ها را اعتبار سنجی کنند	تراکنش قبلی موفقیت در دستیابی به اجماع را تعیین می کند	گره ها از طریق رای گیری مجازی به اجماع می رسند	شرکت کنندگان قادرند از طریق مکانیزم های اجماع مختلف توکن های جدید استخراج کنند
تراکنش ها در هر ثانیه	هر گره دفتر کل مخصوص به خود را پردازش می کند مانبر این مقیاس پذیری و TPS نامحدود است	ساختار داده منحصربه فرد از طریق گراف های غیر مدور جهت دار، مقیاس پذیری و TPS بالا را تضمین می کند	مکانیزم اجماع منحصربه فرد می تواند بار محاسباتی را کاهش دهد مانبر این مقیاس پذیری و TPS بالا ایجاد می کند	از نظر مقیاس پذیری و TPS بسیار محدود است
ساختار داده	داده ها بر روی گره های متعدد پلتفرم توزیع شده است مانبر این مشکل تراکم شبکه وجود ندارد	ساختار داده از مکانیزم گراف غیر مدور جهت دار پیروی می کند که در آن هر تراکنش مستقل است	رای گیری مجازی و شایعه پشت شایعه تضمین می کند که تراکنش ها توسط اکثریت اعتبار سنجی شده اند	داده ها به ترتیب تراکنش هایی که توسط مانبرها در اکوسیستم اعتبار سنجی شده اند در بلوک ها طبقه بندی شده اند
اعتبار سنجی تراکنش ها	گره ها دفتر کل مخصوص به خود را پردازش می کنند از این رو نیازی به انجام این کار توسط مانبرها نیست	موفقیت تراکنش فعلی به توانایی آن در معتبر کردن دو تراکنش قبلی بستگی دارد	اعتبار سنجی تراکنش ها به ازای هر اجماع اتفاق می افتد	مانبرها این اختیار را دارند که تراکنشی را به تأخیر بیندازند یا به کلی کنسل کنند
زمان راه اندازی	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
شبکه های که روی پلتفرم اجرا می شوند	شبکه هولوچین معروف ترین شبکه روی اید پلتفرم است	ByteBall ، NXT ، Tangle مشهور ترین شبکه های هستند که از DAG استفاده می کنند	Swirls و NOIA تنها شبکه های روی هش گراف هستند	بیت کوین و اتریوم مشهور ترین شبکه های ساخته شده بر روی بلاکچین هستند



شکل ۶: ویژگی های عمومی انواع دفتر کل توزیع شده

الگوریتم اجماع

همان طور که پیش از این اشاره شد، یکی از ویژگی های مهم بلاکچین و

انواع دیگر دفاترکل 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 سرویس دهنده شبکه هستند، گره یا نود^۱ گفته می‌شود.

بزرگ‌ترین دلیل استفاده از انواع دفاترکل توزیع شده مانند بلاکچین، بالا بردن امنیت و عدم دستکاری بدون وجود نهاد معتمد و مطمئن بودن از تغییر ناپذیری و خرابی داده‌هاست.

اگر اطلاعات در یکی از سرورها (گره‌ها) به هر دلیلی از بین برود، چندین هزار و حتی میلیون‌ها سرور دیگر آن اطلاعات را در خود ذخیره کرده‌اند. اما هنگام استفاده از بلاکچین یا انواع دیگر دفاترکل توزیع شده، یک مسئله حیاتی مطرح می‌شود. زمانی که قرار است اطلاعات به روزرسانی 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. به این 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

توافق بر سند که اطلاعات را به روز رسانی کنند، این اتفاق خواهد افتاد.

به طور کلی الگوریتم‌های اجماع کاربردهای دیگری هم دارند، مانند:

- تصمیم‌گیری در مورد اینکه آیا یک تراکنش صلاحیت تأیید و ذخیره روی دفترکل توزیع شده را دارد یا خیر؛

- انتخاب گره‌ها برای مدیریت امور روی دفترکل توزیع شده؛

- 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، داده‌ارسالی 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 پرکاربرد آن در بلاکچین، الگوریتم تحمل خطای بی‌زانس^۱، الگوریتم گواه اثبات کار^۲، گواه اثبات سهام^۳ و گواه اثبات سهام و کالتی^۴ 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

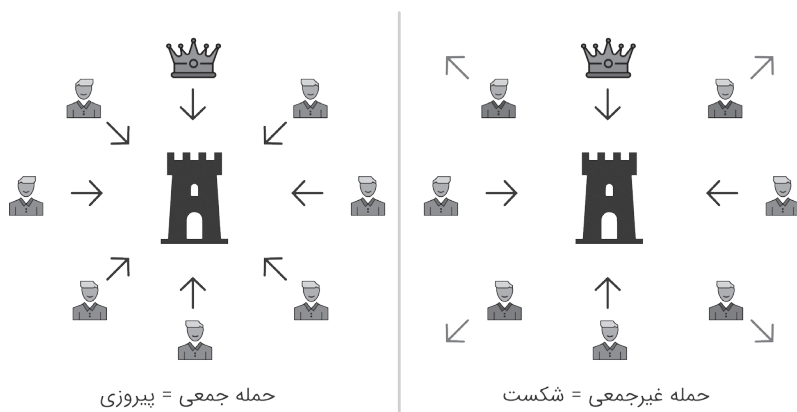
2. Proof-of-Work (PoW)

3. Proof-of-Stake (PoS)

4. Delegated Proof-of-Stake

الگوریتم تحمل خطای بیزانس کاربردی (PBFT)^۱

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^۲، معضلی کلاسیک است که نوعی از مکانیزم اجماع را برای سیستم‌های مبتنی بر رمزنگاری ارائه می‌کند. مکانیزمی محبوب تحت عنوان 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 توزیع شده، اعتبارسنج‌ها^۳ 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 توزیع شده 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 به دست آمده است.

علی‌رغم این که مقیاس‌پذیری و بهره‌وری ارائه شده توسط مکانیزم تحمل‌پذیری خطای بیزانس قابل ملاحظه 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:

۱- تحمل خطای بیزانس کاربردی^۱، یک الگوریتم اجماع است که در اواخر دهه ۱۹۹۰ توسط باریبار الیسکوف^۲ و میگل کاسترو^۳ 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 توزیع شده و بلاکچین است و در هایپرلجر فابریک^۱ نیز مورد استفاده قرار می‌گیرد. در این روش از کمتر از ۲۰ اعتبارسنج برای ارزیابی اجماع شبکه استفاده می‌شود.

۲- توافق بیزانسی یکپارچه^۲ 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 در نتیجه 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 هر کسی 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 یا بنده عدد تصادفی نانس^۳ حل‌کننده مسئله نیز پاداشی تعلق

1. Hyperledger Fabric

2. Federated Byzantine Agreement

3. Nonce

می گیرد که می تواند کاربران بسیاری را تحت عنوان استخراج کننده 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 می کند.

این روش عمدتاً برای محافظت در برابر خطاهای بیزانسی (به طور عمده در برابر خطای دوبار خرج کردن^۱ توسط گره های مخرب) استفاده می شود؛ چراکه در این روش گره ای که به صورت مخرب عمل کند، فرصت کمی برای تحمیل بلوک مخرب در شبکه دارد؛ مگر اینکه حمله کننده بیش از ۵۰ درصد از منابع محاسباتی شبکه را تأمین کند (حمله ۵۱ درصد). بنابراین، الگوریتم اجماع گواه اثبات کار یک روش غیرقابل نفوذ ارائه می دهد، مگر اینکه مهاجم بتواند بیش از ۵۰ درصد منابع را جمع آوری کند.

فراایندهایی که در این مکانیزم صورت می گیرند به شرح زیر هستند:

- ورود تراکنش به دفتر کل توزیع شده؛
- تأیید مشروعیت تراکنش توسط استخراج کنندگان؛
- حل مسئله ریاضی گواه اثبات کار توسط استخراج کنندگان؛
- اهدای جایزه به اولین استخراج کننده ای که عدد تصادفی مسئله را پیدا کرده است؛
- تأیید نهایی تراکنش و ثبت در بلاکچین عمومی توسط همه نودها.

گاهی اوقات، ممکن است بیش از یک گره راه حل را در یک زمان پیدا کند. وقتی این اتفاق می افتد، هر یک از این گره ها یک بلوک را پیشنهاد و به شبکه ارسال می کنند. این بلوک ها توسط بلوک های مجاور برداشت می شود و یک بلاکچین به صورت موقت شکل می گیرد و بلوک ها به زنجیره آنها اضافه می شود. در نهایت پروتکل شاخه ای را که طولانی تر از بقیه می شود به عنوان زنجیره رسمی انتخاب می کند و بقیه را از بین می برد. مهم ترین نقطه قوت این روش این است که برای مثال در بیت کوین گره ای که برای ایجاد یک بلوک جدید انتخاب شده است، بابت ثبت تراکنش ها، پاداش خود

1. Double spending

به صورت بیت کوین را دریافت می کند. به دلیل اینکه انجام محاسبات و استخراج پول کار بسیار پرتلاش و پرهزینه‌ای است، استخراج کنندگان تنها بر روی شاخه‌ای از بلاکچین تمرکز می کنند که به نظر می رسد زنجیره اصلی (یعنی بلاکچین با اکثریت بلوک‌ها) باشد.

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

- **استخراج متمرکز^۱:** به دلیل اینکه اختلافات زیادی در قدرت CPU کامپیوترها وجود دارد، کاربرانی که پردازنده‌های کم قدرت دارند اغلب میدان را به ماشین‌های قدرتمند می بازند. بنابراین، گواه اثبات کار نمی تواند الزامات الگوریتم اجماع مبنی بر اینکه گره‌های تصادفی باید در میان وسیع ترین جمعیت ممکن از شرکت کنندگان انتخاب شوند را برآورده سازد. این ضعف خطر استخراج متمرکز را افزایش می دهد.

- **تأخیر زمانی زیاد:** بلوک‌های جدید تقریباً هر ۱۰ دقیقه تولید می شوند. در نتیجه انتظار برای تأیید نهایی تراکنش‌های یک بلوک تولید شده حدود ۳۰ دقیقه طول می کشد؛ 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 بیت کوین، هفت تراکنش در ثانیه^۲ 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» می شوند. تحت شرایط گواه اثبات

1. Centralized mining

وقتی تعداد محدودی از شرکت‌ها تقریباً کنترل کامل را در قدرت هش کردن به دست می گیرند، فرایند استخراج متمرکز تر می شود.

2. TPS: Transaction per Second

سهام، گره انتخاب شده برای ایجاد بلوک بعدی، از طریق یک فرایند شبه تصادفی انتخاب می‌شود که این انتخاب به دارایی ذخیره شده در کیف پول (یا استخر سهام) مربوط به آن گره بستگی 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 استخراج کنندگان برای حل معمای ریاضی با هدف تأیید تراکنش‌ها و ایجاد بلوک جدید جایزه داده می‌شود، در گواه اثبات سهام این خالق بلوک جدید است که بسته به میزان سرمایه‌اش عایدی کسب می‌کند. قابل ذکر است که در الگوریتم اجماع گواه اثبات سهام برای نقش اعتبارسنج به عنوان تأییدکننده تراکنش‌ها از کلمه فورجر^۱ به جای 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 شدن آنها برای یافتن پاسخ معمای شبکه نیز بیشتر است.

گواه اثبات سهام دارای مزایایی نسبت به گواه اثبات کار است. گواه اثبات سهام قدرت محاسباتی زیادی مصرف نمی‌کند و با ممانعت از ایجاد استخرهای استخراج متمرکز^۲، خطر حملات مخرب را کاهش می‌دهد.

یکی از نقاط ضعف گواه اثبات سهام، در خطر نبودن منبع^۳ است. به این 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 خرج کردن را افزایش دهد.^۱ گواه اثبات سهام چندین زیرگروه نیز دارد. گواه اثبات سهام و کالتی 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 به کار می‌برد، اشاره کرد.

الگوریتم اجماع گواه اثبات سهام و کالتی

گواه اثبات سهام و کالتی یا اعطایی، مدل تغییر یافته 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 به عنوان نماینده انتخاب می‌شوند و در مورد صحت و تأثیرگذاری برخی از شرایط و قوانین تصمیم‌گیری می‌کنند، ضمن این که 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 و کالتی یک الگوریتم اجماع است که برای ایمن‌سازی بلاکچین، توسعه یافته است. این الگوریتم به عنوان 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 و کالتی توسط دنیل لاریمر^۱، مؤسس بیت شیرز^۲ و استیمیت^۳ توسعه یافته است. لاریمر گواه اثبات سهام و کالتی را به عنوان 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 پیاده سازی و نسخه گواه اثبات سهام و کالتی در بیت شیرز اجرا شد. علاوه بر این، گواه اثبات سهام و کالتی طوری برنامه ریزی شده است تا جایگزین مقیاس پذیرتری نسبت به الگوریتم های اجماع سنتی باشد. نمونه های معروف از ارزهای دیجیتال که از گواه اثبات سهام و کالتی استفاده می کنند شامل لیسک، استیم، و یکی چین، بیت شیرز و ای او اس^۴ هستند.

این روش از مزایای زیر برخوردار است:

- کوین های گواه اثبات سهام و کالتی بسیار مقیاس پذیرتر از ارزهای دیجیتال مبتنی بر گواه اثبات کار هستند؛ زیرا این کوین ها به توان محاسباتی زیادی نیاز ندارند و معمولاً برای کاربرانی با تجهیزات ضعیف در دسترس هستند.
- بلاکچین های گواه اثبات سهام و کالتی سریع تر از بلاکچین های مبتنی بر گواه اثبات کار و گواه اثبات سهام هستند.
- کوین های گواه اثبات سهام و کالتی دموکراتیک تر و جامع تر از رقبای خود هستند؛ این الگوریتم در مقایسه با گواه اثبات سهام، قدرت نظارتی بیشتری به کاربران با سهم کمتر در استیکینگ^۵ ارائه می دهد و در مقایسه با گواه اثبات کار به توان محاسباتی زیادی نیاز ندارد. بنابراین از لحاظ مالی به کاربر فشار نمی آورد.
- از آنجایی که الزامات ورود به گواه اثبات سهام و کالتی بسیار کم است، این

1. Daniel Larimer

2. BitShares

3. Steemit

4. Lisk, Steem, Bitshares, EOS

5. Staking

استیکینگ شامل نگهداری دارایی ها 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 به عنوان 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 future is decentralized – the United Nations 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://blocktelegaph.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 دفاتر کل توزیع شده و انواع آن در بخش اول کتاب، در این فصل به انواع محصولاتی که در بستر این فناوری توسعه داده می‌شوند می‌پردازیم. «توکن» واژه عامی است که برای تمامی محصولات بلاکچینی به کار می‌رود 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 دست یافت. در ادامه، تعریف و ویژگی‌های توکن، انواع آن و کاربری‌هایش در اقتصاد حقیقی به صورت 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 «رمزارها» 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 رمزنگاری شده جایگزین موجودیتی شود که دارای ارزش است؛ مانند پول یا دارایی دیجیتال، آنگاه اصطلاح توکن ارزشی^۱ به کار می‌رود. توکن بیت‌کوین تلاشی برای جانشینی ارزش است درست مانند پول. به صورت 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 به عنوان مترادفی برای رمزارز استفاده می شود. البته غالباً این دو عبارت ترکیب شده و اصطلاح توکن رمزارز به کار می رود. به عنوان مثال، واحد محاسبه در بلاکچین بیت کوین، توکن بیت کوین است و واحد محاسبه در بلاکچین اتریوم، توکن اتریوم است.

در رمزارزها یک توکن یا توکن رمزارز، داده توکنایز شده مرتبط با تراکنش هایی است که از طریق اینترنت ارسال و بدون به خطر انداختن داده های حساس ذخیره می شود.

مفهوم توکنایز کردن^۱

توکنایز کردن در عمل برای ده ها سال به عنوان راهی جهت جداسازی داده ها در اکوسیستم هایی مانند بانک های اطلاعاتی بوده است. در این سال ها رمزنگاری با کلیدهای رمزنگاری روش برتری برای محافظت از داده های حساس محسوب می شده است. رمزنگاری یعنی تبدیل داده ها به شکلی که توسط کسانی که کلید رمزگشایی را در اختیار ندارند، غیر قابل خواندن باشد. هدف آن اطمینان از حفظ حریم خصوصی با مخفی کردن اطلاعات از دیگران است. رمزنگاری موارد استفاده مختلفی دارد، از پنهان کردن پیام های خصوصی در برنامه های همتابه همتا گرفته تا انتقال اطلاعات حساس در یک محیط آسیب پذیر.

بنابراین به فرایند محافظت از داده های حساس به وسیله جایگزین کردن آنها با یک عدد که به صورت الگوریتمی تولید شده است، توکنایز کردن می گویند. اغلب اوقات از توکنایز کردن برای جلوگیری از کلاهبرداری در کارت اعتباری استفاده می شود. توکن های کارت اعتباری برای محافظت از داده های حساس مشتریان (مانند شماره کارت اعتباری، آدرس، شماره حساب و غیره) با جایگزین کردن آن با یک سری اعداد و حروف ایجاد شده است که توسط الگوریتم های ریاضی تولید می شوند. توکن ها

خارج از سیستمی که در آن تعریف شده‌اند هیچ معنا و ارزشی ندارند. اما در زیست‌بوم بلاکچین توکن‌ایز کردن به معنای خرد کردن دارایی‌هاست. 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 سرمایه کمتر در برخی دارایی‌ها و پروژه‌های عمرانی سرمایه‌گذاری کنند؛ اما در این روش بستر مناسب فناوری وجود ندارد که در آن معاملات شفاف باشد و قیمت‌گذاری به درستی انجام شود. در بستر 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 دسته‌بندی توکن‌ها وجود دارد که در ادامه براساس دسته‌بندی کاربرد محور این تفکیک انجام می‌شود.

این رویکرد بر مبنای گزارش پژوهشکده پولی و بانکی ایران و براساس مستندات نهاد نظارت بر بازارهای مالی انگلستان^۱ و نهاد نظارت بر بازارهای مالی سوئیس^۲ ارائه شده است. نهاد نظارتی آلمان^۳ نیز بر برخی از جنبه‌های این موضوع تأکید کرده است. این تقسیم‌بندی به صورت شکل ۱ است:

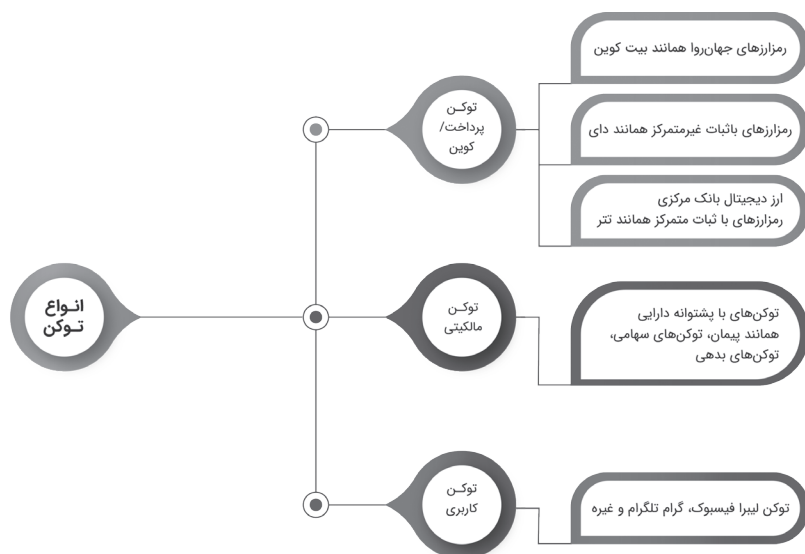
براساس دسته‌بندی اشاره شده، توکن‌ها را می‌توان به سه دسته: پرداخت، بهادار و کاربری تقسیم کرد که در ادامه به صورت تفصیلی توضیح داده می‌شوند. لازم به ذکر است که یکی از اشتباهات مصطلح در ادبیات عرفی این حوزه به مفاهیم توکن و رمزارز برمی‌گردد. باید توجه داشت که توکن، نماینده یک دارایی تأیید شده و دارای ارزش 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^۱ (رمزارز، کوین)

همان‌طور که پیش‌تر اشاره شد، 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 (توکن ارزش یا توکن پول)^۲ نماینده 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

بیت کوین که نماینده یک واحد ارزش بیت کوین است. البته در خصوص بیت کوین تقریباً همه اقتصاددانان معتقدند در حال حاضر کارکرد پول را ندارد و به دلیل محدودیت هایی که دارد در آینده نیز امکان تبدیل شدن به ابزار پرداخت را نخواهد داشت؛ از جمله این محدودیت ها می توان به سرعت پایین تراکنش های قطعی شده (حداقل ۳۰ دقیقه) و کارمزد بالا اشاره کرد. اما توکن هایی همچون لایت کوین، تتر، دای، ریپل و غیره این امکان را دارند که روزی بتوانند به ابزاری برای پرداخت تبدیل شوند. اگر در زمان فعلی رمزارزی مثل بیت کوین جزو توکن پرداخت نام برده می شود، صرفاً یک عبارت عامیانه و غلط مصطلح است و ریشه علمی ندارد.

رمزارزها نوعی توکن ارزش هستند. آنها می توانند جای پول استفاده شوند ولی خودشان ذاتاً ارزشی ندارند. به عبارتی از توکن ها برای نشان دادن دارایی های دیجیتال که قابل تعویض و معامله هستند استفاده می شود.

بنابراین توکن های پرداخت همان رمزارزهایی هستند که نقش ابزار پرداخت یا پول را پیدا می کنند. این توکن ممکن است توسط هیچ نهاد متمرکزی منتشر نشود (مانند DAI) و ممکن است توسط بانک مرکزی منتشر شود. این توکن به عنوان وسیله مبادله، وسیله سنجش و ذخیره ارزش استفاده می شود که با توجه به نوع دسترسی به دفترکل توزیع شده می توان آن را در دو قالب طبقه بندی کرد:

الف) توکن پرداخت در بستر دفترکل توزیع شده عام: می توان گفت این نوع توکن همان رمزارزهای جهان روا همچون لایت کوین است که با استفاده از فناوری رمزنگاری شده طراحی شده و فراتر از مرزهای جغرافیایی در یک شبکه همتا به همتا و به صورت غیر متمرکز فعالیت می کند.

ب) توکن پرداخت در بستر دفترکل توزیع شده خاص: ارز دیجیتال بانک مرکزی را می توان در این طبقه دسته بندی کرد. تفاوت اصلی این دسته با مورد قبلی نوع دسترسی دفترکل توزیع شده آن است. در واقع، مجوز دسترسی در این حالت تنها در اختیار افراد خاص قرار دارد. نمونه ای از این تلاش ها، پروژه جاسپر^۱ کانادا است.

پروژه جاسپر بانک مرکزی کانادا در حال مطالعه روی نوعی ارز دیجیتال بانک مرکزی^۱ است که تناظر یک به یک با دلار کانادا دارد و در شبکه با دسترسی خاص آن، بانک مرکزی کانادا و تعدادی از بانک‌های تجاری این کشور حضور دارند. کدکین برای تسویه بین بانکی و موازی با سامانه تسویه ناخالص آنی^۲ عمل می‌کند (در فصول بعد درباره رمزارز بانک مرکزی توضیحات مفصل‌تری ارائه می‌کنم).

تاریخچه رمزارزها

در سال ۱۹۸۳، دیوید چاوم^۳ نوعی پول دیجیتالی رمزنگاری شده اختراع کرد که ای‌کش^۴ نام داشت. دیوید چاوم بعدها، در سال ۱۹۹۵، پول دیجیتالی دیگری به نام دیجی‌کش^۵ ابداع کرد که روش رمزنگاری آن به گونه‌ای 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^۶ 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 بسازیم: رمزنگاری پول‌های الکترونیکی گمنام»^۷ منتشر شد. تا حدود سال ۲۰۰۹ تمام رمزارزهای موجود به صورت متمرکز بودند و اولین رمزارز یا کوین که به صورت غیرمتمرکز کار می‌کرد، در سال ۲۰۰۹ به وجود آمد که همان بیت‌کوین است. در بلوک پیدایش بیت‌کوین، ساتوشی پیامی نوشت که برای همیشه در تاریخ ثبت شده است. در پارامتر کوین‌بیس^۸، همراه با داده‌های معمول بلوک، پیام زیر که یکی از سرتیترهای نشریه تایمز است درج شد:

نشریه تایمز روز ۳ ژانویه ۲۰۰۹: رئیس خزانه [سلطنتی 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 به عنوان یک برجسب زمانی^۱ درج شده بود تا ثابت کند که بلوک پیش از سوم ژانویه ایجاد نشده بود. با این حال، سریتیر انتخاب شده با علت و هدف اولیه از خلق بیت کوین نیز ارتباط محکمی دارد که طرح آن قصد دارد بیت کوین را جایگزین سیستم پولی و مالی فعلی در جهان کند.

توسعه دهندگان بیت کوین مبانی فلسفی شکل گیری این رمزارز را به مکتب اقتصاد اتریشی^۲ و فلسفه آزادی خواهی^۳ نسبت می دهند. مکتب اقتصاد اتریشی توسط افرادی مثل «کارل منگر»^۴ و «لودویگ فن میزس»^۵ پایه گذاری شد. به طور کلی اقتصاددانان پیرو این مکتب مخالف حضور بانک‌های مرکزی و مؤسسات دولتی در کنترل اقتصاد هستند. آنها همچنین معتقدند که منشأ تمام کنش‌های اقتصادی فرد (و نه جمع) است. از همین رو سنج‌های اقتصادی نمی‌توانند روی تصمیم‌گیری شخصی افراد اثر بگذارند.

یکی دیگر از اصول اقتصاد اتریشی بحث نهایی‌گرایی^۶ 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 آزادی خواهی یا اختیارگرایی حول این باور شکل گرفته است که آزادی عمل باید در تمام شئون زندگی به افراد داده شود. امروزه اندیشه‌های آزادی خواهانه با ایدئولوژی‌های سیاسی آمیخته شده و شاخه‌های مختلفی از آن شکل گرفته است.

مکاتب مذکور سیستم‌های غیرمتمرکز را ترویج می‌کنند و بیت کوین نمونه یک سیستم مالی غیرمتمرکز است که در آن نیازی به نقش آفرینی دولت‌ها و بانک‌ها نیست. به علاوه هم اقتصاد اتریشی و هم فلسفه آزادی فردی تأکید می‌کنند که بیت کوین 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 بیت کوین تاکنون مسیری طولانی طی کرده‌اند. به عنوان یک سیستم پرداخت همتا به همتا شروع به کار و مجموعه‌ای از موارد کاربری را ایجاد کرده‌اند که بسیار فراتر از نقش اولیه رمزارز یعنی انتقال پول است. در حالی که عملکرد اصلی رمزارزها مانند اتریوم و بیت کوین بحث برانگیز است، بی شک 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^۱ را نشان می‌دهد.

رمزارزها همچنان در حال اثبات قابلیت‌های کاربردی خود هستند. در سال‌های آتی، رمزارزها در حال انجام کارهایی هستند که هنوز پیش‌بینی نشده 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 بیت کوین را متوقف کنند. شرایط نامناسب بیت کوین برای پرداخت‌های با هزینه پایین در اواسط سال ۲۰۱۷ باعث شد بیت کوین کش^۲ به عنوان یک انشعاب از بیت کوین آغاز به کار کند. شبکه بیت کوین کش از آن زمان آرمان خود را برای تسهیل پرداخت سریع و کم هزینه، با کمک صدها کسب و کار که بیت کوین کش را در فروشگاه و به صورت آنلاین پذیرش می‌کردند، حفظ کرده است.

- **ذخیره ارزش:** ارزها و شبکه‌هایی که به عنوان شکل جدید ارز بومی کمیاب و همچنین وسیله تسویه حساب استفاده می‌شوند؛ مانند بیت کوین و لایت کوین.
- **پول برنامه پذیر^۳:** قراردادهای هوشمند^۴ در واقع قدیمی‌تر از بیت کوین 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. آراس کی^۱ بستر قراردادی هوشمندی را ابداع کرده که بر روی امنیت بلاکچین بیت کوین و تأثیرات شبکه آن سرمایه‌گذاری کرده است. با افزایش تسلط بیت کوین^۲ بر رمزارزهای دیگر یا همان آلت کوین‌ها، جذابیت ساخت رمزارز بر بستر بیت کوین در مقابل گزینه‌های کمتر غیرمتمرکز مانند ترون^۳ نیز افزایش یافته است. در نتیجه، توسعه‌دهندگانی که قبلاً به سمت بلاکچین به اصطلاح «نسل دوم» رفته بودند، به بیت کوین نگاهی کاملاً جدید دارند. در مورد شبکه بیت کوین کش، پروتکل دفترکل ساده^۴، صدور توکن‌های فرعی را (با استفاده از کدهای رمزگذاری شده‌ای که از ابتدا در پروتکل بیت کوین 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^۵.

• **حریم خصوصی:** تراکنش‌های دیجیتالی خصوصی، مانند ویژگی ناشناس بودن که برخی رمزارزها ارائه می‌دهند؛ مانند مونرو، ورج و زی کش^۶.

• **مالکیت دیجیتال:** روش نوینی در کنترل کردن، انبار کردن و کسب درآمد از اطلاعات را شکل می‌دهد؛ مانند سیبا، بت و گلم^۷.

• **کاربری‌های غیرمتمرکز:** شبکه‌ها، محصولات و خدمات فعال شده توسط رمزارزها با قابلیت تبادل بین دارایی‌های صادرشده روی شبکه (بازارهای پیش‌بینی‌کننده، تبادلات ارز، تسویه حساب)؛ مانند اینترنت غیرمتمرکز (اتریوم)، قراردادهای هوشمند یا قراردادهای سفارشی خودصادرشونده (نئو^۸) و دیگر خدمات رمزارزی (فاکتوم و نیم کوین^۹).

1. RSK: Rootstock

2. Bitcoin dominance

3. Tron

4. Simple Ledger Protocol

5. Dai

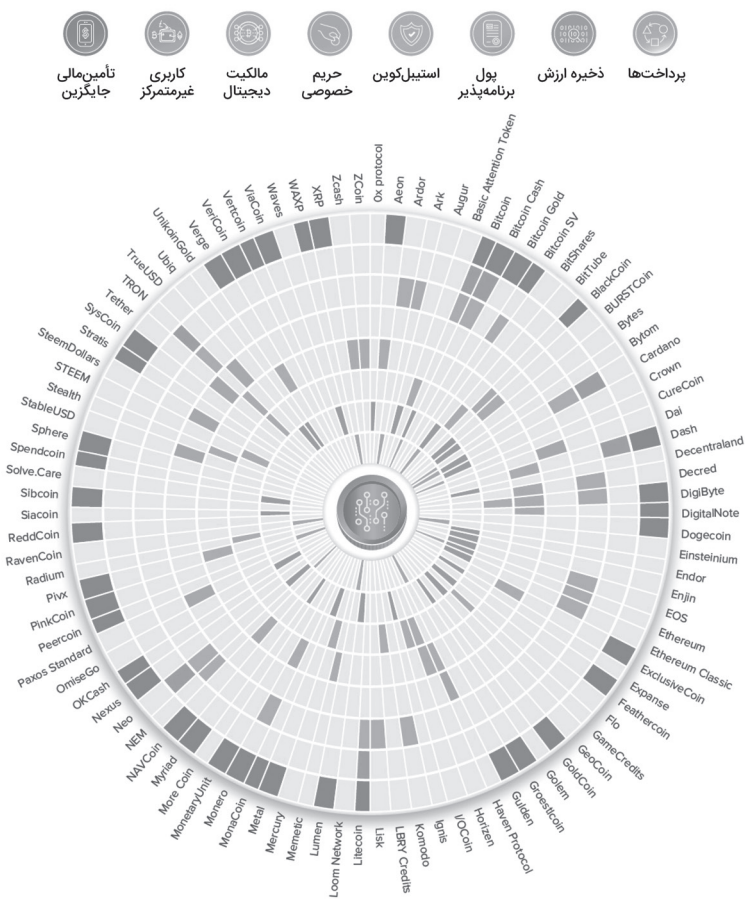
6. Monero, Verge, Zcash

7. Sia, BAT, Golem

8. NEO

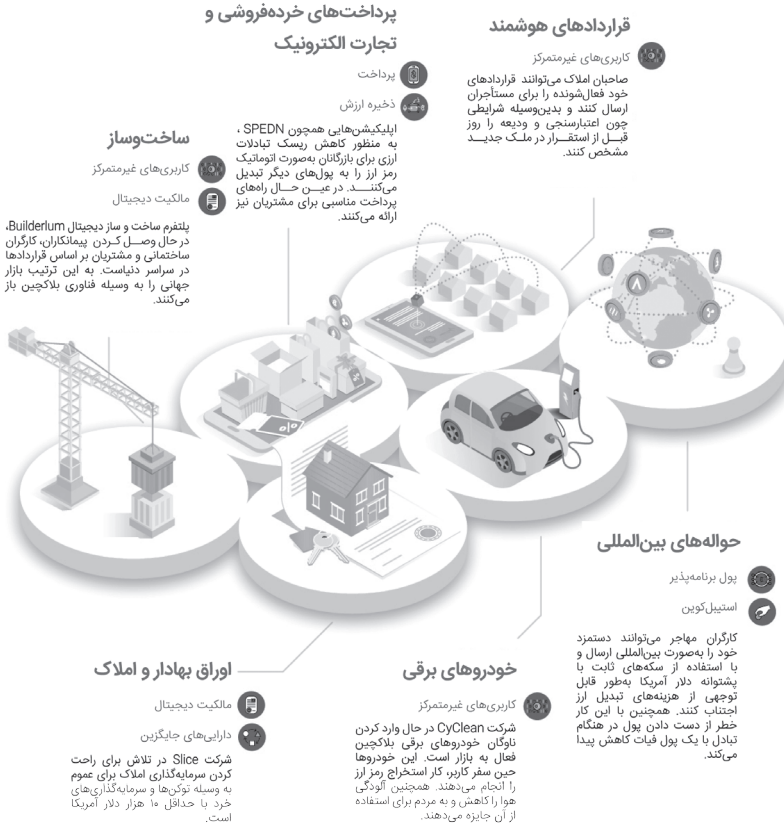
9. Namecoin, Factom

- **تأمین مالی جایگزین:** به روش های تأمین مالی گفته می شود که خارج از سیستم نهادهای بازار پول و سرمایه طراحی شده اند مثل تأمین مالی از طریق عرضه اولیه سکه.
- کاربردهایی که هریک از رمز ارزهای امروزی دارند و ارتباط آنها را با یکدیگر در این اکوسیستم در شکل ۲ طبقه بندی کرده ام.



شکل ۲: طبقه بندی رمزارزها

چند مورد از راهکارهایی را که رمازرها برای چالش‌های امروزی ارائه می‌دهند در شکل ۳ می‌توان مشاهده کرد.



شکل ۳: راهکار رمزارزها در پاسخ به چالش‌های روزمره

بررسی ریپل به عنوان توکن پرداخت

ریپل شرکت بزرگی واقع در سانفرانسیسکو، آمریکا است که برای بانک‌ها و نهادهای مالی، محصولات مالی را غیر متمرکز می‌سازد. هدف ریپل این است که بتواند

انتقال پول بین بانکی و بین‌المللی را سریع‌تر، ارزان‌تر و غیرمتمرکز کند. البته این هدف تا حدودی محقق شده است و اکنون بانک‌ها و شرکت‌های مالی بزرگی برای انجام انتقال‌های پولی خود از محصولات ریپل استفاده می‌کنند.

ریپل محصولات گوناگون برای بانک‌ها و مؤسسات مالی طراحی کرده است که فقط یکی از آنها با ارز دیجیتال ایکس‌آرپی^۱ کار می‌کند. بنابراین، با خرید ایکس‌آرپی، می‌توان روی یکی از محصولات شرکت ریپل سرمایه‌گذاری کرد نه خود ریپل.

ریپل می‌خواهد یک شبکه پرداخت و ارتباطی امن و غیرمتمرکز برای مؤسسات مالی سراسر جهان فراهم کند. می‌توان گفت که هدف ریپل کاملاً در تضاد با بیت‌کوین است.

در حالی که بیت‌کوین با هدف تراکنش‌های همتا به همتا و حذف واسطه‌ها و بانک‌ها روی کار آمده است، طراح ریپل عقیده دارد بانک‌ها به خودی خود بد نیستند و فقط نحوه انجام کار آنهاست که باعث ایجاد مشکلات می‌شود.

ریپل قصد دارد با عرضه محصولات بانکی غیرمتمرکز، مشکل تبادلات بین‌المللی پول در جهان را حل کند. سالانه بیش از ۱۵۵ هزار میلیارد دلار پول به صورت برون‌مرزی در سراسر جهان جابه‌جا می‌شود. مشکلات انتقال پول توسط بانک‌ها و مؤسسات مالی سال‌هاست حل نشده باقی مانده است و با توجه به رشد فناوری، هنوز انتقال بین‌المللی پول‌های کلان بین ۳ تا ۷ روز طول می‌کشد که در نتیجه نیازمند کارمزدهای بسیار بالا و انجام کاغذبازی‌های زیادی است. ریپل می‌خواهد به این مشکلات برای همیشه پایان بخشد و حجم بزرگی از انتقالات پول را انجام دهد.

ریپل رقیب جدی برای سوئیفت است. مزیت ریپل نسبت به سوئیفت، غیرمتمرکز بودن و سرعت بالای تراکنش‌هاست. استلار^۲ را هم می‌توان یکی دیگر از رقبای ریپل در فضای فناوری بلاکچین دانست.

در حال حاضر شرکت ریپل سه محصول اصلی برای بانک‌ها و مؤسسات مالی دارد که عبارتند از:

1. XRP
2. Stellar

- ایکس کارنت^۱
- ایکس ریپید^۲
- ایکس ویا^۳

این‌ها در حال حاضر سه محصول اصلی شرکت ریپل هستند که تحت عنوان یک نام جامع به نام ریپل نت^۴ قرار دارند.

بسیاری از منتقدان ریپل بر این عقیده هستند که این شرکت و ارز دیجیتال آن؛ ایکس آرپی غیر متمرکز نیست و نمی‌تواند در دسته رمزارزها قرار گیرد. با این حال این شرکت مدعی است که تمرکز و کنترل خاصی بر روی محصولات خود ندارد.

با این که تعداد گره‌ها در دفترکل ریپل بسیار کم است، اما هر فردی می‌تواند به عنوان گره که در اجماع ریپل به آن سرور^۵ گفته می‌شود فعالیت کند. البته سرور شدن در ریپل مجموعه شرایطی خاص دارد، اما به هر حال همه می‌توانند به صورت مستقیم به دفترکل متصل شوند. اصل کار تأیید تراکنش‌ها توسط گره‌هایی خاص که به «لیست گره‌های منحصر به فرد»^۶ شهرت دارند، انجام می‌پذیرد. زمانی که ۸۰ درصد گره‌های اعتبار سنج، اعتبار یک تراکنش را پذیرفتند، تراکنش تأیید می‌شود.

ریپل بارها اعلام کرده که به دنبال افزایش تعداد گره‌های اعتبار سنج است تا به تمرکززدایی بیشتر شبکه کمک کند. پروتکل دفترکل ریپل، متن‌باز و دارای یک سری قواعد خاص است که هر کس برای استفاده از آن باید قوانین مربوطه را بپذیرد. بنابراین از نظر تئوری، در صورت نابود شدن شرکت ریپل، دفترکل ریپل و ارز دیجیتال ایکس آرپی به کار خود ادامه می‌دهند. با این حال، اگر شرکت ریپل از بین برود، قطعاً تأثیرات بسیار زیادی روی قیمت و کاربردپذیری ایکس آرپی خواهد گذاشت.

در نهایت می‌توان گفت که ریپل تقریباً یک شبکه نیمه متمرکز و غیر شفاف است و

1. xCurrent
 2. xRapid
 3. xVia
 4. RippleNet
 5. Server
 6. Unique Node Lists

هنوز نمی‌توان به‌طور قطع غیر متمرکز بودن آن را تأیید کرد. از سوی دیگر شاید بتوان گفت که ریپل برای رسیدن به اهداف خود چندان نیازمند غیر متمرکز بودن نیست. ریپل برای شرکت‌های بزرگ ساخته شده است و با اینکه برای مصارف پرداخت هم‌تابه هم‌تا نیز از آن استفاده می‌شود، اما تمرکز اصلی ریپل این مسئله نیست. هدف اصلی پلتفرم ریپل انتقال پول در حجم بالا در سرتاسر جهان با سریع‌ترین زمان ممکن است. تاکنون، ریپل از زمان انتشارش با بیش از ۳۵ میلیون تراکنش پردازش شده بدون مشکل، همچنان پایدار باقی مانده است. این پلتفرم قادر به انجام ۱۵۰۰ تراکنش در ثانیه است و همچنان قصد دارد به اندازه ویزا^۱ یعنی ۵۰,۰۰۰ تراکنش در ثانیه برسد. درحالی‌که، بیت‌کوین می‌تواند حداکثر ۶ و اتریوم ۱۵ تراکنش در ثانیه را هدایت کنند. ایکس‌آرپی خلاف بیت‌کوین، اتریوم، لایت‌کوین و بسیاری دیگر از رمزارزها استخراج نمی‌شود. ایکس‌آرپی به صورت از قبل استخراج شده^۲ در همان ابتدای کار به تعداد ۱۰۰ میلیارد کوین منتشر شد.

۲. توکن اوراق بهادار^۳

توکن اوراق بهادار نماینده یک دارایی بهادار مانند اوراق بدهی، سهام یا مالکیت از طرف ناشر آن است. توکن اوراق بهادار، نوعی ابزار مالی محسوب می‌شود که دارای ارزش است و می‌توان آن را معامله کرد. بسیاری از ابزارهای مالی که امروزه وجود دارند، مانند برگه سهام یا اوراق قرضه می‌توانند به‌صورت توکن بهادار معامله شوند. این نوع توکن حتماً پشتوانه دارایی (مشهود یا غیرمشهود، مجازی یا واقعی) دارد و می‌توان با نگهداری آنها انتظار بازده سرمایه‌گذاری و منفعت نیز داشت. نمونه‌ای از این نوع توکن، توکن وان‌گرم^۴ است که هر توکن نماینده یک گرم طلاست. توکن بهادار نیز همانند سایر توکن‌ها، بر بستر بلاکچین منتشر می‌شود و دارای

1. Visa
2. Pre-mined
3. Security token
4. OneGram

حقوق مشخصی از سهام شرکت‌ها یا دارایی‌های واقعی است. این توکن‌ها می‌توانند از طریق مراکزی نظیر کسب‌وکارها یا دولت‌ها منتشر شوند و همانند دیگر همتایان فعلی و سنتی خود مانند سهام یا اوراق قرضه عمل کنند.

طرفداران توکن‌های بهادار ادعا می‌کنند، این مفهوم را می‌توان با انقلاب مالی برابر دانست. در واقع توکن بهادار می‌تواند مشکلات متعدد تبادل دارایی و خرید و فروش سهام را تا حد زیادی کاهش دهد. به علاوه می‌تواند مفاهیم نامشهود مانند مالکیت معنوی را به اوراق بهادار تبدیل کند همانند توکن‌های غیرمثلی^۱.

زمانی که شرکت‌ها از عرضه اولیه سکه به عنوان الگوی تجاری استفاده و تعدادی توکن تولید و عرضه کردند، امید داشتند به دلیل قدرت و محبوبیت بستر توکن تولید شده در سطح بین‌المللی، به مقبولیت، کارایی و ارزش پیشنهادی مدنظر خود برسند. با قدرت گرفتن این ارزش پیشنهادی، کسب‌وکارها و سرمایه‌گذاران به استفاده از توکن به عنوان پول ترغیب شدند. این مکانیزم سرمایه‌گذاری، به عنوان نسخه بدیلی از مدل «عرضه اولیه عمومی»^۲، توجه همگان را به خود جلب کرد.

از دوران بحران اقتصادی سال ۲۰۰۸، بازپرداخت و سوددهی روش‌های سنتی سرمایه‌گذاری همچون اوراق بهادار، برای سرمایه‌گذاران به اندازه کافی جذاب نبود؛ به همین دلیل، مفاهیم عرضه اولیه سکه و توکن بهادار بیش از مفاهیم سنتی طرفدار پیدا کردند. عرضه توکن بهادار دقیقاً پس از دوران اوج عرضه اولیه سکه ظهور کرد. در واقع از سال‌های ۲۰۱۶ تا ۲۰۱۸، با اوج‌گیری مفاهیم عرضه اولیه سکه، سرمایه‌گذاران متعدد برای ورود به این سبک از سرمایه‌گذاری تلاش می‌کنند.

به علاوه در کشورهایی همچون آمریکا، هزینه‌های صدور اوراق بهادار و موارد مشابه به دلیل تنظیم‌گری‌های متعدد افزایش یافت. به هر حال، همه این موارد در کنار افزایش افراد علاقمند به سرمایه‌گذاری سبب استقبال از روش‌های جدید سرمایه‌گذاری شد.

1. Non Fungible Token (NFT)
2. Initial Public Offerings (IPO)

اوراق استاندارد در مقایسه با اوراق توکنایز شده

به توکن بهادار همچون اوراق استاندارد خریداری شده از یک شرکت فکر کنید، با این تفاوت که اوراق مورد نظر به شکل توکن است. برای درک بهتر، فرض کنید شما سهام یک شرکت را در عرضه اولیه عمومی یا در بورس سهام خریده‌اید و پس از آن، سهام مذکور به حساب شما تخصیص داده می‌شود. سهام توکنایز شده و سهام استاندارد به صورت یکسان کار می‌کنند، با این تفاوت که سهام توکنایز شده شکل دیجیتالی اوراق (توکن‌ها) هستند و به جای اینکه وارد حساب متمرکز شما شوند، به حساب بلاکچینی شما اعتبار می‌بخشند.

روش‌های سنتی افزایش سرمایه چند مشکل عملیاتی دارد. به عنوان مثال، الزامات نظارتی مانند حسابرسی منظم و پایبندی به قوانین سختگیرانه بورس اوراق بهادار، عدم تمایل بخشی از بانک‌ها و دیگر مؤسسات مالی به اعتباردهی و چالش‌های پیش روی صاحبان کسب و کار در متقاعد کردن سرمایه‌گذاران خصوصی برای خرید سهام و عدم دسترسی به بازار بین‌المللی برخی از این مشکلات و محدودیت‌ها هستند.

در مقابل، عرضه مالکیت تجاری به شکل توکن بر بستر بلاکچین انعطاف‌پذیری زیادی در جمع‌آوری سرمایه دارد. این روش کم‌هزینه، راهکار دموکراتیک‌تری برای ارزش‌گذاری واقع‌گرایانه معاملات متناسب با مشارکت مستقیم سرمایه‌گذاران ارائه می‌دهد. زیرا ارزش‌گذاری عمدتاً به نیروهای بازار وابسته است تا به گروه منتخب حامیان مالی یا سرمایه‌گذار فرشته^۱.

اوراق بهادار قابل انتقال هستند، از طرفی انتقال اوراق متعارف شامل تشریفات خاصی است که معاملات در دنیای دیجیتال را پیچیده می‌کند. به طور معمول، انتقال اوراق بهادار نیاز به یک ابزار نوشته شده (و گاهی اوقات تحویل گواهی فیزیکی) یا به‌کار و بستن‌کار کردن حساب‌های اوراق بهادار نگهداری شده توسط اتاق پایپای

1. Angel Investors

سرمایه‌گذاری است که سرمایه یک یا چند شرکت نوپا را فراهم می‌کند. خلاف یک شریک، سرمایه‌گذار فرشته به ندرت در مدیریت شرکت دخالت می‌کند.

یا دیگر متصدیان دارد. توکنایز کردن به صورت الکترونیکی، فرایند ساده‌ای را فراهم می‌کند که بدون امضای سند، مشارکت بانک یا دیگر واسطه‌ها امکان‌پذیر باشد.

مزایای توکن بهادار

از جمله مزایای توکن بهادار به عوامل زیر می‌توان اشاره کرد:

- **بهبود اقتصاد سنتی:** تراکنش‌های مالی به روش سنتی عموماً گران هستند. با وجود واسطه‌ها و کارمزدها نیز طبیعتاً هزینه‌ها بالاتر خواهد رفت. توکن‌های بهادار می‌توانند دست واسطه‌ها را کوتاه کنند و در نهایت موجب کاهش کارمزدها شوند. با استفاده از قراردادهای هوشمند نیز می‌توان، پیچیدگی، هزینه و کارهای اداری تسویه و پایاپای را کاهش داد.
- **مدیریت کردن:** امکان مدیریت فعالیت‌ها روی بلاکچین و تأمین توکن، خدمات و اقدامات شرکتی وجود دارد.
- **سرعت بخشیدن به امور:** بلاکچین این امکان را فراهم می‌کند که زمان خرید و فروش کاهش یابد. مؤسسات مالی سنتی، درگیر تعداد زیادی واسطه هستند که موجب کندی عملکرد آنها می‌شوند. توکن‌های بهادار با حذف این واسطه‌ها عملیات عرضه اوراق را سرعت می‌بخشند. با بالا رفتن سرعت، توکن‌های بهادار می‌توانند به یکی از روش‌های سرمایه‌گذاری محبوب تبدیل شوند. البته طبیعی است که حذف واسطه‌ها و افزایش سرعت، ریسک‌ها و پیامدهای منفی نیز با خود به همراه دارد که برای تصمیم‌گیری به منظور استفاده از این فناوری باید مدنظر قرار گیرد.
- **ایجاد بازار آزاد:** نسل جدیدی از سرمایه‌گذاران از طریق ماهیت جهانی بلاکچین جذب می‌شوند. با استفاده از توکن‌های بهادار، تجار می‌توانند محصولات و خدمات خود را در بستر اینترنت ارائه دهند.
- **افزایش سرمایه‌گذاران:** از آنجایی که معامله‌گران می‌توانند با هر فردی در بستر اینترنت معامله کنند، تعداد سرمایه‌گذاران نیز با وجود چنین بازاری

به صورت نمایی افزایش می یابد.



شکل ۴: مزایای توکن بهادار

- **کاهش نیاز به وکلا:** در آینده، قراردادهای هوشمند طیف گسترده ای از عملکردهای مربوط به توکن های بهادار را عملیاتی خواهند کرد. همین مسئله، نیاز به وکلا را که خود واسطه هایی بالقوه هستند کاهش می دهد. صلاحیت صدور و توزیع و ساختار بندی ابزارهای مالی نیز با استفاده از پروتکل های شبکه تضمین می شود.

- **جلوگیری از دستکاری های احتمالی مؤسسات:** از آن جهت که واسطه ها تا حد زیادی از بین می روند، امکان دستکاری و فساد در مؤسسات مالی نیز به شدت کاهش می یابد و شاید بتوان گفت در روند سرمایه گذاری نشانی از فساد دیده نخواهد شد. در مقابل چون افراد در این شبکه توسط هیچ نهادی تأیید نشده اند، امکان تخلف توسط هر یک از آنها که هویت ناشناسی نیز دارند افزایش می یابد.

- قابلیت تهاتر آسان توکن‌ها با یکدیگر: تبادلات ثانویه به وسیله توکن‌های بهادار می‌تواند به راحتی و به واسطه توکن‌های ثبت شده و قانونمند در پلتفرم‌های مربوطه انجام شود.

چالش‌های توکنایز کردن اوراق بهادار

حذف واسطه‌ها مزیت بزرگی محسوب می‌شود؛ اما نمی‌توان هم واسطه‌ها را حذف کرد و هم مزایایی را که ایجاد می‌کردند نگه داشت. یکی از این مشکلات قراردادن بار مسئولیت معامله بر دوش خریدار یا فروشنده است. یک واسطه، به عنوان مثال یک مؤسسه مالی، تأثیرات مثبتی بر یک اکوسیستم می‌گذارد. تعهد، تبلیغات پیرامون محصول، تحقق خواسته‌های سرمایه‌گذار، تضمین امنیت سرمایه‌گذاری و پیروی از قوانین از جمله تأثیرات مثبتی است که توسط یک واسطه ایجاد می‌شوند. تا جایی که برخی از منتقدین معتقدند بلاکچین از عهده مسئولیت‌هایی که پیش‌تر بر عهده واسطه‌ها و مؤسسات بوده بر نمی‌آیند.

پژوهش‌ها نشان می‌دهد که توکن‌های بهادار در کسب نتایج مورد انتظار موفق نبوده‌اند. در سطح جهانی، تعداد معدودی توکن بهادار در سال گذشته صادر شدند. کارشناسان به مشکلات مختلفی اشاره کردند از جمله:

- در برخی حوزه‌های قضایی و حقوقی، امکان ارائه یک سهم به صورت الکترونیکی وجود ندارد. این که این امر امکان‌پذیر باشد، به قوانین محلی (کشوری) مربوط به نوع خاصی از شرکت که به دنبال صدور توکن بهادار است بستگی دارد.
- سرمایه‌گذاران عمده لازم است اطمینان حاصل کنند که از تمامی قوانین و مقررات پیروی خواهند کرد.
- بسیاری از سرمایه‌گذاران خواهان حریم خصوصی هستند. آنها به بلاکچین اعتماد ندارند؛ زیرا به دیگر افراد این امکان را می‌دهد تا سرمایه‌گذاری‌ها و ارزش تراکنش‌های آنها را رصد کنند.
- برخی سرمایه‌گذاران تمایل ندارند سهام‌های آنها توسط یک کلید خصوصی

بر بستر بلاکچین کنترل شود.

- قوانین نظارتی همچنان به عنوان معضلی برای ناشران توکن های بهادار مسئولیت ایجاد می کند.
- یک مشکل اساسی برای ناشران توکن های بهادار وجود دارد. لازم است هنگام صدور توکن به صورت عمومی، مستندات عمومی ایجاد و بایگانی شوند. برای مثال، در انگلستان و اروپا، این نیازمندی ها و قوانین صدور بسیار مهم هستند و در صورت عدم تطابق با قوانین مربوطه جرائم سنگین در نظر گرفته شده است. شرکت های بزرگ بین المللی ملزم به ارائه سوابق اطلاعات مالی هستند. این امر برای آنها بسیار پر مسئولیت و نگران کننده و قطعاً برای یک استارت آپ دشوارتر است.
- چنانچه کلید عمومی یا خصوصی گم شود، امکان بازیابی آن وجود ندارد و سرمایه موجود در حساب از دست می رود.

ضوابط به کارگیری توکن های بهادار

برای اینکه یک توکن بهادار قابل مبادله باشد؛ در ابتدا باید تعریف شده باشد، سپس مطابق محدودیت های نظارتی ایجاد شود تا با قوانین تجارت برای اشخاص ذی نفع مانند سرمایه گذاران، واسطه ها و نگهدارندگان آن تطابق داشته باشد. مشارکت کنندگان باید از قوانین مختلفی مانند قوانین مبارزه با پولشویی و شناخت مشتریان^۱ و تأییدیه سرمایه گذار معتبر^۲ پیروی کنند. علاوه بر این لازم است مجوز افرادی که قصد استفاده از توکن های بهادار را دارند از طریق قراردادهای هوشمند بررسی و به آنها پاسخ مناسب داده شود. اگر کاربری که سطح تطابق لازم را ندارد تلاش کند توکنی را خریداری کند، قرارداد هوشمند متناظر آن به مقایسه سطح مجوز وی در پایگاه داده داخلی اقدام می کند و به سرعت حساب کاربری وی را نسبت به تکمیل خرید مسدود می سازد.

1. Know Your Customer (KYC) & Anti-Money Laundry (AML)

2. Accredited Investor Verification

بسیاری از توکن‌های بهادار بر بستر اتریوم منتشر می‌شوند. یکی از بسترهایی که توکن‌های بهادار روی آن صادر می‌شود، پروتکل ERC-20^۱ است که برای شبکه اتریوم تعریف شده است. این پروتکل شامل قوانین و استانداردهایی است که باید به‌منظور انتشار توکن‌ها بر بستر شبکه رعایت شوند. نیازمندی‌هایی که در این پروتکل لحاظ شده‌اند با قراردادهای هوشمند نیز یکپارچه هستند. در این پروتکل، فهرستی از قوانین عمومی وجود دارد که در آن به چگونگی انتقال توکن‌ها، تأیید تراکنش‌ها، نحوه دسترسی کاربران به داده‌های یک توکن و تأمین توکن‌ها اشاره شده است.

طبقه‌بندی توکن بهادار به عنوان ابزار بدهی یا ابزار مالکیت

طبق کلیات استاندارد بین‌المللی حسابداری ابزارهای مالی^۲ (IAS32)، هر ابزار مالی باید به عنوان ابزار بدهی یا ابزار مالکیت طبقه‌بندی شود. در این راستا هر نوع توکن باید به دقت بررسی شود تا در طبقه مناسب خود قرار گیرد.

الف) خصوصیات ابزار مالکیت (سهام): مطابق استاندارد مطرح شده، چنانچه هیچ تعهدی برای پرداخت پول یا تحویل دارایی به نهادی دیگر وجود نداشته باشد، ناشر این ابزار مالی را ابزار مالکیت معرفی می‌کند. به عبارتی ابزار سهام، قراردادی است که سود باقیمانده دارایی یک نهاد را بعد از کسر همه بدهی^۳‌هایش نشان می‌دهد. ویژگی‌های دیگری که نشان‌دهنده یک ابزار سهام است شامل موارد زیر می‌شود:

- تاریخ انقضا ندارد.
- سود آن مشارکتی است.

توکن سهامی، به ایجاد و صدور توکن دیجیتال اشاره دارد که نشان‌دهنده سهام سهامداران در یک شرکت یا سازمان است. کسب و کارها با پذیرش رو به رشد بلاکچین، به راحتی می‌توانند خود را با نسخه دیجیتالی شده سهام تطبیق دهند. توکن‌های سهامی به عنوان روشی مناسب جهت افزایش سرمایه در حال ظهور است

1. Ethereum Request for Comments
 2. International Accounting Standards
 3. Liabilities

که در آن سهام یک کسب و کار به شکل دارایی‌های دیجیتال وجود دارد. **ب) خصوصیات ابزار بدهی:** مطابق با استاندارد IAS32، تعهدات مالی^۱ عبارت است از هرگونه مسئولیت قراردادی جهت تحویل وجه یا دارایی مالی به نهادی دیگر یا مبادله ابزارهای مالی با یک نهاد دیگر در شرایطی که به‌طور بالقوه به نفع سازمان نیست.

نکته مهم در ویژگی برجسته ابزارهای بدهی این است که ناشر نمی‌تواند از تعهدات خود شامل پرداخت پول یا ارائه دارایی در قرارداد سر باز زند (مگر تحت شرایط معین). ویژگی‌های دیگر مربوط به اوراق قرضه عبارت است از:

- دوره عمر محدود است؛
- دارنده ابزار، اختیار بازخرید دارد؛
- در صورت پیشامدهای احتمالی آینده که خارج از کنترل ناشر و دارنده است، گزینه بازخرید وجود خواهد داشت؛
- بازدهی ثابت و معین است.

توکن بدهی به تعهدات توکن شده‌ای گفته می‌شود که نشان‌دهنده بدهی ناشر مانند وام مسکن یا اوراق قرضه است. به‌صورت معمول توکن بدهی دو شاخصه مهم دارد که آن را از سایر توکن‌های بهادار متمایز می‌سازد:

- **سود:** به‌صورت کلی توکن بدهی به‌گونه‌ای طراحی می‌شود که سودی مشخص و تضمین شده براساس پرداخت اولیه که برای آن انجام شده را به دارنده خود بپردازد.

- **ریسک:** توکن اوراق بدهی غالباً فاقد ریسک نوسانات قیمتی برای سرمایه‌گذاران است؛ اما دارای ریسک‌های ناشی از عملکرد ناشر است که شاید منجر به نکول طلب سرمایه‌گذاران شود همانند ریسک ورشکستگی ناشر. ویژگی‌های فوق می‌تواند تأثیر زیادی بر نحوه قیمت‌گذاری ابزار بدهی بگذارد و به

همین دلیل از اهمیت زیادی برخوردارند. به منظور بررسی نحوه و میزان تأثیر ریسک و سود اوراق در قیمت گذاری آن باید از مدل سازی کمک گرفت. در بلاکچین، از قراردادهای هوشمندی استفاده می شود که دارای عملگرهایی از قبیل نحوه شرایط بازپرداخت و ریسک های موجود در شرکت هستند که خود مشخص کننده سود اوراق است.

بازدهی برای سرمایه گذاران

الف) توکن بهادار به عنوان ابزار مالکیت (سهام)

همان طور که اشاره شد، مدیران شرکت ناشر سهام می توانند در صورت صلاح دید سود حاصل را بین دارندگان توکن توزیع کنند. از طرف دیگر سرمایه گذاران از افزایش قیمت توکن (عایدی سرمایه ای)^۱ نیز سود کسب می کنند.

ب) توکن بهادار به عنوان ابزار بدهی

در توکن بدهی، ناشر موظف به پرداخت مبالغ تعهد شده در زمان های معین به دارندگان توکن است و از این طریق برای سرمایه گذاران بازدهی کسب می شود و از طرف دیگر در هزینه های مالی ناشر ثبت می شود.

بازخرید نهایی توکن های بهادار

الف) توکن اوراق به عنوان ابزار مالکیت (سهام)

یکی از ویژگی های اصلی ابزارهای سهام، غیرقابل بازخرید بودن و نداشتن تاریخ انقضا است؛ اما بازخرید سهام ممکن است به اختیار شرکت ناشر صورت گیرد، به خصوص اگر شرکت ناشر فعالیت خود را متوقف کند یا پروژه را خاتمه دهد. در چنین مواردی، شرکت هایی که تعهدات محدود دارند معمولاً اعلام ورشکستگی می کنند، کلیه دارایی ها را نقد و با طلبکاران تسویه حساب می کنند. چنانچه سود مازادی باقی ماند، بین سهامداران تقسیم می شود.

1. Capital Gain

ب) توکن اوراق به عنوان ابزار بدهی

یک تعهد مالی هنگامی اعتبار خود را از دست می‌دهد که تعهدات مندرج در قرارداد آن فسخ یا منقضی شده باشد. یکی از ویژگی‌های اصلی ابزار بدهی عمر محدود آن است که در زمان نشر ابزار بدهی تعیین شده است.

بنابراین، پس از بازخرید، شرکت ناشر مکلف به تسویه تعهد ناشی از عرضه آن توکن است و بسته به قوانین مندرج در سپیدنامه، بازخرید نهایی ممکن است به صورت ثابت یا قیمت متغیر باشد (به عنوان مثال ارزش بازار توکن).

نمونه‌ای از توکن بدهی

شرکت فناوری مالی نیوارا^۱ اولین شرکتی است که انتشار اوراق توکنایز شده را در سندباکس سازمان نظارتی امور مالی انگلیس اجرا کرد. نیوارا توانست اوراق قرضه اسمی مبتنی بر اتریوم را بر یک زیرساخت بلاکچین عمومی با استفاده از سندباکس تنظیم‌گری منتشر، تسویه و ثبت کند.

این پروژه شامل انتشار دو نوع اوراق قرضه می‌شود: اوراق قرضه کنترل‌ی که مدلی برای توکنایز کردن پول فیات^۲ فراهم کرد و اوراق قرضه آزمایشی که اولین رمزارز اوراق قرضه بود که روی یک بلاکچین عمومی باز با استفاده از قراردادهای هوشمند به طور کامل تسویه شد. اوراق کنترل‌ی اوراق قرضه مبتنی بر پوند انگلیس^۳ بود که به عنوان اوراق قرضه یورو خصوصی از طریق سیستم‌های سنتی تسویه شد. اوراق قرضه آزمایشی، اوراق قرضه اسمی مبتنی بر اتریوم بود که به طور کامل بر بلاکچین عمومی باز ثبت و تسویه شد.

در فاز اول پروژه، شرکت نیوارا فرایند انتشار معمولی برای ابزار بدهی کوتاه مدت را با استفاده از دفترکل توزیع شده رونمایی کرد که می‌توانست رویکرد سنتی را تسهیل کند.

1. Nivaura

۲. پول فیات ارز دولتی یک کشور است که پشتوانه فیزیکی مانند طلا و نقره ندارد، بلکه پشتوانه آن دولتی است که آن را صادر کرده است.

3. GBP-denominated bond

برای مثال، نیاز به داوطلبان و ثبت‌کننده‌ها را برطرف کرد. فرایند انتقال اوراق از سوی ناشر به سرمایه‌گذاران روی بلاکچین ثبت شد که از این طریق شخصیت‌های حقوقی و ذینفعان را به سرمایه‌گذاران نهایی واقعی متصل کرد. دفترکل توزیع‌شده به دلیل شفافیت بیشتری که ارائه می‌دهد می‌تواند از فرایندهای حسابرسی و اصلاحات مؤثر پشتیبانی کند. این سیستم‌ها می‌توانند شفافیت و دقت را در ارتباط با مالکیت دارایی‌ها افزایش دهند.

فاز دوم پروژه نشان داد که امکان انتشار و پرداخت یک ابزار مالی قابل اجرا از نظر حقوقی، منحصراً روی بلاکچین عمومی و بدون استفاده از زیرساخت‌های بازار مالی مرسوم وجود دارد. نکته مهم این است که بلاکچین شامل یک نهاد ثالث مستقل می‌شود که نیاز به نهاد ثالث ثبت‌کننده را برطرف می‌سازد (در واقع بلاکچین خود ثبت‌کننده است). نیوا را فرایند انتشار را تسهیل می‌کند اما کنترل مستقیمی روی تخصیص دارایی‌ها و مالکیت پول بر روی دفتر ثبت ندارد.

انتشار اوراق قرضه آزمایشی نشان داد که خودکارسازی فرایند انتشار اوراق با امکان توکنایز کردن، می‌تواند هزینه و زمان ورود به بازار را به‌طور چشمگیری کاهش دهد. با ساده‌تر کردن ساختار و مستندسازی، هزینه‌های کارمزد و پیچیدگی‌ها کمتر می‌شود. با حذف ثبت‌کننده، پرداخت‌ها به‌صورت هم‌تابه‌ها با استفاده از قراردادهای هوشمند انجام می‌شود. قراردادهای هوشمند جهت خودکارسازی فرایند سفارش اوراق قرضه و پرداخت سود به کار می‌رود.

همان‌طور که در بالا اشاره شد، توکنایز کردن اوراق قرضه به ناشران شرکتی این امکان را می‌دهد که با ساده‌سازی ساختار به‌طور کارآمدتری عمل کنند؛ تعداد طرف‌های درگیر را کاهش دهند، حجم مستندات موردنیاز را کم کنند، بسیاری از فرایندها را خودکار سازند و در هزینه و زمان صرفه‌جویی کنند. چنین ساختارهایی می‌توانند برای دامنه وسیع‌تری از بنگاه‌های کوچک و متوسط فرصت افزایش سرمایه ایجاد کنند.

محدودیتی که برای این نوع انتشار وجود دارد مسئله مقیاس‌پذیری است؛ آسیب‌های احتمالی جبران‌ناپذیری می‌تواند به قراردادهای هوشمند وارد شود؛ محدودیت‌های عملکردی و ملاحظات حریم خصوصی و همچنین مشکل

تطبیق پذیری که ناشی از ویژگی ناشناس بودن این پلتفرم هاست. مانند دیگر پروژه های سندباکس اداره نظارتی امور مالی، انتشار نیوارا کاملاً منطبق با نیازمندی های قانونگذاری بود. اوراق قرضه اسمی مبتنی بر اتر از فرایندی کاملاً خودکار بهره برد که ابزار اوراق قرضه را روی یک پلتفرم پیاده سازی کرد. علاوه بر این فرایند خودکار سازی شامل مستند سازی حقوقی، عبارات مشخص توافق شده روی پلتفرم و ارائه فرمت پی دی اف به شرکت کنندگان بود. سرمایه گذاران علاقمند بعد از اعلام های مربوط به پولشویی و تأمین مالی تروریسم مجاز شمرده می شوند و هر چند توکن ها برای همه شبکه شفاف است، اما تنها به شرکت کنندگان مجاز تعلق می گیرد. نیوارا مانند نگهبان شبکه عمل می کند یعنی از کلیدهای خصوصی سرمایه گذاران حفاظت می کند.

نمونه ای از توکن سهامی

گروه پلرین^۱ اولین شرکتی بود که منطبق با چارچوب تنظیم گری سوئیس تمام سهام خود را توکنایز کرد. همه سهم های توکنایز شده روی بلاکچین در قالب توکن های اتریوم^۲ منتشر شد. پلرین سهم های خود را با به کارگیری سند دستورالعمل انجمن فناوری و بازارهای سرمایه^۳ با هدف تراکنش های مختص به پلرین توکنایز کرد. در ابتدا همه سهم های پلرین به نام سهامدار اصلی در قالب توکن MPS روی بلاکچین اتریوم توکنایز و ثبت شد. سپس ۵ درصد از کل سهام برای فروش عمومی عرضه و همچنین برای حوزه های قضایی منتخب خارجی مطابق با محدودیت های فروش محلی به طور خصوصی ارائه شد. خریداران باید مراحل شناسایی مشتری و ضد پولشویی را به طور کامل بگذرانند و در دفتر ثبت سهامداران پلرین به عنوان سهامدار ثبت نام کنند. هر چند توکنایز کردن بسیاری از فرایندهای شرکتی مانند ثبت انتقال سهم ها و شناسایی سهامدار را دیجیتالی و ساده می کند، اما پلرین علاوه بر

1. Mt Pelerin

2. ERC20

3. The Capital Markets and Technology Association (CMTA)

توکن‌نیز کردن سهم‌ها، به یک دفتر ثبت خصوصی سهامداران نیز نیاز دارد که توسط بلاکچین جایگزین نمی‌شود.

توکن‌های MPS به‌طور آزاد قابل انتقال هستند، اما برای اینکه یک پذیرنده جدید بتواند به سایر خدمات اجتماعی پلرین (مانند رأی دادن) و خدمات مالی (سود سهام) دسترسی داشته باشد، باید از ناشر برای ثبت نام در دفتر ثبت سهامداران درخواست کند. این درخواست نیز طبق سند اجرایی پلرین شامل تکمیل مراحل مختلف شناسایی و ضدپولشویی می‌شود.

از نظر فناوری، سهم‌های توکن‌نیز شده پلرین به دلیل پیاده‌سازی ویژگی‌های پروتکل «بریج»^۱ پیشرفته‌تر از توکن‌های ERC20 هستند. بریج یک فناوری متن‌باز است که توسط پلرین به منظور ارائه یک چارچوب استاندارد شده برای توکن‌نیز کردن امور مالی توسعه یافته است. این فناوری که در سوئیس مطابق با استاندارد انجمن فناوری و بازار سرمایه طراحی شده است، به عنوان لایه‌ای روی شبکه بلاکچین سازگار با اتریوم کار می‌کند و در ارتباط با فرایند انتشار و تطبیق‌پذیری چرخه عمر توکن‌ها عمل می‌کند. در واقع، پروتکل بریج به ناشر این امکان را می‌دهد که قوانینی مربوط به یک یا چندین توکن را ایجاد و روش انتقال آنها را تعیین کند. اجرای این قوانین توسط یک موتور تنظیم‌گر نظارت می‌شود که می‌تواند در چند بُعد (توکن‌ها، افراد و زمان) عمل کند. با استفاده از این چارچوب، ناشران می‌توانند برای بازارهای اولیه و ثانویه توکن‌های خود چارچوب‌های عملیاتی را که از نظر حقوقی مستحکم هستند تعریف کنند و همچنین قادر به پیاده‌سازی و تطبیق‌پذیری با قوانین در یک محیط تنظیم‌گری و حقوقی در حال تکامل هستند.

در واقع، پلرین در مسیر حرکت به سمت ایجاد یک بانک با نوع جدیدی از سامانه متمرکز بانکداری است که از قراردادهای هوشمند و توکن‌نیز کردن برای نمایش دارایی‌ها به صورت دیجیتالی بهره می‌گیرد. در حال حاضر این پروژه قادر است توکن‌نیز کردن، فرایندهای شناسایی و ضدپولشویی و سایر فناوری‌ها و خدمات

تطبیق پذیری را به نهادهای ثالث ارائه دهد.

۳. توکن کاربردی^۱

توکن کاربردی شامل توکن هایی هستند که دسترسی دیجیتال به یک برنامه یا خدمت را از طریق زیرساخت بلاکچین فراهم می کنند. به عبارت دیگر، این نوع از توکن ها به دارندگان خود اجازه دسترسی به یک محصول یا سرویسی خاص را ارائه می دهد. داشتن این نوع توکن به معنای داشتن مجوز برای دسترسی به خدمات شبکه است. از نمونه های این توکن به توکن های شناسایی مشتری و ایکس آرپی می توان اشاره کرد. به عنوان مثال، فرض کنید یک سازنده رستوران توکنی ارائه می دهد که به دارند آن پس از ساخت رستوران اولویت دسترسی به غذای سرآشپز را با تخفیف می دهد. این رویه می تواند شبیه پلتفرم تأمین مالی جمعی مبتنی بر پاداش باشد که مشتریان در ازای دسترسی سریع تر به محصول مورد نظر خود به پروژۀ کمک مالی کنند. یا فرض کنید یک کارگردان معروف توکنی ارائه دهد که به دارندگان آن اجازه دیدن فیلم ساخته شده را در زمان آینده اعطا کند. توکن های کاربردی در اپلیکیشن یا پلتفرم به خصوصی استفاده می شوند و خارج از آن فاقد ارزش هستند. یکی از متداول ترین روش های استفاده از توکن کاربردی این است که شما می توانید هزینه خرید خود در پلتفرم را با آن پرداخت کنید. برای مثال، می توانید هزینه استفاده از خدمات بهداشتی و سلامتی پلتفرم مدیپدیا^۲ را با استفاده از توکن پرداخت کنید. به عبارتی می توان گفت، توکن کاربردی نوعی توکن پرداخت مختص به خدمات یک اپلیکیشن یا پلتفرم است. توکن های کاربردی را یک شرکت منتشر می کند تا مکانیزمی برای پرداخت هزینه محصولات و خدمات جدید خود در اختیار کاربران بگذارد؛ محصولات و خدمات اشاره شده اغلب توسط فناوری بلاکچین توسعه یافته اند. نکته قابل توجه اینکه، توکن های کاربردی بحث برانگیزترین روش جهت تأمین مالی جمعی است که در آن، توکن ها به خودی خود حق هیچ گونه سود (حقوق مالی یا پولی) را ندارند، اما قابل معامله و نقدشونده هستند و ممکن است با قیمت بالایی نسبت به قیمت

1. Utility token

2. Medipedia

خرید آنها در بازار رمزارزها فروخته شوند. در تأمین مالی جمعی ممکن است استفاده از توکن کاربردی دشوار باشد، زیرا ناشر نه درگیر مدیریت دارایی هاست و نه موظف است توزیع درآمد حاصل از آن را به دارندگان توکن انجام دهد. بنابراین صلاحیت کسب و کار وابسته به عملکرد و سابقه مؤسسان است.

ارزش توکن‌های کاربردی در سودمندی خدمات آنها و ارزش افزوده آن است. ریسک مصرف‌کننده ناشی از خرید چنین توکن‌هایی نارضایتی از عملکرد خدمات است و هیچ نوع خطر سازمانی وجود ندارد. در راستای اهداف نظارتی، پیشنهاد می‌شود توکن‌های کاربردی براساس حقوقی که به دارندگان ارائه می‌دهند، به سه نوع تقسیم شوند:

(۱) توکن‌های کاربردی خالص^۱ (۲) توکن‌های دسترسی^۲ (۳) توکن‌های ترکیبی^۳.

توکن‌های کاربردی خالص

این توکن‌ها، توکن‌های کاربردی هستند که به دارنده خود حق استفاده از خدمات را می‌دهند. قراردادهای هوشمند، معامله این توکن‌ها را در صرافی‌های ثانویه ممنوع می‌کند و فقط دارندگانی که این توکن را می‌خرند می‌توانند از مزایای آن در هنگام شروع خدمات بهره‌مند شوند. به دلیل چنین منعی در فروش مجدد، این توکن‌ها فقط توسط کاربرانی که مایل به استفاده از خدمات هستند خریداری می‌شوند و نه توسط افرادی که اهداف سرمایه‌گذاری در ذهن آنهاست. فایل کوین، سیا و اتر^۴ نمونه‌هایی از توکن‌های کاربردی خالص هستند.

توکن‌های دسترسی و توکن‌های ترکیبی

توکن‌های دسترسی حق استفاده از خدمات اساسی را به دارندگان توکن داده است. با این حال، خلاف توکن‌های کاربردی خالص، در اینجا خرید و فروش توکن‌ها مجاز است. در توکن‌های ترکیبی در عین اینکه به دارنده توکن حق استفاده از خدمات

1. Pure utility tokens
2. Access tokens
3. Hybrid tokens
4. Filecoin, Sia, Ether

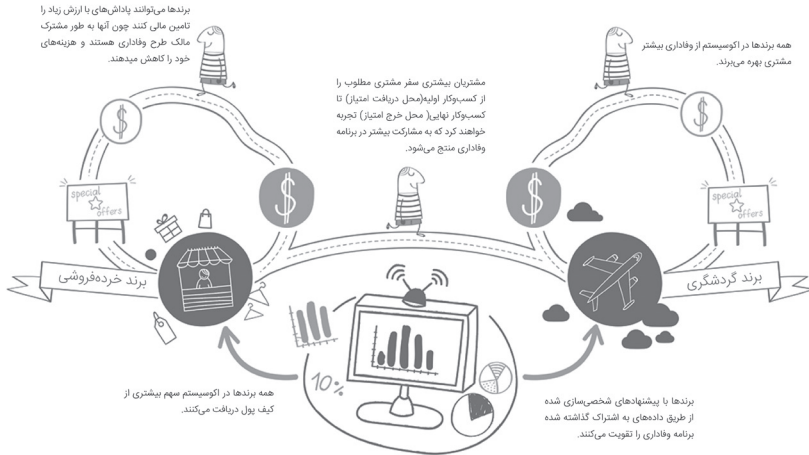
و مشارکت در شبکه داده می‌شود، معاملات توکن نیز مجاز است. روش‌هایی که دارندگان توکن‌های ترکیبی می‌توانند در شبکه نقش داشته باشند، بی‌شمار هستند. با این حال، تعداد بسیار کمی توکن ترکیبی در گردش است که اکثر آنها فقط از نظر قدرت محاسبات و خدمات توسعه امکان مشارکت دارند. بایننس کوین^۱ نمونه‌ای از توکن‌های ترکیبی است.

توکن وفاداری به عنوان نمونه‌ای از توکن‌های کاربردی

وفادار ساختن مشتریان اهمیت زیادی برای کسب و کارها دارد و سالانه هزینه فراوانی نیز صرف این موضوع می‌شود چراکه معمولاً هزینه جذب مشتری جدید بیشتر از حفظ مشتری‌های فعلی است. به همین دلیل کسب و کارهای آنلاین سرمایه‌گذاری زیادی برای حفظ مشتری‌های خود در قالب طرح‌های وفاداری و باشگاه مشتریان ارائه می‌دهند که در واقع نوعی سرمایه‌گذاری استراتژیک محسوب می‌شود. هرچند برنامه‌های وفاداری مشتریان آنها در سال‌های اخیر رشد قابل توجهی داشته است، اما تحقیقات نشان می‌دهد بسیاری از این مشتریان فعال نیستند. گزارشی تحت عنوان گزارش اوراق وفاداری سال ۲۰۱۶^۲ که روی ۱۲ هزار آمریکایی و ۷ هزار کانادایی صورت گرفته بود، نشان داد، تنها ۵۰ درصد این افراد عضو فعال در طرح‌های وفاداری هستند و از میان این افراد نیز حدود یک پنجم آنها هرگز از این امتیازات استفاده نکرده‌اند. این داده‌ها نشان می‌دهند روش‌های قدیمی آن‌طور که باید تأثیرگذار نیستند. دلایل بسیاری برای این ناکارآمدی وجود دارد که در اینجا به برخی از آنها اشاره می‌شود:

- فقدان مدیریت یکپارچه برنامه‌های وفاداری؛
- محدودیت استفاده از این امتیازات در محیط‌های دیگر؛
- هزینه بالای ایجاد و نگهداری یک سیستم وفاداری منحصر به فرد؛
- امنیت سیستم‌های موجود؛
- عدم امکان شخصی‌سازی امکانات براساس نیاز هر مشتری؛

• عدم امکان رهگیری مشتریان، امتیازات و محل هزینه کردن آنها.



شکل ۵: برنامه ائتلافی باشگاه مشتریان

برای حل چالش‌های مذکور در جهان، انتشار توکن وفاداری مطرح شده است. با استفاده از یک شبکه یکپارچه بر بستر بلاکچین برای باشگاه‌های مشتریان کسب و کارهای مختلف می‌توان برنامه وفاداری ائتلافی^۱ ارائه داد که توسط چندین کسب و کار اداره می‌شود و به مشتریان اجازه می‌دهد به کسب و کارهای مختلف مراجعه و با خرید از یک کسب و کار از امتیازها و مزایای دریافتی در کسب و کارهای دیگر نیز استفاده کنند. این سیاست نه تنها از وفاداری مشتری به کسب و کار اولیه کم نمی‌کند، بلکه شوق خرید از فروشگاه اولیه را دو چندان می‌سازد تا با بهره‌مندی از مزایایی که فقط با خرید از آن فروشگاه قابل دستیابی است، بتواند از امکانات شبکه نیز استفاده بیشتری ببرد.

مشتری با عضویت در این شبکه وارد دنیای جدیدی می‌شود که خروج از آن، برای وی مطلوب نیست. انواع سناریوهای وفاداری در قالب برنامه‌های جذاب شبیه

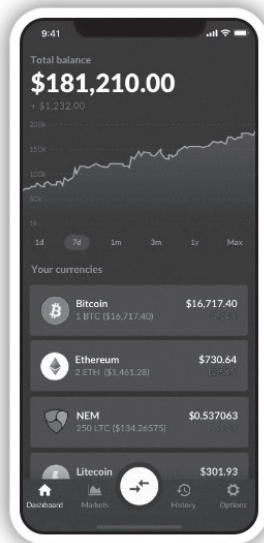
بازی‌های هیجان‌انگیز طراحی می‌شوند. ویژگی این برنامه‌ها به روز بودن طراحی آنها و تغییر مداوم براساس سیاست‌های هر کسب و کار و تجربه خرید هر مشتری است. به مرور زمان مشتری به شبکه اعتماد پیدا می‌کند و ارتباط خود را با آن بیشتر می‌کند. این ارتباط مؤثر کمک می‌کند مشتری بیش از پیش اطلاعات شخصی خود را در اختیار فروشگاه اصلی قرار دهد و در یک چرخه تعاملی، هر یک از کسب و کارها شبکه را تغذیه کند و متقابلاً شبکه نیز به کلیه کسب و کارها سودرسانی می‌کند. از دیگر مزایای باشگاه مشتریان ائتلافی عبارتند از:

- دسترسی به حجم وسیعی از داده‌ها؛
 - بهره‌مندی از مزایای دسترسی به پتانسیل‌های بازار وسیع‌تر؛
 - افزایش جریان نقدینگی؛
 - کاهش هزینه؛
 - افزایش بهره‌وری و آزادی عمل در بازار برای مشتری که حق انتخاب بیشتر و ارزش پیشنهادی بالاتر دریافت می‌کند.
- علاوه بر موارد فوق شبکه بلاکچین بستر لازم برای تبدیل امتیازات وفاداری به توکن‌ها را مهیا می‌کند که در این صورت اعضای شبکه از مزایای استفاده از توکن وفاداری بهره می‌برند. مشتری می‌تواند به راحتی و به سرعت توکن‌های خود را با دیگر مشتریان موجود در شبکه به ازای پول نقد یا رمزارز مبادله و درواقع توکن خود را تبدیل به پول کند.
- این قابلیت تعویض می‌تواند برای مشتریان ارزش و جذابیت ایجاد کند. توکن‌سازی امتیازات وفاداری آنها را منحصر به فرد، قابل تبادل و قابل معامله می‌سازد. نت کوین^۱ یکی از نمونه‌های توکن‌های وفاداری است.

اپلیکیشن موبایلی وفاداری نت‌کوین

هدف این اپلیکیشن این است که مشتری‌ها را برای خرید از خرده‌فروشی‌ها

تشویق کند و براساس موقعیت مکانی آنها پاداشی به ازای خرید به مشتری‌ها بدهد. این نرم‌افزار تعداد زیادی قابلیت و فیلتر دارد تا تجربه اختصاصی شده‌ای برای خرید هر شخص ایجاد کند و درعین حال در بالاترین سطح ممکن از امنیت اطلاعات کاربران محافظت می‌کند. کیف پول موجود در این نرم‌افزار از نوع چندتوکنی است و امکان ارسال، دریافت و ذخیره توکن‌های مختلفی از جمله ETH, LIQUID, NTK و همچنین صدها توکن ERC20 را در یک کیف پول فراهم می‌کند. شکل ۵ شمایی از کیف پول این اپلیکیشن را نمایش می‌دهد که از بلاکچین اتریوم استفاده می‌کند. از دیگر قابلیت‌های این اپلیکیشن، تبلیغات براساس موقعیت مکانی (مشاهده فروشگاه‌ها و تخفیف‌های اطراف براساس موقعیت مکانی، دسته‌بندی و فاصله)، جمع‌آوری توکن از طریق خرید (دریافت توکن با خرید از فروشگاه‌های طرف قرارداد)، مصرف توکن‌ها در فروشگاه‌های طرف قرارداد و کیف پول چندتوکنی دانست.



شکل ۵: کیف پول نت‌کوین

توکن استیمیت و توکن ترون نمونه‌ای از توکن کاربری موفق

توکن استیمیت

پلتفرم استیمیت یک شبکه اجتماعی با برنامه غیر متمرکز و مبتنی بر بلاکچین است. این پروتکل با سیستم پاداش برای محتوا، انقلاب بزرگی در شبکه‌های اجتماعی و وبلاگ‌نویسی ایجاد کرده است. استیمیت بر بستر بلاکچین استیم ایجاد شده است و ارزش اصلی این پلتفرم توکن استیم است. در استیمیت مردم می‌توانند علاوه بر ارسال پست رایگان، از لایک‌ها و باز دیدهای یک پست کسب درآمد کنند.

تفاوت استیمیت با بقیه شبکه‌های اجتماعی

در شبکه‌های اجتماعی معمولی محتواهای خوب پاداشی ندارند و این شبکه‌ها بیشتر به نفع سهامداران آن خواهد بود. در استیمیت به دلیل غیر متمرکز بودن پروژه، تمام پلتفرم توزیع شده و متعلق به کاربران است. اگر پست شخصی جالب باشد و تعداد لایک زیادی کسب کند، به کاربر مورد نظر به صورت توکن‌های استیم و دلار استیم^۲ و یا استیم‌پاور^۳ پاداش داده می‌شود.

شبکه استیمیت مقدار ۷۵ درصد رمزارز تولیدی خود را جهت پاداش به تولید کنندگان محتوا، به اشتراک گذاران و مشارکت کنندگان در نظرات هر محتوا اختصاص داده است.

بنابراین، پلتفرم استیمیت سه توکن قابل معامله دارد:

- استیم؛
- استیم دلار؛
- استیم‌پاور.

توکن استیم، پایه و اساس حساب هر کاربر است که می‌تواند به سایر ارزهای دیجیتال تبدیل و در صرافی‌ها خرید و فروش شود. استیم همانند سایر ارزهای دیجیتال است و می‌توان آن را با دلار استیم معامله کرد یا آن را به سایر حساب‌ها انتقال داد.

1. Tron token

2. SBD (Steem Blockchain Dollars)

3. Steem Power

دلار استیم یک توکن با ارزش ثابت است که از پشتوانه دلار استفاده می‌کند و ارزش هر کدام از آنها حدود یک دلار آمریکاست. این توکن‌ها برای ضمانت دادن به نویسندگان در برابر تورم و نوسانات استیم ساخته شده‌اند. می‌توان دلار استیم را با توکن استیم معامله کرد یا آن را برای اهداف مختلف به سایر حساب‌ها انتقال داد. توکن استیم پاور برای سرمایه‌گذاری بلندمدت و سودرسانی به سرمایه‌گذاران طراحی شده است. کاربران برای کسب درآمد در رأی‌گیری و نظرات باید استیم پاور در حساب خود داشته باشند. توکن‌های استیم پاور به عنوان معیاری از میزان نفوذ و تأثیر کاربران در شبکه استیم عمل می‌کنند. یک کاربر هر چه توکن استیم پاور بیشتری در اختیار داشته باشد، قدرت بیشتری دارد تا بر ارزش پست‌ها و کامنت‌هایی که به آنها رأی می‌دهد تأثیرگذار باشد. روش‌های کسب استیم در این پلتفرم به شرح ذیل است:

- **ارسال پست:** با به اشتراک گذاشتن پست‌های خود، می‌توانید از طریق رأی‌ها و لایک‌های پست خودتان کسب درآمد کنید.

- **رأی و نظر دادن:** اگر یک پست خوب پیدا کنید و بدانید که این پست در آینده محبوب خواهد شد، اگر به آن پست قبل از محبوبیت رأی دهید یا نظر خود را بگویید، سود خوبی کسب خواهید کرد. البته مبلغ سود به میزان استیم پاور بستگی دارد.

- **خرید:** کاربران می‌توانند از صرافی‌های معتبر نسبت به خرید توکن‌های استیم اقدام کنند.

با افزایش روزافزون کاربران شبکه‌های اجتماعی و اهمیت فوق‌العاده این شبکه‌ها در مناسبات اجتماعی لزوم استفاده از یک شبکه اجتماعی غیر متمرکز و با امنیت بالا اهمیتی دوچندان پیدا می‌کند. استیمیت با یک سیستم پاداش‌دهی و تولید رمزارز، به نقد شبکه‌های اجتماعی موجود نظیر فیسبوک پرداخته است چراکه آنها از فعالیت‌های رایگان کاربران جهت کسب سود خود بهره می‌برند اما آنها را در سود خود شریک نمی‌کنند. در کتاب زندگی پس از گوگل^۱ به صورت تفصیلی به این امر پرداخته و

پیش‌بینی شده است طی ده سال آتی هیچ کدام از این شبکه‌های مجازی باقی نخواهند ماند زیرا از کاربران خود سوءاستفاده می‌کنند و راهکارهای بلاکچینی این مشکل را رفع و اکثریت بازار را خواهند گرفت.

توکن ترون

ترون یک پروتکل غیرمتمرکز مبتنی بر فناوری بلاکچین است که با هدف ساخت یک سیستم رایگان با محتوای سرگرمی در سراسر جهان ایجاد شده است. ترون در تلاش است با استفاده از شبکه همتابه‌همتا و ذخیره‌سازی توزیع شده، یک پلتفرم سرگرمی ایجاد کند که به سازندگان اجازه می‌دهد کنترل کامل روی محتوای خود داشته باشند. تقریباً می‌توان گفت که ترون ترکیبی غیرمتمرکز از پلتفرم‌هایی مانند نتفلیکس^۱، یوتیوب^۲ و اپ استور^۳ است. ترون با حذف کارگزارانی که به عنوان واسطه بین کاربران و تولیدکنندگان محتوا فعالیت می‌کنند، می‌تواند به صورت قابل توجهی هزینه‌های مربوط به خرید محتوای بازی و سرگرمی را تحت کنترل درآورد و درعین حال به صورت همزمان فرصتی در اختیار تولیدکنندگان محتوا در محدوده جامعه آماری موردنظر خود قرار دهد. نماد اختصاری ترون TRX است. حجم معاملات TRX با ارزش‌های دیجیتالی همچون ایکس‌ای‌ام^۴، دس^۵ و مونرو^۶ در رقابت است. ترون قابلیت استخراج ندارد و مجموع کل عرضه آن ۱۰۰ میلیارد TRX خواهد بود. در ۱۸ دسامبر ۲۰۱۷ مدیرعامل ترون، جاستین سان^۷، اعلام کرد بنیاد ترون میزان ۳۴,۲ میلیارد توکن TRX را تا ژانویه ۲۰۲۰ مسدود کرده است. متخصصان اغلب معتقدند قفل کردن توکن‌ها می‌تواند ارزش آنها را افزایش دهد. شبکه ترون همانند استیم، توکن دیگری است به نام TRON Power (TP) که در حقیقت پاداش نگهداری TRX و یک تعهد بلندمدت است. کاربران داوطلبی که

-
1. Netflix
 2. YouTube
 3. App Store
 4. XEM
 5. DASH
 6. XMR
 7. Justin Sun

توکن های TRX را در کیف پول خود قفل می کنند، در ازای آن TP دریافت می کنند. TP در مواردی همچون حق رأی و سایر امتیازات در اکوسیستم ترون کاربرد دارد.

عرضه اولیه سکه^۱

ICO (آیکو) مخفف «عرضه اولیه سکه» است و مقصود از آن، ایجاد و فروش توکن های دیجیتالی است. طی اجرای فرایند عرضه اولیه، یک کسب و کار نوپا می تواند به منظور جذب سرمایه برای کار خود، یک توکن دیجیتالی خاص خود بسازد و مقدار مشخصی از آن توکن ها را با یک قیمت اولیه به عموم مردم بفروشد. معمولاً در ازای فروش این توکن ها یک ارز رمزنگاری شده دیگر همچون بیت کوین و اتریوم اخذ می شود و با انجام یک عرضه اولیه سکه و استقبال مردم از آن، کسب و کار نوپا می تواند خود را برای اجرای پروژه اش تأمین مالی کند.

ایجاد یک توکن آسان تر از ایجاد یک کوین است، چراکه نیازی به ایجاد کد جدید یا تغییر کد موجود ندارد و شما فقط باید از یک الگوی استاندارد از پلتفرم هایی مانند اتریوم^۲ استفاده کنید که مبتنی بر بلاکچین است و به هر شخصی این امکان را می دهد که طی چند مرحله توکن ایجاد کند. اتریوم اولین پلتفرمی بود که روند ایجاد توکن را ساده تر کرد.

معمولاً توکن ها از طریق عرضه اولیه سکه ها که نوعی روش جذب سرمایه است ایجاد و توزیع می شوند. ترون^۳ و ای او اس^۴ دو مورد از شناخته شده ترین توکن ها هستند.

مزایا

در عرضه اولیه سهام (اولین فروش سهام یک شرکت خصوصی و در نتیجه تبدیل شدن آن به یک شرکت سهامی عام) سرمایه گذار در ازای مبلغی سهام دریافت خواهد کرد. اما در عرضه اولیه سکه، سهام به این معنای خاص وجود ندارد. شرکت هایی

1. Initial Coin Offering (ICO)
 2. Ethereum
 3. Tron
 4. EOS

که با عرضه اولیه سکه سرمایه جمع می کنند، یک توکن به سرمایه گذار می دهند. این توکن بسته به تعریفی که برایش انجام شده (پرداخت، کاربری یا بهادار) نماینده مالکیت یا حق و حقوقی است که به دارنده اش تعلق می گیرد.

هر شرکت می تواند به آسانی یک عرضه اولیه سکه ایجاد کند و حتی خدمات برخطی وجود دارند که اجازه می دهند طی چند ثانیه توکن رمزارزی ساخته شود. خلاف سهام، توکن ها ارزش ذاتی ندارند و به صورت قانونی توسط یک کشور تضمین نخواهند شد. مدیران عرضه اولیه سکه، توکن ها را با توجه به شرایط از پیش تعیین شده ساخته و سپس با توجه به برنامه های خود بین سرمایه گذاران پخش می کنند.

سرمایه گذاران در یک عرضه اولیه سکه معمولاً به این امید دارند که پروژه ای که توکن هایش را خریداری کرده اند به موفقیت برسد. اگر پروژه به موفقیت برسد ارزش توکن هایی که در عرضه اولیه خریداری شده اند بالا خواهد رفت و فروش آنها سود مناسبی به همراه خواهد داشت و حتی پتانسیل چند برابر شدن سرمایه اولیه وجود دارد که یکی از مزایای اصلی عرضه های اولیه سکه محسوب می شود (در سال ۲۰۱۷ توکن های ۴۳۵ عرضه اولیه سکه با میانگین رشد قیمت ۱۲,۸ برابری روبه رو شدند).

معایب

قوانین و مقررات خاصی برای عرضه اولیه سکه تعیین نشده است. عدم نظارت سازمان های دولتی روی عرضه اولیه سکه سبب شده چنانچه کلاهبرداری اتفاق بیفتد، به احتمال زیاد سرمایه های از دست رفته هرگز به صاحبان خود بازنگردد.

حجم زیاد کلاهبرداری ها باعث شد در سال ۲۰۱۷ بانک مرکزی کشور چین استفاده از توکن ها را ممنوع اعلام کند که کاهش قیمت بیت کوین و اتریوم را به دنبال داشت. از سال ۲۰۱۸ نیز فیس بوک، توییتر و گوگل تبلیغات مربوط به عرضه اولیه سکه را قبول نمی کنند.

بهترین و موفق ترین عرضه اولیه سکه

با رشد روزافزون صنعت رمزارزها می توان میزان موفقیت عرضه اولیه های سکه را

محاسبه کرد. کافی است مقدار پول جمع آوری شده در عرضه اولیه را با نرخ بازگشت سرمایه آن مقایسه کنید تا سنجه‌ای قابل اتکا از موفقیت آن عرضه اولیه را در اختیار داشته باشید.

تاکنون شماری از عرضه اولیه‌ها توانسته‌اند به موفقیت‌های چشمگیری دست پیدا کنند. عرضه اولیه اتریوم یکی از عرضه اولیه‌هایی است که در سال ۲۰۱۴ برگزار و در مدت زمان ۴۲ روز، بیش از ۱۸ میلیون دلار سرمایه جمع آوری کرد و در ادامه، با گذشت زمان به یکی از برترین پروژه‌های حوزه رمزارزها تبدیل شد و توانست پس از بیت‌کوین در جایگاه دوم پرارزش‌ترین رمزارز بازار جای گیرد.

ویژگی‌های نوآورانه این پلتفرم از جمله اپلیکیشن‌های توزیع شده و قراردادهای هوشمند باعث شد تحولی فراگیر در حوزه رمزارزها پدید آید. قیمت این رمزارز در زمان عرضه اولیه، چیزی حدود ۰/۶۷ دلار بود؛ اما اکنون بهای آن از مرز هزار دلار فراتر رفته است. به این ترتیب، سرمایه اولیه کسی که در عرضه اولیه اتریوم مشارکت داشته، امروزه بیش از ۱۵۰۰ برابر شده است.

منابع:

- [1] cryptocurrencyfacts.com/what-is-a-cryptocurrency-token
- [2] adyen.com/knowledge-hub/guides/tokenization-payment-technology-guide
- [3] squareup.com/us/en/townsquare/what-does-tokenization-actually-mean
- [4] en.wikipedia.org/wiki/Cryptocurrency
- [5] inblockchain.info/bitcoin-halving-philosophical-foundations
- [6] news.bitcoin.com/five-of-the-most-important-use-cases-for-cryptocurrency
- [7] [visualizing the new cryptocurrency ecosystem – visual capitalist](https://visualizingthe.newcryptocurrencyecosystem-visualcapitalist)
- [8] danup.ir/what-is-token/
- [9] iribnews.ir/fa/news
- [10] ccmag.ir/501
- [11] ramzarzyar.com/types-of-currency
- [12] zoomit.ir/2019/10/12/341180/security-tokens-arent-yet-worth-hype
- [13] legal500.com/developments/thought-leadership/security-token-offerings-equity-or-debt-how-financial-statements-are-affected
- [14] arzdigital.com
- [15] Shroff N, Venkataraman P. Regulating ICO Tokens and Cryptocurrency in India. Available at SSRN 3134380. 2017 Dec 1.
- [16] movafaghsho.com
- [17] rade.ir
- [18] finmag.ir
- [19] khanesarmaye.com
- [20] mtpelerin.com
- [21] The Tokenisation of Assets and Potential Implications for Financial Markets – OECD 2020
- [22] practicalecommerce.com/how-blockchain-is-changing-loyalty-programs
- [23] “The 2016 Bond Loyalty Report (US edition),” Bond Brand Loyalty, June 2016.
- [24] stampme.com/how-much-does-a-loyalty-program-cost/
- [25] hackernoon.com/blockchain-can-save-customer-loyalty-programs-from-becoming-unfruitful-3992c6bc6053
- [26] blog.currencyalliance.com/2018/09/loyalty-coalitions-v3-0-greater-benefits-for-consumers-and-brands/
- [27] www.practicalecommerce.com/how-blockchain-is-changing-loyalty-programs
- [28] www.netkoin.com/shoppers/
- [29] mihanblockchain.com/
- [30] coiniran.com/what-is-steemit/
- [31] mk-exnews.com
- [32] pay98.app/
- [33] www.visualcapitalist.com

(۳۴) گزارش کارشناسی: تحلیل ماهیت، استخراج و مبادله انواع رمزارزها و توکن‌ها از منظر فقه اسلامی و قوانین کشور، پژوهشکده پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، پاییز ۱۳۹۹.



فصل سوم

قوانین و مقررات رمزارزها

مقدمه

نگرش جهان به صدور و فروش توکن‌ها متفاوت و در حال تغییر است، به گونه‌ای که مواضع کشورهای مختلف از به رسمیت شناختن آنها تا ممنوعیت کامل متغیر است. بسیاری از کشورها در پی تغییر سیاست‌های قانونگذاری خود برای همگام شدن با استقبال گسترده از بازار رمزارزها و سایر داریی‌های دیجیتال هستند.

در زمینه ماهیت رمزارز باید توجه داشت که این فناوری نوپاست و در این زمینه هنوز اتفاق نظری وجود ندارد. به طور کلی، کشورهایی که به این حوزه ورود کرده‌اند در رابطه با ماهیت رمزارز غالباً سه رویکرد دارند. برخی آن را شکلی از پول (ابزار پرداخت)، برخی نوعی از داریی و برخی دیگر ماهیت آن را کالا می‌دانند. در این میان کشورهایی هم هستند که تا امروز هیچگونه اظهار نظر رسمی در این خصوص نداشته‌اند. به عبارتی این مفهوم تبدیل به یک چالش برای مقامات قانونگذار شده است. رمزارزها ویژگی‌های ارز، کالا، و سیستم‌های پرداخت را با هم ترکیب می‌کنند و این در حالی است که طبقه‌بندی آنها در هر کدام از این عناوین در رفتار قانونی و نظارتی مرتبط با آنها و در تعیین نهاد و مقام مسئول اثرگذار است. در ادامه به طور خلاصه و براساس گزارش مرکز پژوهش‌های مجلس، تحولات اخیر توسط قانونگذاران و مقامات نظارتی در حوزه‌های قضایی کلیدی در سراسر جهان و تأثیرات مرتبط با آن در بازار رمزارزها و سایر داریی‌های دیجیتال بررسی می‌شود و سپس قوانین ایران در این زمینه نیز مرور خواهد شد.

قوانین و مقررات کشورهای جهان

رمزارزها در عین داشتن مزیت‌های منحصر به فرد خود، ریسک‌ها و خطراتی در سطح کلان جامعه به همراه دارند که سبب شده دولت‌های مختلف در صدد وضع قوانین و مقررات مرتبط با آنها بایند. این کار دشوار است، چرا که ماهیت غیر متمرکز رمزارزها مانع از نظارت یک نهاد دولتی می‌شود. بنابراین باید این مهم از طریق ارائه‌دهندگان خدمت^۱ این حوزه انجام شود. برخی از کشورها با رویکرد مثبت و تنظیم‌گری با این پدیده نوظهور برخورد کرده‌اند و

1. Service Providers

در مقابل برخی دیگر بارویکرد منفی آن را غیر قانونی اعلام و محدود کردند. برخی نیز موضع نرم‌تری گرفته و تنها یک یا چند وجه از ابعاد رمزارز و توکن را ممنوع کرده‌اند. البته در این میان نیز کشورهایی هستند که تاکنون نتوانسته‌اند واکنش مشخصی نسبت به رمزارزها نشان دهند و اعلام موضع کنند. در ادامه وضعیت قانونگذاری رمزارزها در کشورهای منتخب ارائه می‌شود.

رویکرد مثبت و تنظیم‌گرانه (قانونی)

آمریکا: دولت آمریکای بیت‌کوین را به عنوان ارز مجازی غیر متمرکز قابل تبدیل دسته‌بندی کرده و همانند یک دارایی ذیل قوانین مالیاتی قرار داده است. چنانچه ارائه‌دهنده خدمتی در این حوزه مانند صرافی بخواهد فعالیت داشته باشد باید در فین‌سن ثبت‌نام و برنامه‌های ضد پولشویی را رعایت کند. ضمناً به‌طور منظم به نهادهای مربوطه گزارش فعالیت‌های مشکوک را بدهد.

ژاپن: در ژاپن، مشاغل مرتبط با مبادلات رمزارز، تنظیم‌گری شده‌اند. در سال ۲۰۱۷ دولت ژاپن به‌طور رسمی بیت‌کوین را به عنوان وسیله پرداخت همچون سایر پول‌های متداول پذیرفت. یکی از اهداف مطرح شده از این طرح، جذب گردشگران و سرمایه‌گذاران بین‌المللی است. براساس قانون مالیات بر درآمد آژانس ملی مالیات ژاپن، سود حاصل از فروش رمزارز، درآمد متفرقه (نه سود سرمایه) در نظر گرفته می‌شود؛ هنگامی که درآمد مشمول مالیات یک شخص محاسبه و مالیات تعیین می‌شود، درآمد متفرقه به مبلغ سایر درآمدها اضافه خواهد شد.

آلمان: سازمان نظارت مالی آلمان (بافین)^۱، رمزارزها را به عنوان واحدهای حساب و ابزار مالی محسوب کرده است. ارائه‌دهندگان خدمات این حوزه باید از بافین مجوز فعالیت اخذ کنند. همچنین در سال ۲۰۱۸، دولت آلمان دستورالعملی در مورد نحوه اخذ مالیات بر ارزش افزوده بیت‌کوین و سایر رمزارزها، منتشر کرد. براساس آن، معامله یک ارز سنتی با رمزارزها و برعکس، از مالیات بر ارزش افزوده معاف است اما سایر خدمات، مشمول مالیات خواهند

1. FinCen

2. Bafin

بود. این نهاد اظهار داشته بار مزارزها که صرفاً به عنوان ابزار پرداخت استفاده می شوند، مانند همان ابزارهای پرداخت سنتی بر خورد می شود. در سال ۲۰۱۹، بر اساس قانونی که مجلس آلمان به تصویب رساند از اول ژانویه ۲۰۲۰ به بانک ها اجازه داده شد که بتوانند به خرید و نگهداری رمزارزها بپردازند.

کانادا: استفاده از رمزارزها از جمله بیت کوین، در کانادا مجاز است و می توان از رمزارزها برای خرید کالاها و خدمات اینترنتی استفاده کرده و در فروشگاه هایی که رمزارزها را می پذیرند، خرید کرد. تراکنش های رمزارزها مشمول قوانین ضد پولشویی و مبارزه با تأمین مالی تروریسم است. طبق قوانین مالیاتی جدید این کشور، اگر برای خرید کالا یا خدمتی بیت کوین پرداخت شده باشد، معامله کالا به کالا محسوب می شود و مشمول مالیات معاملات کالا به کالا است و کالاهای خریداری شده با استفاده از رمزارز باید در درآمد فروشنده برای اهداف مالیاتی ثبت شوند. همچنین سود حاصل از معاملات کالا طبق دستورالعمل معاملات در اوراق بهادار به عنوان درآمد یا سرمایه تعریف و مشمول مالیات می شود. به هر حال، رمزارزها در کانادا پول رایج قانونی محسوب نمی شوند و تنها ارز رسمی این کشور دلار کانادا است چرا که طبق قانون پول رایج قانونی عبارت است از: ۱) اسکناس های صادر شده توسط بانک طبق قانون بانکداری کانادا و ۲) سکه های صادر شده طبق قانون ضرابخانه سلطنتی کانادا.

نیوزیلند: بانک مرکزی کشور نیوزیلند اعلام کرده است که نهادهای مالی به غیر از بانک ها نیازی به اجازه بانک مرکزی در خصوص نحوه انتقال پول و ذخیره ارزش ندارند، بنابراین استفاده از بیت کوین برای نهادهای غیر بانکی مجاز است.

استرالیا: استرالیا یکی از معدود کشورهایی است که دولت آن، بیت کوین را به عنوان پول به رسمیت شناخته است و رئیس بانک مرکزی استرالیا در مصاحبه ای درباره بیت کوین اعلام کرد در این کشور هیچ گونه محدودیتی برای افرادی که می خواهند از سایر ارزها برای خرید استفاده کنند وجود ندارد.

سنگاپور: سنگاپور که احتمال می رود در آینده ای نزدیک یکی از عمده ترین مراکز استفاده از بیت کوین باشد، برای آن قوانین مالیاتی ارزش افزوده همچون کالاها وضع کرده است.

تایلند: کشور تایلند از جمله کشورهایی است که دستورالعمل‌های متعددی برای رمزارزها و به‌طور خاص بیت‌کوین تدوین کرده است. صرافی‌های فعال در حوزه معاملات رمزارزها برای تجارت الکترونیک باید مجوز بگیرند و ملزم به اجرایی‌سازی سیاست‌های شناخت و ارزیابی موشکافانه مشتری^۱ هستند. در راستای این سیاست، چنانچه صرافی‌ها وقایع مشکوکی مشاهده کنند باید به کمیته مبارزه با پولشویی کشور اطلاع دهند.

مالزی: کمیسیون بورس و اوراق بهادار مالزی در راستای رونق کسب و کارهای نوپا، در سال ۲۰۱۷ دستورالعملی برای استفاده از پتانسیل تأمین مالی از روش عرضه اولیه سکه تدوین کرده است که کارآفرینان با رعایت اصول مطرح شده در دستورالعمل، می‌توانند به‌طور قانونی و فارغ از تشریفات و محدودیت‌های بورس، به تأمین مالی خود بپردازند.

مکزیک: بانک مرکزی کشور مکزیکی طی اعلامیه‌ای در سال ۲۰۱۴ درخصوص خطرات پولشویی و سرعت رمزارزها هشدارهای لازم را به عموم مردم و مؤسسات مالی داد. اما در قانون فناوری‌های مالی سال ۲۰۱۷، بیت‌کوین در مکزیکی مطابق سرفصل دارایی مجازی این کشور تنظیم‌گری شده است.

قرقیزستان: قانون کشور قرقیزستان بیت‌کوین را به‌عنوان کالا (نه به‌عنوان پول یا اوراق بهادار) به رسمیت می‌شناسد و این امکان وجود دارد که در بورس کالا خرید و فروش شود. استفاده از بیت‌کوین به‌عنوان پول در تسویه‌های داخلی محدود است.

استونی: در ۱۵ مارس ۲۰۱۷ وزارت مالی استونی اعلام کرد؛ استفاده از رمزارزها به‌عنوان وسیله پرداخت هیچ مانع قانونی ندارد.

اوکراین: در ژانویه ۲۰۱۸، واحد امنیت فضای مجازی و شورای امنیت ملی اوکراین اعلام کرد این کشور اجازه فعالیت و گردش کنترل نشده رمزارزها را نمی‌دهد و در تلاش است چارچوب قانونی برای نظارت بر آنها تدوین کند. همچنین در همین زمان، رئیس بخش جرائم رایانه‌ای پلیس اوکراین اعلام کرد اگر وضعیت قانونی رمزارزها در آینده نزدیک تنظیم نشود، گردش رمزارزها را ممنوع خواهد کرد. اما در مارس ۲۰۱۸، دولت

1. Customer Due Diligence (CDD)

این کشور با تکمیل طبقه‌بندی فعالیت‌های اقتصادی در یک بند، فعالیت‌های استخراج را مجاز اعلام کرد.

روسیه: با افزایش استفاده از رمزارزها در روسیه، دولت در مورد چگونگی تعریف قانونی این محصولات، ادغام آنها در سیستم حقوقی و تعیین روش‌های دریافت مالیات بحث کرده است. در ۳۱ ژوئیه ۲۰۲۰، رئیس‌جمهور روسیه، ولادیمیر پوتین، قانون شماره FZ-259 در مورد دارایی‌های مالی دیجیتال (DFAs) و ارزهای دیجیتال را امضا کرد. این قانون موارد مربوط به انتشار، ثبت و گردش دارایی‌های مالی دیجیتال را تنظیم‌گری می‌کند. براساس این قانون، دارایی‌های مالی دیجیتال، حقوق دیجیتالی هستند که می‌توانند به عنوان اوراق بهادار در نظر گرفته شوند با این تفاوت که بر بستر فناوری بلاکچین توسعه داده می‌شوند. در اول دسامبر ۲۰۲۰، وزارت دارایی روسیه لایحه‌ای در مورد اصلاحات بندهای اول و دوم قانون مالیات به مجلس روسیه ارائه داد. این لایحه، شامل مقرراتی است که گردش و مالکیت رمزارزها را تنظیم‌گری و مسئولیت نقض قوانین تعیین شده در این لایحه را مشخص می‌کند. براساس این لایحه، شهروندان، اشخاص حقیقی و حقوقی فعال در روسیه ملزم به افشای اطلاعات رمزارزهای تحت مالکیت خود و پرداخت مالیات مربوطه هستند. این اصلاحات قوانین مالیاتی نشان می‌دهد که رمزارز به عنوان یک دارایی در این کشور به رسمیت شناخته شده است. البته لازم به ذکر است که این لایحه هنوز به تصویب نرسیده و مجلس این کشور در حال بررسی آن است. با این حال طبق مقررات بالادستی در روسیه، واحد پولی این کشور، فقط روبل است و شهروندان نمی‌توانند از رمزارزها به عنوان پول استفاده و با آن اقدام به خرید و فروش کالا و خدمات کنند.

ایران: براساس مصوبه شورای عالی مبارزه با پولشویی در اردیبهشت‌ماه ۱۳۹۷، استفاده از رمزارزها توسط کلیه مؤسسات مالی از جمله بانک‌ها و مؤسسات اعتباری ممنوع است. براساس این اطلاعیه، هرگونه استفاده و خرید و فروش بیت‌کوین و سایر ارزهای دیجیتال در بانک‌ها، مؤسسات مالی، و صرافی‌های دارای مجوز بانک مرکزی رسماً ممنوع اعلام شد. به عبارتی، تنها بانک‌ها و صرافی‌های زیر نظر بانک مرکزی از خرید و فروش بیت‌کوین به طور رسمی منع شده‌اند و این حکم به معنای ممنوعیت کامل بیت‌کوین و رمزارزها نیست. اما براساس مصوبه هیئت وزیران در ششم مردادماه

۱۳۹۸ استفاده از رمزارزها صرفاً با قبول مسئولیت ریسک از سوی متعاملین امکان پذیر است. با توجه به این مصوبه، استخراج رمزارزها با اخذ مجوز از وزارت صنعت، معدن و تجارت مجاز شده است.

محدودیت و ممنوعیت برخی بخش‌ها

امارات: براساس نظر بانک مرکزی این کشور در سال ۲۰۱۷، کلیه معاملات رمزارزها ممنوع اعلام شد. در ژانویه ۲۰۱۸ نیز رئیس کل بانک مرکزی امارات مجدداً در خصوص معاملات رمزارزها هشدار داد. اما در ماه فوریه ۲۰۱۸ دوی به عنوان اولین کشور در منطقه خاورمیانه به یکی از شرکت‌های خود مجوز معامله رمزارزها را داده است.

قطر: در فوریه سال ۲۰۱۸ میلادی، بانک مرکزی قطر طی بخشنامه‌ای به کلیه بانک‌های قطر نسبت به معاملات با بیت کوین هشدار داد. در این بخشنامه، به این نکته اشاره شده که بیت کوین غیرقانونی است و از پشتیبانی بانک مرکزی یا حکومت برخوردار نیست. همچنین معاملات رمزارزها با ریسک بالای نوسانات قیمتی و ریسک استفاده در جرائم مالی همراه است. بر این اساس، بانک‌ها و مؤسسات مالی از فعالیت در زمینه رمزارزها منع شده‌اند.

بحرین: رئیس بانک مرکزی بحرین در خصوص رمزارزها به ویژه بیت کوین هشدار داده است. بنابر اعلام وی، فعالیت‌های مربوط به این ارزها در بحرین غیرقانونی است. با این حال، شهروندان بحرینی می‌توانند در خارج از بحرین به سرمایه‌گذاری در این بخش بپردازند.

مراکش: در اطلاعیه مطبوعاتی که در نوامبر سال ۲۰۱۷ میلادی در وبسایت رسمی دفتر مبادلات مراکش منتشر شد، مبادلات رمزارزها ممنوع و تهدیدات سختی نیز در رابطه با آن اعلام شد.

اکوادور: براساس اعلام بانک مرکزی اکوادور، بیت کوین روش پرداخت مجاز در این کشور نیست. همچنین با توجه به اینکه معاملات مالی با بیت کوین توسط هیچ نهادی در این کشور کنترل، نظارت، و مقررات گذاری نمی‌شود، ریسک مالی آنها بر عهده خود افراد است. البته خرید و فروش اینترنتی رمزارزها مانند بیت کوین بلا مانع است.

رویکرد منفی و بازدارنده (ممنوعیت)

برخی از کشورهای رویکرد ممنوعیت کلی را در مواجهه با رمزارزها اتخاذ کرده‌اند. در این میان برخی به دلایل سیاست‌گذاری این ممنوعیت را وضع کرده‌اند و برخی دیگر همچون کشور مصر علاوه بر بحث سیاست‌گذاری از باب شرعی نیز به این موضوع ورود کرده‌اند. **مصر:** بانک مرکزی مصر در ژانویه ۲۰۱۸، با استناد به ریسک بالای رمزارزها بیانیه‌ای صادر کرد و در آن، در رابطه با دادوستد رمزارزهایی مانند بیت‌کوین هشدار داد و تأکید کرد کلیه مبادلات در این کشور تنها باید براساس ارزش‌های رسمی بانک مرکزی انجام شود. همچنین، براساس فتوای «دارالافتاء مصر» که نهاد مقررات‌گذاری شریعت در این کشور است، معاملات بیت‌کوین حرام اعلام شده است. براساس بیانیه این نهاد، رمزارزها می‌توانند امنیت ملی و سیستم‌های مالی این کشور را مخدوش کنند و ضمناً از این قابلیت برخوردارند که در مواردی همچون تأمین مالی تروریسم و فعالیت‌های تروریستی استفاده شوند و به همین دلیل معاملات آنها شرعاً جایز نیست.

چین: قانون‌گذاری رمزارزها در کشور چین بسیار حائز اهمیت است، زیرا این کشور در صنعت استخراج و معامله رمزارزها سهم عمده‌ای دارد تا جایی که تغییر در سیاست‌های این کشور به‌طور مشخص روی قیمت بیت‌کوین اثر مستقیم دارد. بانک مرکزی چین برای بیش از سه سال، در حال مطالعه رمزارزها بوده و یک مؤسسه پول دیجیتال راه‌اندازی کرده است. ژوژیوچان، رئیس وقت مؤسسه پول دیجیتال وضعیت رمزارزها را در یک کنفرانس مطبوعاتی که در طول نشست سالانه کنگره ملی در مارس ۲۰۱۸ برگزار شد، بررسی کرده است. طبق گفته ژو، قانونگذاران، رمزارزها را به عنوان ابزاری برای پرداخت‌های خرد مثل اسکناس‌های کاغذی، سکه‌ها یا کارت‌های اعتباری، به رسمیت نمی‌شناسند. او گفت سیستم بانکداری هیچ کدام از رمزارزهای موجود و ارائه‌دهنده خدمات مرتبط را نمی‌پذیرد. پیش از این در ۴ سپتامبر ۲۰۱۷، هفت قانونگذار دولتی مشترکاً بیانیه‌ای در مورد جلوگیری از خطرات مالی ناشی از عرضه اولیه سکه در چین منتشر کردند. براساس این اعلامیه، این نوع تأمین مالی که از طریق رمزارزها انجام می‌شود، غیرقانونی است. این بیانیه هشدار داد از آنجا که توکن‌ها را سازمان‌های پولی صادر نکرده‌اند؛ بنابراین مورد قبول حاکمیت نیستند. از این رو وضعیت قانونی مشابهی با ارزهای حاکمیتی ندارند و نمی‌توانند

به عنوان ارز در بازار استفاده شوند و در گردش باشند. براساس این اطلاعیه، بانک‌ها و مؤسسات مالی در چین، از معامله با رمزارز منع شده‌اند و نمی‌توانند به صورت مستقیم و غیرمستقیم، خدمات مرتبط با رمزارز ارائه دهند. شایان ذکر است که در سال ۲۰۱۷ کلیه فعالیت‌های صرافی‌های رمزارزی ممنوع و ۱۷۳ بستر معاملاتی تعطیل شدند. همچنین در سال ۲۰۱۸ کلیه عملیات استخراج بیت‌کوین در چین توسط بانک خلق چین متوقف شد. **پاکستان:** در حال حاضر، هیچ قانون خاصی در رابطه با رمزارزها و نحوه مبادله آن در این کشور وجود ندارد. در می ۲۰۱۷ نیز بانک مرکزی این کشور طی بیانیه‌ای اظهار داشت که ارزهای دیجیتال را به رسمیت نمی‌شناسد و در ۶ آوریل سال بعد از آن نیز با انتشار بیانیه‌ای نسبت به ریسک‌های رمزارزها به عموم مردم هشدار داد.

الجزایر: مقامات این کشور در سال ۲۰۱۸ رسماً استفاده از هر نوع رمزارز را ممنوع اعلام کردند.

بنگلادش: در ۲۴ دسامبر ۲۰۱۷، بانک مرکزی بنگلادش با انتشار بیانیه‌ای غیرقانونی بودن رمزارزها را در این کشور اعلام کرد. براساس این بیانیه، مبادلات مالی با رمزارزها تخطی از مقررات مبارزه با پولشویی و تأمین مالی تروریسم است و از آنجایی که رمزارزها را مغایر با قوانین ضدپولشویی می‌دانند، برای استفاده از رمزارزها مجازات زندان تعیین شده است.

بولیوی: استفاده از رمزارزها در این کشور ممنوع اعلام شده است. براساس بیانیه بانک مرکزی بولیوی، استفاده از هر ابزار دارای ارزش که توسط مقامات پولی این کشور منتشر نشده ممنوع است. همچنین بانک مرکزی بولیوی با توجه به اینکه رمزارزهایی همانند بیت‌کوین مقررات‌گذاری نشده است، در خصوص زیان‌های احتمالی آنها به عموم مردم هشدار داده است.

رویکرد منفعلانه (عدم اتخاذ موضع دقیق در خصوص ممنوعیت یا عدم ممنوعیت)
عربستان سعودی: آژانس پولی عربستان سعودی^۱ در بیانیه‌ای با اشاره به اینکه بیت‌کوین تحت نظارت و به پشتوانه هیچ مرجع قانونی نیست، هشدار می‌دهد که بیت‌کوین صادر کرد.

1. Saudi Arabian Monetary, SAMA

این آژانس در اکتبر سال ۲۰۱۷ میلادی اعلام کرد که پروژه آزمایشی ارز دیجیتال محلی را تنها برای تسویه معاملات بین بانکی در دست بررسی دارد.

انگلستان: انگلستان هیچ قانونی ندارد که به طور خاص به رمزارزها اشاره کند. بنا بر اظهارات رئیس بانک مرکزی انگلستان می توان دریافت که این کشور در صدد قانونگذاری رمزارزها است. یک راه بهتر، قانونگذاری عناصر اکوسیستم دارایی های رمزنگاری شده برای مبارزه با فعالیت های غیرقانونی، ارتقای یکپارچگی بازار، محافظت، ایمنی و درستی نظام مالی خواهد بود. بند ۸۲ قانون ۱۹۹۸ بانکی انگلستان، مشخص می کند که بانک انگلستان مسئولیت محافظت و بالابردن ثبات نظام مالی بریتانیا را بر عهده دارد. براساس این هدف، بانک خطر ناشی از رمزارزها برای ثبات بازارهای مالی بریتانیا را در نظر گرفته است و معین کرده که حجم بازار رمزارز در حال حاضر به منظور ایجاد خطر برای ثبات مالی در بریتانیا به قدر کافی بزرگ نیست. با توجه به امور مالیاتی و گمرک، دولت انگلستان اظهار داشت که رمزارزها هویتی یگانه دارند؛ بنابراین نمی توانند مستقیماً با سایر اشکال سرمایه گذاری و سازوکارهای پرداختی، مقایسه و تطبیق داده شوند. مالیات بر ارزش افزوده فقط توسط تأمین کنندگان کالاها و خدمات فروخته شده در بریتانیا در تبادل با رمزارز، مستلزم پرداخت است.

عمان: بانک مرکزی عمان در سال ۲۰۱۸ میلادی، با انتشار بیانیه ای مطبوعاتی اعلام کرد که هیچ دستورالعمل و سیاستی در زمینه رمزارزها در این کشور وجود ندارد و هیچ مسئولیتی در قبال عواقب مالی احتمالی ناشی از معاملات رمزارزها متوجه این نهاد نخواهد بود.

ارمنستان: در مارس ۲۰۱۸، دولت ارمنستان با استناد به موضع گیری اکثر کشورهای پیشرو در خصوص رمزارزها، سندی را منتشر و طی آن اعلام کرد که استفاده از رمزارزها توصیه نمی شود. این سند در واکنش به پیش نویس قانونی در زمینه توسعه فناوری های دیجیتال که توسط یک حزب سیاسی مخالف مطرح شده بود انتشار یافت. براساس پیش نویس مذکور، فعالیت استخراج مشمول معافیت مالیاتی تا سال ۲۰۳۰ می شود.

شکل ۱ آخرین وضعیت موضع گیری کشورهای جهان در برابر رمزارزها را نشان

می‌دهد. در این شکل، سبز تیره نشانه مجاز بودن، سبز روشن نشانه تاحدی مجاز بودن، زرد نشانه محدودیت^۱، قرمز نشانه غیر مجاز بودن یا ممنوعیت و خاکستری نشانه عدم وجود اطلاعات یا قانونگذاری در کشور مورد نظر است.



شکل ۱: وضعیت رگولاتوری استفاده از رمزارز در جهان

جدول ۱ نیز وضعیت چند کشور را در این حوزه نشان می‌دهد. معمولاً هر کشور، رمزارزها را جهت نظارت و قانونگذاری راحت‌تر در دسته‌های مختلف ارزش^۲، پول^۳، دارایی^۴، کالا^۵ یا کالای تهاتری^۶ قرار می‌دهد که این وضعیت در قسمت دسته‌بندی جدول ذکر شده است. در مواردی که هیچ دسته‌بندی صورت نگرفته است عبارت «بدون دسته» و در موارد نبود اطلاعات کافی، عبارت «بدون اطلاعات» ذکر شده است.

-
1. Restricted
 2. Currency
 3. Money
 4. Property
 5. Commodity
 6. Barter good

جدول ۱: ماهیت رمزارزها در کشورهای جهان

نام کشور	دسته بندی	نام کشور	دسته بندی
۱. بلغارستان	ارز	۲۹. یونان	ارز
۲. کرواسی	ارز	۳۰. ایسلند	ارز
۳. آذربایجان	ارز	۳۱. انگلستان	ارز
۴. باهاماس	ارز	۳۲. ازبکستان	ارز
۵. قبرس	ارز	۳۳. اوکراین	ارز
۶. دانمارک	ارز	۳۴. لیتوانی	ارز
۷. مجارستان	ارز	۳۵. مالت	ارز
۸. استونی	ارز	۳۶. موناکو	ارز
۹. فنلاند	ارز	۳۷. اسپانیا	ارز
۱۰. ایران	ارز	۳۸. سوئیس	ارز
۱۱. ایرلند	ارز	۳۹. ونزوئلا	ارز
۱۲. ایتالیا	ارز	۴۰. سوئد	کالا
۱۳. لیختن اشتاین	ارز	۴۱. تایوان	کالا
۱۴. لوکزامبورگ	ارز	۴۲. ترکیه	کالا
۱۵. مکزیک	ارز	۴۳. بلاروس	کالا
۱۶. اتیوپی	ارز	۴۴. بوسنی و هرزگوین	کالا
۱۷. کاستاریکا	ارز	۴۵. فرانسه	کالا
۱۸. کوبا	ارز	۴۶. برزیل	کالا
۱۹. جمهوری چک	ارز	۴۷. گرینلند	کالا
۲۰. بلژیک	ارز	۴۸. هنگ کنگ	کالا
۲۱. ژاپن	ارز	۴۹. اسرائیل	کالا
۲۲. لتونی	ارز	۵۰. اندونزی	کالا
۲۳. رومانی	ارز	۵۱. هلند	کالا
۲۴. اسلواکی	ارز	۵۲. صربستان	کالا
۲۵. آفریقای جنوبی	ارز	۵۳. تایلند	کالا
۲۶. روسیه	ارز	۵۴. زیمبابوه	کالا
۲۷. سنگاپور	ارز	۵۵. نروژ	کالا
۲۸. اسلونی	ارز	۵۶. اتریش	کالای نهاتری

نام کشور	دسته‌بندی	نام کشور	دسته‌بندی
۵۷. کانادا	کالای تهاتری	۸۷. پاناما	بدون دسته
۵۸. آلمان	کالای تهاتری	۸۸. پرو	بدون دسته
۵۹. فیلیپین	کالای تهاتری	۸۹. امارات متحده عربی	بدون دسته
۶۰. استرالیا	دارایی	۹۰. کلمبیا	بدون دسته
۶۱. هند	دارایی	۹۱. جامائیکا	بدون دسته
۶۲. لهستان	دارایی	۹۲. اکوادور	بدون دسته
۶۳. پورتوریکو	دارایی	۹۳. کنیا	بدون دسته
۶۴. نیوزیلند	دارایی	۹۴. مالزی	بدون دسته
۶۵. ایالات متحده آمریکا	دارایی	۹۵. پاراگوئه	بدون دسته
۶۶. جزایر ویرجین	پول	۹۶. تونس	بدون دسته
۶۷. لیبی	پول	۹۷. بحرین	بدون اطلاعات
۶۸. گرجستان	بدون دسته	۹۸. شیلی	بدون اطلاعات
۶۹. جمهوری دومینیکن	بدون دسته	۹۹. باربادوس	بدون اطلاعات
۷۰. پریتغال	بدون دسته	۱۰۰. مالدیو	بدون اطلاعات
۷۱. کره جنوبی	بدون دسته	۱۰۱. چین	کالا
۷۲. غنا	بدون اطلاعات	۱۰۲. مصر	کالا
۷۳. کویت	بدون اطلاعات	۱۰۳. مراکش	بدون دسته
۷۴. لبنان	بدون اطلاعات	۱۰۴. نپال	بدون دسته
۷۵. کنگو	بدون اطلاعات	۱۰۵. قطر	بدون اطلاعات
۷۶. بلیز	بدون اطلاعات	۱۰۶. الجزیره	ارز
۷۷. مغولستان	بدون اطلاعات	۱۰۷. افغانستان	ارز
۷۸. عراق	بدون اطلاعات	۱۰۸. پاکستان	ارز
۷۹. نیکاراگوئه	بدون اطلاعات	۱۰۹. ویتنام	دارایی
۸۰. قزاقستان	ارز	۱۱۰. بولیوی	بدون اطلاعات
۸۱. قرقیزستان	ارز	۱۱۱. عربستان سعودی	بدون اطلاعات
۸۲. نیجریه	ارز	۱۱۲. بنگلادش	بدون اطلاعات
۸۳. اردن	ارز	۱۱۳. یمن	ارز
۸۴. آلبانی	کالا	۱۱۴. برمودا	بدون اطلاعات
۸۵. آرژانتین	دارایی	۱۱۵. کنگو	بدون اطلاعات
۸۶. اروگوئه	دارایی	۱۱۶. دومینیکا	بدون اطلاعات

نام کشور	دسته بندی	نام کشور	دسته بندی
۱۱۷. فیجی	بدون اطلاعات	۱۳۱. میانمار	بدون اطلاعات
۱۱۸. گینه	بدون اطلاعات	۱۳۲. عمان	بدون اطلاعات
۱۱۹. هندوراس	بدون اطلاعات	۱۳۳. رواندا	بدون اطلاعات
۱۲۰. ماداگاسکار	بدون اطلاعات	۱۳۴. سومالی	بدون اطلاعات
۱۲۱. موزامبیک	بدون اطلاعات	۱۳۵. سودان	بدون اطلاعات
۱۲۲. کره شمالی	بدون اطلاعات	۱۳۶. ترکمنستان	بدون اطلاعات
۱۲۳. فلسطین	بدون اطلاعات	۱۳۷. ارمنستان	بدون اطلاعات
۱۲۴. سنگال	بدون اطلاعات	۱۳۸. بوتان	بدون اطلاعات
۱۲۵. سریلانکا	بدون اطلاعات	۱۳۹. کامرون	بدون اطلاعات
۱۲۶. تاجیکستان	بدون اطلاعات	۱۴۰. گواتمالا	بدون اطلاعات
۱۲۷. آنگولا	بدون اطلاعات	۱۴۱. گینه بیسائو	بدون اطلاعات
۱۲۸. السالوادور	بدون اطلاعات	۱۴۲. ماکائو	بدون اطلاعات
۱۲۹. چاد	بدون اطلاعات	۱۴۳. جیبوتی	بدون اطلاعات
۱۳۰. مالی	بدون اطلاعات	۱۴۴. بورکینافاسو	بدون اطلاعات

قوانین و مقررات ایران

همانطور که در قسمت قبل ذکر شد، خرید و فروش رمزارزها و توکن ها به طور کلی در ایران برای عموم افراد مجاز هستند، حال آنکه قوانینی برای این حوزه تصویب شده است. اولین نسخه از قوانین این حوزه، با نام «الزامات و ضوابط حوزه رمزارزها» توسط اداره نظام های پرداخت بانک مرکزی جمهوری اسلامی ایران در بهمن ۱۳۹۷ منتشر شد.

در مقدمه این سند ذکر شده است بانک مرکزی جمهوری اسلامی ایران تأکید دارد گسترش استفاده از رمزارزها تأثیرات بالقوه ای بر سیاست های پولی و ارزی کشور خواهد داشت و همراه با ایجاد فرصت های جدید، تهدیدهایی را متوجه عموم مردم و سازمان های استفاده کننده از آن خواهد کرد. بنابراین بانک مرکزی جمهوری اسلامی ایران به منظور ممانعت از بروز صدمات، حمایت از حقوق مصرف کنندگان و تسهیل کسب و کار در این حوزه، چارچوب اولیه مقررات مرتبط با رمزارزها را که به تصویب

شورای پول و اعتبار رسیده است، اعلام می کند.

بانک مرکزی بنا بر وظایف مشخص شده در حوزه پولی و بانکی، برای آن بخش از حوزه هایی که می توانند بر سیاست های پولی و مالی کشور تأثیر گذار باشند، سیاست های مربوطه را در این سند تدوین کرده است. در ادامه به مفاد مهم این دستورالعمل اشاره می شود. لازم به ذکر است که نسخه اصلاحیه این سند آماده شده اما منتشر نشده است.

الزامات حوزه رمزارزهای جهان روا

- صدور و انتشار این نوع رمزارزها در اختیار توسعه دهندگان آن است و بانک مرکزی در این زمینه امکان پذیرش نقش و مسئولیتی ندارد.
- استفاده از رمزارزهای جهان روا به عنوان ابزار پرداخت در داخل کشور ممنوع است.
- رمزارزهای جهان روا تنها در صرافی هایی که مقررات آن در بخش الزامات عمومی صرافی ها آورده شده است، قابل خرید و فروش و تبادل هستند.
- توسعه کیف پول رمزارزی برای رمزارزهای جهان روا با در نظر گرفتن مقررات بخش کیف پول رمزارزی، برای اشخاص حقیقی و حقوقی بلامانع است.
- در حال حاضر استخراج رمزارزهای جهان روا در کشور به عنوان یک صنعت در نظر گرفته شده و مقررات گذاری در این حوزه از حیطة وظایف و نظارت بانک مرکزی خارج است.

الزامات حوزه عرضه اولیه سکه/توکن

- توسعه کیف پول رمزارزی برای نگهداری توکن ها با در نظر گرفتن مقررات بخش کیف پول، بلامانع است.
- از دیدگاه بانک مرکزی توکن دارای پشتوانه به چهار دسته توکن با پشتوانه ریال، توکن با پشتوانه طلا و سایر فلزات گران بها، توکن با پشتوانه ارز (دلار، یورو و غیره) و توکن با پشتوانه سایر دارایی های مشهود و غیر مشهود تقسیم می شوند.
- الزامات حوزه عرضه اولیه توکن با پشتوانه ریال، شامل موارد زیر است:

- انتشار توکن با پشتوانه ریال تنها در کنترل و اختیار بانک مرکزی جمهوری اسلامی ایران است.
- توکن با پشتوانه ریال تنها در بانک‌های مجاز و بانک مرکزی جمهوری اسلامی ایران قابل تبادل است.
- توکن با پشتوانه ریال می‌تواند به‌عنوان ابزار پرداخت در کشور استفاده شود.
- توکن با پشتوانه ریال قابلیت استخراج ندارد.
- الزامات حوزه عرضه اولیه توکن با پشتوانه طلا و فلزات گران‌بها، شامل موارد زیر است:
 - انتشار توکن با پشتوانه طلا و سایر فلزات گران‌بها پس از اخذ مجوز بانک مرکزی و با ضمانت بانک‌های کشور مجاز است.
 - توکن با پشتوانه طلا و فلزات گران‌بها در بانک‌های مجاز و صرافی‌ها، که مقررات آن در بخش صرافی‌ها آورده شده است، قابل تبادل است.
 - استفاده از توکن با پشتوانه طلا و فلزات گران‌بها به‌عنوان ابزار پرداخت در کشور ممنوع است.
 - توکن با پشتوانه طلا و فلزات گران‌بها قابلیت استخراج ندارد.
 - الزامات حوزه عرضه اولیه توکن با پشتوانه ارز، شامل موارد زیر است:
 - انتشار توکن با پشتوانه ارز تنها در انحصار بانک‌های دارای مجوز بانک مرکزی جمهوری اسلامی ایران است.
 - توکن با پشتوانه ارز در بانک‌های مجاز و صرافی‌ها، قابل تبادل است.
 - استفاده از توکن با پشتوانه ارز به‌عنوان ابزار پرداخت در کشور ممنوع است.
 - توکن با پشتوانه ارز قابلیت استخراج ندارد.
 - الزامات حوزه عرضه اولیه توکن با پشتوانه سایر دارایی‌های مشهود و غیرمشهود، شامل موارد زیر است:
 - انتشار توکن با پشتوانه سایر دارایی‌ها از حیطه نظارت و اختیارات بانک مرکزی خارج است و تابع قوانین بورس جمهوری اسلامی ایران خواهد بود.
 - مقررات در این حوزه با محوریت سازمان بورس و اوراق بهادار و با همکاری

- بانک مرکزی جمهوری اسلامی ایران تدوین و ابلاغ خواهد شد.
- توکن با پشتوانه سایر دارایی‌ها در بورس کالا و اوراق بهادار، قابل تبادل است.
 - استفاده از توکن با پشتوانه سایر دارایی‌ها به عنوان ابزار پرداخت در کشور ممنوع است.
 - توکن با پشتوانه سایر دارایی‌ها قابلیت استخراج ندارد.
 - الزامات حوزه عرضه اولیه توکن بدون پشتوانه، شامل موارد زیر است:
 - انتشار توکن بدون پشتوانه از حیطه وظایف بانک مرکزی خارج است و تابع قوانین بورس جمهوری اسلامی ایران خواهد بود.
 - توکن بدون پشتوانه در بورس کالا و اوراق بهادار، قابل تبادل است.
 - استفاده از توکن بدون پشتوانه به عنوان ابزار پرداخت در کشور ممنوع است.
 - مقررات گذاری در حوزه استخراج توکن‌های بدون پشتوانه، از حیطه وظایف و نظارت بانک مرکزی خارج است.

الزامات حوزه رمزارز بانک مرکزی (ملی)

- انتشار رمزارز ملی تنها توسط بانک مرکزی جمهوری اسلامی ایران مجاز است.
- رمزارز ملی تنها در بانک‌های مجاز و بانک مرکزی جمهوری اسلامی ایران قابل تبادل است.

منابع:

- (۱) گزارش کارشناسی: تحلیل ماهیت، استخراج و مبادله انواع رمزارزها و توکن‌ها از منظر فقه اسلامی و قوانین کشور، پژوهشکده پولی و بانکی بانک مرکزی جمهوری اسلامی ایران، پاییز ۱۳۹۹.
- (۲) مقدمه‌ای بر تنظیم‌گری رمزارزها در اقتصاد ایران (ویرایش اول)، مرکز پژوهش‌های مجلس، معاونت پژوهش‌های اقتصادی، تیر ۱۳۹۷.
- (۳) الزامات و ضوابط حوزه رمزارزها، اداره نظام‌های پرداخت معاونت فناوری‌های نوین بانک مرکزی جمهوری اسلامی ایران، نسخه ۰۰، بهمن ۱۳۹۷.
- (۴) ارز مجازی: قانونگذاری در کشورهای مختلف و پیشنهادها برای ایران، مرکز پژوهش‌های مجلس شورای اسلامی، شهریور ۱۳۹۷.
- (۵) دستورالعمل صدور جواز و پروانه بهره‌برداری برای فعالیت استخراج رمزارزها _ وزارت صنعت، معدن و تجارت _ شماره ۵۰۰۷.
- (۶) بررسی قانونگذاری رمزارزها در سراسر جهان، اداره حقوقی کتابخانه ملی کنگره آمریکا، ۲۰۱۸، مجموعه‌های ویراماینر و هشن‌بان، ۱۳۹۹.

[7] coin.dance/poli

[8] sena.ir

[9] https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory#North_America

[10] <https://www.loc.gov/item/global-legal-monitor/2021-01-11/russian-federaiion-newt-bill-defines-cryptocurrency-proposes-tax-regulations/>

بهره‌مندی‌ها و مزایای

برای سفارش اینترنتی این کتاب به وبسایت
فروشگاه انتشارات راه پرداخت مراجعه کنید
way2pay.shop



انتشارات راه پرداخت

دارایی دیجیتال مفهومی است که در سال‌های گذشته با رشد رمزارزهایی مانند بیت‌کوین مورد توجه قرار گرفته؛ حالا بسیاری از ما در کنار 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 در کنار دارایی‌های فیزیکی، دارایی‌های دیجیتال نیز در دنیای کسب‌وکارها نقش آفرینی 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.

ISBN 978-622-7702-10-1



۵۰۰ هزار تومان

انتشارات
راه پرداخت



ناشر فناوری و نوآوری
way2pay.press