

عصر
فضای
مجازی

عصر
فضای
مجازی

گزارش شماره ۵۵
بهمن ۱۳۹۹



مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

فناوری زنجیره بلوکه (معالجات تطبیقی، پلتفرم‌ها، کاربردها، فرایند کاری فناوری بلاکچین و...)

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در معاونت فناوری مرکز ملی فضای مجازی

تهیه‌کنندگان: مهندس مجتبی نصیری یار،
دکتر مریم حق شناس

حقوق مادی و معنوی این اثر متعلق به مرکز ملی فضای
مجازی است و استفاده از مطالب آن صرفاً با ذکر مأخذ
بلامانع است.

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش
خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست ۷

مقدمه ۱۱

بخش اول

تعاریف مرتبط با فناوری بلاکچین ۱۵

بخش دوم

مفاهیم مرتبط با فناوری بلاکچین ۱۹

بخش سوم

ارکان فناوری بلاکچین ۲۷

بخش چهارم

انواع بلاکچین ۳۱

بخش پنجم

مقایسه دفاترکل توزیع شده با بلاکچین ۳۷

بخش ششم

تأثیر بلاکچین بر صنایع مختلف ۴۱

بخش هفتم

پلتفرم‌های بلاکچین ۴۵

بخش هشتم

کاربردهای بلاکچین ۶۳

بخش نهم

اکو سیستم کاربردهای بلاکچین ۷۵

بخش دهم

الگوریتم کاربرد فناوری بلاکچین ۸۳

بخش یازدهم

مطالعه موردی کاربرد بلاکچین ۸۷

بخش دوازدهم

راه حل جامع بر مبنای بلاکچین ۹۵

بخش سیزدهم

مخاطرات فناوری بلاکچین برای کشورها ۱۰۱

جمع بندی ۱۰۷

فهرست جداول، نمودارها و عکس‌ها

- ۲-۱- اجزاء بلوک ۲۱
- ۲-۲- فرآیند ساخت زنجیره بلوکی ۲۳
- ۳-۱- اجماع توزیع یافته ۳۰
- ۳-۲- رایانش توزیع یافته ۳۰
- ۴-۱- حالت‌های توزیع یافتگی ۳۵
- ۴-۲- جدول توزیع یافتگی ۳۵
- ۶-۱- میزان تأثیر و امکان‌پذیری فناوری بلاکچین بر صنایع مختلف ۴۴
- ۷-۱- لایه‌های اصلی پلتفرم مایکروسافت ۴۷
- ۷-۲- پلتفرم مایکروسافت در صنعت هواپیمایی ۴۸
- ۷-۳- نمای کلی استارت‌آپ‌های بلاکچینی چین ۴۹
- ۷-۴- نمای کلی صنعت بلاکچین اتریش ۴۹
- ۷-۵- مدل مفهومی پلتفرم بلاکچین ۵۰
- ۷-۶- لوگوی پلتفرم اتریوم ۵۳
- ۷-۷- لوگوی پلتفرم هایپر لجر ۵۴
- ۷-۸- لوگوی پلتفرم مولتی چین ۵۴
- ۷-۹- لوگوی پلتفرم هیدراچین ۵۵
- ۷-۱۰- لوگوی پلتفرم اپن چین ۵۵
- ۷-۱۱- لوگوی پلتفرم آی بی ام ۵۶

- ۱۲-۷- لوگوی پلتفرم چین ۵۶
- ۱۳-۷- لوگوی پلتفرم آیوتا ۵۶
- ۱۴-۷- لوگوی پلتفرم آرتری کوردا ۵۷
- ۱۵-۷- لوگوی پلتفرم ریپل ۵۷
- ۱۶-۷- لوگوی پلتفرم کوروم ۵۸
- ۱۷-۷- جدول مقایسه پلتفرم های مختلف بر اساس معیارهای مشخص ۵۹
- ۱۸-۷- جدول مقایسه دیگری از پلتفرم های مختلف بر اساس معیارهای مشخص ۶۰
- ۱۹-۷- مقایسه پلتفرم ها از منظر سایت BLOCKDATA.TECH ۶۱
- ۱-۹- اکوسیستم آلمان ۷۸
- ۲-۹- اکوسیستم جهانی ۷۸
- ۳-۹- اکوسیستم ایران ۸۱
- ۱-۱۱- فرایند اعطای وام ۸۹
- ۲-۱۱- بکارگیری فناوری بلاکچین در فرایند اعطای وام ۹۰
- ۳-۱۱- نمایش لایه های اصلی در فرایند اعطای وام ۹۲

سخن نخست



فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گسترتری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصر فضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

مقدمه



تمرکز بر نقاط قوت یا ضعف در پذیرش فناوری‌های نوین، پرتگاه مواجهه فعال و مبتکرانه با ابعاد مختلف فضای مجازی است. دستگاه رسانه‌ای در هر صنعتی، سعی در پررنگ نمودن نقاط قوت فناوری‌هایی داشته که می‌توان به کمک آن‌ها، دامنه سلطه آن فناوری را گسترش دهد. برخی از فناوری‌ها به نقاط عطف نظام‌های اجتماعی تبدیل شده‌اند. این نقاط عطف نه فقط در سطح کاربرد، بلکه در فرهنگ و ساختارهای اجتماعی نیز نمایان می‌شود. یکی از فناوری‌هایی که اخیراً بسیار مورد توجه قرار گرفته و عملیات رسانه‌ای سنگینی نیز بر روی آن در حال اجراست، فناوری زنجیره بلوکی یا بلاکچین^۱ می‌باشد. این فناوری، اصطلاحی است که معانی متعددی برای افراد گوناگون دارد؛ برای توسعه دهندگان به عنوان مجموعه‌ای از پروتکل‌ها و رمزگذاری‌ها جهت ذخیره امن اطلاعات در شبکه‌های توزیع یافته، برای تجارت و اقتصاد به عنوان بستری برای طراحی واحدهای پولی دیجیتال، برای مهندسی به منزله عامل تحول نسل آینده اینترنت و برای دیگران، به مثابه وسیله‌ای برای دگرگونی جامعه و اقتصاد در جهت دست یافتن به جهانی غیرمتمرکز

محسوب می شود. دامنه این علم بسیار گسترده است و این یکی از دلایلی است که می گویند بلاکچین بزرگترین اختراع بشر بعد از اینترنت است. فناوری زنجیره بلوکی، یک دفتر کل ذخیره سازی شده است که داده ها در آن دسته دسته در بلوک هایی هم ساختار ذخیره شده و هر بلوک با استفاده از یک کد رمز، به بلوک بعد از خود متصل می شود. در صورت اتصال یک بلوک به زنجیره، صحت و اصالت داده های آن مورد تایید قرار گرفته و یک زنجیره متصل و معتبر به وجود می آید. بنابراین بلاکچین تنها یک تکنولوژی نیست بلکه یک فرهنگ و یک اجتماع است که هدف غایی آن رسیدن به جهانی منصفانه تر به وسیله تمرکز زدایی است.

در این کتاب، پس از بیان مقدمه و تعاریف مختلف این فناوری و مفاهیم مرتبط به آن، ارکان فناوری و سپس انواع آن توضیح داده شده است. پس از بیان تفاوت دفاتر کل توزیع شده با فناوری زنجیره بلوکی، پلتفرم های بلاکچین معرفی و مقایسه شده اند، در بخش دیگری کاربردهای مختلف فناوری بلاکچین بیان شده است. در بخش دیگری با بررسی اکوسیستم های کاربردهای بلاکچین در کشورهای آلمان، جهان و ایران، الگوریتم کاربرد این فناوری و راه حل جامع بر مبنای این فناوری تشریح شده است. در پایان نیز، مطالعه موردی درباره کاربرد این فناوری در اعطاء وام خرید کالای ایرانی و جمع بندی و پیشنهادات ارائه شده است.

بخش اول

تعاریف مرتبط با فناوری بلاکچین



بخش اول

تعاریف مرتبط با فناوری بلاکچین

۱-۱- دفتر کل توزیع شده^۱

اجماعی از داده‌های دیجیتال تکراری، اشتراک‌گذاری و همگام‌سازی شده است که از لحاظ جغرافیایی در جاهای مختلف، کشورها یا موسسات گسترده شده است. هیچ مدیر مرکزی یا ذخیره‌سازی متمرکز داده‌ای وجود ندارد. دفاتر کل توزیع شده، پایگاه داده‌ای است که بر اساس سازوکار و معماری داده توسط مشارکت‌کنندگان شبکه نگهداری و به‌روزرسانی می‌شود.^۲

۱-۲- هش^۳

رشته‌ای از اعداد و حروف است که توسط یک تابع ریاضی تولید می‌شود. به نحوی که تعدادی کاراکتر متغیر را به عنوان ورودی گرفته و آن را به رشته‌ای از اعداد و حروف با تعدادی ثابت تبدیل می‌کند. به طوری که کوچکترین تغییر در ورودی، مقدار خروجی را به طور کامل دگرگون می‌کند.

۱-۳- تراکنش^۴

تراکنش، توسط دو عامل مشتری و دیگری سرویس‌دهنده شکل می‌گیرد. بدین صورت که ابتدا درخواستی برای خدمت‌دهنده (مثلاً بانک)

1. Distributed Ledger
2. <https://fa.wikipedia.org>
3. Hash

4. Transaction

فرستاده می‌شود و اگر کل تقاضای مشتری به درستی انجام شود، مشتری در این تراکنش پس از دریافت رسید از سوی خدمت دهنده، حتماً باید تأیید انجام درخواستش را دریافت کند. و اگر یکی از مراحل این فرایند به درستی صورت نگیرد، کل تراکنش نادیده گرفته می‌شود.^۱

۴-۱- بلاکچین

بلاکچین از دو کلمه بلوک^۲ و زنجیره^۳ ایجاد شده است. این فناوری در حقیقت زنجیره‌ای از بلوک‌هاست. بر اساس تعاریفی متعدد، بلاکچین، یک دفتر کل یا پایگاه داده توزیع شده است. بدین معنی که مجموعه‌ای از بلوک‌ها که هر یک حاوی اطلاعات و رمزگذاری خاص است، به صورت زنجیروار با یکدیگر در ارتباط هستند و می‌توان با آن تراکنش‌ها را به صورت دائمی ذخیره کرد به طوری که قابل حذف نبوده و تنها به طور مداوم در حال به‌روز شدن است.

بلاکچین یک نوع پایگاه داده غیر متمرکز است که سوابق رمزنگاری شده معاملات دیجیتال را در یک فهرست توزیع شده نگه می‌دارد. به عبارتی، بلاکچین دارای یک شبکه توزیع شده از پایگاه داده‌های تکرار شونده است که از طریق اینترنت/ شبکه همگام سازی شده و برای هر کسی که به شبکه دسترسی دارد، قابل دسترسی است. بنا به تعریف دیگری، یک نوع سیستم ثبت اطلاعات و گزارش است که میان همه اعضای شبکه به اشتراک گذاشته می‌شوند و با استفاده از رمزنگاری امکان حذف و تغییر اطلاعات ثبت شده تقریباً غیرممکن است.

1. <https://fa.wikipedia.org>
2. Block
3. Chain

بخش دوم

مفاهیم مرتبط با فناوری بلاکچین



بخش دوم

مفاهیم مرتبط با فناوری بلاکچین

۲-۱- بلوک

مجموعه‌ای از تراکنش‌هاست که به یکدیگر متصل شده‌اند. هر بلوک همانطور که در شکل ۲-۱-۲ نمایش داده شده است، شامل داده^۱، هش^۲، هش بلوک قبلی^۳، سرتیتز بلوک^۴ و زمان^۴ است، در ادامه تعاریف هر کدام از اجزاء ارائه شده است:



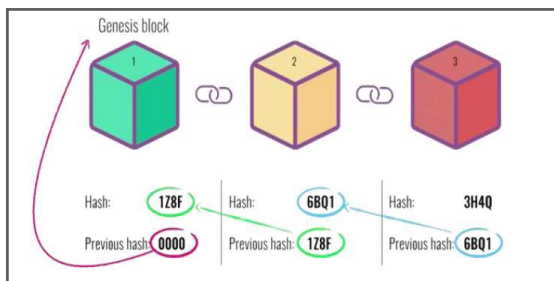
۲-۱- اجزاء بلوک

۱. داده/محتوی: به مجموعه‌ای از تراکنش‌ها در یک بلوک می‌گویند.

۲. هـش: یک رشته منحصر به فرد است که در زمان ایجاد یک بلوک، محاسبه می‌شود و هر تغییری در بلوک موجب تغییر در آن می‌گردد، از این رو پارامتری کاربردی برای تشخیص تغییرات در بلوک به حساب می‌آید. به طوری که اگر هـش تغییر کند به معنای آن است که این بلوک دیگر بلوک سابق نیست.
۳. هـش بلوک قبلی: با توجه به اینکه هـش بلوک قبلی برای ایجاد هـش بلوک بعدی مورد استفاده قرار می‌گیرد، پس تغییر هـش هر بلوک، باعث تغییر و انقطاع زنجیره بلوکی می‌شود.
۴. سر تیتز بلوک: مجموعه‌ای از اطلاعات کلی همانند نوع داده، دسته داده و ... در هر بلوک است.
۵. زمان: زمان ایجاد هر بلوک و اتصال آن به زنجیره بلوکی می‌باشد.

۲-۲- ساخت زنجیره بلوکی

ابتدا دسته‌ای از تراکنش‌ها انتخاب شده و صحت و درستی این تراکنش‌ها نسبت به زنجیره بلوکی قبلی (زنجیره بلوکی که تاکنون تشکیل شده است) سنجیده شده سپس برای این مجموعه تراکنش و سایر اطلاعات تکمیلی همانند زمان، هـش بلوک قبلی و ... هـش مخصوص این بلوک ایجاد شده و در آن ذخیره می‌شود، فرآیند زنجیر کردن این بلوک در زمان ذخیره‌سازی هـش بلوک قبلی در این بلوک و ایجاد هـش مربوطه انجام می‌پذیرد.



۲-۲- فرآیند ساخت زنجیره بلوکی

این زنجیره بلوکی، ۳ ویژگی شاخص دارد. اولین ویژگی که این دفتر کل را از سایر روش‌های ذخیره‌سازی متمایز می‌کند، ذخیره‌سازی توزیع‌شده یا غیرمتمرکز این زنجیره است. همزمان بر روی تجهیزات ذخیره‌سازی کاربران متعدد قرار دارد و هر کسی می‌تواند نسخه‌ای از آن را داشته باشد. البته اجازه دسترسی و نگهداری از نسخ نیز، منوط به نوع زنجیره بلوکی است. یعنی اگر زنجیره اختصاصی باشد، صرفاً کسانی که صلاحیت دارند، می‌توانند یک نسخه از آن را نگهداری کنند و دسترسی عمومی صرفاً در زنجیره‌های بلوکی عمومی ممکن است. این دسترسی می‌تواند شامل ایجاد و مشاهده تراکنش و یا ساخت بلوک باشد. ویژگی مذکور به توسعه فایل سیستم‌های توزیع‌شده^۱ (IPFS) - که پروتکل و شبکه‌ای برای ایجاد محتوای قابل آدرس‌دهی و به صورت نظیر به نظیر^۲، برای اشتراک‌گذاری و ذخیره‌سازی محتوای فرا رسانه‌ای^۳ در فایل سیستم‌های توزیع‌شده است، بسیار کمک خواهد کرد.

بر اساس ویژگی دوم که رمزگذاری داده هاست، محتوای هر بلوک پس از تکمیل و تایید، رمزنگاری شده و به یک کد رمز تبدیل می‌شود. از این کد رمز برای اتصال میان بلوک‌های متوالی استفاده

می‌شود، به این صورت که اتصال بلوک‌های هر زنجیره از طریق جاسازی کد رمز هر بلوک در بلوک بعدی خود صورت می‌پذیرد. ذخیره‌سازی داده‌ها به نحوی انجام می‌شود که کد رمز هیچ یک از بلوک‌ها شبیه هم نباشد. ویژگی متمایز سوم این زنجیره نسبت به سایر روش‌های ذخیره‌سازی، غیرقابل تغییر بودن داده‌های آن است. از آنجاییکه حذف یک بلوک منجر به قطع زنجیره خواهد شد و تغییر محتویات هر بلوک نیز موجب تغییر کد رمز همان بلوک می‌شود. بدلیل عدم همخوانی کد رمز جدید بلوک با کد رمز سابق، بلوک‌های بعدی نامعتبر شده و متعاقبا قطع زنجیره را موجب می‌شود.

۲-۳- مکانیزم بلاکچین

در مکانیزم زنجیره بلوکی، داده‌ها دسته‌دسته در بلوک‌هایی هم‌ساختار ذخیره شده و هر بلوک با استفاده از یک کد رمز به بلوک بعد از خود متصل می‌شود. در صورت اتصال یک بلوک به زنجیره، صحت و اصالت داده‌های آن مورد تایید قرار گرفته و یک زنجیره متصل و معتبر به وجود می‌آید، در حقیقت فناوری بلاکچین، یک فناوری بنیادی نیست بلکه مجموعه‌ای از فرایندهای هش‌گذاری و رمزنگاری، توزیع جمعی و ... است که باعث ایجاد ایده بلاکچینی شده‌اند.

۲-۴- استخراج کننده / اعتبار سنج

استخراج کردن یا اصطلاحا ماینینگ، به فرآیند ایجاد بلوک از تجمیع تعدادی تراکنش، بر اساس قوانینی خاص، رمزگذاری، زنجیر و توزیع نمودن آنها توسط کاربران در شبکه اطلاق شده و عموماً با انواع روش‌های مرسوم در تئوری بازی‌ها، مشوق‌هایی برای کاربران جهت تکمیل این فرآیند، به عنوان پاداش در نظر گرفته می‌شود.

۵-۲- قراردادهای هوشمند^۱

قرارداد هوشمند، مجموعه‌ای از قوانین توافقی است که تراکنش‌های کسب و کار براساس آن توافقات اجرا می‌شوند و در بلاکچین ذخیره و به صورت خودکار به عنوان بخشی از هر تراکنش اجرا میشوند^۲. قراردادهای هوشمند شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای تمام اقدامات هدف گذاری شده به طور خودکار می‌باشند. اساساً یک قرارداد هوشمند، کدهای کامپیوتری است که به عنوان مجموعه‌ای از قوانین، برای همکاری بین دوطرف یک مبادله، از پیش تعیین شده است. به عنوان یک نرم افزار میانی، تسهیل، تأیید و اجرای یک مذاکره یا قرارداد را تضمین می‌کند. یک قرارداد هوشمند می‌تواند نماینده یک قرارداد، حقوق مالکیت/بهره برداری و یا کالای فیزیکی (به کمک فناوری‌های بارکد و RFID) باشد.

۶-۲- انواع کاربران بلاکچین

کاربران این فناوری، از منظر استفاده از آن، به ۴ دسته (ماینرها)، (ایجادکنندگان تراکنش)، (حکمرانان فناوری بلاکچین) و (استفاده کننده داده) تقسیم می‌شوند.



بخش سوم

ارکان فناوری بلاکچین



✓ هویت: مجموعه عوامل موثر در فناوری بلاکچین، می بایست طبق مکانیزم مشخصی احراز هویت شوند، از جمله این مکانیزم‌ها می‌توان به امضاء دیجیتال، بارکد و... اشاره نمود.

✓ شبکه^۱: به اتصال دو یا چند سیستم که قابلیت انتقال اطلاعات دارند شبکه می‌گویند. شبکه انواع مختلفی دارد:

نظیر به نظیر: یکی از اصولی که شبکه بلاکچین به آن پایبند است ارتباط نظیر به نظیر اعضای شبکه^۲ است، که در این ارتباط هیچ عضوی به عنوان واسط و یا سرور در میان نیست.

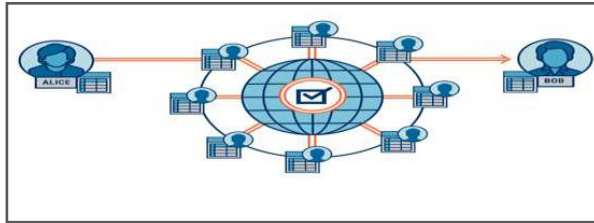
اجماع توزیع یافته: یکی از وظایف مهم در مکانیزم بلاکچین، مسئله قضاوت و تایید صحت تراکنش‌های انجام شده است، این قدرت قضاوت میان اعضای شبکه تقسیم میشود. به نحوی که برای صحت تراکنشی، باید ۵۰ درصد به علاوه یکی از اعضا که استخراج کننده^۳ شناخته می‌شود. آن را تایید کنند. به این روند در اصطلاح اجماع توزیع یافته می‌گویند که یکی از ارکان اصلی تمرکز زدایی به شمار می‌رود. در فناوری بلاکچین برای ارزیابی و تأیید از پروتکل‌های اجماع^۴ مختلفی استفاده می‌کنند که موجب افزایش بار محاسباتی و به عبارتی

ناممکن شدن رمز گشایی و نفوذ به زنجیره می گردد.



۳-۱- اجماع توزیع یافته

رایانش توزیع یافته^۱: رایانش توزیع یافته، سیستمی است که اجزای آن بر روی گره‌های شبکه‌ای مختلف قرار می‌گیرند و با ارسال پیام به یکدیگر متصل می‌شوند، با توجه به اصل تمرکززدایی بلاکچین، بار محاسباتی میان ماینرها تقسیم می‌گردد و در اصطلاح رایانش به صورت توزیع یافته صورت می‌گیرد. رایانش توزیع شده، مدلی است که در آن اجزای یک سیستم نرم‌افزاری در میان رایانه‌های متعدد در جهت بهبود کارایی و عملکرد، به اشتراک گذاشته می‌شوند.^۲



۳-۲- رایانش توزیع یافته

- ✓ پروتکل: قواعد و قوانین مربوط به ارسال، تایید، ثبت و پاداش تراکنش‌ها در فناوری بلاکچین است.
- ✓ پلتفرم: زیرساختی که بلاکچین بر روی آن با استفاده از پروتکل‌ها، ارتباطات توزیع یافته و هویت اجرا می‌شود.

1. Distributed Computing
2. <https://whatis.techtarget.com/definition/distributed-computing>

بخش چهارم

انواع بلاکچین



بخش چهارم

انواع بلاکچین

بر اساس مطالعات پارلمان اتحادیه اروپا در فوریه ۲۰۱۷، فناوری بلاکچین از منظر حدود دسترسی، هدف کاربرد در انحصار و توزیع یافتگی به دسته های متفاوتی تقسیم بندی می شود.

۱-۴- از منظر حدود دسترسی

بلاکچین از منظر حدود دسترسی به دو دسته عمومی^۱ (امکان دسترسی عموم کاربران به کل یا بخشی از داده ها بدون مجوز) و خصوصی^۲ (امکان دسترسی عده خاصی از کاربران به کل یا بخشی از داده ها) تقسیم می شود. در نوع عمومی، منبع قدرت و اختیاری برای صدور اجازه برای مشارکت در ایجاد، چک کردن و خواندن تراکنش ها و زنجیره بلوکی وجود نداشته و همه اعضا می توانند مشارکت نمایند. در نوع خصوصی، سطح دسترسی برای تعدادی از عملکردها همچون مدیریت کاربران، مدیریت پروتکل، مدیریت شبکه، چک کردن و اضافه نمودن تراکنش یا زنجیره بلوکی تعریف می شود. این موضوع به بازیگران اصلی در یک حوزه کسب و کار (همانند دولت ها و بانک ها) این امکان را می دهد که بتوانند بلاکچین خود را کنترل نمایند.^۳

۲-۴- از منظر هدف کاربرد در انحصار^۱

بلاکچین از منظر هدف کاربرد در انحصار، به دو دسته ضد انحصاری و انحصاری تقسیم‌بندی می‌شود. در نوع اول، از ویژگی‌های بلاکچین برای از حذف انحصار در یک کاربرد یا کسب و کار استفاده می‌شود، مانند: استفاده از بلاکچین در موضوعات داده‌های باز و بیت کوین. اما در نوع انحصاری، از ویژگی‌های بلاکچین برای ایجاد انحصار در یک کاربرد یا کسب و کاری استفاده می‌شود. در این بلاکچین افراد خاصی برای تأیید فعالیت‌ها انتخاب می‌شود. داده‌ها قابل مشاهده برای عموم هستند اما می‌توان از یک سری اطلاعات خاص محافظت کرد. مانند: تأیید اصالت محصول و کالا، صدور پاسپورت و شناسنامه و انواع مجوزها.

۳-۴- از منظر توزیع

بلاکچین از منظر توزیع شدگی، مطابق شکل ۱-۴- و جدول ۲-۴- به سه حالت متمرکز^۲ (مدیریت شبکه توسط یک هسته مرکزی)، غیرمتمرکز^۳ (مدیریت شبکه توسط چند گره به صورت غیرمتمرکز) و توزیع یافته^۴ (مدیریت شبکه توسط کاربران) تقسیم می‌شود. در حالت متمرکز، تمام عملیات قانون‌گذاری، ماینینگ و... در یک نقطه متمرکز و الباقی کارکردها برای عموم به اشتراک گذاشته می‌شود. شبکه‌های متمرکز توسط یک نهاد واحد کنترل می‌شوند. چنین شبکه‌هایی تحمل خطا ندارند، برخی ارزها مانند Ripple و Tether توسط شرکت‌های متمرکز کنترل می‌شوند.^۵ شبکه‌های غیرمتمرکز، شبکه‌هایی هستند که در آن کاربران نهایی به گره‌های قابل اعتمادی متصل می‌شوند که به یکدیگر متصل هستند، مانند Electrum.

1. <https://arzdigital.com/what-is-blockchain-technology>

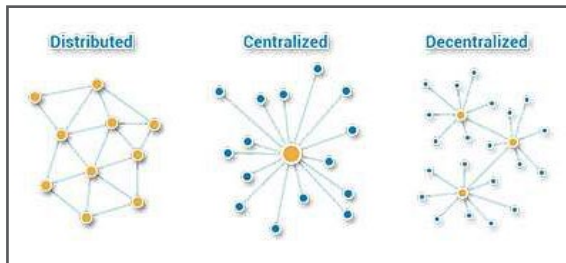
2. Centralized

3. Decentralized

4. Distributed

5. <https://u.today/cryptotips-centralized-decentralized-distributed-networks-explained>

چنین طیفی به کاربر نهایی برای دانلود یا تایید بلاکچین نیاز ندارد، در عوض، کاربران با یکی از سرورهای ممکن ارتباط برقرار می کنند. هر یک از سرورها هم با یکدیگر ارتباط برقرار می کنند. در واقع در حالت غیر متمرکز در نقاط خاصی کار کردها بصورت خصوصی ذخیره شده و الباقی دسترسی ها بصورت عمومی توزیع می شوند. اکثر رمزنگاری ها بر روی شبکه های توزیع شده صورت می گیرد. در این شبکه ها، هر کاربر می تواند با هر کاربر دیگری در شبکه ارتباط برقرار کند. چنین شبکه هایی بیشترین مقاومت را دارند. در واقع در حالت توزیع شده، هر کاربر فقط به اطلاعات عمومی دسترسی دارد.



۴-۱- حالت های توزیع یافتگی

توزیع یافتگی	عمومی	خصوصی	انحصاری	ضد انحصاری
متمرکز	*			*
متمرکز		*	*	
غیر متمرکز		*		*
غیر متمرکز	*			*
توزیع یافته	*			*

۴-۲- جدول توزیع یافتگی

بخش پنجم

مقایسه دفا ترکل توزیع شده با بلاکچین



مقایسه دفاتر کل توزیع شده با بلاکچین

شرکت‌ها از تکنولوژی دفتر کل توزیع شده برای پردازش یا تأیید اعتبار معاملات یا سایر رکوردها استفاده می‌کنند. رکوردها در صورت به اجماع رسیدن اکثریت، در دفتر کل^۱ ذخیره می‌شوند. هر رکورد ذخیره شده در دفتر توزیع شده، زمانبندی شده است و امضای رمزنگاری خاص خود را دارد. همه شرکت کنندگان در دفتر کل، می‌توانند تمام سوابق را مشاهده کنند. این فناوری یک تاریخچه قابل تایید و قابل اطمینان از تمام اطلاعات ذخیره شده را فراهم می‌کند. اغلب، تکنولوژی دفتر کل توزیع شده با عنوان DLT در محافل مالی و دولتی به کار می‌رود.^۲

بلاکچین، دفتر کل توزیع شده نیست. بلکه تنها یک نوعی از دفتر کل توزیع شده است که دارای سازوکار مختص به خود است. دفاتر کل متعددی مانند هش گراف^۳، تنگل^۴ و... نیز وجود دارد که بلاکچین یکی از انواع آنها است. در این دفتر کل، اطلاعات و داده‌ها رمزنگاری می‌شوند و در بلوک‌های بهم پیوسته قرار داده می‌شوند. بلاکچین نیز انواع مختلفی دارد که بر اساس چارچوب‌های مختلفی کار می‌کند.

1. Ledger

2. <https://media.consensus.net/blockchain-vs-distributed-ledger-technologies1-e0289a87b16>

3. Hash Graph

4. Tangle

بخش هشتم

تأثير بلاکچین بر صنایع مختلف



تأثیر بلاکچین بر صنایع مختلف

بر اساس تحقیقات صورت پذیرفته، اهمیت استراتژیک بلاکچین در صنایع مهم تبیین شده است. لذا بررسی میزان تأثیر و امکان‌سنجی صنایع مختلف برای درک بهتر ارزش استراتژیک بلاکچین و چگونگی بهره‌گیری از آن الزامی است. بر اساس نتایج تجزیه و تحلیل مک‌کینزی^۱ در صنایع مختلف، سه دیدگاه اصلی در خصوص ارزش استراتژیک بلاکچین ایجاد شده است:

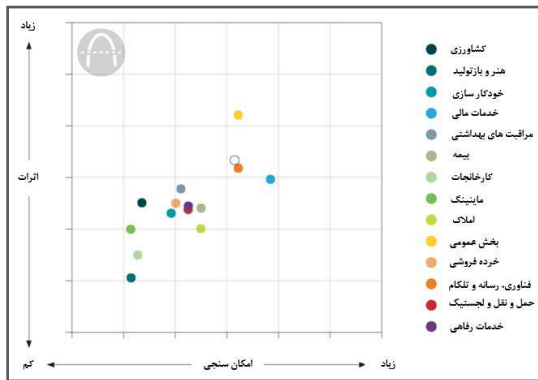
(۱) این فناوری برای ایجاد ارزش نیازمند واسطه‌گر نیست. در واقع واقعیتی است که موجب مشوق سازی جهت انجام برنامه‌های تجاری مجاز می‌شود.

(۲) این فناوری عمدتاً و به‌طور کوتاه‌مدت، قبل از ایجاد مدل‌های تجاری در کاهش هزینه‌ها تحول ایجاد خواهد کرد.

(۳) این فناوری در طی ۳ تا ۵ سال آینده، به دلیل وجود مسئله رقابت در ایجاد استانداردهای مشترک، از میزان امکان‌سنجی کمی برخوردار است.

فرصت‌هایی که این فناوری در صنایع مختلف ایجاد نموده، به تفکیک بر اساس شاخص‌های میزان تأثیر (Impact) و امکان‌سنجی

(Feasibility) در نمودار ۱-۶- نمایش داده شده است. به طور مثال از جنبه میزان تأثیر این فناوری، می‌توان به تأثیرپذیری زیاد بخش عمومی (Public sector) اشاره کرد. همچنین از جنبه امکان‌سنجی، خدمات مالی بیشترین میزان را داراست. در صنعت خرده‌فروشی نیز، از لحاظ میزان تأثیر و امکان‌سنجی، حد میانه‌روی و تعادل مشاهده شده است.



۱-۶- میزان تأثیر و امکان‌پذیری فناوری بلاکچین بر صنایع مختلف

بخش هفتم

پلتفرم‌های بلاکچین

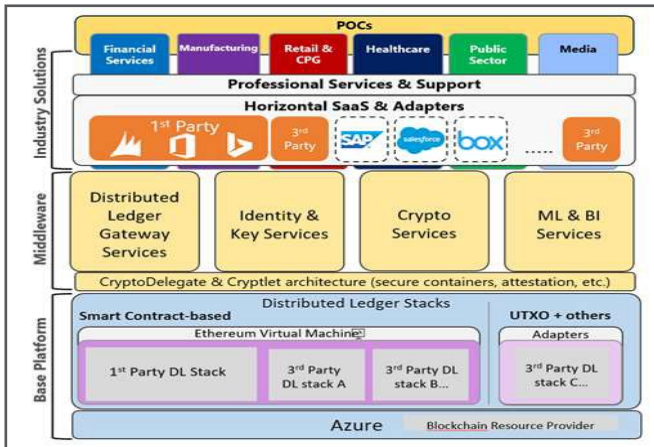


بخش هفتم

پلتفرم‌های بلاکچین

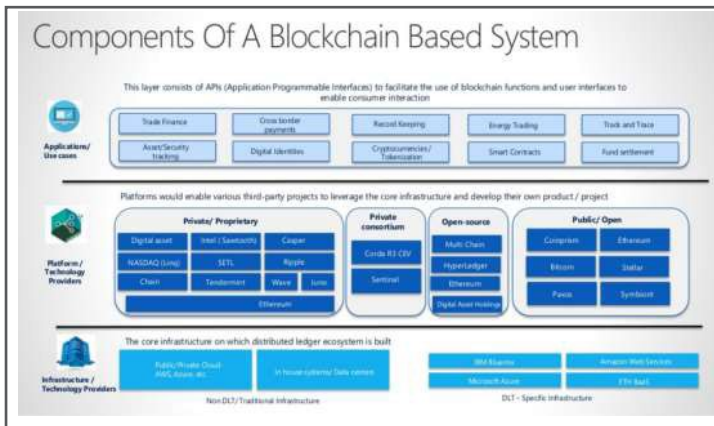
۷-۱- اجزاء پلتفرم‌های بلاکچین

طبق مطالعات انجام شده، اجزاء هر یک از پلتفرم‌های بلاکچین، متفاوت هستند. به عنوان مثال، اجزای پلتفرم شرکت مایکروسافت که به سه لایه پلتفرم پایه، لایه میانی (واسط) و لایه راه‌حل‌های صنعتی تقسیم‌بندی شده، در شکل ۷-۱ نشان داده شده است.

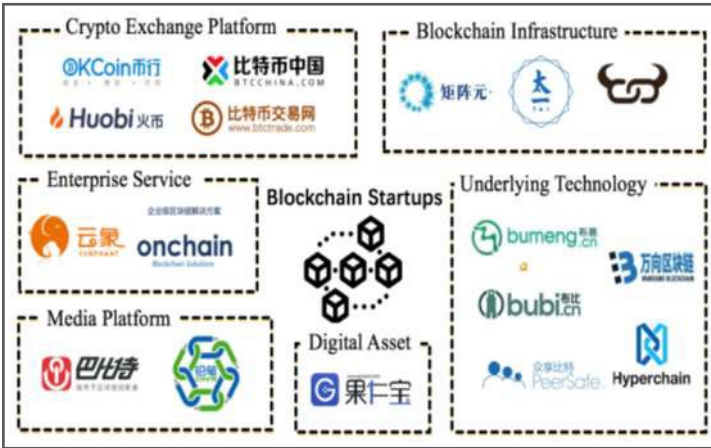


۷-۱- لایه‌های اصلی پلتفرم مایکروسافت

پلتفرم مایکروسافت در صنعت هواپیمایی و لجستیک، تقسیم بندی دیگری دارد که مطابق شکل ۲-۷- دارای سه لایه تامین کنندگان فناوری زیرساخت، تامین کنندگان فناوری پلتفرم ها و اپلیکیشن ها/ موارد مورد مطالعه است. لایه اول، زیرساخت مرکزی است که زیست بوم دفاتر کل توزیع شده بر روی آن توسعه می یابند. در لایه دوم، پلتفرم ها، شرایطی را برای سایر توسعه دهندگان پروژه های خود و هسته پلتفرم فراهم می کند تا توسعه یابند.



۲-۷- پلتفرم مایکروسافت در صنعت هواپیمایی



۳-۷- نمای کلی استارت‌آپ‌های بلاکچینی چین

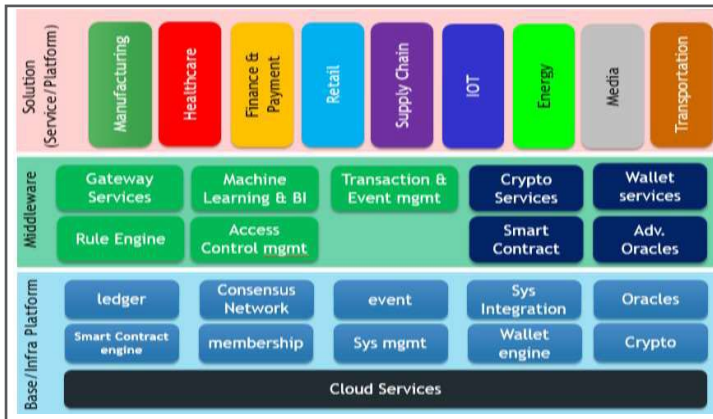


۴-۷- نمای کلی صنعت بلاکچین اتریش

۲-۷- مدل مفهومی پلتفرم بلاکچین

بر اساس مطالعات صورت گرفته و بررسی پلتفرم‌های مختلف، نهایتاً

مدل مفهومی تجمیعی مطابق شکل ۵-۷- برای پلتفرم‌های بلاکچین طراحی گردید که در سه سطح پلتفرم پایه (زیرساختی)، لایه میانی (واسط) و راه‌حل‌ها (پلتفرم‌ها / سرویس‌ها) تقسیم بندی می‌شود.



۵-۷- مدل مفهومی پلتفرم بلاکچین

این مدل، در لایه اول علاوه بر سرویس ابری^۱، دارای اجزاء دیگری مانند دفترکل، شبکه اجماع^۲ و ... است که در ادامه به تشریح هر یک از آنها می‌پردازیم:

* دفتر کل: از جنس پایگاه داده و شامل تراکنش، بلوک، زنجیره و هش‌های ایجاد شده است.

* شبکه اجماع: مسئولیت مدیریت مکانیزم‌ها و یکپارچگی دفترکل تکرار شده^۳ در شبکه اجماع را به عهده دارد.

* رخداد^۴: ایجادکننده اعلان‌های مربوط به عملیات مشخصی در سیستم، مانند ایجاد بلوک جدید و اعلان‌های مربوط به قرارداد هوشمند (توزیع رخدادها را شامل نمی‌شود)، است.

1. Cloud services
2. Consensus Network
3. Replicated

4. Event

* یکپارچگی سیستم^۱: مسئول یکپارچگی داخلی و ارتباطات چندجانبه خارجی سیستم را به عهده دارد (جزئی از سیستم بلاکچین نیست اما از آن استفاده می کند)

* اوراکلز^۲: مسئولیت فیدکردن اطلاعات خارج از بلاکچین به داخل سیستم را به صورت امن و قابل اعتماد بر عهده دارد و به دو صورت نرم افزاری و سخت افزاری وجود دارد.

* موتور قرارداد هوشمند: تراکنش‌های شبکه کسب و کار را به صورت کد کامپیوتری تجمیع کرده و منجر به دریافت یا ثبت تراکنش در پلتفرم بلاکچین می‌شود.

* عضویت^۳: مدیریت هویت و گواهی‌های تراکنش‌ها

* مدیریت سیستم^۴: مسئولیت ایجاد، تغییر و نظارت بر اجزاء پلتفرم بلاکچین را به عهده دارد.

* موتور اعتباری^۵: مدیریت اعتبارات کاربر به صورت امن.

* رمزنگاری^۶: مدیریت رمز ارز و موضوعات مرتبط همچون ICO^۷

لایه دوم نیز دارای اجزایی مانند درگاه سرویس^۸، موتور قوانین^۹ و ... است که در ادامه به تشریح آنها می‌پردازیم:

* درگاه سرویس: مدیریت خدمات مربوط به توزیع دفاتر کل و ارتباطات نظیر به نظیر یا سایر ارتباطات را بر عهده دارد.

* موتور قوانین: موتور مدیریت قوانین و قواعد کسب و کاری سیستم (قواعد پذیرش یا رد تراکنش‌ها).

* یادگیری ماشین و هوش تجاری^{۱۰}: خدمات یادگیری ماشینی و هوشمندی کسب و کار.

* مدیریت رخداد و تراکنش^{۱۱}: مدیریت تراکنش‌ها و رخدادهای سیستم.

1. System Integration
2. Oracles
3. Membership
4. System mgmt
5. Wallet Engine
6. Cryptocurrency

7. Initial Coin Offering
8. Gateway Service
9. Rule Engine
10. Machine learning & BI
11. Transaction & Event mgmt

* مدیریت کنترل دسترسی^۱: مدیریت سطح دسترسی کارکردها، تراکنش ها، بلوک ها، گزارش ها یا اجزاء سیستم.

* سرویس های رمزنگاری^۲: خدمات رمز ارز همانند انتقال ارز، افزایش موجودی، انواع پرداخت.

* سرویس های اعتباری^۳: خدمات کیف پول مانند امنیت بیشتر، پرداخت های تکرار شونده، نگهداری چند نوع رمز ارز.

* قرارداد هوشمند: خدمات قراردادهای هوشمند پیشرفته تر نسبت به موتور اصلی، شامل رویه های خودکار ذخیره شده^۴ و trigger هایی که به صورت چند جانبه تاثیر می گذارند.

* اوراکلز پیشرفته: خدمات اوراکلز پیشرفته (توسعه پروتکل های SNMP).

لايه سوم نیز دارای اجزایی است که نشان از ارائه سرویس بلاکچینی در حوزه های مختلفی مانند تولید، بهداشت و سلامت، مالی و پرداخت، خرده فروشی، زنجیره تامین، اینترنت اشیا، انرژی، رسانه و حمل و نقل است.

۳-۷- عناصر یک پلتفرم بلاکچینی موفق

از جمله عوامل تأثیرگذار بر موفقیت یک پلتفرم بلاکچینی، می توان به محرمانگی، شفافیت، کاهش هزینه های عملیاتی و کاهش هزینه تراکنش ها اشاره کرد. از لحاظ محرمانگی، این فناوری باید دارای قابلیت هایی همچون دفاتر کل جداگانه^۵، ایجاد تراکنش های محرمانه و قابلیت Zero-knowledge validation باشد. شفافیت، عامل مهم دیگری است که فناوری بلاکچین از آن برخوردار است و مانع بسیاری از سوءاستفاده ها می شود. بلاکچین، ترکیبی از حریم خصوصی و مسئولیت پذیری است و این ویژگی خاص، این فناوری را امن کرده و مزیتی خوب برای کاربران و تهدیدی جدی برای مجرمان سایبری است.

1. Access control mgmt
3. Wallet Services

2. Crypto Services
4. Stored Precedes

۵. دفاتر کل جداگانه، پایگاه داده ای است که بر اساس سازوکار و معماری داده توسط مشارکت کنندگان به صورت جدا نگهداری و به روزرسانی می شود.

پلتفرم‌های بلاکچینی موفق باید موجب کاهش هزینه‌های عملیاتی با کمک کاهش مداخلات دستی، پیوستگی در بازرسی^۱ و تقسیم هزینه شوند و همچنین هزینه‌های مربوط به تراکنش‌ها را نیز کاهش دهند.

۴-۷- انواع پلتفرم‌های بلاکچین

بسیاری از کارشناسان بر این باورند که فناوری بلاکچین موجب ایجاد تحولی همانند انقلاب اینترنت خواهد شد. به همین دلیل توسعه‌دهندگان بسیاری در سراسر دنیا به فکر طراحی و اجرای انواع برنامه‌های کاربردی بر بستر این فناوری هستند. همچنین پلتفرم‌های بلاکچین متعددی در چند سال اخیر ارائه شده‌اند. تفاوت‌های ساختاری و فنی موجود میان این پلتفرم‌ها، گاهی موجب سردرگمی توسعه‌دهندگان می‌شود.

❖ اتریوم^۲

اتریوم، یک پلتفرم بلاکچینی است که به کاربران این امکان می‌دهد تا از برنامه‌های غیرمتمرکزی که بر بلاکچین اجرا می‌شود استفاده کنند. اتریوم، پروژه‌ای متن‌باز^۳ است که توسط تعدادی از کاربران در سراسر دنیا ایجاد شده است. پروتکل اتریوم برخلاف پروتکل بیت‌کوین بسیار منعطف و قابل‌ویرایش است.



۶-۷- لوگوی پلتفرم اتریوم

❖ هایپرلجر^۴

هایپرلجر پروژه‌ای متن‌باز است که هدف از آن ایجاد زمینه‌ای برای

پیشرفت فناوری‌های مرتبط با صنایع مختلف بر بستر بلاکچین است. این پروژه چندملیتی و حاصل همکاری شرکت‌های بزرگی در حوزه امور مالی، بانکداری، اینترنت اشیاء، زنجیره تامین، تولید و نیز فناوری است. پروژه‌هایی توسط شرکت‌های عضو هایپرلجر تعریف شده است. ساوتوث^۱، یکی از اصلی‌ترین پروژه‌های مبتنی بر هایپرلجر است که توسط اینتل اجرایی شده و از مجموعه ماژولار بلاکچینی پشتیبانی می‌کند.



۷-۷- لوگوی پلتفرم هایپر لجر

❖ مولتی چین^۲

مولتی چین، پلتفرمی برای ایجاد و اجرای بلاکچین‌های خصوصی (بلاکچین‌های نیازمند مجوز) برای شبکه‌های درون سازمانی و یا بین سازمانی است. هدف این پلتفرم، غلبه بر یک مانع کلیدی در اجرایی کردن فناوری بلاکچین در موسسات مالی بوده است. مولتی چین نسخه بهبودیافته نرم‌افزار بیت کوین است.



۸-۷- لوگوی پلتفرم مولتی چین

❖ هیدراچین^۳

پلتفرم هیدراچین، حاصل همکاری دو پروژه برین بات^۴ و اتریوم است. در واقع یک شاخه از پلتفرم اتریوم است که برای ایجاد برنامه‌های

1. Sawtooth
2. Multichain
3. HydraChain

4. brainbot

مقیاس‌پذیر و مبتنی بر بلاکچین که مطابق مقررات و نیازهای سازمانی هستند ایجاد شده است.



۹-۷- لوگوی پلتفرم هیدراچین

❖ اپن چین^۱

پلتفرم اپن چین توسط کوین پریزم^۲ طراحی شده است. این پلتفرم ادعا می‌کند که گزینه مناسب برای سازمان‌هایی است که می‌خواهند دارایی‌های دیجیتال را منتشر و مدیریت کنند. اپن چین رویکردی متفاوت با بیت کوین را برای اجرای بلاکچین در پیش می‌گیرد. به همین دلیل، یک نظام توافق عمومی تقسیم شده در آن جاری است. به همین دلیل، هر نمونه اپن چین فقط داری یک مسئول برای تایید تراکنش‌هاست که این البته به دارایی‌های تبادل شده در آن بستگی دارد. همین نکته سبب می‌شود تا معماری کلاینت-سرور (متمرکز) ایجاد شود. اپن چین بر این باور است که این ساختار کارآمدتر و مورد اطمینان‌تر از معماری شبکه نظیر به نظیر است.



۱۰-۷- لوگوی پلتفرم اپن چین

❖ آی‌بی‌ام^۳

شرکت معروف آی‌بی‌ام نیز یک پلتفرم بلاکچین راه‌اندازی کرده است.

این خدمت به عنوان بخشی از کاتالوگ بلومیکس^۱ این شرکت در دسترس است. این پلتفرم بر اساس پروژه هایپرلجر ساخته شده است، اما امنیت و امکانات زیرساختی بیشتری را در اختیار شرکتها قرار می‌دهد.



۱۱-۷- لوگوی پلتفرم آی بی ام

❖ چین^۲

این پلتفرم ادعا می‌کند که گزینه مناسبی برای کاربردهای مالی است. این پلتفرم بر اساس نرم‌افزار چین کور^۲ که شامل پروتکل چین است، توسعه یافته است. هم‌اکنون نسخه متن باز آن به صورت رایگان در اختیار توسعه‌دهندگان قرار دارد.



۱۲-۷- لوگوی پلتفرم چین

❖ آیوتا^۴

آیوتا با بلاکچین استاندارد (معمول) تفاوت‌هایی دارد. بر اساس مفهوم دفتر کل توزیع شده بدون بلوک^۵ که اصطلاحاً «تنگل» نام دارد توسعه یافته است. امکان انجام بی‌نیایت تراکنش، آن هم بدون کارمزد در این سامانه فراهم شده است.



۱۳-۷- لوگوی پلتفرم آیوتا

1. Bluemix
2. Chain
3. Chain Core

4. IOTA
5. blockless distributes ledger

❖ آرتری کوردا^۱

این پلتفرم توسط کنسرسیوم بانکی ۳ برای ایجاد ارتباط بین بانک‌های عضو این گروه ساخته شده است. در این پلتفرم، برخلاف بلاکچین‌های متعارف، هر نمود تنها تراکنش‌هایی را می‌بیند که در آن سهمیم است و به این ترتیب پردازش میلیون‌ها تراکنش در ثانیه ممکن می‌شود. اما این سیستم به وجود واسطه‌هایی وابسته است که با ماهیت بدون واسطه بلاکچین‌ها در تضاد هستند.



۱۴-۷- لوگوی پلتفرم آرتری کوردا

❖ ریپل^۲

یک پروتکل منبع باز است که به منظور انجام معاملات سریع و ارزان طراحی شده است. این پلتفرم علاوه بر رمزارز خود (Ripple)، به همه افراد این امکان را می‌دهد تا از طریق شبکه Ripple Net رمزارز خود را بسازند.



۱۵-۷- لوگوی پلتفرم ریپل

❖ کوروم^۳

پلتفرمی برای ارائه ابزارهای مالی است که توسط جی پی مورگان چیس به همراه بانک ملی کانادا و دیگر شرکت‌های بزرگ، در حال آزمایش است.

1. R3 Corda
2. Ripple
3. Quorum

درواقع هدف این بانکها از انجام چنین کاری ایجاد و ساده کردن مبادلات تجاری، پرداخت، پرداخت‌های نرخ بهره و دیگر فرایندها بوده است.



۱۶-۷- یوگویی پلتفرم کوروم

۵-۷- مقایسه پلتفرمها

با وجود تعداد زیادی از پلتفرم‌های بلاکچین، معیار اصلی در انتخاب پلتفرم‌های بلاکچین معرفی شده، سهولت طراحی نمونه اولیه (پروتوتایپ) بر روی آن پلتفرم، بخش صنعتی مورد تمرکز، مالکیت، نوع دفترکل، رمزارز، میزان بکارگیری توسط ارائه دهندگان خدمات بلاکچین^۱، میزان استفاده در صنایع مختلف^۲، ارزش سرمایه رمز ارز، الگوریتم اجماع و بهره‌گیری از قراردادهای هوشمند در نظر گرفته شده است. این پلتفرم‌ها در جداول زیر براساس معیارهای مختلف مورد مقایسه قرار گرفته‌اند.

۱. بر اساس پاسخ دریافت شده از ۱۵ ارائه دهنده خدمات بلاکچین مطرح.
۲. براساس پاسخ‌های ارائه شده توسط شرکت‌ها در صنایع مختلف که از فناوری بلاکچین استفاده می‌نمایند.

۱۷-۷- جدول مقایسه پلتفرم‌های مختلف بر اساس معیارهای مشخص

پلتفرم	محبوبیت : (وضعیت در گیت‌هاب (تعداد ستاره‌ها، فورک‌ها و ...)	فعالیت (میزان فعالیت توسعه پلتفرم در گیت‌هاب)	نوع شبکه: (عمومی، خصوصی)	هزینه: (رایگان یا دارای قیمت‌های مختلف برای لایه‌های متفاوت شبکه)	زبان (پشتیبانی شده: (زبان‌های برنامه‌نویسی قابل پشتیبانی در SDK پلتفرم)	گیت‌هاب: (نام پروژه ذخیره شده روی گیت‌هاب برای (ها) SKD)
اتریوم	بالا	تعداد زیادی دنبال‌کنندگان در گیت‌هاب	عمومی، مبتنی بر قرارداد هوشمند	اتر (Ether) به ازای هر تراکنش و خدمات پردازشی	Python, C++, Go	pyethereum) و (Python gptethereum) و (GoLang cppethereum)
هایپرلجر	بالا	تعداد زیادی دنبال‌کنندگان در گیت‌هاب	عمومی و نیز خصوصی	متن باز	Python (برای Sawtooth)	sawtooth-core) (Python
مولتی‌چین	متوسط	به‌روزرسانی مرتب در گیت‌هاب	خصوصی، نیازمند مجوز	رایگان، متن باز	Python, c#, JavaScript, PHP, Ruby	savior (Python) و Multichain-Node) و (JavaScript
هیدراچین	پایین	به‌روزرسانی مرتب در گیت‌هاب	خصوصی، نیازمند مجوز	رایگان، متن باز	Python	libphp-multichain) و (PHP multichain-) client (Ruby hydrachain) (Python
آین چین	متوسط	به‌روزرسانی مرتب در گیت‌هاب	خصوصی	متن باز	Javascript	openchain-js) (JavaScript
آی‌بی‌ام	متوسط	به‌روزرسانی مرتب در گیت‌هاب	خصوصی / مجوزدار	طرح رایگان با امکانات محدود/ قابلیت ارتقاء به نسخه پولی (شرکتی) با امکانات بیشتر	JavaScript و Go	IBM-blockchain-) js (JavaScript
چین	متوسط	به‌روزرسانی مرتب در گیت‌هاب	مجوزدار	پولی و برای شرکت‌ها	Java, Rubym Node.JS	sdk-Java (Java) و sdk-Ruby (Ruby) sdk-nodejs) (Node.JS/JavaScript
آیو‌تا	پایین	به‌روزرسانی مرتب در گیت‌هاب	عمومی و مجوزدار	بر اساس توکن آیو‌تا، قیمت‌گذاری هنوز مشخص نیست	Phyton, C, Javascript	lib.py (Java) و lib.js) و ccurl (C) (JavaScript

۱۸-۷- جدول مقایسه دیگری از پلتفرم‌های مختلف بر اساس معیارهای مشخص

معیارها پلتفرم	بخش صنعتی مورد تمرکز	مالکیت	نوع دفترکل	رمز ارز	میزان بکارگیری توسط ارائه دهندگان خدمت بلاکچین	میزان استفاده در صنایع مختلف	ارزش سرمایه رمز ارز مرتبط (میلیارد دلار)	الگوریتم اجماع	بهره‌گیری از فرازاد‌های هوشمند
اتریوم	بین صنعتی	توسعه‌دهنده اتریوم	عمومی	اتر ETH	30%	2%	91.5 (% 18)	Proof of work (POW)	بله
هالیبرلجر	بین صنعتی	بنیان‌گذار لینوکس	خصوصی	-	30%	2%	-	Pluggable framework	بله
آرتری گوردا	خدمات مالی	کنسرسیوم R3	خصوصی	-	60%	3%	-	Pluggable framework	بله
ریپل	خدمات مالی	از مایشگاه‌های ریپل	خصوصی	ریپل XRP	30%	4%	43.9 (% 9)	Probabilistic voting	خیر
کوروم	بین صنعتی	توسعه‌دهندگان اتریوم و جیبی چیس مورگان JP Morgan (chase)	خصوصی	-	27%	10%	-	Majority voting	بله

در ادامه پلتفرم‌های بلاکچین دیگری با شاخص‌ها و پارامترهای متفاوتی مانند شهرت استفاده، اندازه سرمایه، مشارکت کنندگان مهم، کل رمز ارز عرضه شده، رمز ارز در گردش، پروتکل‌های اجماع، الگوریتم‌های هش، زبان‌های برنامه نویسی / اسکریپتی، منبع باز بودن، قابلیت‌های دیجیتالی کردن، تعداد تراکنش در ثانیه، ساینز تراکنش، تاریخ اصلی عرضه، تعداد کیف‌های حمایت شده، زمان تولید بلوک، زمان تاییدیه، پیام رمزگذاری شده، کنترل حساب، قراردادهای هوشمند، تمرکز زدایی، عمومی / خصوصی، نوع توکن، مکانیزم اجماع، Market Cap و.... مقایسه شده‌اند.

BLOCKDATA

| PLATFORMS COMPARED |

VERSION 1.4
ISSUE DATE 14/04/18









NAME	QTUM	ETHEREUM	NEO	WANCHAIN	LISK	ARK	EOS	STRATIS	WAVES
TOKEN	QTUM	ETH	NEO	WAN	LSK	ARK	EOS	STRAT	WAVES
ISSUE DATE	16/10/2017	24/07/2014	09/04/2014	03/10/2017	04/05/2016	25/02/2017	02/07/2017	06/06/2016	15/04/2016
LANGUAGE SUPPORT	Solidity	Solidity	C#, Java, NET, Kotlin, Python	Solidity	JavaScript	JavaScript	WASM Assembly, C++	C#, NET	Scala
CONSENSUS MECHANISM	PoS	Proof of Work	eBFT	PoS	DPoS	DPoS	DPoS	PoS	LPoS
TPS	70 ps	15 ps	1000 ps (P)	N/A	5 ps	25 ps	100,000 ps (P)	20,000 ps (P)	100 ps
BLOCKTIME	120 s	15 s	15 s	N/A	10 s	5 s	0.5 s	60 s	3 s
DAPPS	✓	✓	✓	✓	✓	✓	✓	✓	✓
SDK	✓	✓	✓	In progress	In progress	In progress	✓	✓	✓
ATOMIC SWAPS	✓	✓	✓	✓	✓	In progress	✓	✓	In progress
SIDECAINS	✓	✓	✓	✓	In progress	In progress	✓	✓	In progress
SMART CONTRACTS	✓	✓	✓	✓	In progress	In progress	✓	✓	In progress
CIRCULATING SUPPLY	82,664,316	100,343,205	65,000,000	106,152,485	107,066,862	103,273,336	696,143,402	10,303,028	100,000,000
MARKET CAP	\$920,027,330	\$49,831,325,284	\$2,462,830,100	\$303,742,679	\$464,482,915	\$154,362,288	\$9,241,800,098	\$281,680,063	\$344,546,000
FUNDS RAISED	-\$15,800,000	-\$14,400,000	-\$1,000,000	-\$10,550,180	-\$5,700,000	-\$1,000,000	-\$105,000,000	-\$493,940	-\$14,400,000
TEAM SIZE	18	133	41	42	44	34	40	32	60

۱۹-۷- مقایسه پلتفرم‌ها از منظر سایت BLOCKDATA.TECH

	ETH	NULS	ARDOR	NEO	WAVES	LISK	EOS	CARDANO	ICON	ARK	STRATIS	WANCHAIN	NXT
Language	C#, C++, Rust	Java	Java	C#	Scala	JavaScript	C++	Haskell	Python	JavaScript	C#, NET	C#, C++	Java
Consensus	Proof of Work	Proof of Work	Proof of Work	eBFT	LPoS	DPoS	DPoS	PoS	LFT	DPoS	PoS	Proof of Work	Proof of Work
Block Time (seconds)	14-15	15	60	15-20	3	10	0.5	20	1	6	6	60	13
Smart Contracts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Atomic Swaps	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Contract Languages	Solidity	Java	Java	C#, Java, NET, Kotlin, Python	ROSE	N/A	C, C++	Plutus	Python	N/A	C#, NET	Solidity	Java
DEX	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Side / Child Chains	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Privacy Features	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Mainnet Launch	July 2015	July 2018	Jan 2018	Oct 2016	Jan 2016	May 2016	Jun 2016	Sept 2017	Jun 2018	Mar 2017	Aug 2016	Jan 2018	Nov 2013
Token Creation	✓	✓	✓	Free	0.0001 WAVES	Free	0.1 LSK	Free	0.155881 ADA	0.01 ICON	0.001 STRAT	21000 GAS	1 NXT
Transaction Cost	21000 GAS	0.01 NULS	1 ARDR	Free	0.0001 WAVES	0.1 LSK	Free	0.155881 ADA	0.01 ICON	0.001 STRAT	21000 GAS	21000 GAS	1 NXT
% Top 10 mainexchange addresses control	5.91%	>90%	24.21%	58.12%	18.52%	18.52%	N/A	23.01%	31.50%	20.34%	20.34%	N/A	20.58%
Wallet	Web, Windows, MacOS, Linux, Android, iOS, Ledger, & More	Windows, MacOS, Linux	Web, Windows, MacOS, Linux, Android	Windows, MacOS, Linux, Ledger	Windows, MacOS, Linux	Windows, MacOS, Linux	TELOS, Web, Windows, MacOS, Linux	Web	Web	Desktop, Ledger, Web, Android, iOS	Ledger, Web, Desktop, iOS, Mac, Linux, Android, iOS	Windows, MacOS, Linux	Web, Windows, MacOS, Linux, Android
Main Selling Point	Popularity, Smart Contracts	Modular	Child Chains, Built-in Contracts & Features	NEP-5, Digital Identity	Fast and Secure, DEX	JavaScript based Smart Contracts	Scalable, Flexible, Fast	Improved EVM with sidechains and PoS	Multiple Blockchain Integrations	Smartbridge	Simple Easy Smart Contracts	Improved ETH with PoS & Asset Privacy	Built-in Contracts

Blockchain-as-a-Service (BaaS) Platform 2018: Part I
as of 2018.02

	 Ethereum/ETH	 Stellar/XLM	 NEO/NEO	 ARDOR/ARDR (RDD/RRR)	 EOS/EOS	 NEM/XEM
Year	07/2014	2014	12/2016	01/2018 (MAY 2018)	06/2017	03/2015
Total Supply	~ 100M+	~ 100B+	100M	~ 1B	900M	~ 9B
Circulating Supply	~ 98M	~ 18B+	100M	~ 1B	680M +	~ 9B
Consensus Protocol	PoW	Stellar Consensus Protocol (SCP)	dBFT	PoS	dPoS	Proof of Importance (PoI)
Avg. Block Time	14-15 sec	3.5 sec	2-3 min	1 min	3 sec	1 min
Transaction per Second (TPS)	~ 16	~ 1K+	~ 1K	~ 1K	Up to 1M*	Up to 3K
Hash Algorithm	KECCAK-256	ED25519	SHA-256 & RIPEMD160	SHA-256	SHA-256	SHA-3-S12
Programming Tool	Solidity	JavaScript, Java, Go	C#, JavaScript, Python, Java	Java	JavaScript	Java
Fuel Token	ETH	XLM	GAS	IGNIS	EOS	XEM
Founder	Vitalik Buterin	Jed McCaleb	Da Hongfei & Erik Zhang	Jean-Luc & Lior Yaffe	Brendan Blumer & Dan Larimer	Lon Wong
Country	Canada	USA	China	USA	USA	Malaysia

۶-۷- لزوم پلتفرم بلاکچینی بومی در سطح ملی

بکارگیری فناوری زینجیره بلوکی در کشور، ضرورت و نیازی است که برای صنایع مختلف تهدیداتی را به همراه دارد و حتی در برخی حوزه‌ها از بعد نظام کسب‌وکار و مالیات، این فناوری باعث می‌شود تا اقتصاد کشور از حوزه حاکمیت ملی خارج شده و در حوزه حاکمیت مالکان پلتفرم‌های بزرگ قرار گیرد، لذا شکل‌گیری پلتفرم‌های بومی در کشور ضروری است و با شکل‌گیری پلتفرم‌های موفق در دنیا، شاهد شکل‌گیری بازارهای بزرگ جهانی و تضعیف حاکمیت ملی خواهیم بود. ایجاد پلتفرم‌های بلاکچینی در سطح ملی را نیز می‌توان از دو منظر کارکردی و غیرکارکردی مورد توجه قرار داد. از بعد کارکردی، پوشش نیازمندی‌های لازم برای ایجاد سیستم‌های عمومی و خصوصی الزامی است و از بعد غیرکارکردی، امنیت و تعامل‌پذیری با سایر سیستم‌ها (بلاکچینی و غیر بلاکچینی) نیز حائز اهمیت است.

بخش هشتم

کاربردهای بلاکچین



این فناوری در هر فرآیندی که مبتنی بر داده باشد، قابل استفاده بوده و درآمدزایی آن نیز موضوعی است که به زیست بوم صنعت مربوطه یا کاربرد و عوامل دیگری از جمله شرایط بازار، تجهیزات مورد استفاده، نوع خدمت و هزینه های آن بستگی دارد. مطالعات و گزارشات موید آن است که این فناوری سرمایه‌گذاری‌های کلانی را به خود جذب کرده است. منابع مالی اختصاص یافته به این حوزه تنها از طریق سرمایه‌گذاری های عمومی، پس از جذب ۷,۲ میلیارد دلار در نیمه اول سال میلادی جاری، رقم سرمایه‌گذاری خود را جمعاً به ۱۹ میلیارد دلار رسانده است. بیش از ۳۰۰ استارت‌آپ در آمریکا، بیش از ۵۰ مجموعه در انگلستان و حدود ۴۰ مجموعه در سنگاپور ایجاد شده اند که بین ۱۰ تا ۵۰ نفر در آن ها فعالیت می‌کنند. شرکت آلفابت (گوگل) در حال اجرای پروژه های بلاکچینی خود بوده و حتی برخی از شرکت های بزرگ فناوری همچون Microsoft، IBM و Oracle Corporation نسخه آزمایشی سکوهای مبتنی بر زنجیره بلوکی خود را اجرایی کرده اند و بر همین اساس، اکثر کشورهای دنیا در حال تعیین موضع حقوقی خود نسبت به کاربرد این فناوری هستند.

همچنین شرکت های بزرگی مانند:

JPMorga. TOYOTA ، ICBC. British Petroleum ، Allianz. Walmart.
Nestle. Alibaba

و گوگل در حال سرمایه و گوگل در حال سرمایه گذاری مستقیم در پروژه های بلاکچینی و استفاده از کاربردهای این فناوری در کسب و کار خود هستند. از مهمترین کاربردهای فناوری بلاکچین می توان به موارد ذیل اشاره نمود:

۱-۸- خدمات بانکی

اذهان عمومی کاربرد زنجیره بلوکی را به رمز ارزها محدود دانسته و تبلیغات بگونه ای است که این فناوری برای بهره برداران از آن، بسیار درآمد زا می باشد، ولی حقیقت آن است که فارغ از موضوع رمز ارزها و استفاده از آن ها به عنوان پول، دارایی یا کالا، موضوعات مرتبط دیگری در حوزه مالی و بانکداری همچون جمع آوری سرمایه به صورت عمومی، اجاره دادن اقلام غیر قابل اجاره، همانند اطلاعات یا سهم بازار یک شرکت، ردیابی سبدهای سرمایه گذاری مطرح است. به عنوان نمونه شرکت ICBC ثبت اختراعی انجام داده است که از فناوری بلاکچین برای تایید گواهینامه های دیجیتالی به جای یک مقام مرکزی استفاده می نماید و یا بانک آمریکایی JPMorgan Chase & Co به کمک سکوی Quorum (که نسخه شخصی سازی شده سکوی زیرساختی بلاکچین اتریوم برای سازمان ها است) در حال بکارگیری این فناوری در خدمات خود است. همچنین شرکت توپوتا در حال تحقیق در مورد پرداخت های بلاکچینی برای اتومبیل های خود ران است.

۲-۸- حوزه سلامت

برخلاف وضعیت کنونی درمان که پرونده های سلامت به صورت کاغذی و یا الکترونیکی در سیستم های متعددی ایجاد و ذخیره می شوند، با توجه به حساسیت بالای اطلاعات سلامت شهروندان، پرونده سلامت مبتنی بر بلاکچین می تواند منحصر به فرد و کامل بوده و فرد را از زمان تولد تا فوت مشایعت نماید. در این حالت، تاریخچه سلامت هر فرد بدون توجه به این موضوع که چند بار پزشک یا خدمات بیمه خود را تغییر داده است، ثبت و نگهداری شده و در مواقع ضروری، سریعاً قابل دسترسی است. شرکت MedRec با کمک MIT Media Lab نمونه ای از بستر بلاکچین در حوزه سلامت است. لذا هدف این رویکرد، ارائه خدمات پایه حوزه سلامت بر بستر سکوی دولت (وزارت بهداشت) بر اساس فناوری بلاکچین، به شرکت های خصوصی تخصصی برای ایجاد خدمات ارزش افزوده همه جامعه است.

۳-۸- حوزه سیاسی

رای گیری و بی نظمی انتخاباتی موضوعاتی هستند که دولت ها از گذشته تا به حال با آن ها مواجهند. اما سیستم های رای گیری مبتنی بر فناوری بلاکچین بواسطه ساختار امنی که دارند، غیرقابل هک و دستکاری هستند. این سیستم ها امکان مدیریت غیرقابل خدشه فرآیند رای گیری را از ثبت نام تا تایید هویت و شمارش آراء فراهم خواهند کرد. رای گیری با استفاده از این تکنولوژی، موجب افزایش تعامل و مشارکت شهروندان، بهبود ارتباطات نهادهای سیاسی با مردم و شفافیت در فرآیند رای گیری (تایید هویت، رای، شمارش و ...) می شود. از طرفی وجود بعضی از ریسک های مشابه در سایر سیستم های

رای گیری نظیر: اجبار، دسترسی، گمنامی و ... چالش محسوب می شود. شرکت Flux در استرالیا، راهکاری برای جمع آوری آراء مردم به نمایندگان، پیگیری خواسته های آنها از نمایندگان و مقایسه تعهدات انتخاباتی و عملکرد نماینده ها جهت استفاده در مجلس را بر پایه فناوری بلاکچین ایجاد نموده است.

۴-۸- نفت و انرژی

در این حوزه شرکت های بزرگی به دنبال مهیاسازی امکان مدیریت، توزیع و تبادل منابع تولید انرژی و یا انرژی تولید شده در نقاط گوناگون جهان هستند. شرکت هلندی Royal Dutch Shell با ارزش سهام ۳۰۶ میلیارد دلاری و درآمد سالیانه ۳۲۲ میلیارد دلار، علاوه بر سرمایه گذاری مستقیم در فناوری بلاکچین، با کمک شرکت British Petroleum به دنبال ایجاد سکوی مبادله کالاهای انرژی^۱ است. همچنین شرکت زیمنس با سرمایه گذاری مستقیم در استارتاپ LO3energy به دنبال ایجاد بستری است که همسایه های یک منطقه بتوانند به طور مستقیم، به خرید و فروش انرژی الکتریکی ایجاد شده از منبع خورشیدی خود بپردازند.

۵-۸- خدمات بیمه

بازار جهانی بیمه بر اساس مدیریت اعتماد بوده و بلاکچین روش جدیدی را در جهت مدیریت این اعتماد ارائه نموده است. این فناوری می تواند در تایید اطلاعات زیادی که در قراردادهای بیمه وجود دارند مورد استفاده قرار گیرد و ساختاری هوشمند، دقیق، قابل پیگرد و سریع را برای این صنعت فراهم نماید. شرکت Allianz به دنبال زیرساختی برای ایجاد خدمات «خود بیمه ای» و ایجاد یک دارایی/ارزش

دیجیتال قابل نقل و انتقال برای کاربران خود است.

۸-۶- مجوزها و پروانه‌ها

صدور، ذخیره و بازیابی اسناد مجوزی و همچنین تأیید پروانه آنها، جزو کارهای کلیدی مدیریت مجوزها و پروانه‌ها است. اعتبارسنجی مجوزها و پروانه‌ها را می‌توان از اساسی‌ترین مشکلات این حوزه برشمرد. از آنجا که بلوک‌های یک زنجیره توسط گروهی از بازیگران مورد تأیید قرار می‌گیرد، پس عدم وجود بلوک مربوط به یک مجوز یا پروانه خاص، به منزله بی‌اعتباری آن است. به طور مثال بکارگیری این ویژگی در بازار مسکن، تخلفات این حوزه را به صفر خواهد رساند.

۸-۷- قراردادهای هوشمند

قراردادهای هوشمند، فرایند معاملات را به صورت کاملاً تضمینی و بدون نیاز به اشخاص ثالث انجام می‌دهند. فعالیت و ثبت قرارداد هوشمند، قابل پیگیری و غیرقابل برگشت است. قراردادهای هوشمند شامل تمام اطلاعات مربوط به شرایط قرارداد و اجرای تمام اقدامات هدف گذاری شده به طور خودکار می‌شوند و امکان ضمانت در اجرا را فراهم نموده است. قبل از پیدایش زنجیره بلوکی، این نوع از قراردادها در حد یک طرح بود ولی اکنون می‌تواند از ساماندهی بازارهای خرد و کلان تا سامانه‌های حمل و نقل، از نظام بانکداری تا امور مالیاتی و بطور کلی هر فعالیتی که بر مبنای ثبت و صدور اسناد و مدارک و اطمینان از صحت و غیرقابل خدشه بودن اطلاعات صورت می‌پذیرد، بکار گرفته شود.

۸-۸- توسعه کلان داده

بیش از ۹۵ درصد از خدمات ابری ارائه شده در فضای مجازی، تحت مدیریت

آمریکاست. به عبارت دیگر، بیش از ۹۵ درصد از داده‌های مربوط به کاربران کشورهای مختلف، در آمریکا ذخیره می‌شوند. این موضوع به مهمترین ابزارهای تسلط غرب بر دیگر کشورها تبدیل شده است، چرا که تحلیل آن، اطلاعات دقیق جمعیت شناختی از کشورهای مختلف را در اختیار نظام سلطه قرار می‌دهد. با اینحال چگونگی ذخیره‌سازی و زمان‌بر بودن تحلیل و نتیجه‌گیری از داده‌ها، دو چالش اصلی استفاده از کلان داده‌هاست. ویژگی ساختاری زنجیره بلوکی (یعنی قالب‌بندی داده‌ها و زنجیر کردن بلوک‌های مرتبط به هم) هم ذخیره‌سازی داده‌ها را نظام‌مند می‌کند و این انتظام به نحوی است که امکان رصد و تحلیل موضوعات مختلف را از بدو پیدایش (لحظه صفر) فراهم می‌کند.

۹-۸- زنجیره تامین

فناوری بلاکچین، توانایی زیادی در اثبات و تضمین اصالت داده و تراکنش‌ها و همچنین ثبت، تصدیق و ردیابی کالا با هزینه کم را دارد. از اینرو، شرکت‌های بزرگی همچون سامسونگ، Walmart، Pfizer (شرکت بزرگ توزیع دارو)، Nestle، Alibaba برای مدیریت زنجیره تامین و شعب، اصالت محصولات و قطعات، جلوگیری از احتکار و کنترل موجودی شبکه توزیع، تخصیص منابع و محصولات به بازار هدف مشخص، درحال بکارگیری این فناوری هستند.

۱۰-۸- سازمان‌های خودگردان

فناوری بلاکچین می‌تواند در توسعه سازمان‌های غیرمتمرکز و خودگردان بسیار موثر باشد. داشتن قوانین و قواعد مختص خود و عدم انتظام به قوانین حاکم در کشورها یا ارگان‌های تنظیمی و نظارتی،

از ویژگی‌های آنها است. یک نمونه بارز این حوزه، اپلیکیشن‌های حمل و نقل مستقل در شبکه فنی-اجتماعی است، به نحوی که هر فرد می‌تواند در نقش راننده مسافری را جابه‌جا نموده و از اعتباری که به دست می‌آورد (این اعتبار خارج از این سیستم هیچ ارزشی ندارد) از خدمات سایر افراد این شبکه برای مسافرت خود استفاده نماید. Aragon one و Backfeed دو استارت‌آپ بزرگ جهت مهیا سازی زیرساختی برای شکل‌گیری این نوع سازمان‌ها هستند.

۱۱-۸- شرط‌بندی و قماربازی آنلاین

از مهمترین ویژگی‌های لازم برای این نوع سیستم‌ها می‌توان به مواردی از جمله غیرقابل‌هک بودن، پردازش پرداخت‌های مکرر، مدیریت شرط‌های متنوع با ارزش‌های مختلف از کشورهای مختلف، اجتناب از قوانین ضد قمار در کشورهای خاص، امکان تصدیق موجودی، انتقال میزان شرط و امکان گمنامی کاربران اشاره نمود. مزیت‌های فناوری بلاکچین، این ویژگی‌ها را بطور کامل پوشش می‌دهد. از این رو بسیاری از بازیگران بزرگ این صنعت همانند Zero Edge به توسعه سکوی شرط‌بندی و قماربازی آنلاین، بر مبنای فناوری بلاکچین پرداخته است.

۱۲-۸- اینترنت اشیا

با توجه به گزارشات گارتنر، تعداد اشیاء متصل به اینترنت در سال ۲۰۲۰ میلادی بیش از ۲۰ میلیارد دستگاه بوده و ارزش بازاری بالغ بر ۳ تریلیون دلار خواهد داشت. بزرگترین چالش و نگرانی در این حوزه امنیت آن است که به دو دسته کلی تقسیم می‌شود. اول دسترسی غیر مجاز به اشیاء و دوم تغییر در داده‌هاست. موضوع بعدی مقیاس‌پذیری

این حجم از شبکه و تراکنش‌ها است که برای ارائه پاسخ مناسب به این نیازمندی، همواره استفاده از سرورهای متمرکز پیشنهاد می‌شود، که این موضوع باعث ایجاد نقطه شکست واحد در سیستم و همچنین ایجاد هدف مشخص برای هکرها می‌گردد. این نقطه دقیقاً همان زمانی است که معماری شبکه اینترنت اشیاء قبل از شکل‌گیری مورد انتقاد قرار می‌گیرد. فناوری بلاکچین می‌تواند پاسخ مناسبی برای این چالش‌ها داشته باشد. IBM سکویی برای مدیریت اینترنت اشیاء بر مبنای بلاکچین ارائه کرده است.

۱۳-۸- عرضه اولیه رمز ارز

عرضه اولیه ارز دیجیتال، به فرآیندی اطلاق می‌شود که در آن با استفاده از عرضه اولیه، مقدار مشخصی ارز مجازی به صورت عمومی، به جمع‌آوری سرمایه با ارز واقعی پرداخته می‌شود. روشی مانند فروش سهام و اوراق که در آن عرضه بر اساس اعتبار برگزارکننده آن صورت گرفته و خریداران در پروژه یا زیست بومی که در حال توسعه است، شریک می‌شوند. این روش در ۳ سال اخیر بسیار فراگیر شده، به نحوی که در سال جاری میلادی بیش از ۱۱۰۰ ICO برگزار شده و سرمایه‌ای حدود ۷,۵ میلیارد دلار جمع‌آوری شده و نسبت به سال پیش ۲۰ درصد افزایش داشته است.

۱۴-۸- تغییر ماهیت اینترنت

وسعت کاربردپذیری فناوری بلاکچین، به مرور موجب تغییر ماهیت اینترنت نیز خواهد شد. اگرچه اینترنت در ۲۰ سال اخیر برنامه‌هایی از جمله پیام‌رسان‌ها، خدمات ابری، زیست بوم‌های فنی-اجتماعی، فنی-اقتصادی، روابط شبکه‌ای، خدمات جهانی بانکی و اینترنت اشیاء را ارائه

نموده است. پیش بینی جهانی در خصوص محصولات ناشی از ترکیب فناوری بلاکچین با سایر فناوری های فضای مجازی به این صورت است: ایجاد سازوکارهای لازم برای مدیریت غیر متمرکز زیست بوم یا سازمان ها، انتقال قدرت حاکمیت از کشورها به شرکت ها و کاربران، توسعه ارزشهای دیجیتال به صورت موازی با ارزشهای فیزیکی، محقق شدن وب ۳ به کمک این فناوری از جمله عواملی هستند که تغییرات بنیادی در اینترنت فعلی ایجاد خواهند نمود. از سوی دیگر ضرورت تداوم ارائه خدمت در صورت ایجاد هرگونه قطعی یا خرابی در سیستم های ذخیره سازی، باعث شده است که توسعه دهندگان، تمهیدات فراوانی برای ایجاد پشتیبان و توزیع جغرافیایی آن ببیندیشند. لذا نیاز به امکان توزیع داده ها به نحوی که غیرقابل تغییر باشند روز افزون شده است. به علاوه با توجه به ماهیت امن بودن رکوردهای داخل بلاکچین و غیرقابل تغییر بودن آن ها، استناد به داده های موجود در زنجیره، برای صدور احکام قضایی در حال توسعه و گسترش است. دو استارتاپ Blockstack و meta mask به دنبال ایجاد روشی برای استفاده از خدمات اینترنت با حکمرانی کاربران بوده و تاکنون چند محصول را نیز ارائه نموده اند.

۱۵-۸- توزیع هدفمند وام / یارانه / دلار

یکی از کاربردهای بسیار مفید و مورد نیاز فناوری بلاکچین در شرایط کنونی کشور، ایجاد سیستمی غیرمتمرکز، غیرقابل تغییر و شفاف برای توزیع هدفمند وام، یارانه و دلار است. با این روش می توان به آسانی تخصیص تسهیلات به بازارهای هدف و جلوگیری از انحراف در تخصیص منابع، گردش منابع صرفاً درون چرخه های موردنظر

Industrial and Commercial Bank of China ذخیره‌سازی و توزیع
مایحتاج عمومی و جلوگیری از احتکار را تضمین نمود. به‌عنوان یک
کاربرد عملی از بکارگیری این سامانه می‌توان به زنجیره تامین کالاهای
اساسی با استفاده از ارز دولتی اشاره کرد. در زنجیره بلوکی، زنجیره
کلیه ذینفعان شامل دریافت کنندگان ارز، کالاهای دریافت کننده ارز
دولتی، واردکنندگان کالا، انبارهای ذخیره‌کننده کالا، توزیع کنندگان
عمده و خرد کالا و خریداران کالا، ثبت و قابل رهگیری خواهند بود.

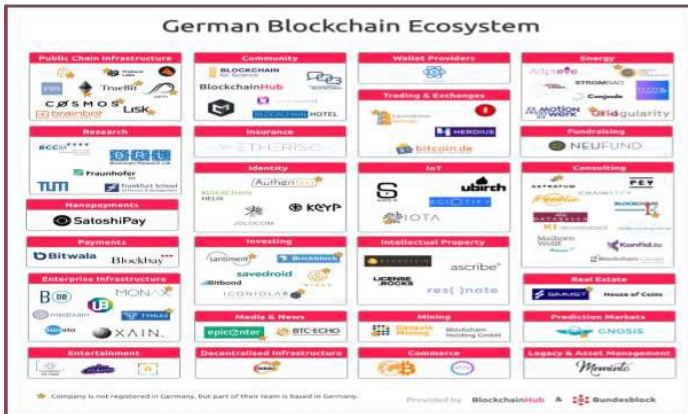
بخش نهم

اکوسیستم کاربردهای بلاکچین



۹-۱- اکوسیستم آلمان

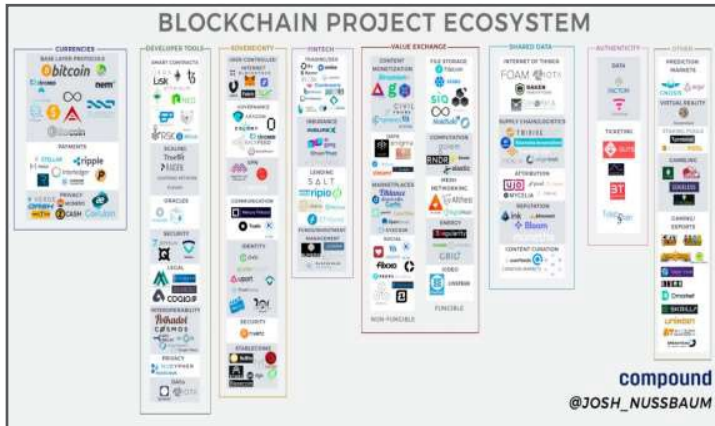
کشور آلمان دارای اکوسیستم بلاکچینی است که مطابق شکل ۲۱ دو دسته شرکت در آن درج شده‌اند. شرکت‌هایی که مقر اصلی آنها در آلمان است یا بطور واضح ثبت این کشور هستند. شرکت‌هایی که مقر اصلی آنها در آلمان نمی‌باشد اما دارای دفاتر و نیروی کار در این کشور هستند (با علامت ستاره مشخص گردیده‌اند). دسته بندی‌های متفاوتی در این اکوسیستم اعم از مالکیت معنوی، حقوق و مدیریت دارایی، زیرساخت زنجیره عمومی^۱، جامعه، ارائه دهندگان کیف پول^۲، انرژی، جستجو، صرافی و بازرگانی، پرداخت، هویت، بیمه، اینترنت اشیا، مشاوره، سرمایه‌گذاری، حریم خصوصی، خدمات مشاوره املاک^۳، زیرساخت‌های سازمانی، رسانه و اخبار، ماینینگ‌ها، پیش‌بینی بازار، سرگرمی و زیرساخت غیرمتمرکز وجود دارد.



۹-۱- اکوسیستم آلمان

۹-۲- اکوسیستم جهانی

اکوسیستم جهانی بلاکچین که توسط جان نوسباوم ارائه شده مطابق شکل ۹-۲- دارای ۸ دسته بندی مجزا است.



۹-۲- اکوسیستم جهانی

0 رمز ارز^۱: دارای سه زیرشاخه پروتکل های لایه پایه و زیرساخت رمز ارز، پرداخت و حریم خصوصی است که هرکدام دارای اجزایی همچون بیت کوین، Ripple و Zcash میباشد که کاربردهای وسیعی در این حوزه دارند. به عنوان مثال Zcash برای کاربرانی که مایل به مخفی کردن تراکنش هایشان هستند کارایی دارد. 0 ابزارهای توسعه^۲: این دسته با ۸ زیرشاخه قرارداد هوشمند، مقیاس گذاری، اوراکلز، امنیت، قانون، قابلیت همکاری، حریم خصوصی و Dag's^۳ و جزء بزرگترین بخش های اکوسیستم جهانی است. به عنوان مثال، ایجاد یک بازار اطلاعاتی غیرمتمرکز می تواند به تعدادی از زیر شاخه های ابزارهای برنامه نویسی مانند Ethereum برای قراردادهای هوشمند، Truebit برای Scailing، NuCypher برای رمزگذاری مجدد پروکسی، ZeppelinOS برای امنیت و Matterium برای اجرای قانون کمک کند.

0 حق حاکمیت^۴: این دسته دارای ۷ زیرشاخه اینترنتی که توسط کاربران کنترل می شود، حاکمیت توزیع شده، شبکه های خصوصی مجازی، ارتباطات غیرمتمرکز، هویت، امنیت و رمز ارزهای با پشتوانه فیزیکی و یا رمز ارزهایی که قیمت آنها ثابت نگه داشته می شود^۵، است. این دسته بندی ها با توجه به وضعیت فعلی بلاکچین و نیاز به امنیت و حاکمیت مناسب به سبب ایجاد اعتماد به این فناوری دسته بندی گردیده است.

0 فینتک^۶: دارای ۴ زیرشاخه تجارت / Dex^۷، بیمه، امانت دهی (قرض دادن) و مدیریت سرمایه و امور مالی است. ابزارهای موجود در این دسته بندی، موجب ایجاد انعطاف در مقابل ارزهای بومی

1. Currencies
2. Developer Tools
3. Directed Acyclic Graph
4. Sovereignty

5. Stablecoins
6. Fintech
7. Decentralized Exchange

و اقتصادهای نوظهور کشورها می‌گردد. با ظهور بازارهایی همچون وام و بیمه و استفاده مردم از آنها به صورت جداگانه (بسته به مشخصات ریسک آنها)، هزینه‌ها کاهش می‌یابد.

0 تبادل ارزش^۱: این گروه به دو زیرشاخه قابل تعویض/ مبادله (تئاتر)^۲ و غیرقابل تعویض/ مبادله (حقوق استفاده) تقسیم میشود، که در قابل تعویض‌ها، ذخیره سازی فایل، محاسبه، شبکه‌سازی، انرژی و ویدئو قرار دارند. اما در غیرقابل تعویض‌ها، کسب درآمد از محتوا، داده، اجتماعی و سهم بازار قرار دارند. قابل تعویض‌ها، بازارهایی هستند که کاربران را قادر می‌سازد تا کالاها و خدمات مبادله‌ای مانند ذخیره‌سازی، محاسبه، اتصال به اینترنت، پهنای باند، انرژی، و غیره را مبادله کنند.

0 داده‌های به اشتراک گذاشته شده^۳: دارای ۵ زیرشاخه اینترنت اشیاء، زنجیره تامین/تدارکات، مجوزها، شهرت و حقوق محتوی به اشتراک گذاشته شده است. به طور مثال در مورد مدل لایه داده مشترک، می‌توان به سیستم‌های توزیع جهانی صنعت هواپیمایی اشاره کرد. GDS یک انبار داده متمرکز از اطلاعات موجودی تمام شرکت های هواپیمایی از جمله مسیرها و قیمت گذاری به منظور ایجاد هماهنگی و عرضه است. در پروتکل‌های بلوک زنی داده، کاربران می‌توانند داده‌هایی چون شهرت را به پروتکل های داده مشترک متصل کنند و در نتیجه کاهش موانع ورود؛ افزایش رقابت و افزایش سرعت نوآوری را در پی خواهد داشت.

0 اعتبار/صحت^۴: از ۲ زیرشاخه داده و فروش بلیط تشکیل شده است. بورس اوراق بهادار دارای دارایی های دیجیتال بومی در یک

بلوک زنجیره ای خاص است و پروژه های این زیرشاخه، از این دارایی های دیجیتال برای ارائه کالاهای دنیای واقعی یا داده ها استفاده می کنند.

0 سایر موارد: دارای 5 زیرشاخه شامل پیش بینی بازار، قمار، واقعیت مجازی، بازی و سرگرمی و... است.

۳-۹- اکوسیستم ایران

اکوسیستم ایران مطابق شکل ۳-۹، دارای ۴ لایه مهم رسانه های و محتوا/ شرکت ها/ خدمات و استارتآپها است. در لایه اول استارتآپ هایی وجود دارد که ارائه کننده سرویس هایی در این زیست بوم هستند. در لایه دوم مجموعه هایی با ارائه خدماتی همچون مبادله ارز قرار دارند. در لایه سوم شرکتهای یا سازمانهایی هستند که نقش شتاب دهنده در این فناوری و در لایه آخر رسانهها قرار دارند که نقش مهمی در عرضه این فناوری ایفا میکنند.



۳-۹- اکوسیستم ایران

بخش دهم

الگوریتم کاربرد فناوری بلاکچین



بخش دهم

الگوریتم کاربرد فناوری بلاکچین

این الگوریتم دارای پنج مرحله یا سوال (بله/خیر) است که در پایان، پس از طی این فرآیندها به این نتیجه خواهیم رسید که آیا از بلاکچین باید استفاده کرد یا خیر:

- ۱- حوزه مورد مطالعه، دارای پایگاه داده است؟
 - ۲- آیا کاربران متعددی، این پایگاه داده را به روز رسانی می کنند؟
 - ۳- آیا اعتماد هر یک از کاربران به یکدیگر الزامی است؟
 - ۴- آیا منشا مشکلات از جانب یک مرجع استناد متمرکز یا شخص ثالث است؟
 - ۵- آیا تراکنش ها به هم وابسته هستند یا با هم تعامل دارند؟
- در پاسخ به سوالات بالا در صورت تایید وارد مرحله بعد شده و در صورت عدم تایید، باید از راه‌حل‌هایی مانند، عدم استفاده از بلاکچین، استفاده از یک پایگاه داده مرکزی، استفاده از چند پایگاه داده مرکزی، بهره‌گیری از یک شخص ثالث یا میانجی و استفاده از پایگاه داده Master/Slave استفاده کنیم.

بخش یازدهم

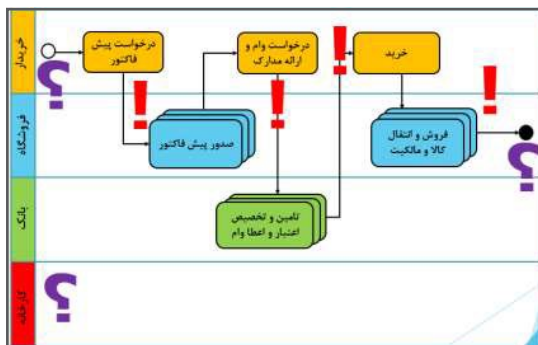
مطالعه موردی کاربرد بلاکچین



بخش یازدهم

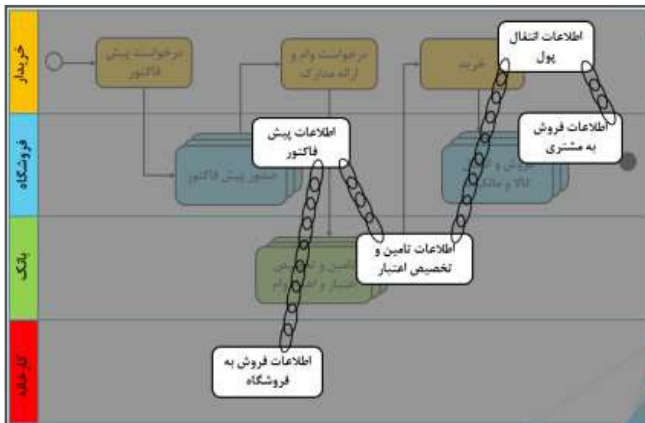
مطالعه موردی کاربرد بلاکچین

در توضیح فرایند اعطای وام، ابتدا خریدار درخواست پیش فاکتور ارائه داده و سپس در بخش فروشگاه، پیش فاکتور صادر میشود. خریدار مدارک مربوط به وام را به بانک تحویل میدهد تا تامین اعتبار شود، بانک پس از بررسی های لازم، وام را به خریدار اختصاص میدهد تا کالا را از طریق فروشگاه تهیه نماید. در این فرایند، کارخانه نقشی در تهیه کردن کالای مربوطه ندارد و از خریدار آغاز شده و به فروشگاه ختم میشود. بنابراین نمیتوان فرایند را به درستی رصد و بازبینی کرد و از نحوه عملکرد این فرایند مطلع شد. لذا اگر با هدف رفع این مشکلات، از فناوری بلاکچین استفاده کنیم به چه صورت خواهد بود؟



۱-۱۱- فرایند اعطای وام

حال بر اساس بکارگیری فناوری بلاکچین، در این فرایند، اطلاعات فروش به فروشگاه توسط کارخانه ارائه شود، همراه با اطلاعات پیش فاکترو و همچنین اطلاعات مربوط به تامین اعتبار وام که توسط بانک صورت می‌گرفت و اطلاعات انتقال پول و در نهایت اطلاعات فروش کالا به مشتری که آیا واقعا محقق می‌گردد یا خیر به طور شفاف و به صورت زنجیره ای از اطلاعات نمایش داده میشود. این اطلاعات زنجیروار در اختیار تمامی ارکان فرایند، خریدار-فروشگاه-بانک و کارخانه قرار می‌گیرد و توسط همه نظارت میشود.



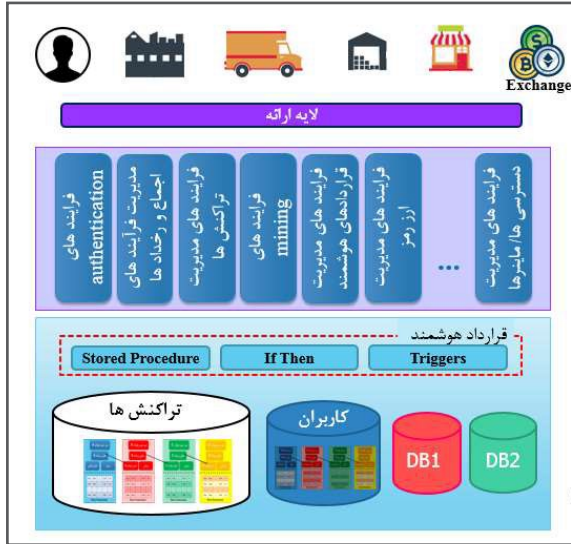
۱۱-۲- بکارگیری فناوری بلاکچین در فرایند اعطای وام

بنابراین می توان گفت که درباره عملکرد بلاکچین در اعطا وام برای خرید کالای ایرانی ابتدا باید به سوالاتی نظیر، چه کالایی؟ تولید کدام کارخانه؟ میزان سود کارخانه؟ از کانال کدام فروشگاه؟ میزان سود فروشگاه؟ توسط چه بانکی تامین اعتبار شده؟ مبلغ اعتبار چقدر بوده؟ توسط چه کسی خریداری شده است؟ چه میزان

از این اعتبارات به منابع تولیدی (کارخانه‌ها) بازگشته است؟ پاسخ دهیم. بلاکچین در این مثال، در واقع پایگاه داده تکرار شونده‌ای است که از طریق شبکه بین تمامی اعضای شبکه توزیع میشود و برای همه قابل دسترس است. اعضای شبکه خریدار-فروشگاه-بانک و کارخانه هستند. هر یک از اعضا، فعالیت و سیستم مجزایی دارند. آنها با استفاده از کلیدهای عمومی خود، اطلاعات مربوطه را اعلام میکنند. مثلاً کارخانه اطلاعات مربوط به (نام کالا، مشخصات، کد کالا، سریال، تولید کننده، بهای تمام شده، سود کارخانه، بارکد و عکس کالا)، فروشگاه اطلاعات مربوط به (نام فروشگاه، سود فروشگاه)، بانک اطلاعات مربوط به نام بانک و اعتبار آن و در نهایت خریدار هم اطلاعات مربوط به خود را در شبکه در اختیار همه قرار میدهند. هر تراکنش ایجاد شده در شبکه، باید شامل رکوردی از اطلاعات تمامی اعضا مربوط به آن کالای مشخص باشد.

اولین بلوک، با استفاده از مجموعه‌ای از تراکنش‌ها، زمان، هش اولیه و هش ایجاد شده از این تراکنش‌ها ایجاد می‌شود. حال باید کلیه تراکنش و رکورد های بلوک تایید و تصدیق شود. برای بلوک اول بسیار سخت خواهد بود و به اجماعی خارج از سیستم نیاز دارد تا اطلاعات اولیه هر یک از اعضا دقیقاً بررسی شود. بقیه بلوک‌ها با بلوک اول مقایسه میشوند. برای ساخت بلوک دوم، ماینر با انتخاب تراکنش‌های ایجاد شده در شبکه، کلیه تراکنش و رکوردها را با استفاده از بلوک قبلی تایید و تصدیق و سپس هش جدید را ساخته و در نتیجه بلوک جدید ایجاد میشود و به همین ترتیب زنجیره‌ای از بلوک‌ها را خواهیم داشت. در شکل زیر نمای اصلی سیستم بلاکچینی

ارائه شده است. در لایه اول، بلوک‌ها ایجاد میشوند و در لایه بعدی فرایندهای مدیریتی و مدیریت رخدادها و عملکر ماینرها و در لایه ارائه توسط کاربرنهایی مورد استفاده قرار میگیرد.



۳-۱۱- نمایش لایه‌های اصلی در فرآیند اعطای وام

اهداف مهم فرآیند خرید کالا با فناوری بلاکچینی، عبارتند از:

- اطمینان از شفافیت، تخصیص اعتبار به بازار هدف مشخص شده.
- جلوگیری از انحراف در تخصیص منابع (اعتبار تخصیص داده شده فقط و فقط برای خرید کالاهای موردنظر (ایرانی) صرف شود)
- ایجاد یک زیست بوم مطمئن، با مدیریت غیر متمرکز و با دسترسی عمومی جهت مدیریت اعطا وام خرید کالای ایرانی
- جذب سرمایه لازم از جامعه (غیر از منابع در اختیار)

میتوان نتیجه گرفت که به منظور اجرای این سیستم در خرید کالا،

می بایست بسترهای زیر نیز محیا گردد:

- در هر زمانی که چرخه خرید تکمیل شد، اعتبار به تولید کننده کالا سرعاً تعلق گیرد
- واسطه ها حذف گردند.
- سود دریافتی کارخانه و فروشگاه ها منطقی و قابل کنترل گردد
- تنها درصد سود مشخص هر بخش قابل تبدیل به ریال بوده و امکان خروج از چرخه را دارد
- از احتکار کالا جلوگیری شود
- فرآیند تولید محصول تا رسیدن آن به دست مشتری توزیع شده باشد
- تایید صحت تراکنش های داخل این زیست بوم

بخش دوازدهم

راه حل جامع بر مبنای بلاکچین



گام‌های ایجاد راه‌حلی جامع بر مبنای فناوری بلاکچین به شرح ذیل ارائه و توضیح داده شده است.

(۱) شناسایی یک مورد کاربرد مناسب (Use-case)

(۲) شناسایی مناسب‌ترین مکانیزم اجماع: بلاکچین واقعی، باعث توانمندسازی رمز ارز بیت کوین شده و از proof of work به عنوان مکانیزم اجماع استفاده نموده است. ولی امروزه چندین سیستم دفترکل توزیع شده وجود دارند که از مکانیزم‌های دیگری همچون موارد زیر نیز استفاده می‌کنند.

▪ Proof of stake, Byzantine fault tolerant, Deposit based consensus, Federated Byzantine Agreement, Proof of Elapsed Time, Derived PBFT, Redundant Byzantine Fault Tolerance, Simplified Byzantine Fault Tolerance, Federated consensus, Round Robin and Delegated Proof of Stake.

(۳) شناسایی مناسب‌ترین پلتفرم توسعه بلاکچین: اکثر پلتفرم‌های بلاکچین متن باز و رایگان بوده و بر اساس مکانیزم‌های اجماع، با یکدیگر متفاوت هستند.

۴) طراحی گره‌ها: موضوع دیگری که باید در این مرحله به آن توجه نمود این است که آیا گره‌ها بر اساس تکنولوژی ابری فعالیت می‌کنند. سپس موضوعاتی همچون پردازشگر، حافظه و فضای ذخیره‌سازی مطرح می‌شود. همچنین باید در خصوص سیستم عامل مربوطه نیز تصمیم‌گیری شود، گره‌ها در این گام مجوزهای متفاوتی دارند. عمومی/خصوصی/انحصاری و غیر انحصاری.

۵) طراحی نمونه ای از بلاکچین: اکثر پلتفرم‌ها باید در خصوص عناصر ذیل با دقت پیکره‌بندی شوند.

Permissions	Parameters
Asset issuance	Native assets
Asset re-issuance	Address formats
Atomic exchanges	Key formats
Key management	Block signatures
Multi signatures	Hand-shaking

۶) ساخت API ها: دسته‌های اصلی API های مورد نیاز عبارتند از:

- تولید key pairs و addresses
- انجام نظارت بر کارکردهای مربوطه
- Data authentication از طریق امضاهای دیجیتالی و هش‌ها
- ذخیره و بازیابی داده‌ها
- مدیریت چرخه عمر هوشمند دارایی‌ها، صدور، پرداخت، مبادله، سپرده و انفصال
- قراردادهای هوشمند

۷) طراحی رابط کاربری ادمین و کاربر (تکنولوژیک):

front end and programming languages

external databases

servers

۸) افزودن فناوری‌های آینده: غنی‌سازی راه‌حل‌های بلاکچین با یکپارچه‌سازی آنها با هوش مصنوعی

Biometrics, Bots, Cloud, Cognitive services, Containers, Data Analytics, Internet of Things and Machine Learning

بخش سیزدهم

مخاطرات فناوری بلاکچین برای کشورها



مخاطرات فناوری بلاکچین برای کشورها

علیرغم گستردگی کاربرد و تحولی که توسط این فناوری قابل تحقق است، مخاطراتی دربردارد. از جمله این چالش‌ها می‌توان به موارد ذیل اشاره نمود:

۱) غیرمتمرکز بودن بلاکچین در تعارض با تعاریف متداول حکومت‌ها و دولت‌هاست. در جوامع کنونی تصمیم‌گیری، اجرا و نظارت بصورت متمرکز توسط نهادهای اجتماعی صورت می‌پذیرد، حال آنکه در زیست بوم بلاکچین، راهبری امور بین کاربران (عموم کاربران یا کاربران خاص) توزیع شده است و هیچ فعالیتی بدون جلب رضایت «نصف بعلاوه یک راهبران» انجام نخواهد شد. بعبارت دیگر گسترش بلاکچین در خدمات، به مرور قدرت اداره جامعه را از حالت سخت و دستوری به حالت نرم و توافقی تغییر خواهد داد و بر همین اساس، گسترش بدون ضابطه بلاکچین، به مرور قدرت دولت‌های مرکزی را کاهش و آن‌ها را به موجودیت‌هایی فرمایشی تبدیل خواهد کرد.

۲) از سوی دیگر با توسعه مفهوم عدم متمرکز، معنای مسئولیت در کارها نیز تغییر پیدا کرده و لزوماً یک شخص / سازمان به تنهایی

مسئول پاسخ دهی در خصوص یک خدمت نخواهد بود.

۳) ایجاد مشکل برای حریم خصوصی و امنیت کاربران (که ناشی از ذخیره‌سازی غیرقابل حذف سابقه تراکنش‌های افراد یا سیستم هاست) را می‌توان بعنوان چالش بعدی در نظر گرفت. نامشخص بودن مرز عمومی یا خصوصی بودن اطلاعات و از بین رفتن حق فراموشی کاربران دو جنبه اساسی این چالش را تشکیل می‌دهند. بنابراین ایجاد مقررات به منظور تفکیک حدود و تضمین حقوق، سپس الزام سامانه‌ها و سکوها‌ی مبتنی بر بلاکچین به رعایت این مقررات چالشی در گسترش کاربرد این فناوری است.

۴) حاکمیت پلتفرم: گسترش تنوع و فراگیر بودن خدمات مبتنی بر سکوها همانند احراز هویت، پرداخت، شبکه‌های اجتماعی، تبادل کالا، اطلاع‌رسانی، تولید، انرژی، آموزش و حمل و نقل باعث شده عملاً حجم زیادی از اطلاعات در اختیار صاحبان پلتفرم قرار گیرد. به عبارت دیگر کامل‌ترین و یکپارچه‌ترین اطلاعات در اختیار صاحبان پلتفرم (مثل گوگل، IBM، Microsoft، facebook، amazon، Uber، alibaba) است. داده در فضای مجازی نقش کالا در فضای فیزیکی دارد، هرکسی که اطلاعات بیشتر و با کیفیت‌تری در اختیار داشته باشد، می‌تواند خدمات بهتری ارائه نموده، در فضای کسب و کار قانون‌گذاری و جهت‌دهی انجام داده و بر زیست بوم مربوطه حکومت نماید. پلتفرم‌های بلاکچینی به عنوان نسل جدیدی از پلتفرم‌های زیرساختی خدمات، در آینده این حوزه نقش به‌سزایی ایفا می‌نمایند.

۵) در حوزه قضایی حذف شخص ثالث (چه در نقش شاهد و چه در

نقش بنگاه) از فرآیند معامله، تغییرات و چالش‌های بنیادینی در نظام قضایی کشور بوجود خواهد آورد.

۶) ایجاد ارز رقیب برای نظام مالی کشور، چالش بنیادین دیگری است که ساختارهای اقتصادی موجود را تهدید می‌کند. امروزه پیشنهادات زیادی برای قانونی شدن رمز ارزها در دنیا و بانک‌های بزرگ مطرح است، به نحوی که انتقال منابع مالی بدون نیاز به دخالت بانک مرکزی را مقدور ساخته است. بدین معنا که انتقال پول از طریق بانک یا موسسه مالی انجام نشده و امکان نظارت بر تراکنش‌های مالی توسط هیچ ارگان حاکمیتی مقدور نخواهد بود. موافقین داخلی بلاکچین و رمزارزها با استناد به همین گزاره مدعی قابلیت رمزارزها در دور زدن تحریم هستند که در پاسخ به این موضوع می‌توان به چند نکته اشاره کرد:

- اولاً ما در رمز ارزهای معتبر جهانی جزو تنظیم‌کنندگان قواعد تأیید تراکنش نبوده و مصرف‌کننده هستیم.

- ثانیاً، مبدا و مقصد تراکنش قابل شناسایی است و با توجه به تعمیم تحریم‌های کنونی به رمزارزها از سوی وزارت خزانه‌داری آمریکا، امکان اعمال تحریم بر دارندگان و استخراج‌کنندگان رمزارز داخلی همچنان وجود دارد.

- ثالثاً گسترش استفاده از رمزارزها نه تنها موجب افزایش خروج ارز از کشور می‌شود، بلکه حذف ریال از مبادلات روزمره را نیز در پی خواهد داشت. لذا نمی‌توان در خصوص کارکردهای مالی بلاکچین ساده انگاری کرد.

جمع بندی



با استفاده و رشد روز افزون جهانی این فناوری، در این گزارش پس از تعاریف و مفاهیم به بحث پلتفرم ها و کاربرد این فناوری و مقایسه ای بین اکوسیستم ایران با برخی از اکوسیستم های معروف دنیا پرداختیم. با توجه به اهمیت این موضوع و ضرورت پرداختن به آن، نادیده گرفتن کاربردها و آثار این فناوری و یا انفعال در برابر آن، حاکمیت را با چالش جدی روبرو و هسته های حکمرانی را از مرزهای داخلی به سمت جغرافیای خارج و تحت مدیریت مجموعه های بی هویت خارجی هدایت خواهد کرد. لذا باید قبل از چیده شدن زمین بازی توسط کشورهای سلطه طلب، نسبت به سیاست گذاری و مدیریت مناسب این روند اقدام نموده و نقش کشور را در حاکمیت جهانی پررنگ تر نمود.

مدیریت هوشمندانه این فناوری در شئون مختلف اجرایی-تقنینی-قضایی، ماهیت حکمرانی را از جایگاه بالادستی و دستوری به قدرتی نرم با قابلیت اثرگذاری نقطه ای تغییر خواهد داد. نادیده گرفتن کاربردها و آثار این فناوری و یا انفعال در برابر آن، هسته های حکمرانی را از مرزهای جغرافیای خارج و تحت مدیریت مجموعه های بی هویت خارجی

خواهد برد. لذا مرکز ملی فضای مجازی، بعنوان بازوی مواجهه فعال نظام در عرصه فضای مجازی، به این نتیجه رسیده است که باید قبل از چیده شدن زمین بازی توسط کشورهای سلطه طلب، نسبت به سیاست‌گذاری و مدیریت مناسب این روند اقدام نموده و نقش کشور را در حاکمیت جهانی پررنگ تر نمود. از این رو انجام فعالیت‌های ذیل توسط مراجع مربوطه پیشنهاد می‌گردد:

- (۱) تدوین اصول و الزامات مدیریت روند زنجیره بلوکی در حوزه‌های توسعه، کاربرد و انتقال فناوری.
- (۲) هدف‌گذاری هماهنگ در خصوص تعیین محل ورود به این روند و مدیریت منابع داخلی و خارجی، برای بخش‌های مختلف حاکمیت.
- (۳) تدوین و تصویب قوانین و مقررات توسعه و به‌کارگیری این فناوری با اولویت‌بندی در مسائل اقتصادی، خدمات سلامت، احراز هویت، پولی بانکی، ثبت‌اسناد، بیمه، صنعت و تجارت.
- (۴) شناسایی و برنامه‌ریزی توسعه کاربردهای اولویت‌دار در حوزه امنیتی و نظامی.



مرکز ملی فضای مجازی
پروژه نگاه فضای مجازی

csri.majazi.ir