دوفصلنامه محاسبات و سامانه های توزیع شده
سال ششم، شماره ۱، شماره پیاپی ۱۱، صفحه ۱۱۸ تا ۱۳۶، سال ۱۴۰۲

فناوری بلاکچین:
مروری بر مفاهیم، چالش‌های بلاک‌چین در خدمات عمومی و طبقه‌بندی توکن‌های بلاکچین

سمیه کدخدا ده‌خانی[1]،حمید زنگی آبادی زاده[2]، مهدی قاسمی[3] ، مائده رحمانی[4] و فرشید وظیفه دوست[5]
[1]فارغ التحصیل مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم
Emailsk65@gmail.com
[2]دانشجوی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز ،دانشگاه پیام نور مرکز بین الملل کیش
Hamid.zangiabadi@gmail.com @gmail.com
[3] دانشجوی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز ،دانشگاه پیام نور مرکز بین الملل کیش
Mahdikmg1@gmail.com
[4]دانشجوی مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار ،دانشگاه پیام نور مرکز بین الملل کیش
Maede9708@gmail.com
[5] فارغ التحصیل مقطع کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم
Vazifehdoostfarshid@gmail.com

چکیده

بلاک‌چین مبتنی بر یک پایگاه داده غیرمتمرکز و غیرقابل تغییر است که ثبت دارایی‌ها و پیگیری تراکنش‌ها در یک شبکه شرکتی را ساده‌تر می‌کند. یک دارایی ممکن است مشهود یا نامشهود باشد. در شبکه بلاک‌چین، تقریباً هر چیزی با ارزش ممکن است ذخیره و مبادله شود، که ریسک را کاهش می‌دهد و کارایی را برای همه کاربران بهبود می‌بخشد. به طور کلی، بلاک‌چین یک دفتر دیجیتالی از تراکنش‌هایی است که در حال ثبت هستند. غیرمتمرکز است و توسط هیچ فرد، گروه یا شرکتی کنترل نمی‌شود. به عنوان یک فناوری ساختاریافته، تغییر بلاکچین بدون تایید افرادی که از آن استفاده می کنند بسیار دشوار است. بلاک‌چین داده‌ها را به عنوان یک دفتر کل غیرمتمرکز ذخیره می‌کند. شرکت کنندگان در این شبکه می‌توانند تراکنش‌ها را بخوانند، بنویسند و تأیید کنند. تراکنش‌ها قابل تغییر یا حذف نیستند. برای پشتیبانی و ایمن‌سازی سیستم بلاک‌چین، از امضای دیجیتال، توابع هش و سایر توابع رمزنگاری استفاده می‌شود. فناوری بلاک‌چین، دارای انواع اصلی توکن است، از جمله توکن‌های قابل تعویض، که همه توکن‌ها دارای ارزش برابر و توکن‌های غیرقابل تعویض دارای ویژگی‌های منحصر به فردی و قابل تعویض نیستند. در واقع، توکن‌های غیرقابل تعویض دارایی‌های دیجیتالی با یک شناسه منحصربه‌فرد هستند که در یک بلاکچین ذخیره می‌شوند. در این مقاله مروری به بررسی مفاهیم پایه‌ای بلاکچین، چالش‌های استفاده از آن و طبقه‌بندی توکن‌های بلاکچین (توکن‌های قابل تعویض، توکن-های غیر قابل تعویض و توکن‌های نیمه قابل تعویض) پرداخته می‌شود.

کلمات کلیدی: بلاکچین، تراکنش، توکن، رمزنگاری، بیت کوین، اتریوم و ماینر.

تاریخچه مقاله:
تاریخ ارسال: ۱۴۰۲/۰۱/۲۴
تاریخ اصلاحات: ۱۴۰۲/۰۵/۲۷
تاریخ پذیرش: ۱۴۰۲/۰۶/۱۶
تاریخ انتشار: ۱۴۰۲/۰۶/۳۰
ایمیل نویسنده مسئول: Hamid.zangiabadi@gmail.com

۱ - مقدمه

مفهوم بلاکچین با کاغذ سفید[1] بیت کوین برای حل مشکل خرج مضاعف، هنگام اجرای تراکنش از طریق یک رسانه ارتباطی بدون تکیه بر شخص ثالث قابل اعتماد مانند یک موسسه مالی یا یک بانک، معرفی شد. اولین بلاکچین عمومی پشت بیت کوین با مجموعه‌ای از عملکردهای خاص، یعنی ارزهای غیرمتمرکز و برنامه‌های نقدی الکترونیکی همتا به همتا توسعه یافت. بنابراین، سفارشی‌سازی بلاک‌چین بیت‌کوین عملاً دشوار بود و با استفاده از یک سیستم برنامه‌نویسی به نام اسکریپت[2] برای اهداف دیگر، پشتیبانی قابل برنامه‌ریزی بسیار

[1] White Paper

[2] Script

پایینی داشت. ویتالیک بوترین[3] متوجه این مشکل شد و پلتفرم بلاکچین اتریوم را با یک زبان برنامه‌نویسی کامل تورینگ داخلی معرفی کرد که به هر کسی اجازه می‌داد برنامه‌هایی به نام قراردادهای هوشمند بنویسد و برنامه‌های غیرمتمرکز را اجرا کند. پروتکل‌هایی مانند ارزها، سیستم‌های هویت و سیستم‌های شهرت را می‌توان با حداقل تعداد کد برای اجرا در پلتفرم اتریوم پیاده‌سازی کرد[۱]. بلاکچین فناوری مرکزی و زیربنایی ارزهای دیجیتال است، یکی از نمونه‌های نوآوری است که برای جنبش انقلاب مدیریت کسب‌وکار نقش اساسی دارد و یک فناوری نوظهور و سودمند است که پتانسیل تأثیر قابل توجهی بر عملکرد یک تعداد سازمان‌های تجاری بزرگ را دارد[۲].

در بلاکچین، داده‌ها در یک دفتر کل توزیع شده نگهداری می‌شوند. این فناوری بلاکچین برای ارائه یکپارچگی و در دسترس بودن است که به شرکت کنندگان در شبکه بلاکچین اجازه می‌دهد تا تراکنش‌های ثبت شده در یک دفتر کل توزیع شده را بنویسند، بخوانند و تأیید کنند. با این حال، عملیات حذف و اصلاح تراکنش‌ها و سایر اطلاعات ذخیره شده در دفتر کل را مجاز نمی‌داند. سیستم بلاکچین توسط پروتکل‌های رمزنگاری به‌عنوان مثال، امضاهای دیجیتال، توابع هش و...پشتیبانی و ایمن می‌شود. این موارد اولیه تضمین می‌کنند که تراکنش‌هایی که در دفتر ثبت می‌شوند از یکپارچگی محافظت می‌شوند، صحت تأیید می‌شوند و رد نمی‌شوند. علاوه بر این، به‌عنوان یک شبکه توزیع‌شده، برای اینکه به کل مجموعه شرکت‌کنندگان اجازه دهد روی یک رکورد یکپارچه به توافق برسند، فناوری بلاکچین همچنین به یک پروتکل اجماع نیاز دارد که اساساً مجموعه‌ای از قوانین است که باید توسط هر شرکت‌کننده دنبال شود تا به یک رکورد جهانی نمای یکپارچه دست یابد[۳]. در این مقاله مروری به بررسی مفاهیم پایه‌ای ساختار، تاریخچه، ویژگی‌های، معماری، چالش‌های استفاده از بلاک‌چین در خدمات عمومی، انواع این فناوری، طبقه‌بندی پلتفرم‌های بلاکچین، لایه‌های بلاکچین، برنامه‌های کاربردی بلاک‌چین و ارز دیجیتال، توکن‌سازی برای بلاکچین که شامل طبقه‌بندی در توکن‌های بلاکچین (توکن‌های قابل تعویض، توکن‌های غیر قابل تعویض و توکن‌های نیمه قابل تعویض) پرداخته شده است.

۲ – بلاکچین

بلاک‌چین مجموعه‌ای دیجیتالی از تراکنش‌ها است که در یک دفتر کل توزیع شده در یک شبکه غیرمتمرکز نظارت و ثبت می‌شود، به این معنی که شبکه هیچ مرجع کنترل مرکزی ندارد. بلاک‌چین از بلوک‌های داده گسسته‌ای تشکیل شده است که هر کدام حاوی رکوردی از اطلاعات هستند و به صورت زمانی به یکدیگر متصل هستند. این واقعیت که این پیوندها قابل تغییر نیستند به ایجاد اعتماد در شبکه کمک می‌کند. با محافظت از تبادل اطلاعات در حین وقوع، این سیستم پیشگامانه آنها را مدیریت می‌کند. تمرکززدایی از جمع‌آوری، ذخیره و پردازش داده‌ها با حصول اطمینان از یکپارچگی و تغییرناپذیری داده‌ها، اهداف فناوری بلاک‌چین هستند. بلاک‌چین یک دفتر کل دیجیتال است که اطلاعات را در ساختار داده‌ای به نام بلوک ذخیره می‌کند و آن را به یک پایگاه داده تبدیل می‌کند. پایگاه‌های داده نیز اطلاعات را در جداول ذخیره می‌کنند، اما نمی‌توان گفت که پایگاه داده یک بلاک‌چین است، با وجود اینکه بلاک‌چین یک پایگاه داده است. به دلیل تنوع در معماری، طراحی، رفتار و امنیت، نمی‌توان آنها را به جای یکدیگر مورد استفاده قرار داد. فناوری همتا به همتا یا بلاک‌چین به این معنی است که هیچ نهاد واحدی داده‌ها را کنترل نمی‌کند. توانایی‌ها در یک موجودیت متمرکز نیستند زیرا به‌روزرسانی اطلاعات از طریق مکانیزم اجماع انجام می‌شود. بنابراین، قدرت‌ها در یک نهاد متمرکز نیستند و به همین دلیل است که از دموکراسی در کار حمایت می‌کند. ورودی‌های غیرقابل تغییر داده نیز یکی از ویژگی‌های فناوری بلاک‌چین است. هر ورودی در یک بلاک‌چین دارای خاصیت یک رکورد غیرقابل تغییر است زیرا با یک هش رمزنگاری محافظت می‌شود. در حالی که در پایگاه داده معماری یک مدل کلاینت-سرور است و مدیر می‌تواند تمام رکوردها را تغییر دهد، یا حتی حذف کند. شباهت‌های کمی بین هر دو وجود دارد، اما بسیاری از محققان استدلال می‌کنند که وقتی برنامه‌ها غیرقابل اعتماد هستند، بلاک‌چین‌ها مناسب هستند، در حالی که پایگاه‌های داده زمانی مناسب هستند که عملکرد مهم‌تر از امنیت باشد[۴].

بلاکچین یک دنباله زمانی از تراکنش‌های سفت و سخت است که توسط گروهی از رایانه‌ها با استفاده از الگوریتم‌های خاص مدیریت می‌شود. هر کامپیوتری که در این گروه شرکت می‌کند یک گره نامیده می‌شود و هر گره یک نسخه از

[3] Vitalik Buterin

داده‌ها را به اشتراک می‌گذارد که به عنوان دفتر کل دیجیتال نامیده می‌شود. هرگره سوابق تراکنش‌ها را در چندین بلوک متوالی نگهداری می‌کند و از الگوریتم یکسانی برای رسیدن به توافق مشترک استفاده می‌کند. این تراکنش‌ها در هر گره در یک شبکه توزیع شده نظیر به نظیر ذخیره می‌شوند [۵].

۳ – ساختار بلاکچین

اولین نسل از فناوری بلاک‌چین در ابتدا در برنامه‌های کاربردی ارزهای دیجیتال معرفی شد. در آن زمان، جهان بر این باور بود که این فناوری می‌تواند بیشتر از کاربردهای ارزی انجام دهد. از این نظر، اتریوم نماینده نسل دوم فناوری بلاک‌چین است. قراردادهای هوشمند، نرم‌افزارهای مبتنی بر بلاک‌چین هستند که با رعایت معیارهای خاصی اجرا می‌شوند. آنها توسط رویدادی مانند تاریخ انقضا، یا دستیابی به یک قیمت خاص ایجاد می‌شوند. دولت الکترونیک فناوری بلاک‌چین را مانند بسیاری از صنایع دیگر برای حمایت از تحول مدیریت عمومی و تسهیل ارائه خدمات عمومی شفاف و ایمن بررسی کرده است. داده‌های شخصی جزء مشترک خدمات دولت الکترونیک است، بنابراین باید به دقت محافظت شود. به منظور رعایت حریم خصوصی کاربران هنگام انتشار تراکنش‌ها در دفتر کل، و در نظر گرفتن محدودیت‌های قانونی مانند محدودیت‌های اعمال‌شده توسط مقررات عمومی حفاظت از داده‌ها، راه‌حل‌های پیشنهادی باید بتوانند مجوزهای لازم را به طرف‌های مدیریت دولتی و سایر ذینفعان اعطا کرده و دسترسی داشته باشند. فناوری بلاک‌چین دارای محدودیت‌های مختلف، چالش‌های اجرایی، چالش‌های امنیتی، و چالش‌های اقتصادی، مقرراتی و سیاسی است[۴].

۴- تاریخچه بلاکچین

فناوری بلاکچین یک دفتر کل توزیع شده است که این قدرت را دارد که طیف گسترده‌ای از کسب و کارها را به طور کامل متحول کند. این یک روش ضد دستکاری، شفاف و ایمن برای ذخیره داده‌ها است. بلاک‌چین بر روی یک شبکه کامپیوتری ساخته شده است که دفتر کل معاملات را به اشتراک می‌گذارد. شبکه هر تراکنش را قبل از اضافه کردن آن به دفتر کل احراز هویت می‌کند. این امر هک یا خراب کردن داده های یک بلاک‌چین را بسیار دشوار می‌کند. با استفاده از نام مستعار ساتوشی ناکاموتو، یک فرد یا گروه ناشناس از افراد برای اولین بار در سال ۲۰۰۸ از کلمه "بلاکچین" استفاده کردند. ناکاموتو از فناوری بلاک‌چین برای ایجاد ارز دیجیتال بیت کوین استفاده کرد که اولین بار در سال ۲۰۰۹ به عنوان دفتر کل توزیع شده پشت تراکنش های بیت کوین معرفی شد. فناوری بلاک‌چین به ارزهای دیجیتال محدود نمی‌شود. این پتانسیل را دارد که در طیف گسترده‌ای از کاربردها مانند مراقبت‌های بهداشتی، مدیریت زنجیره تامین، خدمات مالی اینترنت اشیا استفاده شود. فناوری بلاک‌چین مزایای بالقوه زیادی دارد. این می‌تواند به تراکنش‌های کارآمدتر و ایمن‌تر، شفافیت بهبود یافته و کاهش هزینه‌ها منجر شود. با این وجود، برای استفاده کامل از قابلیت‌های فناوری بلاکچین، چندین مشکل وجود دارد که باید حل شود. این چالش‌ها شامل مقیاس‌پذیری، امنیت و حریم خصوصی است. هدف این نظرسنجی این است که به خوانندگان درک گسترده‌ای از ویژگی‌های برجسته فناوری بلاک‌چین، الگوریتم‌های اجماع بلاک‌چین مختلف و کاربردهای آینده نگر بدهد. این نظرسنجی با ارائه یک بررسی کامل از فناوری بلاک-چین که برای محققان، توسعه‌دهندگان و شرکت‌هایی که می‌خواهند بیشتر درباره این فناوری جدید بدانند، مفید خواهد بود.

فناوری بلاکچین در اوایل دهه ۱۹۸۰ زمانی که دیوید چاوم پروتکل بلاکچین را پیشنهاد کرد، شکل گرفت. استوارت هابر و دبلیو اسکات استورنتا در مقاله‌ای در سال ۱۹۹۱ یک روش مهر زمانی توزیع شده را با استفاده از رمزنگاری برای ایمن کردن دفتر کل شرح دادند. توسعه بیشتر توسط نیک سابو در اواخر دهه ۱۹۹۰ انجام شد که مفهوم ارز دیجیتال را با استفاده از فناوری بلاک‌چین برای امنیت تراکنش‌ها معرفی کرد. پیشرفت بزرگ در فناوری بلاک‌چین در سال ۲۰۰۸ زمانی که ساتوشی ناکاموتو برگه سفید بیت کوین را منتشر کرد رخ داد. این مقاله یک سیستم نقدی الکترونیکی همتا به همتا را نشان می‌دهد که از بلاک‌چین برای امنیت تراکنش استفاده می‌کند. بیت کوین در سال ۲۰۰۹ راه اندازی شد و به سرعت به عنوان شکل جدیدی از ارز دیجیتال محبوبیت یافت. اتریوم که در سال ۲۰۱۵ توسط ویتالیک بوترین معرفی شد، قابلیت‌های بلاک‌چین را به عنوان یک پلتفرم همه کاره‌تر گسترش داد. اتریوم توسعه برنامه‌های غیرمتمرکز را که روی بلاک‌چین کار می‌کنند را امکان‌پذیر می‌کند. برنامه‌های غیرمتمرکز مختلفی از جمله بازی، توکن های غیرقابل تعویض و امور مالی غیرمتمرکز بر روی اتریوم ساخته شده‌اند. بنیاد اتریوم پروژه اتریوم ۲.۰ را در سال

۲۰۲۰ با هدف افزایش مقیاس پذیری، امنیت و کارایی معرفی کرد. این پروژه هنوز در حال توسعه است و انتظار می‌رود تا سال ۲۰۲۳ تکمیل شود. همانطور که در شکل ۱ نشان داده شده است.

شکل۱: تاریخچه بلاکچین (اعتبار عکس/تصویر: اصلی)[۶]

۵- ویژگی‌های بلاک‌چین

بلاک‌چین یک فناوری دفتر کل توزیع شده جدید، یکپارچه‌سازی ذخیره‌سازی توزیع شده، الگوریتم رمزگذاری، انتقال همتا به همتا، مکانیسم اجماع، قرارداد هوشمند و سایر فناوری‌ها است که می‌تواند به اشتراک‌گذاری اطلاعات و چشم انداز فوق‌العاده بین چندین طرف را تحقق بخشد، کارایی پردازش کسب و کار را بهبوددادە و باعث کاهش هزینه‌ها شود. در حال حاضر، با توسعه سریع جامعه، فناوری بلاک‌چین پتانسیل قوی در بسیاری از زمینه ها، مانند کاربرد در زنجیره تامین، پزشکی، امور مالی، حفاظت از حریم خصوصی، یادگیری فدرال و سایر زمینه‌های صنعتی نشان داده است. با این حال، در سناریوهای کاربردی مختلف، الزامات مختلفی برای کنترل دسترسی بلاک‌چین، توان عملیاتی، اندازه شبکه و غیره وجود دارد. نحوه تعامل با داده‌ها و انتقال ارزش بین سیستم‌های مختلف بلاک‌چین به کانون تحقیقات در دانشگاه و صنعت تبدیل شده است[۷]. پس از راه اندازی بلاکچین در سال ۲۰۰۸، به عنوان یک نوآوری مخرب که ممکن است نحوه تعامل افراد، ایجاد هزینه‌های خودکار، پیگیری و نظارت بر تراکنش‌ها را تغییر دهد، به تکامل خود ادامه داد. الزام مقامات مرکزی برای نظارت و کنترل تراکنش‌ها و تعاملات بین اعضای مختلف ممکن است با استفاده از زنجیره بلوکی حذف شود که می‌تواند مقرون به صرفه باشد[۸].

در یک محیط غیرقابل اعتماد، بلاکچین ویژگی‌های مطلوبی از جمله عدم تمرکز، استقلال، یکپارچگی، تغییرناپذیری، تأیید، تحمل خطا، ناشناس بودن، قابلیت حسابرسی و شفافیت را در اختیار کاربران قرار می‌دهد که با این ویژگی‌های پیشرفته، فناوری بلاکچین در چند سال اخیر توجه دانشگاهی و صنعتی زیادی را به خود جلب کرده است. برای اینکه به کسی کمک کند تا فناوری بلاکچین و مسائل امنیتی بلاکچین را درک کند، به ویژه برای کاربرانی که از بلاکچین برای انجام تراکنش‌ها استفاده می‌کنند و برای محققانی که فناوری بلاکچین را توسعه می‌دهند و مسائل امنیتی بلاکچین را بررسی می‌کنند، تلاش و زمان بسیاری از محققان صرف انجام این کار شد[۳].

بلاکچین، یک سیستم دفتر کل توزیع شده، تراکنش-های ایمن، باز و غیرقابل تغییر را امکان‌پذیر می‌کند. این شبکه-ای از پایگاه داده مشترک رایانه‌ها است که به روز نگه داشته می‌شود. هر بلوک در زنجیره بلوکی شامل مجموعه ای از تراکنش‌ها است و هر بلوک به بلوک قبلی در زنجیره مرتبط است. در نتیجه، تغییر داده‌های موجود در بلاکچین مستلزم تغییر هر بلوک در زنجیره است که انجام آن را بسیار دشوار می‌کند. ویژگی‌های اصلی بلاکچین در زیر ذکر شده است[۶]:

تغییرناپذیری: تغییرناپذیری بلاکچین به این معنی است که وقتی داده‌ها به بلاکچین اضافه می‌شوند، نمی‌توان آن‌ها را به راحتی تغییر داد یا حذف کرد. این باعث می‌شود بلاکچین برای برنامه‌هایی که به درجه بالایی از امنیت و شفافیت نیاز دارند، مانند تراکنش‌های مالی و مدیریت زنجیره تامین، ایده‌آل باشد.

شفافیت: به دلیل شفافیت ببلاکچین، تمام گره‌های شبکه به تراکنش‌های یکسان و یک کپی از بلاکچین دسترسی دارند. این امر باعث می‌شود که کلاهبرداری یا فساد به شدت چالش برانگیز باشد.

امنیت: امنیت بلاکچین از طریق استفاده از انواع تکنیک‌های رمزنگاری مانند توابع هش، امضای دیجیتال و رمزگذاری به دست می‌آید. این به این دلیل است که ب بلاکچین مبتنی بر رمزنگاری است که یک فناوری بسیار امن است. رمزنگاری استفاده شده در بلاکچین دسترسی کاربران غیرمجاز به داده‌های موجود در بلاکچین را بسیار دشوار می‌کند.

تمرکززدایی: تمرکززدایی از بلاکچین از طریق استفاده از شبکه همتا به همتا حاصل می‌شود. این بدان معناست که هیچ مرجع مرکزی وجود ندارد که بلاکچین را کنترل کند. در عوض، بلاکچین توسط گره‌های موجود در شبکه کنترل می-شود. این امر سانسور یا دستکاری زنجیره بلوکی را برای هر

نهادی بسیار دشوار می‌کند. این امر آن را در برابر سانسور و دستکاری بسیار مقاوم می‌کند.

پایداری: تراکنش‌ها را می‌توان به سرعت تأیید کرد و تراکنش-های نامعتبر توسط ماینرهای صادق پذیرفته نمی‌شوند. تقریباً غیرممکن است که تراکنش‌ها را پس از گنجاندن در بلاکچین حذف یا بازگردانید. بلوک‌های حاوی تراکنش‌های نامعتبر را می‌توان فوراً کشف کرد[۹].

ناشناس بودن: هر کاربر می‌تواند با یک آدرس تولید شده با بلاکچین تعامل داشته باشد که هویت واقعی کاربر را آشکار نمی‌کند. توجه داشته باشید که بلاکچین به دلیل ضمانت حفظ حریم خصوصی به دلیل محدودیت ذاتی، نمی‌تواند حفظ کامل حریم خصوصی را تضمین کند[۹].

قابلیت حسابرسی: بلاکچین بیت کوین داده‌های موجودی کاربر را بر اساس مدل خروجی تراکنش خرج نشده ذخیره می‌کند. هر تراکنش باید به برخی از تراکنش‌های خرج نشده قبلی اشاره کند. هنگامی که تراکنش جاری در بلاکچین ثبت می‌شود، وضعیت تراکنش‌های خرج نشده ارجاعی از مصرف نشده به مصرف شده تغییر می‌کند. بنابراین تراکنش‌ها را می-توان به راحتی تأیید و ردیابی کرد[۹].

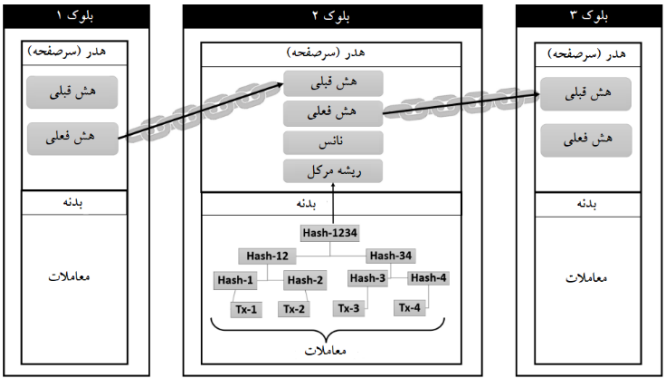
۶- معماری بلاکچین

زنجیره بلوکی مجموعه‌ای از بلوک‌های داده‌ای است که به طور مداوم در حال گسترش هستند که به یکدیگر متصل شده‌اند تا یک زنجیره طولانی را تشکیل دهند. همانطور که در شکل ۲ توضیح داده شده است. این شبکه از بلوک‌های داده متصل یک دفتر کل توزیع شده را نشان می‌دهد که در یک شبکه همتا به همتا منتشر می‌شود. دفتر کل توزیع شده شامل مجموعه‌ای از داده‌های دیجیتال است که از طریق یک شبکه همتا به همتا همگام‌سازی، تکثیر، توزیع و به اشتراک گذاشته می‌شوند. هر دستگاهی که به شبکه اصلی متصل است، آخرین نسخه دفتر کل مشترک را حفظ می‌کند، به عنوان مثال، هر همتا در شبکه یک کپی از دفتر کل دارد که با دیگری یکسان است. دفتر کل عمدتاً با ایمنی آن مشخص می‌شود و پایگاه داده تنها با افزودن بلوک‌های جدید به زنجیره قابل گسترش است. تغییرات در رکوردهایی که قبلاً در زنجیره ثبت شده‌اند از نظر محاسباتی غیرممکن است. در نتیجه، مزیت اصلی دفتر کل توزیع شده توصیف شده، ماهیت غیرمتمرکز آن است. در واقع، هیچ مرجع مرکزی وجود ندارد که دفتر کل را کنترل کند. با این حال، هر گره زمانی که یک بلوک جدید به زنجیره بلوکی اضافه می‌شود، دفتر کل خود را با استفاده از یک مکانیسم اجماع مشترک به روز می‌کند. علاوه بر این، در زنجیره بلوکی و به ویژه در شبکه‌های ارزهای دیجیتال، صحت داده‌ها اغلب توسط یک فناوری رمزگذاری نامتقارن به نام رمزنگاری کلید عمومی تأیید می‌شود. در این فناوری، فرستنده و گیرنده هر دو دارای یک جفت کلید متشکل از یک کلید عمومی و یک کلید خصوصی هستند. کلید خصوصی منحصراً در دسترس گره‌هایی است که آن را ایجاد کرده‌اند، در حالی که کلید عمومی نسبتاً آزادانه در سراسر شبکه پخش می‌شود. فرستنده داده‌ها را با استفاده از کلید عمومی گیرنده رمزگذاری می‌کند. از آنجایی که داده‌ها با استفاده از کلید عمومی گیرنده رمزگذاری می‌شوند، تنها با استفاده از کلید خصوصی گیرنده می‌توان آنها را رمزگشایی کرد. علاوه بر این، در مورد ارسال تراکنش‌ها در شبکه بلاکچین، تراکنش تنها پس از امضای دیجیتالی کامل تلقی می‌شود. پس از آن، تراکنش توسط فرستنده با استفاده از کلید خصوصی او امضا می‌شود. برای گیرنده، اصالت تراکنش، یعنی هویت فرستنده، می‌تواند با استفاده از کلید عمومی مرتبط (متعلق به فرستنده) بررسی شود. به این ترتیب، تمام تراکنش‌ها به طور خودکار توسط گره-ها بررسی و احراز هویت می‌شوند و شبکه هر گونه تراکنش احراز هویت نشده را رد می‌کند. لطفاً توجه داشته باشید که در شبکه بلاکچین، یک تراکنش معتبر و استخراج شده غیرقابل برگشت است[۱۰].

در واقع، تغییر داده‌های موجود در بلوک‌ها به دلیل ویژگی‌های رمزنگاری بلاکچین دشوار است. در عمل، بلوک‌ها از طریق یک مرجع هش به هم متصل می‌شوند، زیرا هر بلوک بعدی علاوه بر مقدار هش بلوک واقعی، مقدار هش بلوک قبلی را نیز دارد (شکل ۲). ایجاد یک مقدار هش از طریق استفاده از یک الگوریتم هش رمزنگاری پیچیده و ریاضی امکان‌پذیر است، که هر نوع ورودی را می‌پذیرد و یک عدد با طول ثابت به نام مقدار هش را خروجی می‌دهد. مشخصه اصلی یک تابع هش این است که اگر یک کسری در ورودی تغییر کند، کل مقدار خروجی تغییر خواهد کرد. در نتیجه، اگر یک مهاجم برای مثال سعی کند داده‌ها را در بلوک ۱ ویرایش کند، مقدار هش آن بلوک در بلوک ۲ تغییر می‌کند، و بنابراین نفوذگر باید مقدار هش را تغییر دهد. آن بلوک علاوه بر این، از آنجایی که بلوک۲

هش بلوک۱ را انجام می‌دهد، هر گونه تغییر در هش مقدار هش بلوک۲ در بلوک۳ را تغییر می‌دهد. در نتیجه، اگر کسی بخواهد یک بلوک را اصلاح کند، باید داده‌ها را برای تمام بلوک‌های بعدی در بلاکچین تغییر دهد. علاوه بر این، حتی اگر مقدار هش یک بلوک مشخص باشد، محاسبه ورودی تابع هش به دلیل ویژگی غیرقابل وارونگی تابع هش دشوار است. سوال بعدی این است که چگونه می‌توان بلوک های جدید را به شبکه اضافه کرد. در واقع، اگر مورد خاص ارز دیجیتال بیت کوین در نظر گرفته شود، انواع خاصی از گره‌ها به نام «ماینرها» وجود دارند که مسئول ساختن بلوک‌های جدید در زنجیره هستند. وظیفه ماینر به روز رسانی (از تراکنش های قبلی) سوابق دفتر کل عمومی بلاکچین است. هر گره شبکه می‌تواند یک ماینر باشد. ماینرها ساعت‌ها طول می‌کشد تا یک بلوک جدید ایجاد کنند، زیرا آنها باید یک پازل ریاضی به نام "اثبات کار[4] " را حل کنند. چندین ماینر می‌توانند به صورت موازی کار کنند تا یک بلوک جدید اضافه کنند. با این وجود، تنها یک ماینر می‌تواند در لحظه یک بلوک جدید اضافه کند. اولین ماینری که مشکل اثبات کار را حل می‌کند می‌تواند آن بلوک جدید را ماین کند. برای رفع مشکل استخراج اثبات کار، به قدرت محاسباتی عظیمی نیاز است. می‌توان کل فرآیند را به چند مرحله تقسیم کرد[۱۰]:

- برای شروع استخراج یک بلوک جدید، یک ماینر تراکنش‌ها را از شبکه مشترک جمع‌آوری کرده و آنها را در یک بلوک سازماندهی می‌کند.
- ماینر ارزش هش قبلی بلاکچین را تأیید می‌کند و آن را با تراکنش‌ها در بلوک جدید مورد نظر سپرده می‌کند.
- ماینر متغیری به نام" نانس[5]" را بدست آورده و در همان بلوک ذخیره می کند (شکل ۲). این مقدار متغیر می‌تواند در هر زمان توسط ماینر تغییر یابد.
- ماینر اکنون پازل اثبات کار شبکه را بررسی خواهد کرد. مشکل شامل یافتن یک مقدار هش ویژه برای کل بلوک جدید است که با چندین صفر شروع می‌شود. این مقدار هش ویژه را می‌توان با تغییر مقدار نانس یافت، که تنها پارامتری است که ماینر می‌تواند آن را تغییر دهد. هنگامی که ماینر همان مقدار صفرهای ابتدایی را برای یک مقدار غیرانسی معین کشف کرد، می‌تواند پاسخ را در شبکه پخش کند و نشان دهد که در استخراج یک بلوک جدید موفق بوده است. توجه داشته باشید که تعداد صفرهای متوالی سطح دشواری استخراج را نشان می‌دهد.



شکل۲: معماری کلی بلاکچین[۱۰].

گره‌های ماینرهای، نیز مسئول تأیید تمام داده‌های موجود در یک بلوک هستند. برای این منظور، داده‌های یک بلوک با شکل درخت مرکل ذخیره می‌شوند که یک ساختار داده خاص را به شکل درخت مبتنی بر هش نشان می‌دهد (شکل ۲). درختان تأیید داده‌ها را ساده می‌کنند و بهتر است با استفاده از تابع هش همه تراکنش‌ها در نظر گرفته شود، نه از ساختار درخت مرکل. اگر یک تراکنش منفرد تغییر کند، کل نتیجه هش تغییر می‌کند و تشخیص داده‌های تغییر یافته غیرممکن می‌شود. با این حال، با استفاده از ساختار خاص درخت مرکل، می‌توان در هر کسری از درخت ببینیم که کدام قسمت مقدار هش اشتباه را ارائه می‌کند. فرض کنید یک مهاجم، تراکنش Tx-3 را تغییر می‌دهد .در نتیجه، به راحتی می‌توان تشخیص داد که فقط سمت راست درخت مرکل خروجی‌های هش نادرست می‌دهد. از آنجایی که مقادیر هش Tx-3 و Tx-4 اشتباه خواهد بود، نیازی به بررسی Tx-1 و Tx-2 نیست و در نتیجه، درخت مرکل برای تأیید داده‌ها در سیستم های توزیع شده همتا به همتا بسیار مفید است[۱۰].

۷- چالش‌های استفاده از بلاکچین در خدمات عمومی

در ابتدایی‌ترین شکل، بلاکچین یک شبکه توزیع‌شده است که مجموعه‌ای سازمان‌یافته از اسناد مختلف را شامل می‌شود که توسط اتصالاتی به نام زنجیره‌ها به هم مرتبط شده‌اند. فقط کاربران ثبت نام شده به جزئیات ذخیره شده در

[4] Proof of Work

[5] Nonce

این بلوک‌ها که مربوط به تراکنش‌های مختلف است دسترسی دارند. مجوز کاربر توسط یک سری پویا از کلیدهای رمزگذاری خود مدیریت حفظ می‌شود، هر کاربر تأیید شده یک کلید منحصر به فرد حساس به زمان دریافت می‌کند که اگر تایمر رمزگشایی منقضی شود، به طور خودکار آن را مسدود می‌کند. بدون نیاز به یک مرجع مرکزی، فناوری بلاکچین یک تنظیمات محاسباتی توزیع شده را امکان‌پذیر می‌کند. بلاکچین یک پلتفرم جدید است که امکان محاسبات مستقل‌تر را فراهم می‌کند. در طول رشد بی‌سابقه بیت‌کوین به‌عنوان یک ارز دیجیتال در سال‌های ۲۰۱۷-۲۰۱۸، محبوبیت آن افزایش یافت. با این حال، ارز دیجیتال تنها کاربرد یا استفاده زنجیره بلوکی نیست. کاربردهای گسترده‌ای در مشاغل از جمله جمع‌آوری داده‌ها و اشتراک‌گذاری در محیط های مختلف دارد[۱۱]. در زیر چالش‌های استفاده از بلاکچین در خدمات عمومی ذکر شده است [۴]:

امنیت: مشکلات امنیتی زیادی در بلاکچین وجود دارد. برخی از این مسائل امنیتی در نسل اول و دوم بلاکچین رایج است و برخی دیگر مختص نسل دوم یعنی قراردادهای هوشمند است.

حریم خصوصی: از آنجا که یک بلاکچین توزیع شده است، هر گره کاملی که تراکنش‌ها را پردازش می‌کند و زنجیره بلاک را ایجاد می‌کند باید به داده‌های تراکنش واقعی بلاکچین دسترسی داشته باشد. این بدان معناست که در یک ارز رمزنگاری شده مانند بیت‌کوین، زنجیره بلوکی برای همه قابل دسترسی است و هر تراکنش را می‌توان به بلوک پیدایش اولیه ردیابی کرد و اجازه می‌دهد تا چندین ظاهر افراد را به هم متصل کرده و هویت آنها را آشکار کند. علاوه بر این، برنامه‌هایی که بر قراردادهای هوشمند متکی هستند، مانند سیستم‌های دولت الکترونیک، ممکن است مقدار قابل توجهی از داده‌های محرمانه را در مورد شهروندان، مشتریان، کارمندان، محصولات و تحقیقات جمع‌آوری، ذخیره و مدیریت کنند. وقتی چنین اطلاعاتی به خطر بیفتد، معمولاً اعتماد و اطمینان کاربران از بین می‌رود. حریم خصوصی را می‌توان با توجه به دیدگاه هویت و دیدگاه داده افزایش داد.

مقیاس‌پذیری: استفاده از فناوری بلاکچین در خدمات دولتی منجر به ذخیره حجم زیادی از داده‌ها در زنجیره می شود در حالی که خدمات باید فوراً معرفی شوند. دو مشکل در مورد مقیاس‌پذیری، توان عملیاتی و ظرفیت وجود دارد. اولین مورد از زمان انتظار برای استخراج و گنجاندن هر تراکنش در یک بلوک ایجاد می‌شود زیرا اندازه بلوک محدود است. علاوه بر این، اگر زمان تولید بلوک کوتاه باشد، فورک‌های زیادی تولید می‌شود، بنابراین نمی‌توان زمان تولید بلوک را به طور مصنوعی کاهش داد. از طرف دیگر، اگر تمام داده‌ها در یک زنجیره ذخیره شوند، اندازه زنجیره بیش از حد بزرگ می‌شود. اندازه بلاکچین فعلی بیت کوین و اتریوم ۱۶۳.۳۴ گیگابایت و در نتیجه ۶۶۷.۱۰ گیگابایت است. تا سال ۲۰۲۰ راه‌های مختلفی برای حل این مسائل وجود دارد.

۸- انواع فناوری بلاکچین

در میان تمام فناوری‌های موجود برای امنیت داده‌ها و حفظ حریم خصوصی، بلاکچین به دلیل ویژگی‌هایی اصلی مانند تغییر ناپذیری و برگشت‌ناپذیری، کارآمدترین فناوری است. بلاکچین نسبت به تغییر داده‌ها سرکش است. هرگاه تغییری در تراکنش‌های دفتر کل ایجاد شود، تغییرات به همه گره‌ها توزیع می‌شود تا رونوشت خاص خود از دفتر را تأیید و به‌روزرسانی کنند. هنگامی که تراکنش از تمام گره‌های شبکه تأیید شد، امکان تغییر تراکنش بدون تغییر بلوک‌های بعدی و قبلی وجود ندارد. بنابراین، تراکنش‌های بلاکچین غیرقابل برگشت هستند و داده‌های آن‌ها دائماً اضافه می‌شوند. هر بلوک با پیوندی که به آن زنجیره نیز می‌گویند متصل است. بلوک بعدی شامل هش بلوک قبلی برای بازدید از زنجیره به ترتیب زمانی معکوس است. بلاکچین از ساختار غیرمتمرکز و توزیع شده همراه با ویژگی‌های رمزنگاری استفاده می‌کند که باعث می‌شود به روشی منحصر به فرد کار کند. در جایی که امنیت و محرمانه بودن اطلاعات اولویت اول شبکه است، فناوری بلاک‌چین ترجیح داده می‌شود. در اینترنت اشیا، کنترل دسترسی را می‌توان با پیاده‌سازی بلاکچین کارآمدتر به دست آورد. علاوه بر این، از ادبیات، واضح است که استفاده از بلاکچین نتایج بسیار خوبی برای موارد استفاده دیگر مانند کار شبکه موقت خودرو، مراقبت‌های بهداشتی و زنجیره تامین خواهد داشت[۵]. در زیر انواع فناوری بلاچکین اشاره شده است:

بلاکچین خصوصی: نوعی بلاکچین است که در آن اطلاعات به صورت خصوصی در یک شرکت تنها نگهداری می شود. کاملاً مجاز است، و همچنین هر گره‌ای که می‌خواهد متصل شود باید بخشی از چنین گروه خاصی شود. بلاکچین خصوصی عملی است و اغلب برای گزینه‌های منحصر به فرد

شرکت برای ردیابی انتقال اطلاعات بین چندین دفاتر استفاده می‌شود. ریپل و هایپر لجر دو نمونه از بلاکچین خصوصی هستند[۱۲].

بلاکچین ترکیبی: یک بلاکچین ترکیبی دفتر کل خصوصی و عمومی را در یک دفتر کل دیجیتالی واحد ترکیب می‌کند[۱۳].

بلاکچین کنسرسیوم: زنجیره بلوک خصوصی و فدرال که معمولاً به عنوان بلاکچین کنسرسیوم شناخته می‌شود، کاملاً مشابه هستند. یک گروه مشتری تنظیم شده بخشی از این شبکه "نیمه خصوصی" است. به عنوان یک دفتر کل قابل تأیید، هماهنگ، کاملاً شفاف و توزیع شده در نظر گرفته می‌شود که انتقال داده ها را در بین کاربران ثبت می‌کند. به همین دلیل، به ندرت بسیاری از گره‌ها در شبکه زنجیره بلوک قادر به داشتن امتیازات اجماع هستند[۱۲].

بلاکچین عمومی: بلاکچینی که برای دسترسی عموم باز است به عنوان بلاکچین عمومی شناخته می‌شود. همه ممکن است در روند دستیابی به اجماع شرکت کنند و بنابراین می‌توانند بلافاصله تراکنش‌ها را در سیستم بلاکچین عمومی بررسی و تأیید کنند. اکوسیستم‌های رمزنگاری از جمله بیت کوین، اتریال و بسیاری دیگر نمونه‌های انگشت شماری از پیاده‌سازی زنجیره بلوک هستند. حریم خصوصی و قابل اعتماد بودن زنجیره بلوک بیت کوین با استفاده از احراز هویت رمزنگاری تضمین می‌شود زیرا فناوری زنجیره بلوک به زیرساخت سرور مرکزی متکی نیست[۱۲].

۹- طبقه‌بندی پلتفرم‌های بلاکچین

فناوری بلاکچین می‌تواند به دستیابی به هفت هدف هزینه، کیفیت، سرعت، وابستگی، کاهش ریسک، پایداری و همچنین انعطاف‌پذیری، مدیریت زنجیره تامین کمک کند. بلاکچین را به عنوان قابلیتی برای شکستن سیلوهای داده و ارائه یک منبع داده در دیجیتالی کردن با کمک کنترل داده در زمان واقعی که برای همه شرکای مورد اعتماد در شبکه مورد نیاز است، مورد بحث قرار داده است. با کمک بلاکچین اعتماد و امنیت را می‌توان به راحتی افزایش داد و جدای از این، ارزش‌های تجاری نیز وجود دارد که با بهبود کارایی، شهرت و پاسخگویی به اعتمادسازی با کمک بلاک چین کمک می‌کند[۱۴]. در این بخش فرعی، یک تحلیل مقایسه‌ای از رایج‌ترین و محبوب‌ترین پیاده‌سازی‌های بلاکچین منبع باز را مورد بحث و بررسی قرار داده شده است. با بیت کوین شروع سپس پیاده سازی‌های اتریوم، فابریک هایپرلجر، Quorum و کوردا ۳ مورد بحث قرار می‌گیرد[۱۵]:

بیت کوین: بیت کوین مفهوم بلاکچین را به دنیا معرفی کرد. توسط ساتوشی ناکاموتو ایجاد شد. از زمان معرفی آن محبوب بوده است و مشتقات بسیاری را در سراسر جهان روشن کرده است. این یک رکورد دفتر کل بدون مجوز است، به این معنی که دفتر کل تمام تراکنش های بیت کوین به صورت عمومی در دسترس است و در گره های سراسر جهان توزیع می شود. از زمان ایجاد آن در سال ۲۰۰۸، بسیاری استدلال کرده‌اند که بیت‌کوین باید به‌عنوان یک کالای سوداگرانه و نه صرفاً یک ارز رمزنگاری‌شده در نظر گرفته شود. نمادهای مورد استفاده برای بیت کوین BTC یا XBT هستند. BTC مخفف بیت کوین است. این اختصارات از سوی سازمان استاندارد بین المللی آمده است که فهرستی از ارزهای بین المللی شناخته شده را نگهداری می‌کند. "X" نیز نشان می دهد که ارز با کشور خاصی مرتبط نیست. بسیاری از برنامه‌های کاربردی فین تک بر روی دفتر کل توزیع شده بیت کوین ساخته شده اند، جایی که می‌توان سوابق تراکنش‌ها را به راحتی تأیید کرد.

اتریوم: اتریوم به عنوان یک پروتکل جایگزین برای بیت کوین ایجاد شد و امکان ساخت برنامه‌های غیرمتمرکز، نوشتن قراردادهای هوشمند و مدیریت دارایی های دیجیتال را فراهم می‌کند. اتریوم یک پلتفرم بلاکچین بدون مجوز و منبع باز است. کیت‌های پیاده‌سازی و توسعه قرارداد هوشمند آن محبوب‌ترین پلتفرم بلاکچین برای برنامه‌های غیرمتمرکز است. اتریوم دارای یک ارز دیجیتال بومی به نام اتر است که دارای سه هدف اصلی: تسویه تراکنش‌ها از طریق تبادل اتر و فعال کردن عملیات شبکه با استفاده از اتر به عنوان ارز برای پرداخت هزینه تراکنش و ذخیره ارزش است. اتریوم دارای بزرگترین اکوسیستم سازمانی در جهان است، با یک جامعه فنی فعال متشکل از بیش از ۳۰۰۰۰۰ توسعه دهنده و متخصص زیرساخت هماهنگ شده توسط اتحاد سازمانی اتریوم که به ترویج پذیرش اتریوم اختصاص دارد و شامل کشورهای جهان است. با این حال، اتریوم از نظر مقیاس‌پذیری، نوسانات قراردادهای هوشمند، فقدان یک سیاست پولی مشخص و برخی عدم اطمینان در قوانین کمیسیون بورس و اوراق بهادار دارای محدودیت‌هایی است. شتاب اجرای اتریوم برای خدمات مالی ناشی از قابلیت‌های

قرارداد هوشمند بلاکچین و مشارکت شدید آن در امور مالی غیرمتمرکز است. اتریوم ۱.۰ از اثبات کار به عنوان الگوریتم اجماع خود استفاده کرد که در نتیجه حدود ۴۰ تراکنش در ثانیه انجام شد. بعداً، اتریوم ۲.۰ جایگزین اثبات کار با اثبات سهام شد. اتریوم ۲.۰ اخیراً به پلتفرم ترجیحی فین‌تک تبدیل شده است زیرا می‌تواند تا ۳۰۰۰ تراکنش در ثانیه را انجام دهد که سریع‌تر و در عین حال کارآمدتر از بیت‌کوین یا اتریوم ۱.۰ است.

فابریک هایپرلجر: یک کنسرسیوم منبع باز است که تحت عنوان فاین لینوکس نگهداری می‌شود و دارای بیش از ۲۰۰ عضو از شرکت‌های مختلف جهانی، از جمله خدمات مالی، است که پذیرش بلاکچین را برای کاربردهای صنعتی نیز امکان پذیر می‌کند. فابریک هایپرلجر یک پلتفرم بلاکچین مجاز و خصوصی است که گره‌های شرکت کننده می‌توانند دارایی‌ها را انتقال دهند. تراکنش‌ها توسط کد زنجیره‌ای هدایت می‌شوند. کد زنجیره‌ای چیزی است که عملکرد یک قرارداد هوشمند را در چارچوب فابریک هایپرلجر اجرا می‌کند. اجرای کد زنجیره‌ای تعاملات بین گره‌ها و دفتر کل مشترک را ایجاد می‌کند. تمام گره‌های داخل شبکه باید هویت گره‌های دیگر را بدانند و حفظ کنند. زیرشبکه‌هایی در شبکه بزرگ‌تر فابریک هایپرلجر وجود دارند که کانال نامیده می‌شوند. کانال‌ها به زیر مجموعه خاصی از گره‌ها محدود می‌شوند. یک کانال می‌تواند دفتر کل خود را ایجاد کند که فقط رکوردی از تراکنش‌ها و دارایی‌های دیجیتال خود را حفظ می‌کند و تنها می‌تواند توسط گره‌های آن کانال قابل دسترسی یا مشاهده باشد. فابریک هایپرلجر از یک ماژول امنیتی سخت افزار پشتیبانی می‌کند که برای مدیریت و محافظت از کلیدهای دیجیتال و معماری مدولار آن که از اجزای پلاگین پشتیبانی می‌کند، حیاتی است.

متمرکز بر سازمان[۶]: متمرکز بر سازمان یک نسخه مجاز از بلاکچین اتریوم است. این توسط جی پی مورگان[7] توسعه داده شد و بعدا توسط کنسنسیس[۸] خریداری شد. از آنجایی که این یک بلاکچین مجاز است، گره‌ها باید قبل از ورود به شبکه متمرکز بر سازمانتأیید شوند. الگوریتم‌های اجماع مورد استفاده متمرکز بر سازمانبه جای اجرای PoW اتریوم ۱.۰ و بیت‌کوین، RAFT و IBFT هستند. حریم خصوصی در متمرکز بر سازمان حفظ می‌شود زیرا تراکنش‌ها برای اعضای شبکه بزرگتر قابل مشاهده نیستند. این شبیه به کانال‌های هایپرلجر است، که در آن برخی از تراکنش‌ها فقط برای گروه کوچک‌تری از گره‌های شبکه که در یک دفتر کوچک‌تر و خصوصی نگهداری می‌شوند قابل مشاهده است. متمرکز بر سازمان به عنوان یک شبکه گاز رایگان نامیده می‌شود، به این معنی که هیچ "هزینه استخراج" برای تراکنش‌ها وجود ندارد، و هیچ هزینه ارز دیجیتال مرتبط با تراکنش های آن وجود ندارد (یعنی گاز روی صفر تنظیم شده است).

فریم‌ورک کوردا ۳: این پلتفرم یک پروژه نرم‌افزاری خصوصی، دارای مجوز و منبع باز است که شبکه کوردا را ایجاد می کند. مزیت اصلی کوردا سهولت در مدیریت قراردادها و دستیابی به توافقات بین طرفین است، به خصوص زمانی که اعتماد کافی بین طرفین با استفاده از قراردادهای هوشمند وجود ندارد. برخلاف هایپرلجر یا اتریوم، برای دستیابی به اجماع، از ایده استخرهای اسناد رسمی استفاده می کند. جزئیات این روش اجماع را می‌توان در مقدمه کتاب سفید پلتفرم کوردا یافت. کوردا عمدتاً بر روی خدمات مالی برای ایجاد یک شبکه مستقل جهانی تمرکز می‌کند و بنابراین بسیاری از اجزای ساختار بلاکچین معمولی را که باعث زمان و سربار محاسباتی می‌شوند، حذف می‌کند. با این حال، عملکرد کامل پلتفرم بلاکچین کوردا را می‌توان با استفاده از اجزای ارائه شده توسط هایپرلجر به دست آورد. علاوه بر سرعت‌های عملیاتی سریع ارائه شده توسط کوردا، به شرکت‌های فین‌تک نیز کمک می‌کند تا هزینه‌ها و کارایی همکاری‌های بین شرکتی را بهینه کنند، جایی که داده‌ها را فقط می‌توان بین گره‌های مجاز به اشتراک گذاشت.

متمرکز بر سازمان سریعترین عملیات تراکنش را در مقایسه با سایر بلاکچین‌های پیاده‌سازی اصلی ارائه می دهد. با این حال، انعطاف‌پذیری کمتری دارد. اتریوم امنیت را با مقیاس‌پذیری محدود فراهم می‌کند و کارایی کمتری دارد (یعنی تراکنش‌های کم در ثانیه) و بنابراین در موقعیت‌های بحرانی زمانی کاربرد ندارد. فابریک هایپرلجر معاملات را بسیار سریعتر از اتریوم انجام می‌دهد. این مورد انتظار است زیرا دومی مبتنی بر یک بلاکچین بدون مجوز است.

[6] Quorum
[7] JP Morgan
[8] ConsenSys

کوردا۳ همچنین دارای نرخ تراکنش‌های بالاتری نسبت به اتریوم ۱.۰ است اما توان عملیاتی کمتری نسبت به فابریک هایپرلج دارد .همانطور که قبلا ذکر شد، یک فابریک هایپرلجر با اجزای"پلاگین و بازی[9]" خود می‌تواند ساخته شود تا عملکردی مشابه با پلتفرم کوردا داشته باشد. با این حال، بالاترین تراکنش توسط اتریوم ۲.۰ گزارش شده است. هنوز استانداردی در مورد معیارهای عملکرد بلاکچین وجود ندارد. آزمایش‌ها توسط منابع محدود می‌شوند و اغلب بر موارد استفاده خاص متمرکز هستند. بنابراین، این اندازه‌گیری ها لزوما دقیق نیستند[۱۵].

۱۰- لایه‌های بلاکچین

فناوری بلاکچین توسط استوارت‌هابر، دبلیو اسکات، استورنتتا و دیو بایر و ساتوشی ناکاموتو در سال ۲۰۰۸ اختراع شد تا به عنوان دفتر کل معاملات عمومی عمل کند. اصطلاح بلاکچین اولین بار به عنوان "زنجیره بلوک های امن رمزنگاری شده" توصیف شد. اصطلاح رمزنگاری به یک اصطلاح پرطرفدار در دانشگاه‌ها و صنعت تبدیل شده است. بیت‌کوین به محبوب‌ترین ارز دیجیتال تبدیل شده است که موفقیت چشمگیری کسب کرده است. همچنین به عنوان فناوری هسته‌ای شناخته می‌شود که برای ساخت بیت کوین استفاده می شود. اساساً، بلاکچین را می‌توان به عنوان یک رجیستری بانک داده توزیع شده که در میان گره‌های یک شبکه کامپیوتری ادغام شده است، توضیح داد. در سیستم بلاکچین اطلاعات ثبت می‌شود که هک یا اصلاح آن را دشوار می‌کند. سیستم بلاکچین از طریق گروهی از گره ها عمل می‌کند و هر گره از کپی دفتر کل دیجیتال تشکیل شده است. در هر تراکنش، تراکنش با احراز هویت توسط اکثر گره‌های شبکه به شبکه اضافه می‌شود. نام بلاکچین به این نام خوانده می‌شود، زیرا ساختار از زنجیره‌ای از بلوک‌ها تشکیل شده است که هر کدام زمانی که ظرفیت ذخیره‌سازی یک بلوک به دست می‌آید، بسته می‌شود و به بلوکی که قبل از آن آمده است متصل می‌شود و یک زنجیره داده به نام بلاکچین تولید می‌کند. بلاکچین به عنوان یک پایگاه داده، اطلاعات را با وسایل الکترونیکی در قالب دیجیتال ذخیره می‌کند. مفهوم بیت‌کوین را می‌توان معادل اینترنت دانست که فناوری‌ها و کاربردهای زیادی دارد. به گفته دیگران، بلاکچین مطمئناً تجارت را به روشی مشابه آنچه اینترنت انجام داد، تغییر خواهد داد. بلاکچین را می‌توان به عنوان داده‌های ساختار یافته تعریف کرد که نوعی پایگاه داده به اشتراک گذاشته شده است به نحوی که داده‌ها را ذخیره می‌کند. اطلاعات در قالب گروه-هایی به نام بلوک جمع‌آوری می‌شود و مجموعه اطلاعات را در خود نگهداری می‌کند. داده‌ها در بلوک‌هایی که از طریق رمزنگاری با هم متحد می‌شوند، ساختار یافته‌اند. در ساختار زنجیره‌ای هر بلوک جدید به بلوک قبلی مربوط می‌شود و اولین بلوک ساختار به نام بلوک پیدایش شناخته می‌شود. هنگامی که به صورت غیرمتمرکز استفاده می‌شود، این ساختار داده یک جدول زمانی از داده‌ها ایجاد می‌کند که قابل تغییر نیستند. هنگامی که بلاکچین پر می‌شود، ایجاد شده و در این جدول زمانی گنجانده می‌شود. چارچوب بلاکچین شامل ماژول‌های اساسی و تمام اجزای خاص است که توسط توسعه دهنده بر اساس آنها پیاده سازی شده است. چارچوب را می‌توان به لایه های مختلفی تقسیم کرد که در شکل ۳ نشان داده شده است[۱۶]:

شکل۳: نمایی از لایه های بلاکچین

لایه زیرساخت سخت‌افزاری: داده‌های بلاکچین به طور ایمن در سرور داده ذخیره می‌شود. هنگامی که هر کاربری در وب می‌گردد یا از هر برنامه بلاکچین استفاده می‌کند، ماشین کاربران درخواست دسترسی به داده‌ها را از سرور می‌کند. چارچوبی که این تبادل داده را تسریع می‌کند، به عنوان

[9] plug-n-play

معماری سرویس گیرنده-سرور شناخته می‌شود. به اشتراک-گذاری داده‌ها سریعتر است و با سهولت اتفاق می‌افتد زیرا بلاکچین شبکه های همتا هستند زیرا به مشتریان اجازه می‌دهد تا با "همسالان" ارتباط برقرار کنند. این مجموعه عظیمی از دستگاه‌هایی است که داده‌ها را از یکدیگر درخواست می‌کنند و با یکدیگر ارتباط برقرار می‌کنند. بنابراین، به این ترتیب یک دفتر کل توزیع شده ایجاد می‌شود. گره دستگاهی است که با دستگاه دیگری در شبکه ارتباط برقرار می‌کند. داده های تراکنش به طور تصادفی توسط هر گره تأیید می‌شود.

لایه شبکه: این لایه بلاکچین را قادر می‌سازد تا با کاربران و محیط اطراف ارتباط برقرار کند. این سیستم با پروتکل‌های IP و اتصال شبکه همتا به همتا غیرمتمرکز است. هر گره باید بتواند گره‌های دیگر را در شبکه برای ارتباط سریع کشف کند. ارتباط بین گره‌ای توسط لایه شبکه تسهیل می‌شود.

لایه داده‌ها: در این سطح ، داده‌ها و الگوریتم های مورد نیاز تعریف می‌شوند. یک بلاکچین از "بلوک" تشکیل شده است که حاوی داده های منتقل شده است. این بلوک‌های ساختمانی بلاکچین است که در این لایه ایجاد شده است. بلوک اول ، H یک "بلوک پیدایش" نیازی به بلوک قبلی ندارد. هر زمان که یک بلوک جدید اضافه شود، بلوک‌های بعدی به بلوک پیدایش مرتبط می‌شوند.

لایه اجماع: لایه مهمی از بلاکچین است. این لایه تراکنش‌ها را فعال می‌کند و بدون آن ممکن است کل سیستم کار نکند. یک تراکنش باید همان نتیجه را تولید کند که توسط چندین گره پردازش شده و اعتبار سنجی شود. این مکانیسم اجماع نامیده می‌شود.

لایه کاربردی: این لایه نشان دهنده برنامه‌های مختلفی است که از بلاکچین استفاده می‌کنند..

۱۱- برنامه‌های کاربردی بلاکچین

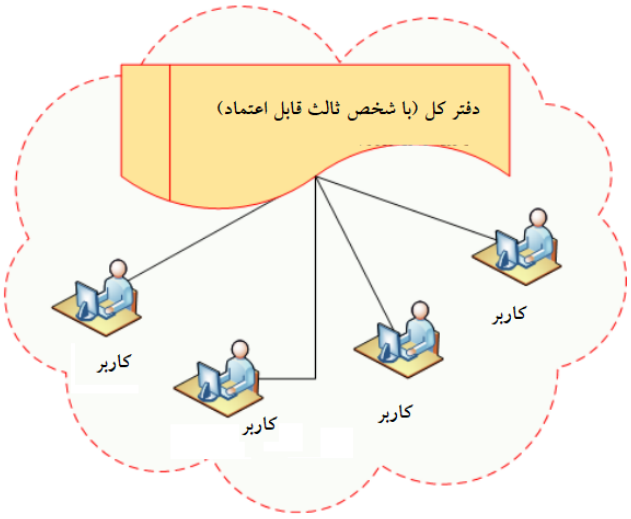
برنامه‌های کاربردی بلاکچین و ارز دیجیتال:

یکی از فعال‌ترین حوزه‌های بلاکچین در بخش مالی به ویژه در حوزه ارزهای دیجیتال است. از زمان ظهور اولین حامل بیت کوین در بلاکچین، ارزهای دیجیتال مختلفی ظهور کرده‌اند. از آنجایی که مکانیسم‌های ناشناس بودن، قابلیت تأیید، عدم تمرکز و اجماع بیت‌کوین مشخص است، ارزش بیت‌کوین اکنون به ۶۳۰۰ دلار در هر بیت‌کوین رسیده است. در همان زمان، برخی دیگر از ارزهای دیجیتال با ویژگی‌های بهبودیافته‌تر ظهور کرده‌اند و بازار پررونق ارزهای دیجیتال را تشکیل می‌دهند. در میان آنها، اتریوم یک پلتفرم بلاکچین عمومی ایجاد کرد که در آن قراردادهای هوشمند می‌توانند در سال ۲۰۱۵ مستقر شوند. با ظهور قراردادها، فناوری بلاکچین در طیف وسیع‌تری از سناریوهای تجاری از جمله پردازش قرارداد، تغییرات مالکیت، اینترنت اشیاء و اقتصاد اشتراکی استفاده می‌شود. بلاکچین علاوه بر استفاده در حوزه ارزهای دیجیتال، به طور فزاینده‌ای در خدمات مالی از جمله بورس اوراق بهادار، پرداخت های فرامرزی، قراردادهای خرید مجدد و هویت‌های دیجیتال مورد استفاده قرار می‌گیرد. با استفاده از ماهیت دفتر کل تراکنش‌های توزیع شده بلاکچین ، بانک انگلستان سانتاندر از فناوری ارائه شده توسط پروتکل پرداخت و شبکه مبادله مبتنی بر ریپل برای انتقال پرداخت ها در زمان واقعی از طریق یک برنامه تلفن همراه استفاده کرد. بورس اوراق بهادار استرالیا ادعا کرد که از فناوری بیت کوین برای جایگزینی سیستم تسویه فعلی با هدف کاهش هزینه‌های تراکنش و سریع‌تر و ایمن‌تر کردن تراکنش‌ها استفاده خواهد شد. اکسیژن یک شرکت تجاری مستقر در لندن، راه-اندازی پلتفرم بلاکچین خود را اعلام کرد. هنگامی که قرارداد بازخرید شروع می شود، بانک و وام گیرنده به ترتیب پول و وثیقه خود را به آدرس قرارداد هوشمند از پیش تعریف شده ارسال می‌کنند، که در گردش وثیقه قفل می‌شود، پول را به حساب وام گیرنده واریز می‌کند و به پیگیری همه تراکنش‌ها ادامه می‌دهد. گرایش به سمت تامین مالی الکترونیکی آن را برای بلاکچین طبیعی می‌کند و خرید مجدد را به یک اتاق تسویه خودکار تبدیل می‌کند. بسیاری از بانک‌ها نیز در سال‌های اخیر شروع به سرمایه‌گذاری روی بلاکچین کرده‌اند. بانک فیدور یک بانک آنلاین در آلمان و اولین بانک جریان اصلی است که ارز مجازی و بلاکچین را آزمایش کرده است. با همکاری یک صرافی بیت کوین کارکن که دفتر مرکزی آن در سانفرانسیسکو قرار دارد، مبادله یورو و بیت کوین در اکتبر ۲۰۱۳ راه اندازی شد. بانک فیدور با آزمایشگاه ریپل برای ارائه خدمات انتقال با نرخ پایین با استفاده از فناوری پرداخت طرف مقابل همکاری می‌کند. در فوریه ۲۰۱۵، این بانک با bitcoin.de همکاری کرد تا سرویس انتقال بیت‌کوین نظیر به نظیر را راه‌اندازی کند. سیتی بانک سه سیستم مستقل را بر اساس فناوری توزیع داخلی بلاکچین ساخته است. فناوری بلاکچین نیز یکی از پنج حوزه اصلی تمرکز است که سیتی گروپ در جولای ۲۰۱۵

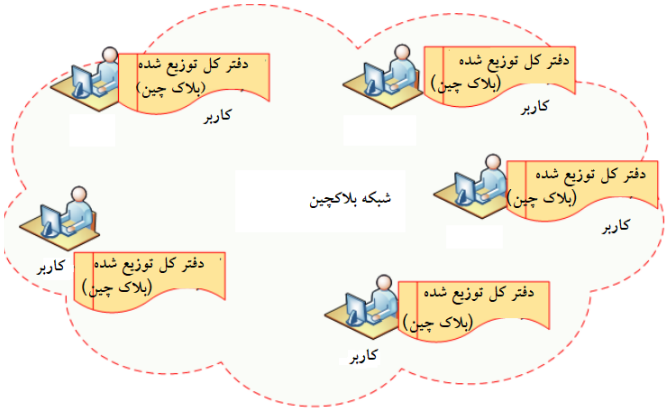
منتشر کرد. اگرچه مکانیسم اعتماد غیرمتمرکز فناوری بلاکچین می‌تواند مشکل تبادل ارزش را در مقیاس جهانی بهتر حل کند. با این حال، از عملیات واقعی فعلی، هنوز محدودیت‌هایی در جنبه‌های زیر وجود دارد. اولین مورد امنیت بلاکچین است. بلاکچین با تسهیلات مالی سنتی متفاوت است. تسهیلات مالی سنتی توسط یک سازمان کنترل می‌شود و امکانات نرم‌افزاری و سخت‌افزاری مرتبط در دسترس عموم نیست، اما بلاکچین یک برنامه باز است و کد سیستم بلاکچین بین شرکت کنندگان به اشتراک گذاشته می‌شود. در نتیجه، برنامه‌های مبتنی بر بلاکچین نسبت به امکانات مالی سنتی آسیب‌پذیرتر هستند. دوم حفاظت از حریم خصوصی بلاکچین است. در مدل کسب و کار مالی سنتی، داده‌ها در سرور مرکزی ذخیره می‌شوند و اپراتور سیستم از حریم خصوصی داده‌ها محافظت می‌کند. در برنامه‌های کاربردی مبتنی بر بلاکچین ، داده‌ها به صورت عمومی شفاف هستند و هر شرکت کننده می‌تواند یک نسخه پشتیبان کامل از داده‌ها دریافت کند. علیرغم وجود "شبه ناشناس" در بلاکچین ، برای موسسات مالی، در برخی از سناریوهای تجاری مالی که باید مخفی نگه داشته شوند، این مدل برای پاسخگویی به نیازهای خدمات مالی پیچیده بسیار ساده است[۱۷].

بلاکچین و بیت‌کوین: بیت کوین یکی از موضوعات پرطرفدار تحقیقات در سال‌های اخیر بوده است. یک کاربر ناشناس به نام ساتوشی ناکاتومو در سال ۲۰۰۸ مقاله ای با عنوان «بیت کوین: یک سیستم نقدی الکترونیکی همتا به همتا» در انجمن بنیاد P2P بارگذاری کرد. با افزایش علاقه به این فناوری، حجم مالی در حال چرخش روی بیت کوین توجه دانشگاهیان را به خود جلب کرد. در ابتدا مطالعاتی در مورد نحوه عملکرد فناوری بیت کوین و چارچوب آن انجام شد. زیسکیند و همکاران (۲۰۱۵) یکی از اولین مقالات دانشگاهی را در مورد سیستماتیک کاری بیت کوین در سال ۲۰۱۵ منتشر کرد، در حالی که ژنگ و همکاران(۲۰۱۸)، مطالعه جامع‌تری را توسعه داد. زیسکیند و همکاران (۲۰۱۵) مفهوم شبکه همتا به همتا بیت کوین و همچنین قابلیت اطمینان و حریم خصوصی را برجسته کردند، محققان اظهار داشتند که فناوری‌های ایجاد شده در بلاکچین مانند بیت کوین می‌تواند یک تغییر پارادایم در حریم خصوصی ایجاد کند و در مورد مزایای پلتفرم‌های غیرمتمرکز اشاره کرد. ژنگ و همکاران (۲۰۱۸) از سوی دیگر، رابطه بیت کوین با بازارهای سهام، به ویژه داو جونز را بررسی کرد. در آن سال‌ها، بیت کوین توانست با رسیدن به ارزش ۱۰ میلیارد دلاری در سال ۲۰۱۶ در مرکز توجه قرار گیرد و پتانسیل بیت کوین برای داشتن ارزش قابل توجهی از ارزهای ملی نیز موضوع تحقیق قرار گرفته است[۱۸].

در واقع امروزه، فناوری بلاکچین بسیار محبوب است. بلاکچین‌ها زنجیره‌ای از بلوک‌های اطلاعاتی هستند. گروهی از محققان برای اولین بار در سال ۱۹۹۱ در مورد این فناوری گزارش دادند. هدف اصلی این بود که تاریخ گذشته یا دستکاری در اسناد دیجیتالی ایجاد نشود، بلکه در عوض آنها را مهر زمانی می گذاشتند تا نتوان آنها را دستکاری کرد. ارز دیجیتالی مانند بیت کوین از فناوری بلاکچین به عنوان مکانیزم زیربنایی خود استفاده می کند. در دسامبر سال ۲۰۱۷، ارز دیجیتال بیت کوین با ارزش گذاری بی‌سابقه ای به اوج خود رسید و سر و صدایی در اطراف ارز دیجیتال ایجاد کرد. چندین ارز رمزنگاری شده از زمان شروع بیت کوین در بازار ظاهر شده‌اند که هر کدام دارای ارزش بازار میلیاردها دلار هستند. ساتوشی ناکاموتو، مفهوم بلاکچین را در سال ۲۰۰۸ معرفی کرد و از آن به عنوان مبنایی برای بیت کوین در سال ۲۰۰۹ استفاده کرد. هر کسی می‌تواند به یک بلاکچین دسترسی داشته باشد زیرا یک دفتر کل توزیع شده است. یکی از ویژگی‌های جالب بلاکچین این است که پس از وارد شدن، نمی‌توان آن‌ها را تغییر داد. یک بلوک بلاکچین شامل برخی داده‌ها، هش خود بلوک و هش بلوک قبل از آن است. انواع مختلفی از داده‌ها در هر بلوک ذخیره می‌شود. جایگزینی برای دفتر کل سنتی، بلاکچین اساسا یک "پایگاه داده توزیع شده" چند طرفه است که در آن همه تراکنش‌ها ثبت و قابل ردیابی هستند. اساساً، زنجیره‌ای از بلوک‌ها را می‌توان به عنوان یک دفتر کل در نظر گرفت که هر بلوک نشان دهنده یک صفحه است. ماینینگ به تولید بلوک‌های جدید ادامه می‌دهد که به طور مداوم به بلاکچین اضافه می‌شوند. همانطور که در شکل ۴ نشان داده شده است، یک شخص ثالث قابل اعتماد برای فناوری‌های دفتر کل سنتی مورد نیاز است. فناوری بلاکچین، همانطور که در شکل ۵ نشان داده شده است، در یک شبکه همتا به همتا عمل می‌کند، به این معنی که تراکنش‌ها توسط شخص ثالث قابل اعتماد مدیریت نمی‌شوند[۱۹].



شکل ۴: فناوری دفتر مرکزی متمرکز سنتی با شخص ثالث قابل اعتماد



شکل۵: فناوری دفترکل توزیع شده بدون شخص ثالث قابل اعتماد.

دامنه‌های مختلف دیگر ویژگی‌های فناوری بلاکچین که برای بهبود استانداردهای برنامه‌ها تطبیق داده شده اند به طور خلاصه بخش‌های جهانی مانند سازمان‌های اینترنتی، خدمات بانکی، صنایع اتوماسیون و حتی بخش‌های دولتی ویژگی‌های بلاکچین را برای افزایش مهارت، بهبود امنیت و مقیاس‌پذیری سازمان‌های خود در نظر می‌گیرند[۲۰].

- اولین کاربرد بلاکچین ، ارز دیجیتال با بلاکچین است که یکی از برنامه‌های محبوب است. بنابراین، ارزهای دیجیتال در حال معرفی هستند.
- تحقیقات قابل توجهی در مورد برنامه های کاربردی مراقبت‌های بهداشتی مبتنی بر بلاکچین و شهرهای هوشمند در حال انجام است.
- بیشترین استفاده از بلاکچین در بخش مالی انجام می‌شود، جایی که بلاکچین برای حفظ سابقه تراکنش اقتصادی استفاده می‌شود که به طور غیرمستقیم سطح فساد را کاهش می‌دهد.
- مدیریت انرژی نیز با کمک بلاکچین ساخته شده است. توسعه بلاکچین به اجرای مراحل نت اشیاء محلی انرژی می‌دهد.
- با استفاده از بلاکچین فقط رأی دهندگان واجد شرایط می‌توانند رأی دهند، رأی‌ها دستکاری نمی‌شوند، هیچ کس دو بار رأی نمی‌دهد. این می‌تواند دسترسی را افزایش دهد تا فرآیند رای گیری به آسانی فشار دادن چند کلید روی تلفن همراه آسان شود.
- این فناوری همچنین در صنعت پزشکی برای تکمیل تاریخچه پزشکی هر بیمار استفاده می‌شود و روشی مطمئن برای ثبت و پیگیری تاریخچه پزشکی کامل هر بیمار ارائه می‌دهد.

هنگامی که یک سیستم پیچیده رفتار نامناسبی دارد، درک انتساب هر جزء از طریق مدیریت زنجیره تامین، از جمله سازنده، تاریخ تولید، دسته و حتی برنامه ماشین تولید بسیار مهم است[۲۰].

۱۲- توکن‌سازی برای بلاکچین

توکن معمولاً نمایش دیجیتالی از دارایی موجود در دنیای فیزیکی یا مجازی است. در حوزه بلاکچین، یک توکن می‌تواند برای نشان دادن برخی از ارزهای دیجیتال مانند بیت‌کوین یا اتر استفاده شود. از نظر فنی، یک توکن توسط یک الگوریتم تعریف شده در یک قرارداد هوشمند بر روی یک زنجیره بلوکی پیاده سازی می‌شود و قراردادهای هوشمند اساساً برنامه‌های رایانه‌ای هستند که با اجرای خودکار مجموعه‌ای از شرایط از پیش تعریف‌شده به شیوه‌ای قابل ردیابی و برگشت‌ناپذیر بدون دخالت شخص ثالث، یک قرارداد را تأیید یا اجرا می‌کنند. خروجی یک قرارداد هوشمند را می‌توان به معنای واقعی کلمه یک توکن در نظر گرفت. به عنوان مثال، پلتفرم اتریوم می‌تواند برای ایجاد قراردادهای هوشمند دلخواه مورد استفاده قرار گیرد، که توکن‌های آن (با نام مستعار، توکن های اتریوم) می‌توانند برای نشان دادن دارایی‌های دیجیتال مختلف مورد استفاده قرار گیرند. این توکن‌ها می‌توانند هر چیزی را هم از اشیاء فیزیکی و هم از اشیای مجازی نشان دهند. آنها می‌توانند از آنها برای اهداف مختلفی به عنوان مثال، ثبت اطلاعات داده‌های تراکنش یا پرداخت هزینه برای دسترسی به یک شبکه

استفاده کنند. فرآیند نگاشت بین توکن و دارایی نماینده آن در ابتدا کاملاً ساختگی است. توکن حاوی مدل دارایی است که توسط یک قرارداد هوشمند برای تضمین منحصر به فرد بودن داده ها تأیید شده است. به طور کلی، توکن‌ها به سیستم‌عامل‌ها وابسته نیستند و شامل محتوای فیزیکی درون آن نمی‌شوند و از طریق قرارداد هوشمند، به راحتی می‌توان اعتبار یک توکن را تأیید کرد[۲۱].

توکن‌سازی فرآیند تبدیل داده‌ها/دارایی‌ها به یک توالی دیجیتالی تصادفی از کاراکترها (معروف به یک نشانه) است. فرآیند نمایش دارایی‌های فیزیکی/مجازی را ساده می‌کند و از داده‌های حساس محافظت می‌کند، به عنوان مثال، با جایگزین کردن داده‌های غیرحساس در یک توکن. توکن صرفاً به عنوان یک مرجع به داده‌ها یا دارایی‌های اصلی برای برنامه‌های بلاکچین عمل می‌کند، اما نمی‌توان از آن برای تعیین این مقادیر استفاده کرد. یک توکن به خودی خود حاوی برخی از اطلاعات ارزش اقتصادی در آن نیست و ارزش پولی یک توکن معمولاً توسط بازار تعیین می‌شود. تا زمانی که توسط قرارداد هوشمند اعتبار سنجی شود، توکن می‌تواند در برنامه‌های کاربردی متعددی استفاده شود یا در بازار مورد معامله قرار گیرد. به عنوان مثال، توکن‌سازی اکثر واسطه‌های مالی، قانونی و نظارتی را حذف می‌کند و در نتیجه هزینه‌های تراکنش به میزان قابل توجهی کاهش می‌یابد. با این حال، فرآیند توکن‌سازی در بلاکچین هنوز در مراحل اولیه خود است و چالش‌ها و خطرات زیادی برای غلبه بر آن وجود دارد. از جمله چالش‌های نظارتی و فنی، برای تحقق کامل پتانسیل توکن‌سازی در بلاکچین وجود دارد. برای مثال، فقدان شفافیت نظارتی برای دارایی‌های توکن‌شده به یک مانع مهم برای اجرای گسترده‌تر تبدیل می‌شود و از منظر فنی، راه مطمئنی برای اطمینان از سازگاری بین دارایی‌های زنجیره‌ای و دارایی‌های خارج از زنجیره وجود ندارد. در این بخش، بر نمایش دارایی‌های خارج از زنجیره فیزیکی/مجازی و دارایی‌های دیجیتال روی زنجیره از ویژگی‌های تعویض‌پذیری تمرکز می‌شود. به طور خاص، تقریباً توکن‌ها را به سه دسته تقسیم می‌کنیم: توکن‌های قابل تعویض (FT[10])، توکن‌های غیرقابل تعویض (NFT[11]) و توکن‌های نیمه قابل تعویض(SFT[12])[۲۱].

۱-۱۲ طبقه‌بندی در توکن‌های بلاکچین

در فرآیند توکن‌سازی برای بلاکچین، در واقع انواع بسیاری از توکن‌ها برای کاربردهای مختلف وجود دارد. به جای بحث در مورد این توکن‌های مبتنی بر کاربرد خاص، با توجه به قابلیت تعویض دارایی‌ها در بلاکچین ، تقریباً آنها با توجه که در بالا گفتیم به سه توکن معروف طبقه‌بندی می‌شود: توکن‌های قابل تعویض، توکن‌های غیرقابل تعویض و توکن‌های نیمه قابل تعویض[۲۱].

در حوزه بلاکچین ، توکن‌ها می‌توانند برای نشان دادن دارایی‌های دیجیتال استفاده شوند. با این حال، مفهوم توکن منحصر به بلاکچین نیست. از لحاظ تاریخی، توکن‌ها برای ایمن کردن تراکنش‌های دیجیتالی، به عنوان مثال، تراکنش‌های بانکی استفاده می‌شدند. امروزه، توکن‌ها به عنوان یکی از کاربردهای حیاتی فناوری بلاکچین در نظر گرفته می‌شوند و توکن‌ها به‌عنوان «مرکزی برای اکثر نوآوری‌های اجتماعی و اقتصادی توسعه‌یافته با فناوری بلاکچین» توصیف می‌شوند. از دیدگاه فنی، توکن‌ها بخشی از اطلاعات دیجیتال هستند . به‌عنوان مثال، خطوط کد رایانه‌ای، که جزئیات نشان‌دهنده توکن را نشان می‌دهد. در حالی که، از منظر قانونی، توکن‌ها می‌توانند دارایی‌های دیجیتالی را نشان دهند که می‌توانند تقریباً هر مقداری را که روی آن توافق شده و توسط پروتکل‌های رمزنگاری ایمن شده است، به عنوان مثال، ارزهای رمزنگاری شده، مشخص کنند و همچنین، برخی از حقوق، مانند حقوق دسترسی، می‌توانند به صورت توکن نشان داده شوند و دارایی‌ها هم از دنیای واقعی (مانند املاک و مستغلات، کالاهای جمع‌آوری‌شده، کالاها و حتی سهام شرکت) و هم از دنیای مجازی (به عنوان مثال، رمزارزها (ارزها، بلیط های بخت آزمایی، یا حتی مهارت های شخصیت در بازی های آنلاین) همگی می‌توانند برای پردازش بیشتر توکن شوند.

در واقع NFTها نوعی از ارزهای دیجیتال هستند که از طریق قراردادهای هوشمند به وجود آمده اند. برای کارکرد-NFTها به قراردادهای هوشمند نیاز است. قرارداد هوشمند یک برنامه کامپیوتری است که حاوی کدهایی است که توسط ماشین قابل خواندن است. هنگامی که یک قرارداد هوشمند ایجاد شد، می‌توان آن را به صورت مستقل اجرا کرد و دیگر

[10] fungible tokens
[11] non-fungible tokens
[12] semi-fungible tokens

نیازی به نظارت ندارد. قرارداد هوشمند را می‌توان به عنوان یک قرارداد دیجیتالی توصیف کرد که ضد دستکاری است. کد قرارداد هوشمند شامل شرایط انجام معامله است. در مقایسه با ارز دیجیتال کلاسیک، یک NFT نشان دهنده مالکیت یک آیتم دیجیتال یا فیزیکی منحصر به فرد است. به همین دلیل NFT ها را می‌توان به وضوح از یکدیگر متمایز کرد. با توجه به[۲۲]، یک NFT یک رمز رمزنگاری منحصر به فرد، جدایی ناپذیر، غیرقابل جایگزین و قابل تأیید است که یک آیتم خاص را، چه به صورت دیجیتالی یا فیزیکی، در یک بلاکچین نشان می‌دهد. یکی دیگر از دلایل ظهور NFTها، توسعه دهنده سیستم بلاکچین اتریوم، ویتالیک بوترین، بود که می‌خواست از مفهوم بلاکچین برای چیزی بیش از پول استفاده کند[۲۳].

توکن‌های قابل تعویض: قابلیت تعویض یک توکن به این واقعیت اشاره دارد که توکن دارای محتوای یکسان یا مشابه در مقایسه با سایر توکن‌های قابل تعویض است. بنابراین، توکن‌های قابل تعویض با دارایی دیگری از همان دسته، قابل تعویض/جایگزین شدن یا برابر هستند. به عنوان مثال، یک توکن قابل تعویض را می‌توان به آسانی با دارایی‌های دیگر با همان ارزش وام داده شده یا معادل آن که ممکن است تقسیم یا مبادله شود جایگزین کرد. آنها با یکدیگر یکسان هستند و می‌توانند به واحدهای کوچکتر تقسیم شوند که بر مقادیر آنها تأثیر نمی-گذارد. علاوه بر این، توکن‌های قابل تعویض معمولا منحصر به فرد نیستند. به عنوان مثال، یک توکن پرداخت همیشه قابل تعویض است، که قابل تعویض، تقسیم پذیر و ماهیت منحصر به فرد نیست. همانطور که گلاتز بیان کرد، "از دیدگاه فنی، یک توکن قابل تعویض به عنوان لیستی از آدرس‌های بلاکچین (حساب های کاربر) که دارای تعدادی (مقدار) مرتبط با آنها هستند، همراه با (۱) مجموعه‌ای از روش‌های مورد استفاده پیاده‌سازی می‌شود. برای دستکاری آن لیست، مانند «انتقال توکن‌های n از آدرس a به آدرس b » ، و (۲) قوانین برای تعیین اینکه چه کسی می‌تواند آن فهرست را به چه طریقی دستکاری کند. نمونه‌ای از توکن‌های قابل تعویض است. این مشخصاتی است که توسط جامعه اتریوم (جامعه‌ای که ERC ها را تأیید می‌کند) ایجاد شده است که عملکردهای اساسی خاصی را مشخص می‌کند و معیارهایی را برای یک توکن برای مطابقت با عملکرد صحیح در بلاکچین‌های اتریوم ارائه می‌دهد. توکن ERC-20توکنی است که از دستورالعمل‌های ERC-20 پیروی می‌کند. آنها دارای برخی ویژگی‌های ذاتی هستند که یک توکن را از نظر نوع و ارزش با توکن دیگر یکسان می‌کند. برای مثال، یک توکن ERC-20 به طور مشابه عمل می کند. به ETH در بلاکچین اتریوم، در آن یک توکن همیشه ارزشی برابر با تمام توکن‌های دیگر دارد. علاوه بر این، استاندارد ERC-20 یک رابط مشترک برای توکن‌های قابل تعویض مشخص می‌کند که قابل تقسیم هستند و قابل تشخیص نیستند، که بیشتر قابلیت همکاری را در میان جامعه بلاکچین اتریوم تضمین می‌کند. با این حال، استفاده از نوع توکن ERC-20 در سایر سناریوهای بلاکچین هنوز راه زیادی در پیش دارد. یکی از محدودیت‌های توکن‌های قابل تعویض این است که بسیاری از دارایی‌های ارزشمند مانند آثار هنری، املاک و مستغلات را نمی‌توان به طور مؤثری تقسیم کرد و از ماهیت این دارایی‌ها جدا کرد. و این دارایی‌ها معمولا دارایی‌های منحصربه‌فردی هستند که برای پیگیری مالکیت مورد نیاز هستند، که برای نشان دادن به توکن‌های غیرقابل تعویض نیاز دارند[۲۱].

توکن‌های غیر قابل تعویض: توکن غیر قابل تعویض یک توکن رمزنگاری منحصر به فرد و غیرقابل تکرار است که می‌تواند برای پیگیری مالکیت دارایی‌های فردی مورد استفاده قرار گیرد. توکن‌های غیرقابل تعویض از لحاظ قابلیت تعویض، یکنواختی و تقسیم‌پذیری از قابل تعویض‌پذیری به توکن‌های دیگر متفاوت هستند. یک توکن غیر قابل تعویض را نمی‌توان در طبیعت تقسیم کرد، که در آن هر یک حاوی اطلاعات و ویژگی‌های متمایز است تا خود را از دیگران به طور منحصر به فرد شناسایی کند. این ویژگی باعث می‌شود که NFTها با یکدیگر مبادله نشوند. به طور کلی، هر توکن غیر قابل تعویض منحصر به فرد است و با دیگران متفاوت است. استاندارد-ERC 20چارچوب تکنولوژیکی و بهترین شیوه‌ها را برای ایجاد توکن قابل تعویض تحت بلاکچین‌های اتریوم ارائه می‌کند. به طور مشابه، استاندارد ERC-721 همین کار را برای توکن‌های غیرقابل تعویض انجام داد، که به توسعه‌دهندگان اجازه می‌دهد یک نمایش دارایی دیجیتالی ایجاد کنند که می‌تواند در زنجیره بلوکی مبادله و ردیابی شود. ایجاد این استاندارد جدید به دلیل این واقعیت است که تفاوت قابل توجهی بین توکن‌های قابل تعویض و غیرقابل تعویض در طبیعت وجود دارد. به عنوان مثال، مفهوم قابل تعویض معمولاً ظرفیت هر قطعه از یک کالا را برای مبادله با قطعات دیگر کالای مشابه توصیف می‌کند. به عنوان

مثال، دو فرد می‌توانند مقدار یکسانی از دارایی‌ها را بدون هیچ سود یا ضرری مبادله کنند، و حتی اگر این دارایی‌ها به اشکال مختلف باشند، ارزش‌ها باید یکسان باشد. در حالی که غیر قابل تعویض بودن مخالف است زیرا هر نشانه منحصر به فرد است و نمی‌توان آن را به قطعات کوچک تقسیم کرد یا با قطعات دیگر در یک قطعه بزرگ ادغام کرد. به عنوان مثال، ERC-721 جریمه می‌کند که هر توکن NFT باید یک شناسه منحصر به فرد جهانی داشته باشد، که مالکیت آن می‌تواند با کمک ابرداده شناسایی و منتقل شود. به طور کلی، استاندارد ERC-721 رابطی را مشخص می‌کند که هر قرارداد هوشمند روی اتریوم که می‌خواهد توکن‌های ERC-721 ایجاد کند، باید آن را پیاده‌سازی کند[۲۱].

علاوه برNFT ها، ارزهای رمزنگاری شده در بلاکچین وجود دارد که می‌توان آن‌ها را به عنوان ارزهای دیجیتالی که بدون واسطه قابل انتقال هستند، درک کرد. در حالی که ارزهای رمزپایه که توکن‌های قابل تعویض نیز نامیده می‌شوند، بر اساس استاندارد ERC-20 عمل می‌کنند، توکن‌های غیرقابل تعویض براساس استاندارد ERC-721 عمل می‌کنند. این چارچوب فن‌آوری و بهترین روش‌ها برای ایجاد توکن‌ها است. این استانداردها به توسعه دهندگان تضمین می‌کنند که NFT ها می‌توانند به طور دائم در حال کار باشند[۲۴]. معرفی یک استاندارد توکن جدید ضروری بود زیرا تفاوت‌های عمده ای بین این دو استاندارد وجود دارد .توکن های ERC-20 را می‌توان به قطعات کوچک تقسیم کرد و همچنین بین دو فرد بدون ضرر یا سود مبادله کرد. رمز ERC-20 را می‌توان به عنوان اسکناسی در نظر گرفت که می‌تواند با هر اسکناس دیگری با همان ارزش مبادله شود. در مقابل، توکن‌های ERC-721 فردی هستند و نمی‌توانند با سایر توکن‌ها به اشتراک گذاشته یا ترکیب شوند. در ابتدا، NFTها بر روی بلاکچین اتریوم ایجاد شدند، اما سیستم های بلاکچین بیشتر و بیشتر از استاندارد NFT خود استفاده می‌کنند. سومین استاندارد، توکن‌های نیمه قابل تعویض است که دارای ویژگی‌های ژتون‌های تعویض‌پذیر و غیرقابل تعویض هستند. از جمله این موارد می توان به بلیط هواپیما یا بلیط سینما اشاره کرد. شکل ۶ تفاوت بین توکن‌ها را نشان می‌دهد[۲۳].

شکل۶: نمایی از توکن های مختلف[۲۳].

یکی از کاربردهای نمونه NFT ها بازی Axie Infinity است. در این بازی NFT ها نشان دهنده موجودات کلکسیونی دیجیتال هستند. هدف بازی جمع آوری آواتارهای دیجیتال و استفاده از آنها در مبارزات و فعالیت‌های دیگر است. هر NFT در این بازی نشان دهنده یک دارایی دیجیتال منحصر به فرد است که در بلاکچین ذخیره و غیرمتمرکز شده است. یک ست شروع بازی حدود ۳۰۰ دلار قیمت دارد. هر بار که Axie اینفینیتی NFT در بازار فروخته می‌شود، توسعه دهنده هزینه ای دریافت می‌کند که منبع درآمد است[۲۳].

توکن‌های نیمه قابل تعویض: استانداردهای توکن‌های دارایی‌های قابل تعویض و غیرقابل تعویض معمولاً برای هر نوع توکن قراردادهای متمایز دارند، که ممکن است برخی از بایت کدهای اضافی را روی بلاکچین قرار دهد و عملکرد خاصی را به دلیل ماهیت جداسازی هر قرارداد توکن محدود کند. توکن‌های نیمه قابل تعویض، دسته جدیدی از توکن‌ها هستند که هم ویژگی‌های توکن‌های تعویض‌پذیر و هم توکن‌های غیرقابل تعویض را دارند. آنها رابط های انعطاف پذیرتری برای نمایش برخی دارایی ها یا فرآیندهای پیچیده ارائه می دهند. در ادبیات، ERC-721 تنها استاندارد نشانه‌ای نیست که برای NFT ها وجود دارد. استاندارد اتریوم ERC-1155 (استاندارد چند توکن) یکی دیگر از انواع قابل‌توجه اتریوم است که گزینه‌های «نیمه تعویض‌پذیر» و پتانسیل نمایش دارایی‌های قابل تعویض و غیرقابل تعویض را ارائه می‌دهد. این یک رابط برای نشان دادن در NFT به عنوان مثال، یک توکن ERC-1155 عملکرد شناسایی توکن با نام مستعار (شناسه توکن) را گسترش می‌دهد، که می‌تواند انواع توکن‌های قابل تنظیم را ارائه دهد. این نوع توکن ممکن است حاوی اطلاعات سفارشی‌شده باشد، به‌عنوان مثال، ابرداده، اطلاعات مهر زمانی، عرضه، و سایر ویژگی‌ها. به طور کلی، توکن ERC-1155 یک استاندارد پیشنهادی جدید برای ایجاد توکن‌های قابل تعویض و غیرقابل تعویض در یک قرارداد است. در حال حاضر، نه اطلاعات زیادی در مورد

استاندارد توکن‌های ERC-1155 وجود دارد و نه اطلاعات زیادی در مورد توکن‌های نیمه تعویض‌پذیر. به طور کلی، توکن‌های نیمه قابل تعویض می‌توانند ویژگی‌های دارایی‌های قابل تعویض و غیرقابل تعویض را نگه دارند و نشان دهند. بنابراین، توکن‌های نیمه قابل تعویض ممکن است برای ایجاد و بسته‌بندی کنش‌های ترانس توکن (بدون آن) کارآمدتر باشند. نیاز به یک قرارداد توکن منحصر به فرد دستوری برای هر توکن ایجاد شده (به عنوان مثال، توکن ERC-1155 سطحی از انعطاف پذیری را نسبت به توکن ERC-721 ارائه می دهد)، به عنوان مثال، ایجاد توکن‌های انعطاف‌پذیر، قابل تنظیم مجدد یا قابل تعویض با ویژگی‌های غیر قابل تعویض. بر این اساس، ساختارهای توکن و رابط‌های SFT ها نیز پیچیده‌تر خواهند بود[۲۱].

۱۲- نتیجه‌گیری

بلاکچین یک پایگاه داده دفتر کل توزیع شده است که شامل سوابق یا تراکنش‌ها یا حوادث دیجیتالی مختلفی است که توسط شرکت کنندگان اجرا می‌شود. برخی از مقالات برای توضیح در مورد فناوری بلاکچین و نحوه عملکرد آن در گذشته اخیر منتشر شده است. ارزهای رمزنگاری شده یکی از محبوب-ترین نمونه‌های فناوری بلاکچین هستند که بیت کوین نیز نامیده شده است. جدای از این ارزهای دیجیتال، پیامدهای انسانی این بلاکچین مانند زنجیره تامین، خدمات مالی و ساخت نیز وجود دارد. در واقع فنآوری بلاکچین یک سیستم ایجاد پایگاه داده غیرقابل تغییر، امن و توزیع‌شده از معاملات است. بلاکچین در ابتدا برای ایجاد یک فهرست توزیع شده از معاملات مالی که بر بانک مرکزی، شرکت اعتباری و یا سایر مؤسسات مالی متکی نبودند، ایجاد شد و این فنّاوری از طریق انجام معاملاتی درزمینه‌ی مسائل حقوقی، پرونده پزشکی، صورتحساب بیمه و قراردادهای هوشمند توسعه داده شده است. فنّاوری بلاکچین می‌تواند مدیریت زنجیره تأمین را در تعدادی از راهها ازجمله: از بین بردن تقلب و اشتباهات، کاهش تأخیر کاغذبازی، بهبود مدیریت موجودی، شناسایی سریعتر موارد، کم کردن هزینه‌های پیک و افزایش اعتماد مصرف کننده و شریک بهبود بخشد. در این مقاله نیز مفاهیم پایه‌ای، خدمات عمومی، طبقه‌بندی پلتفرم‌های بلاکچین و طبقه‌بندی توکن‌های بلاکچین (توکن‌های قابل تعویض، توکن‌های غیر قابل تعویض و توکن‌های نیمه قابل تعویض) در این مقاله بررسی شد امید است این مرور برای علاقه‌مندان به این موضوع در کاربردهای مختلف تحقیقاتی مناسب باشد.

۱۳- منابع

1. *Gamage, H., H. Weerasinghe, and N. Dias, A survey on blockchain technology concepts, applications, and issues. SN Computer Science, 2020. 1(2): p. 1-15.*
2. *Pal, A., C.K. Tiwari, and N. Haldar, Blockchain for business management: Applications, challenges and potentials. The Journal of High Technology Management Research, 2021. 32(2): p. 100414.*
3. *Guo, H. and X. Yu, A Survey on Blockchain Technology and its security. Blockchain: Research and Applications, 2022. 3(2): p. 100067.*
4. *Mansour, M., et al., A Survey on Blockchain in E-Government Services: Status and Challenges. arXiv preprint arXiv:2402.02483, 2024.*
5. *Patil, P., M. Sangeetha, and V. Bhaskar, Blockchain for IoT access control, security and privacy: a review. Wireless Personal Communications, 2021. 117(3): p. 1815-1834.*
6. *Liu, J. and J. Wu, A Comprehensive Survey on Blockchain Technology and Its Applications. Highlights in Science, Engineering and Technology, 2024. 85: p. 128-138.*
7. *Li, L., J. Wu, and W. Cui, A review of blockchain cross-chain technology. IET Blockchain, 2023. 3(3): p. 149-158.*
8. *Habib, G., et al., Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 2022. 14(11): p. 341.*
9. *Zheng, Z., et al. An overview of blockchain technology: Architecture, consensus, and future trends. in 2017 IEEE international congress on big data (BigData congress). 2017. Ieee.*
10. *Krichen, M., et al., Blockchain for modern applications: A survey. Sensors, 2022. 22(14): p. 5274.*
11. *Askar, S., I.S. Abdulkhaleq, and S.W. Kareem, Blockchain systems: analysis, applications, & risks. International Journal of Science and Business, 2021. 5(6): p. 163-173.*
12. *Miraj, J., I. SAMI, and M.G. Abbas, Blockchain Technology: A Research Review. Harf-o-Sukhan, 2023. 7(3): p. 642-660.*
13. *Joshi, S., et al., Adoption of Blockchain Technology for Privacy and Security in the*

Context of Industry 4.0. Wireless Communications and Mobile Computing, 2022. 2022.

14. *Chetanpal Singh, R.T., and Jatinder Warraich, Blockchain in Supply Chain Management. DOI: http://dx.doi.org/10.24018/ejeng.2022.7.5.2888 Vol 7 | Issue 5 | October 2022, 2022.*
15. *Renduchintala, T., et al., A survey of blockchain applications in the fintech sector. Journal of Open Innovation: Technology, Market, and Complexity, 2022. 8(4): p. 185.*
16. *Tanvee Bandekar, D.A.A., Snehal Kulkarni, BLOCKCHAIN TECHNOLOGY: OVERVIEW AND APPLICATIONS. International Research Journal of Modernization in Engineering Technology and Science (Peer-Reviewed, Open Access, Fully Refereed International Journal), 2022.*
17. *Chen, W., et al. A survey of blockchain applications in different domains. in Proceedings of the 2018 International Conference on Blockchain Technology and Application. 2018.*
18. *KILIÇASLAN, F. and H. EKİZLER, FACTORS EFFECTING PURCHASE INTENTION IN BLOCKCHAIN AND NFT (NON-FUNGIBLE TOKEN) TECHNOLOGIES. Journal of Research in Business, 2022. 7(2): p. 604-623.*
19. *Vaigandla, K.K., et al., Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications. Mesopotamian Journal of CyberSecurity, 2023. 2023: p. 73-85.*
20. *Dong, S., et al., Blockchain technology and application: an overview. PeerJ Computer Science, 2023. 9: p. e1705.*
21. *Wang, G. and M. Nixon. SoK: Tokenization on blockchain. in Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion. 2021.*
22. *Valeonti, F., et al., Crypto collectibles, museum funding and OpenGLAM: challenges, opportunities and the potential of Non-Fungible Tokens (NFTs). Applied Sciences, 2021. 11(21): p. 9931.*
23. *Gonserkewitz, P., E. Karger, and M. Jagals, NON-FUNGIBLE TOKENS: USE CASES OF NFTS AND FUTURE RESEARCH AGENDA. Risk Governance & Control: Financial Markets & Institutions, 2022. 12(3).*
24. *Ali, M. and S. Bagui, Introduction to NFTs: the future of digital collectibles. International Journal of Advanced Computer Science and Applications, 2021. 12(10): p. 50-56.*

سمیه کدخدا ده خانی، فارغ التحصیل مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز دانشگاه پیام‌نور قشم می باشد، او به عنوان کارشناس فناوری در دانشگاه پیام‌نور استان کرمان مشغول به کار می‌باشد و نشانه رایانامه ایشان:

Emailsk65@gmail.com

حمید زنگی آبادی زاده، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان:

Hamid.zangiabadi@gmail.com

مهدی قاسمی، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان:

Mahdikmg1@gmail.com

مائده رحمانی، دانشجوی کارشناسی ارشد مهندسی کامپیوتر گرایش نرم افزار، دانشگاه پیام نور مرکز بین الملل کیش می باشد و نشانه رایانامه ایشان:

Maede9708@gmail.com

فرشید وظیفه دوست، فارغ التحصیل در مقطع کارشناسی ارشد رشته مهندسی کامپیوتر گرایش هوش مصنوعی و رباتیکز از دانشگاه پیام نور مرکز بین الملل قشم می باشد و نشانه رایانامه ایشان:

Vazifehdoostfarshid@gmail.com

س. کدخدا ده خانی، ح. زنگی آبادی زاده، م. قاســـمی، م. رحمانی و ف. وظیفه دوســـت. فناوری بلاکچین: مروری بر مفاهیم، چالش‌های بلاک‌چین در خدمات عمومی و طبقه‌بندی توکن‌های بلاکچین. دو فصلنامه محاسبات و سامانه‌های توزیع شده، سال ششم، شماره ۱، شماره پیاپی ۱۱، صفحه ۱۱۸ تا ۱۳۶، سال ۱۴۰۲

How to cite: S.kadkhodadehkhani, H.Zangiabadi Zadeh ،M.Ghasemi ،F.Vazifehdoost ،M.Rahmani. Blockchain Technology: A Review of Concepts, Blockchain Challenges in Public Services, and Blockchain Token Classification, Journal of Distributed Computing and Systems (JDCS), Vol 6, Issue 1, Page 118-136, 2023.

Blockchain Technology: A Review of Concepts, Blockchain Challenges in Public Services, and Blockchain Token Classification

S.kadkhodadehkhani[4], H.Zangiabadi Zadeh[1] ،M.Ghasemi[3] M.Rahmani[5] ،F.Vazifehdoost[5]
[1] Payam Noor University, Qeshm International Center.
[2] Payam Noor University, Kish International Center.
[3] Payam Noor University, Kish International Center.
[4] Payam Noor University, Kish.
[5] Payam Noor University, Qeshm International Center.

Abstract

Blockchain is based on a decentralized, immutable database that simplifies the recording of assets and tracking of transactions across a corporate network. An asset may be tangible or intangible. On a blockchain network, almost anything of value may be stored and exchanged, which reduces risk and improves efficiency for all users. In general, a blockchain is a digital ledger of transactions that are being recorded. It is decentralized and not controlled by any one person, group, or company. As a structured technology, it is very difficult to change a blockchain without the approval of the people who use it. Blockchain stores data as a decentralized ledger. Participants in the network can read, write, and verify transactions. Transactions cannot be changed or deleted. To support and secure the blockchain system, digital signatures, hash functions, and other cryptographic functions are used. Blockchain technology has two main types of tokens, including fungible tokens, where all tokens have equal value, and non-fungible tokens, which have unique characteristics and are not fungible. In fact, non-fungible tokens are digital assets with a unique identifier that are stored on a blockchain. This review article examines the basic concepts of blockchain, the challenges of using it, and the classification of blockchain tokens (fungible tokens, non-fungible tokens, and semi-fungible tokens).