فناوری دفاتر کل توزیع شده فراتر از فناوری زنجیره بلوکی

کد موضوعی: ۲۸۰
شماره مسلسل: ۱۵۹۲۰
تیرماه ۱۳۹۷

معاونت پژوهش‌های زیربنایی و امور تولیدی
دفتر: مطالعات ارتباطات و فناوری‌های نوین

به نام خدا

فهرست مطالب

فناوری دفاتر کل توزیع شده فراتر از فناوری زنجیره بلوکی

چکیده

دفاتر کل توزیع شده زیرساخت‌هایی راهبردی هستند که نهادهای کلان مانند نظام بانکی، بورس و اوراق بهادار، دفاتر اسناد رسمی و زیرساخت‌های ارتباطی را دگرگون خواهند کرد و سامانه‌های مربوط به توسعه ارزهای رمزپایه ملی و بسیاری از پروژه‌های آینده دولت الکترونیکی براساس آنها در کشور و جهان درحال شکل‌گیری است. دفتر کل توزیع شده، پایگاه داده‌ای است که براساس سازوکار تفاهم و معماری داده مورد قبول مشارکت‌کنندگان شبکه، نگهداری و به‌روزرسانی می‌شود. تصمیم آگاهانه درباره این‌گونه پروژه‌ها و سیاستگذاری ابعاد مختلف آنها به شناخت صحیح از اجزا، عناصر و شاخص‌های ارزیابی این سامانه‌ها نیازمند است. در این گزارش عناصر اصلی سامانه‌های دفاتر کل توزیع شده و اهداف این سامانه‌ها معرفی شده است. بررسی‌ها نشان می‌دهد امضای دیجیتالی مهمترین رکن یک سامانه دفتر کل توزیع شده است و باید در گزینش یک دفتر کل توزیع شده حتماً مقاومت سازوکار امضای الکترونیکی آن در برابر حملات سایبری[1] مدنظر قرار گیرد. سازوکارهای تفاهم انواع مختلفی دارند، اما هدف واحد جایگزینی شبکه ذی‌نفعان با نهادهای متمرکز را دنبال می‌کنند و هرکدام مزایا و معایبی دارند که در این گزارش تشریح شده است. معماری داده دفاتر کل توزیع شده در پایداری سامانه و حفظ سرعت

۱. رایانه‌های کوانتومی.

سامانه زیر بار تقاضا نقش مهمی دارد. زنجیره بلوکی تنها یک گونه از معماری داده‌ها در طراحی دفاتر کل توزیع شده به‌شمار می‌رود. سایر معماری‌ها قابلیت‌های جدیدی نسبت به زنجیره بلوکی فراهم می‌آورند و برای برخی کاربردها مفیدتر هستند. قراردادهای هوشمند و عرضه اولیه سکه فرصت‌های بی‌نظیری برای تسهیل کارآفرینی، کاهش هزینه‌های دفتری و افزایش سرعت و شفافیت فراهم می‌آورند. از نظر فنی پشتیبانی از قراردادهای هوشمند یک قابلیت نرم‌افزاری است که باید از ابتدا در طراحی سامانه دفاتر کل توزیع شده مدنظر قرار گیرد. بهره‌مندی از مزایای قراردادهای هوشمند و مصادیق آن همچون عرضه اولیه سکه به حمایت قانونگذار نیازمند است. مهمترین زیرساخت مورد نیاز برای بهره‌گیری از مزایای قراردادهای هوشمند رعایت استانداردهای داده باز در خدمات دولت الکترونیکی است، قانونگذار با الزام دستگاه‌ها به انتشار داده به‌صورت استاندارد باز می‌تواند هزینه‌های جاری و آینده را هم در بخش دولتی و هم در بخش خصوصی کاهش دهد. به رسمیت شناخته شدن کفایت ثبت اطلاعات سهام و سایر تراکنش‌ها در دفاتر کل توزیع شده و تسهیل مقررات برای امکان‌پذیر ساختن تولید ژتون‌های خدماتی برای ایده‌های کارآفرینانه در زمینه عرضه اولیه سکه می‌تواند در دستور کار قرار گیرد.

مقدمه

دفتر کل توزیع شده،[1] پایگاه داده‌ای است که براساس سازوکار تفاهم و معماری داده مورد قبول مشارکت‌کنندگان شبکه، نگهداری و به‌روزرسانی می‌شود. دفاتر کل توزیع شده به فناوری‌هایی گفته می‌شود که با معرفی فناوری زنجیره بلوکی بیتکوین در سال ۲۰۰۹

1. Distributed Ledger Technologies (DLT)

میلادی تغییر و تحول در نظام مالی و اقتصادی و ساختارهای سنتی و فناورانه تازه‌تأسیس را آغاز کرده‌اند. به بیان دیگر دفاتر کل توزیع شده نه‌تنها بازمهندسی خدمات سنتی همچون، بانکداری و بورس و دفاتر اسناد رسمی را ممکن کرده‌اند، بلکه شیوه‌ای نو برای عرضه خدماتی همچون عرضه زیرساخت‌های کلان رایانشی و اینترنتی و اینترنت اشیا پدید آورده‌اند (رجبی و فریور، ۱۳۹۶).

شبکه ارز دیجیتال بیتکوین اولین، معروف‌ترین و درحال حاضر بزرگ‌ترین شبکه دفاتر کل توزیع شده از لحاظ ارزش اقتصادی به‌شمار می‌رود، به صورتی‌که تصور عموم از فناوری دفاتر کل توزیع شده بیشتر براساس بیتکوین شکل گرفته است، اما شبکه بیتکوین بهترین و تنها نوع پیاده‌سازی دفاتر کل توزیع شده نیست (رجبی و فریور، ۱۳۹۶). به‌طور مثال دفاتر کل توزیع شده مورد استفاده در اتریوم و آیوتا از نظر فنی تفاوت‌های مهمی با بیتکوین دارند. به بیان دیگر زنجیره بلوکی نوآوری اصلی مخترع بیتکوین برای حل مشکل نیاز به اعتماد به طرف ثالث در مبادلات بود، اما امروزه دفاتر کل توزیع شده بدون زنجیره بلوکی و استفاده از گراف جهتدار بی دور[1] به‌جای زنجیره بلوک‌ها مطرح است.

استفاده از فناوری دفاتر کل توزیع شده در بازمهندسی فرآیندهای عرضه خدمات دولت الکترونیکی و سایر خدمات عمومی ازسوی مراکز سیاست‌پژوهی پیشنهاد شده است. اما همان‌طور که تجربه بیتکوین نشان داده است انتخاب یک معماری نامناسب می‌تواند اصلاح عملکرد سامانه در آینده را با مخاطرات زیادی مواجه کند. به‌عبارت‌دیگر درحال حاضر برخی دستگاه‌های اجرایی استفاده از فناوری زنجیره بلوکی برای ایجاد ارزهای رمزپایه را پیشنهاد می‌دهند، اما بررسی کارشناسی این نوع پیشنهادها نیازمند دانش فنی

1. Directed Acyclic Graph (DAG)

و شاخص‌های ارزیابی است. بنابراین در این گزارش تلاش می‌شود جنبه‌های فنی سازوکارهای مورد استفاده و معماری‌های مختلف دفاتر کل توزیع شده بررسی شود تا به نمایندگان مجلس شورای اسلامی در نقد مصادیق مختلف این فناوری کمک شود. برای این منظور ابتدا انواع سازوکارهای فناوری‌های دفاتر کل توزیع شده تشریح می‌شود، سپس چند نمونه از معماری‌های مختلف دفاتر کل توزیع شده بررسی می‌شود.

۱. اجزای اصلی دفاتر کل توزیع شده

فناوری دفاتر کل توزیع شده از ترکیب فناوری‌های رمزنگاری و قابلیت شبکه‌های همتا ـ همتا،[1] استفاده می‌کنند. سازوکاری که در همه دفاتر کل توزیع شده مشترک است و همه به نوعی از آنها استفاده می‌کنند امضای دیجیتالی است. سازوکارهای حصول تفاهم[2] که در این گزارش به دو دسته کلی سازوکار اثبات کار،[3] سازوکار اثبات سهم[4] تقسیم می‌شوند در دفاتر کل توزیع شده مختلف برای حفظ امنیت و پایداری سوابق تراکنش‌ها نقش دارند و از یکی از آنها یا هر دو آنها در طراحی سامانه‌ها استفاده می‌شود. معماری‌های داده مختلف برای ایجاد و برقراری ارتباط میان داده‌ها در دفاتر کل توزیع شده مورد استفاده قرار می‌گیرند که معروف‌ترین آنها زنجیره بلوکی است، اما روش‌های دیگری نیز برای معماری داده دفاتر کل توزیع شده وجود دارند. انتخاب معماری داده نیز در سرعت و تعداد تراکنش‌های قابل اجرا در یک سامانه دفتر کل توزیع شده نقش دارند. بنابراین ابتدا

1. Peer to Peer
2. Consensus Mechanisms
3. Proof of Work (POW)
4. Proof of Stake (POS)

سازوکارهای امضای دیجیتالی مورد استفاده در دفاتر کل توزیع شده بررسی می‌شود. سپس چند نمونه از سازوکارهای حصول تفاهم مورد بررسی قرار می‌گیرند و در نهایت معماری‌های داده مهم در دفاتر کل توزیع شده بررسی می‌شوند.

۱-۱. امضای دیجیتالی

امضای دیجیتالی معادل امضای حقیقی در فضای مجازی است که برای احراز هویت افراد در این فضا استفاده می‌شود. در هرکدام از ارزهای رمزپایه یا سامانه‌های دفاتر کل توزیع شده از یک یا چند مدل از مدل‌ها و الگوریتم‌های رمزنگاری برای امضا استفاده می‌شود. امضای دیجیتالی طبیعتاً نمی‌تواند برای اعتبارسنجی به یک طرف ثالث تکیه داشته باشد. برای این منظور در برخی سامانه‌های دفاتر کل از سازوکارهای کلید خصوصی و کلید عمومی استفاده می‌شود. داشتن کلید خصوصی باعث می‌شود فرد بتواند در معاملات مختلف از کلیدهای عمومی مختلفی استفاده کند. کلید خصوصی مانند گذرواژه و کلید عمومی مانند آدرس ایمیل یک فرد است، با این تفاوت که کلیدهای عمومی از هر تراکنش به تراکنش دیگر تغییر می‌کنند و از این نظر امنیت بالاتری دارند (The Royal Fork, 2014). با دانستن کلید خصوصی یک شخص می‌توان همه کلیدهای عمومی را شناسایی کرد. اما با داشتن گذرواژه یک شخص نمی‌توان آدرس ایمیل او را پیدا کرد. برای حل این مشکل در سامانه‌های دفاتر کل توزیع شده، بازه انتخاب آدرس خصوصی باید گسترده باشد (Apodaca, 2017).[۱]

---

۱. به‌طور مثال در شبکه بیتکوین کاربران می‌توانند کلیدهای خصوصی خاص خودشان را از میان تعداد ۱۰ به توان ۷۷ گزینه (یك عدد ۷۸ رقمي) انتخاب کنند. این تعداد آنقدر زیاد است که برخی ادعا می‌کنند یک رایانه با توان یک هزار میلیارد (یک تریلیون) تراکنش در ثانیه به‌اندازه یک میلیون برابر عمر تخمین زده شده برای جهان زمان لازم دارد که همه گزینه‌های آدرس را پردازش کند.

البته تعداد جای‌گشت‌ها به تنهایی مهم نیستند،[1] بلکه الگوریتم امضا اهمیت بیشتری دارد. در هر سامانه دفتر کل توزیع شده از یک یا چند مدل امضای دیجیتالی[2] (Ripple, 2017) استفاده می‌شود. امضای دیجیتالی رمزنگاری منحنی بیضوی[3] یکی از الگوریتم‌های رایج است که انواع مختلفی دارد[4] (IETF, 2017; Hall and Keller, 2014). امضاهای مبتنی‌بر الگوریتم‌های برهم‌ریزی[5] نیز پیشنهاد شده که هنوز در مرحله قبل از استانداردسازی قرار دارند (Kampanakis, 2017) (Hülsing, 2015). تحقیقات نشان می‌دهد که امضاهای دیجیتالی رمزنگاری منحنی بیضوی و بسیاری از سامانه‌های کلید عمومی می‌تواند با اختراع رایانه‌های کوانتومی با استفاده از حملات مبتنی‌بر الگوریتم شور[6] رمزگشایی شوند (Marc, et al. 2016) (Hülsing, 2015). به‌عبارت دیگر این‌طور پیش‌بینی شده که تا سال ۲۰۲۷ میلادی الگوریتم‌های مشابه امضای دیجیتالی بیتکوین در هم خواهد شکست (Aggarwal, Brennen and Miklo 2017). اما در مورد الگوریتم‌های برهم‌ریزی ادعا شده که این الگوریتم‌ها در مقابل حملات رایانه‌های کوانتومی مقاوم خواهند بود (I Anshel, 2017).

درهم شکستن فرمول امضای دیجیتالی یک ارز رمزپایه می‌تواند اعتماد به این شبکه‌ها را از میان ببرد. بنابراین طراحان سامانه‌های دفتر کل توزیع شده باید پاسخ

---

۱. مثلاً در سامانه جیمیل (Gmail) هر کاربر می‌تواند هر گذرواژه‌ای که بالای هشت کاراکتر باشد انتخاب کند و تعداد بیشتری گذرواژه در این سامانه قابل استفاده است و سامانه سازوکارهایی برای مقابله با حملات حدس همه گذرواژه‌ها دارد.

۲. مثلاً در شبکه ریپل از دو مدل امضای دیجیتالی استفاده می‌شود و اعلام شده است که در آینده اگر رایانه‌های کوانتومی رایج شود می‌توان از امضاهای دیگر هم در این شبکه استفاده کرد.

3. Elliptic Curve Digital Signature Algorithm

٤. دو مدل استاندارد آن یکی توسط سازمان ملی استاندارد ایالات متحده آمریکا و دیگری توسط انجمن بین‌المللي با نام کارگروه مهندسی اینترنت (IETF) پیشنهاد شده‌اند.

5. Hash

6. Shor's algorithm

روشنی در مورد الگوریتم امضای دیجیتالی خود ارائه کنند.

۲-۱. سازوکارهای حصول تفاهم

دفاتر کل توزیع شده سامانه‌هایی هستند که در آن مشارکت‌کنندگانی که از لحاظ جغرافیایی، زمانی و مکانی پراکنده هستند، با کمک سازوکارهایی در مورد وضعیت درست سامانه به تفاهم می‌رسند. به این سازوکارهای حصول تفاهم، مدل تفاهم نیز گفته می‌شود. مدل‌های تفاهم بر دو دسته کلی سازوکار اثبات کار و سازوکار اثبات سهم قابل تقسیم هستند.

۱-۲-۱. سازوکار اثبات کار

سازوکار اثبات کار، سازوکاری است که به یک عضو شبکه امکان می‌دهد که به دیگران ثابت کند که برای مدتی معین، مقدار مشخصی منابع رایانشی استفاده کرده است (Wattenhofer, 2016). هدف این سازوکار ایجاد جامعه‌ای است که در آن همه برای تأیید اعتبار تراکنش‌های یک شبکه با یکدیگر رقابت کنند تا در نتیجه آن حمله به سامانه دشوار شود (Aste, 2016).

از این سازوکار ابتدا برای مقابله با حملات سایبری همچون حملات توزیع شده ممانعت از خدمت[1] و با هدف مقابله با فرسایش منابع سامانه‌های رایانه‌ای بر اثر ارسال درخواست‌های جعلی پیشنهاد شد. این مفهوم برای اولین بار در سال ۱۹۹۳ پیشنهاد شد و عبارت سازوکار اثبات کار هم در سال ۱۹۹۹ یعنی ۹ سال قبل از اختراع بیتکوین معرفی شده است. اما استفاده از این سازوکار در ایجاد تفاهم بدون نیاز به اعتماد به شخص ثالث

1. Distributed Denial-Of-Service (DDOS)

نوآوری ساتوشی ناکاموتو مخترع (یا مخترعان) بیتکوین بوده است (Rosic 2017).

سازوکار اثبات کار در دفاتر کل توزیع شده به این‌صورت است که یک مسئله با سختی قابل تنظیم مطرح می‌شود و کسی که جواب مسئله را در زمان مناسبی به‌دست آورد برای انجام یک عمل ازسوی اعضای دیگر مشروعیت پیدا می‌کند. حل کردن این مسائل دشوار است اما بررسی درستی جواب در آنها ساده است (Gervais, 2016). این مسائل برای این طراحی می‌شوند که دو هدف دنبال شود (Verify.as 2017): یکی اینکه سازوکاری ایجاد شود که همه افراد با رایانه شخصی خودشان بتوانند در فرآیند بررسی تراکنش‌های شبکه و اعتبارسنجی آنها مشارکت کنند. هدف دوم این است که تراکنش‌های قدیمی نسبت به تغییر مصونیت پیدا کنند.

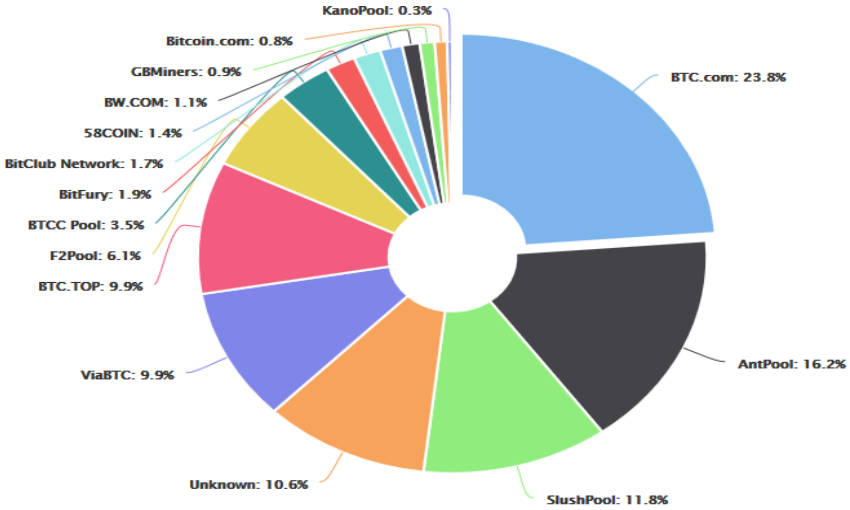
ازآنجاکه در این شبکه‌ها معمولاً برای اعتبارسنجی تراکنش‌ها پاداش تعیین می‌شود، برخی افراد در ایجاد سخت‌افزارهای تخصصی برای حل مسائل طرح شده در سازوکار اثبات کار سرمایه‌گذاری خواهند کرد. ازآنجاکه پاداش حل مسئله در بیشتر موارد فقط به نفر اول اهدا می‌شود و سختی مسئله روزبه‌روز افزایش پیدا می‌کند به‌تدریج افراد آماتور و غیرحرفه‌ای از موفقیت در رقابت حل مسئله ناامید می‌شوند و تأیید تراکنش‌ها در انحصار گروه‌هایی از متخصصان رایانه‌ای قرار می‌گیرد. به‌علاوه همواره این امکان وجود دارد که یک کاربر با توان رایانشی بالا وارد شبکه شده و انحصار قدرت پردازش را در اختیار بگیرد.

به‌طور مثال همان‌طور که در شکل زیر مشاهده می‌شود در شبکه بیتکوین هم‌اکنون[1] سه مجموعه بی‌تی‌سی داتکام، انتپول و اسلاشپول قدرتشان معادل ۵۱/۸ درصد کل اعضا است و مدت‌زمان زیادی یکی از مجموعه‌های قدرتمند و عناصر انحصاری تأییدکننده

۱. تاریخ بازبینی: ۱۳ اسفندماه ۱۳۹۶.

تراکنش‌ها هستند. این‌گونه انحصارها هدف اولیه از تکیه بر سازوکار اثبات کار را زیر سؤال می‌برند (Ittay Eyal, 2014).

شکل ۱. توزیع سهم بازیگران عمده از تأیید تراکنش‌های شبکه بیتکوین



Source: BLOCKCHAIN.INFO

ازآنجاکه حل مسئله پیش‌شرط انجام تراکنش است، اصلاح یک تراکنش یا مجموعه تراکنش نیز به داشتن پاسخ آن مسئله و مسائل طرح شده قبلی در زمانی کوتاه نیازمند است. این خود باعث می‌شود که از تراکنش‌های قدیمی در مقابل تغییرات آتی محافظت شود. البته یک راهکار دیگر برای محافظت از تراکنش‌های قدیمی، مشخص کردن یک نقطه غیرقابل بازگشت در سامانه است. به این صورت که پس از مثلاً ۱۰۰ بار تأیید یک تراکنش در سامانه دیگر آن تراکنش قابل تغییر نباشد و همه گره‌های شبکه آن تراکنش

را قطعی فرض کنند (V. Buterin, 2017).

سختی زیاد مسئله اثبات کار می‌تواند موجب تأخیر و کُندی شبکه و اتلاف زیاد منابع و مصرف انرژی بالا شود، اما سهولت بیش از حد مسئله نیز باعث می‌شود که همزمان چندین نفر به راه‌حل برسند و نوعی آشوب در سامانه ایجاد می‌کند و افراد برای تأیید تراکنش‌های خود به یک مرحله تأیید اکتفا نخواهند کرد و در نتیجه افزایش سرعت از این موضوع حاصل نخواهد شد. درحال حاضر مسائل اثبات کار مختلفی در سامانه‌های دفاتر کل توزیع شده استفاده می‌شود[۱] (Buntinx, 2017) (Percival and Josefsson, 2016). این مسائل با این هدف طراحی شدند که افراد با رایانه‌های معمولی بتوانند تراکنش‌ها را اعتبارسنجی کنند اما پس از مدتی که ارزش ارز دیجیتالی بالا می‌رود افراد حرفه‌ای مدارهای مجتمع با کاربرد حل مسائل سازوکار اثبات کار ایجاد می‌کنند و انحصار رفع شده دوباره ایجاد می‌شود. تلاش‌هایی از جنس ایجاد محدودیت ورودی خروجی در دشوارسازی ایجاد انحصار موفق بوده‌اند اما موفقیت نهایی این روش‌ها قابل تضمین نیست.

به‌طور کلی کسانی که از سازوکار اثبات کار برای تأیید و نگهداری استفاده می‌کنند باید دلایل خود برای انتخاب این سازوکار و نوع مسئله انتخابی را اعلام کنند. برای رفع نواقصی همچون مصرف انرژی بالا، انحصار و امکان به بازی گرفته شدن سامانه در سازوکار اثبات کار، سازوکار اثبات سهم پیشنهاد شده است.

---

۱. از آن جمله می‌توان به استفاده از الگوریتم‌های درهم‌سازی مانند SHA256 (Secure Hash Algorithm-256)اشاره کرد که به پردازنده قوی نیاز دارد. گروه دیگر مسائل اثبات کار اسکریپت (Scrypt با Script متفاوت است) است که به قدرت حافظه زیادی نیاز دارند و انجمن کارگروه اینترنت یک نمونه استاندارد برای آنها معرفی کرده است. نوع دیگر مسائل اثبات کار ایکس ۱۱[۱] (X11) نام دارد که از ۱۱ مرحله تابع درهم‌ریزی ساده تشکیل شده است که مصرف انرژی الکتریکی پایینی دارد. نوع دیگر مسائل اثبات کار با تکیه بر محدودیت ورودی و خروجی (I/o bond) به‌جای توان رایانشی در تلاش برای عدم ایجاد انحصار است.

۲-۲-۱. سازوکار اثبات سهم

هدف الگوریتم‌های حصول تفاهم در یک شبکه دفاتر کل توزیع شده این است که به افراد متکثر امکان داده شود که بدون نیاز به اعتماد به یکدیگر یا هرگونه مرجع مرکزی در مورد وضعیت جاری دفاتر کل به تفاهم برسند. پیش از اختراع بیتکوین و استفاده از سازوکار اثبات کار هیچ راهکاری برای این موضوع پیشنهاد نشده بود. در آن مقطع بهینگی حصول تفاهم بدون نیاز به اعتماد چندان اهمیتی نداشت. بیتکوین نشان داد که نیل به چنین تفاهمی امکان‌پذیر است و ایده‌های دیگر همچون سازوکار اثبات سهم نیز به‌تبع آن ازسوی صاحب‌نظران مطرح شدند.

سازوکار اثبات سهم رده‌ای از الگوریتم‌های حصول تفاهم هستند که بر سهم اقتصادی اعتباردهنده در شبکه تکیه دارند. در دفاتر کل توزیع شده عمومی مبتنی‌بر سازوکار اثبات سهم مجموعه‌ای از اعتباردهنده‌ها به نوبت بلوک‌ها یا تراکنش‌های جدید را پیشنهاد کرده و به رأی می‌گذارند. وزن آرای هر رأی‌دهنده در هرکدام از سازوکارهای اثبات سهم به‌صورت خودکار سنجیده می‌شود. در برخی سازوکارهای اثبات سهم هر میزان ارزی که فرد در حساب داشته باشد یا برای رأی‌دهی اعلام کند می‌تواند از شانس بیشتری برای ایجاد بلوک یا تأیید تراکنش برخوردار باشد. بعضی سازوکارها نیز براساس ترکیبی از میزان و مدت نگهداری سهم، شانس انتخاب شدن فرد افزایش پیدا می‌کند. ازآنجاکه همه افراد نمی‌توانند همواره برخط باشند تا از سامانه محافظت کنند در برخی از سازوکارهای اثبات سهم افراد نماینده‌ای[1] انتخاب کرده و او به‌جای آنها در مورد اعتبار تراکنش‌ها و ایجاد بلوک‌ها نظر داده و اقدام می‌کند.

1. Delegate

به‌نظر می‌رسد فناوری اثبات سهم به نوعی به بازتولید نظام بانکی قدیمی منجر می‌شود و بیشتر از اینکه ایجاد تفاهم بدون نیاز به اعتماد به طرف ثالث از این سامانه‌ها حاصل شود شخص ثالث مورد اعتماد به دارنده بیشترین منابع در سامانه مبدل می‌شود. همان‌طور که در نظام بانکی فعلی نیز بانک‌ها یا بیشترین میزان پول را در اختیار دارند یا نمایندگی دارندگان بیشترین پول را برعهده دارند (Poelstra, 2015). به‌علاوه در سامانه‌های اثبات کار کسانی که در یک رقابت ریاضی موفق به اثبات قدرت پردازش خود شده‌اند ایجاد بلوک جدید را برعهده می‌گیرند و این می‌تواند توانایی آنها در ایجاد سریع بلوک و اعتبارسنجی سایر تراکنش‌ها را نیز تضمین کند. اما در سامانه‌های اثبات سهم لزوماً این موضوع محقق نخواهد شد.

۲. انواع دفاتر کل توزیع شده براساس معماری‌های داده

به‌طور کلی معماری داده به مدل‌ها، سیاست‌ها، قوانین یا استانداردهایی اطلاق می‌شود که تعیین می‌کنند در یک سامانه چه داده‌ای گردآوری شود، چگونه ذخیره و تنظیم شود (Business Dictionary, 2017). در اینجا منظور از معماری داده این است که تراکنش‌ها و اطلاعات چگونه ذخیره و به هم مرتبط شوند و حفظ امنیت آنها چگونه دنبال شود. دفاتر کل توزیع شده معماری‌های داده مختلفی دارند (Xu, 2017) که در ادامه به تفکیک تشریح می‌شوند.

۲-۱. دفاتر کل توزیع شده مبتنی‌بر زنجیره‌های بلوکی

دفاتر کل توزیع شده مبتنی‌بر ساختار داده زنجیره بلوکی شناخته‌ترین نوع دفاتر کل

توزیع شده هستند. ساختار داده در این دفاتر کل توزیع شده به این صورت است که تراکنش‌های یک بازه زمانی اعتبارسنجی شده و در یک بلوک ذخیره می‌شوند. این بلوک از داده رمزگذاری شده و کسی می‌تواند اطلاعات آن بلوک را تغییر دهد که کد رمزگذاری اولیه را در اختیار داشته باشد. هر بلوک از داده‌های رمزگذاری شده علاوه‌بر رمز خودش حاوی مسئله‌ای از بلوک قبلی است و به‌صورت زنجیره‌ای به آن مرتبط است. بلوک‌های تراکنش آینده نیز همگی باید به یک زنجیره از بلوک‌های قبلی متصل باشند. اگر مقادیر یکی از بلوک‌های قدیمی تغییر کند، مقدار خروجی مسئله‌اش نیز تغییر می‌کند و دیگر اعضای شبکه بدون نیاز به پردازش کل داده‌ها متوجه این تغییر می‌شوند، به این مفهوم درخت مرکل[1] می‌گویند. گاهی اوقات که دو بلوک در یک زمان ایجاد شوند، بخشی از شبکه یک بلوک را به رسمیت می‌شناسد و بخشی دیگر بلوک دیگر را به رسمیت می‌شناسد. هرکدام از طرفین که زودتر بلوک بعدی را ایجاد کند و کشف مسئله آن را به شبکه اعلام کند زنجیره بلوکی بلندتری را تشکیل خواهد داد و افرادی که روی زنجیره کوتاه‌تر کار می‌کنند زنجیره خود را رها کرده و به کار روی زنجیره طولانی‌تر می‌پیوندند. به همین دلیل در دفاتر کل توزیع شده مبتنی‌بر فناوری زنجیره بلوکی همواره بلندترین زنجیره معتبر است و ساختار نهایی آنها به‌صورت یک زنجیره خطی خواهد بود.

محدودیت در ظرفیت بلوک و رقابت برای کسب سود از ایجاد بلوک‌های جدید باعث می‌شود که تعداد تراکنش‌هایی که در هر مرحله در یک بلوک ذخیره می‌شوند محدود باشد. سامانه به ایجادکنندگان بلوک جدید واحد ارز رمزگذاری شده (معدن‌کاوی) اهدا می‌کند. اخذ کارمزد از تراکنش‌های اعتبارسنجی و افزوده شده در بلوک، منبع دیگر درآمد

1. Merkle Tree

ایجادکنندگان بلوک جدید است. بنابراین تراکنش‌هایی که میزان کارمزد بیشتری پرداخت کنند شانس بیشتری برای افزوده شدن به بلوک‌ها را خواهند داشت (Mengerian, 2017). افزایش ظرفیت بلوک می‌تواند تعداد تراکنش‌های تأیید شده قابل درج در یک بلوک را افزایش دهد، اما رقابت برای کشف بلوک بعدی می‌تواند موجب شود که از همه ظرفیت بلوک برای افزودن تراکنش‌ها استفاده نشود. این مسائل باعث شده سامانه‌هایی که زمانی با هزینه اندک و سرعت بالا تراکنش‌های مالی را امکان‌پذیر می‌ساختند روزبه‌روز کُندتر و گرانقیمت‌تر شوند.

به‌طور مثال در سال ۱۳۹۲ تعداد تراکنش‌های روزانه سامانه بیتکوین از تعداد تراکنش‌های روزانه بانک ملی ایران کمتر بود، به همین دلیل حدوداً هر ۱۰ دقیقه تراکنش‌ها تأیید می‌شد و معمولاً یک بار تأیید تراکنش کفایت می‌کرد (ا. رجبی، ۱۳۹۳). اما امروزه برای اینکه از قطعی شدن یک تراکنش با کارمزد اندک اطمینان حاصل شود باید گاهی اوقات تا هفت ساعت زمان صرف شود. علاوه‌بر این، دفاتر کل توزیع شده دارای ساختار داده زنجیره بلوکی که از سازوکار اثبات کار استفاده می‌کنند با افزایش سختی مسئله بر میزان مصرف انرژی می‌افزایند و این می‌تواند مشکلات زیست‌محیطی ایجاد کند (Tayo, 2017).

برای حل مشکل کاهش سرعت در معماری داده زنجیره بلوکی پیشنهاد ایجاد زنجیره‌های بلوکی موازی پیشنهاد شده است. به این‌صورت که کاربران در بلوک‌های موازی تراکنش‌های میان خودشان را انجام می‌دهند و در بازه‌های مشخص نتایج تراکنش‌های زنجیره‌های بلوکی موازی در زنجیره بلوکی بزرگ‌تر ادغام می‌شود. این موضوع علاوه‌بر اینکه راهکاری موقتی است و اشباع زنجیره‌های بلوکی موازی می‌تواند موجب کاهش سرعت در آینده شود، تقسیم توان رایانشی در میان زنجیره‌های بلوکی مختلف نیز می‌تواند

موجب افزایش مخاطرات امنیتی شود مگر اینکه زنجیره‌های موازی به زنجیره اصلی مرتبط شوند (Ray, 2018). در طراحی یک دفتر کل توزیع شده مبتنی‌بر زنجیره بلوکی پشتیبانی از زنجیره‌های موازی می‌تواند یکی از شاخصه‌های ارزیابی ارزهای رمزپایه باشد.

برای حل این مشکلات برخی معماری‌های داده جایگزین پیشنهاد شده است که علاوه‌بر حفظ امنیت بتوان سرعت تراکنش‌ها را افزایش داد.

۲-۲. دفاتر کل توزیع شده مبتنی‌بر الگوریتم‌های مقاوم در برابر شرایط بیزانسی

شرایط بیزانسی[1] عبارتی است که به مسئله فرماندهان بیزانسی اشاره دارد. این مسئله به این‌صورت طرح شده است که گروهی از فرماندهان بیزانسی که هرکدام یک واحد نظامی مستقل را اداره می‌کنند قصد محاصره و حمله به یک شهر را دارند آنها برای برقراری ارتباط به عده‌ای پیغام‌رسان تکیه دارند. حمله موفق نیازمند حمله همزمان همه واحدها در زمانی مشخص است. مشکل اینجاست که بعضی از این فرماندهان خائن هستند و بعضی پیغام‌رسان‌ها نیز خائن هستند یا در جریان ارسال پیام به دست دشمن کشته می‌شوند.

راه‌حل اولیه این مسئله ازسوی مطرح‌کننده آن به این‌صورت پیشنهاد شد که می‌توان سازوکاری داشت که اگر تا یک‌سوم فرماندهان هم خیانت کنند خیانت آنها کشف و از شکست عملیات جلوگیری شود. این سازوکار در سامانه‌های پیچیده متعددی همچون هواپیماها، فضاپیماها و نیروگاه‌های هسته‌ای قابل پیاده‌سازی است تا از این طریق اهداف نیازمند عملکرد صحیح همه اجزای سامانه محقق شود (Konstantopoulos, 2017).

1. Byzantine Setting

ساتوشی ناکوموتو مخترع بیتکوین نیز سازوکار اثبات کار پیشنهادی خود را[1] راه‌حلی مقاوم در شرایط بیزانسی دانسته است (Nakamoto, 2008). اما پس از طرح سازوکار اثبات کار بیتکوین برخی پیشنهادهای جایگزین برای حصول تفاهم استفاده از زنجیره بلوک‌ها برای حصول تفاهم را غیرضروری می‌دانستند.

به‌طور مثال در برخی سازوکارهای مقاوم در برابر شرایط بیزانسی مبتنی‌بر اثبات سهم، حق اعتبارسنجی تراکنش‌های یک مرحله و ثبت آنها در یک بلوک به‌صورت تصادفی به یک اعتبارسنج تفویض می‌شود. اما اینکه آیا بلوک رسمیت پیدا کند یا خیر از طریق یک فرآیند چندمرحله‌ای صورت می‌گیرد که در هر مرحله، اعتبارسنج‌ها یک رأی برای آن بلوک مشخص ارسال می‌کنند و در انتهای فرآیند، همه اعتبارسنج‌ها موافقت می‌کنند که آیا یک بلوک جزء شبکه باشد یا خیر. نکته اینجاست که این بلوک‌ها ممکن است در امتداد هم زنجیر نشوند و تنها یک بلوک مورد تفاهم در هر مرحله ایجاد شود و بلوک جدید به اندازه و طول زنجیره قبل از خود وابسته نباشد (C. Cachin, 2017).

البته این نوع معماری‌های داده به‌دلیل اینکه بلوک تراکنش‌ها برای تأیید باید میان همه گره‌های شبکه در گردش باشد نمی‌تواند برای تعداد زیادی تراکنش مورد استفاده قرار گیرد و مشکل کاهش سرعت بر اثر افزایش تعداد گره‌ها و تراکنش‌های درخواستی در این نوع از معماری‌های داده دفاتر کل توزیع شده نیز وجود خواهد داشت (Vukolić, 2015).

۳-۲. دفاتر کل توزیع شده مبتنی‌بر گراف جهتدار بی‌دور

گراف جهتدار بی‌دور به گرافی گفته می‌شود که هیچ دور جهتداری ندارد (یعنی هیچ

---

۱. که از رمزنگاری و امضای دیجیتالی هم استفاده کرده و به‌این‌ترتیب امکان پیغام‌رسانی جعلی را کاهش داده و یک مسئله ساده‌سازی شده شرایط بیزانسی را حل می‌کند.

مسیر جهتداری که گره ابتدا و انتهای آن یکی باشد وجود ندارد). در دفاتر کل توزیع شده مبتنی‌بر زنجیره بلوکی واحدهای تراکنشی که در یک بازه زمانی رخ داده‌اند باید در یک بلوک ذخیره و همزمان تأیید یا رد می‌شوند، اما در دفاتر کل توزیع شده مبتنی‌بر گراف جهتدار بی‌دور هر تراکنش در حکم یک بلوک است (LeMahieu, 2017).

دفاتر کل توزیع شده مبتنی‌بر گراف جهتدار بی‌دور بیشتر در مرحله ایده هستند و خود انواع مختلفی دارند. در اینجا معمولاً گره‌های همسایه تراکنش‌های یکدیگر را کنترل می‌کنند و در صورتی‌که تراکنشی با تراکنش‌های اولیه که در بخش‌های عمیق‌تر گراف قرار دارد در تناقض باشد تراکنش جدیدتر رد می‌شود. ازآنجاکه در این سامانه‌ها هر تراکنش حکم یک بلوک را دارد تأیید تراکنش‌ها ازسوی کاربران با توان رایانشی اندک نیز ممکن می‌شود. ازسوی‌دیگر برای تأثیرگذاری بر روند بررسی و تأیید تراکنش‌ها، استفاده از توان رایانشی بالا جای خود را به ایجاد گره‌های بسیار زیاد کنترل شده ازسوی یک فرد واحد (حملات سیبیل)[1] می‌دهد. اما تأیید تراکنش‌ها به‌صورت منطقه‌ای باعث می‌شود این‌گونه حملات تنها در یک بخش از گراف تأثیرگذار باشند (C. a. Cachin, 2017).

به‌صورت کلی استفاده از گراف جهتدار بی‌دور باعث می‌شود سازوکارهای تأیید تراکنش‌ها نسبت به زنجیره‌های بلوکی توزیع شده‌تر باشند و امکان مشارکت کاربران با توان رایانشی کمتر در این سامانه‌ها حفظ می‌شود. این‌گونه سامانه‌ها معمولاً با افزایش تعداد کاربران ایمن‌تر خواهند بود. سرعت تأیید اولیه یک تراکنش در این دفاتر کل افزایش می‌یابد، اما تأیید اولیه یک تراکنش در یک شبکه توزیع شده به معنای پذیرش سریع‌تر آن تراکنش ازسوی کل گره‌های دفاتر کل توزیع شده نیست و کاربران بسته به مبلغ و

۱. Sybil Attack: برگرفته از نام شخصیتی داستانی که دچار بیماری اختلال هویت بوده است.

سطح اعتماد و نوع تراکنش باید تعداد تأییدهای بیشتری برای یک تراکنش دریافت کنند تا تراکنش از دید اکثریت شبکه مورد تأیید قرار گیرد (de la Rosa, 2017). در کاربردهای مربوط به اینترنت اشیا که ارتباط مالی مستمر میان دو ماشین برقرار می‌شود یک بار تأیید تراکنش می‌تواند کفایت کند، اما سایر کاربردها همچون دریافت‌ها و پرداخت‌های مقطعی نیازمندی خاص خود را خواهند داشت (Ryszkiewicz, 2018).

در برخی منابع از گراف جهتدار بی‌دور به‌عنوان جایگزینی برای سازوکار اثبات کار و سازوکار اثبات سهم یاد می‌شود (d'Anconia, 2017). اما استفاده از این نوع معماری داده هم با استفاده از سازوکار اثبات کار و هم با استفاده از سازوکار اثبات سهم برای ایجاد سامانه دفاتر کل توزیع شده نیز پیشنهاد شده است (Boyen, 2016). برخی منابع از دفاتر کل توزیع شده مبتنی‌بر گراف جهتدار بی‌دور به‌عنوان زنجیره بلوکی نسل سوم یاد می‌کنند (Lee, 2018) اما بررسی‌ها نشان می‌دهد این نامگذاری‌ها قبلاً برای مفاهیم دیگر نیز استفاده شده است (Swan, 2015). ازآنجاکه هیچ نهاد استانداردگذاری معتبری از این طبقه‌بندی‌ها حمایت نکرده، باید میزان انطباق هر معماری داده با نیازهای ایجاد دفتر کل توزیع شده بررسی شود.

بنابراین در یک طرح پیشنهادی برای دفاتر کل توزیع شده باید ازسوی طراح مشخص شود که چرا از معماری داده گراف جهتدار بی‌دور استفاده می‌شود یا نمی‌شود و در کنار آن از کدام سازوکارحصول تفاهم بهره گرفته خواهد شد؟

دفاتر کل توزیع شده براساس اجزای کلیدی و سازوکارهای حصول تفاهم و معماری‌های مختلف داده مورد بررسی قرار گرفتند. یک جنبه دیگر از مقایسه سامانه‌های دفاتر کل توزیع شده براساس هدف کارکردی آنهاست.

۳. انواع دفاتر کل توزیع شده براساس هدف کاربردی

مخترع بیتکوین هدف ایجاد یک ابزار پرداخت بدون نیاز به اعتماد به شخص ثالث را دنبال می‌کرد اما توسعه بستر نرم‌افزاری آن برای حفظ امنیت انعطاف کمتری دارد. در اصطلاح برنامه‌نویسی اگر یک زبان برنامه‌نویسی یا برنامه کاربردی انعطاف کامل داشته باشد که با آن بتوان هر نوع کاری که از یک رایانه انتظار می‌رود را انجام دهد به آن تورینگ کامل می‌گویند. انتخاب گزینه تورینگ کامل بودن یا نبودن یکی از گزینه‌هایی است که در طراحی سامانه نیازمند توجه است.

سامانه اتریوم بزرگ‌ترین ارز رمزپایه پس از بیتکوین است که بر ایجاد قابلیت انعطاف‌پذیری در سامانه دفاتر کل توزیع شده آن تلاش زیادی شده است. مفاهیم جدید دفاتر کل توزیع شده و نوآوری‌های جدید این حوزه در ارز رمزپایه اتریوم پیاده‌سازی شده‌اند. مفاهیمی مانند قرارداد هوشمند، عرضه اولیه سکه از طریق ژتون[1] و ژتون‌وارسازی با الهام از موفقیت بیتکوین و لزوم بهره‌گیری سامانه‌های دفاتر کل توزیع شده برای اهداف جدید در این حوزه مطرح شده‌اند.

۳-۱. قرارداد هوشمند

عبارت قرارداد هوشمند اولین بار بیش از ۲۰ سال پیش توسط نیک زابو[2] مطرح شد. ایده اولیه آن‌طور که او می‌نویسد این است که «بسیاری از عبارات قراردادی (همچون وثایق، اوراق قرضه، تحدید حقوق دارایی و مانند آن) می‌تواند در نرم‌افزارها و سخت‌افزارهایی که با

1. Token

۲. Nick Szabo: یکی از افرادی که احتمال می‌رود ساتوشی ناکومتو مخترع بیتکوین باشد.

آن مواجهیم تعبیه شوند به صورتی‌که عدول از قرارداد را برای طرفین هزینه‌بر سازد». زابو وسایل فروش خودکار (وندینگ) را از نمونه‌های اولیه این قراردادها می‌دانست زیرا آنها وجه را اخذ کرده و محصول را به طرف دوم قرارداد تحویل می‌دهند (Szabo, 1997).

قراردادهای هوشمند از جنس نرم‌افزار هستند و از لحاظ حقوقی قرارداد محسوب نمی‌شوند. اما یک دفتر کل توزیع شده را به صورتی به‌کار خواهند گرفت که قادر خواهد بود علاوه‌بر نگهداری از سوابق مالی به‌صورت خودکار مفاد موافقتنامه‌های چندجانبه را پیاده‌سازی کند. قراردادهای هوشمند توسط شبکه‌های رایانه‌ای دارای مکانیسم تفاهم واحد در مورد ترتیب اقدامات منتج از کد قرارداد به تفاهم می‌رسند. مثلاً در یک قرارداد هوشمند شرایط می‌تواند طوری تعریف شود که به‌محض اینکه کالایی وارد گمرک ایران شود مبلغ کالا به فروشنده پرداخت شود. در اینجا نیاز است که زیرساخت‌های لازم برای تعریف چنین قراردادهایی ازسوی دولت‌ها ایجاد شود. زیرساخت اصلی برای این موضوع رعایت استانداردهای داده‌های باز در انتشار این داده‌هاست. یعنی اگر دستگاه‌های متصدی خدمات عمومی داده‌های خود را به‌صورت استاندارد داده باز منتشر نکنند، تعریف قرارداد هوشمند روی این داده‌ها به‌سادگی صورت نخواهد گرفت.

قراردادهای هوشمند می‌تواند موجب صرفه‌جویی مالی و افزایش سرعت چشمگیر در اجرای مراحل اداری شوند. اما در نبود زیرساخت لازم برای این‌گونه قراردادها نمی‌توان آینده روشنی برای توسعه این فناوری متصور بود. بنابراین در صورتی‌که پشتیبانی از قرارداد هوشمند ازجمله اهداف توسعه دفاتر کل توزیع شده باشد. باید برنامه مشخصی در مورد استاندارد داده باز درخواست شود.

بیتکوین به‌دلیل خاص منظوره بودنش از قراردادهای هوشمند به‌خوبی پشتیبانی

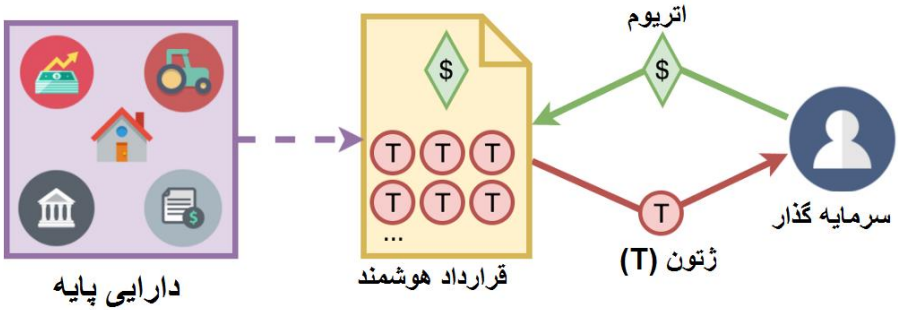
نمی‌کرد، بنابراین سامانه‌های دفاتر کل توزیع شده دیگر همچون اتریوم برای رفع این نقص طراحی شدند. این سامانه‌ها علاوه‌بر اینکه امکان مبادله ارزها را ممکن می‌سازند از تعریف و اجرای قراردادهای هوشمند نیز پشتیبانی می‌کنند (V. Buterin, 2013).

۲-۳. عرضه اولیه سکه

ارزهای رمزپایه به سه دسته تقسیم می‌شوند. گروهی نیاز به استخراج دارند. گروهی از قبل استخراج شده‌اند. گروهی نیز ترکیبی از دو نوع اول هستند یعنی مقداری از ارز از قبل استخراج شده است و مابقی با سازوکارهای معدن‌کاوی استخراج می‌شود. به‌طور مثال هنگامی که سامانه اتریوم درحال راه‌اندازی بود قبل از اینکه این شبکه کاملاً راه بیفتد مقداری از ارزهای آینده خود را در مقابل دریافت بیتکوین به کاربران و توسعه‌دهندگان عرضه کرد. پس از راه افتادن شبکه اتریوم این سامانه از طریق سازوکار اثبات کار و معدن‌کاوی و استخراج واحدهای جدید ارز دیجیتال خود را ایجاد می‌کند. این خود گونه‌ای از تأمین مالی است. به این مدل از تأمین مالی عرضه اولیه سکه می‌گویند که از عبارت عرضه اولیه سهام[1] الهام گرفته شده است. به بیان دیگر عرضه اولیه سکه نوعی استفاده خلاقانه از قابلیت‌های دفاتر کل توزیع شده و قراردادهای هوشمند است و از نظر فنی مانند راه‌اندازی یک ارز رمزپایه است. همان‌طور که در شکل ۲ مشاهده می‌شود در عرضه اولیه سکه یک دارایی پایه در قالب ژتون‌های الکترونیکی به‌ازای یک دارایی دیگر معامله می‌شود.

1. Intitial Public Offering (IPO)

شکل۲. فرآیند عرضه اولیه سکه در سامانه ارز رمزپایه اتریوم



Source: Blockgeeks.

همان‌طور که مشاهده می‌شود این ژتون‌ها در قالب یک قرارداد هوشمند به خریداران داده می‌شوند و طبق قرارداد هوشمند که به‌صورت خودکار مفاد آن اجرا می‌شود ژتون‌ها قابل دادوستد هستند و همان‌طور که در نمونه اتریوم ذکر شد، خود این ژتون‌ها می‌توانند ارز رمزپایه جدیدی باشند. به‌صورت کلی در عرضه اولیه سکه سه دسته ژتون به خریداران عرضه می‌شود (Wilmoth, 2018):

۱-۲-۳. ژتون سهام

یکی از کاربردهای قراردادهای هوشمند ایجاد توانایی عرضه سهام یا ژتون‌های سهام از طریق عرضه اولیه سکه است. این روش به شرکت‌های نوپا کمک می‌کند که به‌سادگی و به‌سرعت (مثلاً ۲۰ دقیقه) وارد بازارهای مالی شده و تأمین مالی برای ایده یا محصول خودشان را با جذب سرمایه از سراسر دنیا آغاز کنند (Neto, 2017). این شیوه، مبادله سهام را برای افراد تازه‌کار ساده می‌سازد و به آنها کمک می‌کند که در اداره شرکت سهامی نقش فعال‌تری داشته باشند، زیرا با استفاده از دفاتر کل توزیع شده به‌سادگی و شفافیت

آرای سهام‌داران اخذ می‌شود.

به‌علت فقدان رهنمودهای قانونی، در سطح جهان شرکت‌هایی نوپای اندکی ژتون سهام عرضه کرده‌اند. اگر مقرراتی وضع شود که در آن ثبت اسامی سهام‌داران در یک مدل از دفاتر کل توزیع شده کفایت کند، کمک زیادی به توسعه این روش تأمین مالی خواهد شد.

۲-۲-۳. ژتون‌های اوراق بهادار

اوراق بهادار طبقه‌بندی وسیعی است که می‌تواند به هرگونه دارایی قابل معامله اطلاق شود. اوراق بهادار قابل معامله تنوع زیادی دارند دارایی‌های پایه زیادی همچون فلزات ارزشمند و ژتون‌های پشتیبانی شده توسط دارایی‌های غیرمنقول را شامل می‌شوند. در این موارد قوانین بورس و اوراق بهادار بر عرضه اولیه ژتون‌های اوراق بهادار قابل اعمال است اما باید نظارت‌های جدیدی شکل بگیرند.

۳-۲-۳. ژتون‌های خدماتی

معمولاً بیشتر ژتون‌ها در حکم اوراق بهادار هستند، زیرا اکثریت مشارکت‌کنندگان در عرضه اولیه سکه، فروش عمومی آنها را در حکم فرصت سرمایه‌گذاری تلقی می‌کنند. اگر یک ژتون شرایط قانونی اوراق بهادار را برآورده نکند می‌تواند به‌عنوان یک ژتون خدماتی طبقه‌بندی شود. عنوان دیگری که ژتون‌های خدماتی را با آن طبقه‌بندی می‌کنند سکه‌های برنامه کاربردی یا ژتون برنامه کاربردی است. ژتون‌های خدماتی بهره گرفتن از یک محصول یا خدمت را ممکن می‌سازند.

برای نمونه فایل‌کوین،[1] شرکتی نوپاست که از فضای ذخیره‌سازی استفاده نشده

1. Filecoin

رایانه‌ها برای عرضه خدمات ذخیره‌سازی ابری استفاده خواهد کرد. مشارکت‌کنندگان در عرضه اولیه سکه می‌توانند هنگامی که فایل‌کوین راه‌اندازی شد از ژتون‌های خود برای خریداری فضای ذخیره‌سازی استفاده کنند. ازآنجاکه عرضه کل این سکه‌ها معمولاً ثابت است، ژتون‌ها ممکن است در طول زمان با افزایش تقاضا ارزش پیدا کنند. در اینجا حمایت از کسب‌وکارها می‌تواند به تدوین قوانین حمایتی نیازمند باشد.

به‌صورت کلی در طراحی یک سامانه دفتر کل توزیع شده، خدمات، کاربردها و اهدافی که سامانه از آن پشتیبانی خواهد کرد باید قبل از توسعه مشخص شود. چون معماری نرم‌افزارها از اهداف مشخص به یک اندازه حمایت نمی‌کنند.

۴. شاخص‌های ارزیابی و نقد دفاتر کل توزیع شده

۴-۱. شاخص‌های کمّی‌وکیفی عمومی

عملکرد دفاتر کل توزیع شده را می‌توان براساس شاخص‌های کمّی‌وکیفی زیر مقایسه کرد (KOTESKA, 2017):

ـ **ظرفیت پذیرش تقاضا:** حداکثر تعداد تراکنش‌هایی که در هر ثانیه توسط هر گره و کل شبکه قابل پذیرش است. پذیرش تقاضای تراکنش به معنای اعتبار آن تراکنش نخواهد بود و باید توسط شبکه اعتبارسنجی شوند. محدودیت در پذیرش تقاضا می‌تواند تأیید تقاضاهای مشروع را محدود کند.

ـ **سرعت پردازش شبکه:** پارامتری که حداکثر تعداد یا متوسط تعداد تراکنش‌هایی که یک سامانه در هر ثانیه می‌تواند پردازش کند را می‌سنجد. مثلاً در شبکه

بیتکوین در لحظه بررسی[۱] در هر ثانیه به‌طور متوسط ۲/۲ تراکنش انجام می‌شود.

ـ **متوسط تأخیر اعتبارسنجی:** متوسط زمانی که از لحظه ثبت تقاضای تراکنش تا اعتبارسنجی آن مصرف می‌شود. این شاخص متوسط زمانی که کاربران باید تا تأیید تراکنش‌هایشان صبر کنند را می‌سنجد.

ـ **بی‌ثباتی تأخیر:** شاخصی که تنوع زمان پردازش تراکنش‌ها را می‌سنجد، مثلاً در شبکه بیتکوین در حالت آرمانی در یک ثانیه ۹ تراکنش تأیید می‌شود و در حالت مطلوب چهار تا پنج تراکنش تأیید می‌شود. هرچه تنوع زمان پردازش تراکنش کمتر باشد سامانه قابل پیش‌بینی‌تر خواهد بود.

ـ **سطح امنیت:** سنجش امنیت سامانه به یک مدل تهدید نیازمند[۲] است که در آن مهاجمین، مهاجمین نوع و مقیاس حملات آنها به سامانه تعریف شود. مدل باید سامانه دفتر کل توزیع شده را در زمینه پایداری بلوک‌های دفتر کل و تراکنش‌ها، مقاومت در برابر سانسور تراکنش‌ها، مقاومت در برابر حملات ممانعت از خدمت، الزامات اعتماد به کاربران و اوراکل‌ها،[۳] حکمرانی بر پروتکل، خدمات عضویت گره‌ها و محرمانگی و ناشناسی کاربران بررسی کند.

ـ **سطح محرمانگی:** توانایی سامانه دفاتر کل توزیع شده در پنهان کردن تراکنش‌ها یا هویت مشارکت‌کنندگان را می‌سنجد. هرچه اطلاعات هویتی کمتری ذخیره شود، سطح محرمانگی افزایش پیدا می‌کند.

ـ **کارمزد تراکنش:** کاربران مقدار اندکی کارمزد در شبکه می‌پردازند تا تراکنش

---

۱. طبق آمار Blookchain.info در تاریخ ۲۲ اسفند براساس تعداد تراکنش‌های انجام شده در ۲۴ ساعت گذشته.
2. Threat Model
3. Oraceles

آنها پردازش و قرارداد هوشمند اجرا شود. این کارمزدها برای پوشش هزینه‌های نگهداری و حفاظت تراکنش‌ها در مقابل مخاطرات رایانشی استفاده می‌شوند.

ـ **الزامات سخت‌افزاری:** حافظه/فضای ذخیره‌سازی به‌ازای هر گره، منابع پردازشی که برای اعتبارسنجی تراکنش‌ها و بلوک‌ها استفاده از شبکه نیاز است.

ـ **مقیاس‌پذیری:** تعداد گره‌ها، تراکنش‌ها، کاربران و میزان توزیع جغرافیایی که سامانه دفاتر کل توزیع شده بدون کاهش عملکرد می‌تواند پشتیبانی کند.

ـ **سطح پیچیدگی:** پیچیدگی توسعه، نگهداری و اجرای زیرساخت‌های سامانه دفاتر کل توزیع شده را می‌سنجد.

ـ **محدودیت‌های قرارداد هوشمند دفاتر کل توزیع شده:** محدودیت‌های کدهایی که سامانه زنجیره بلوکی براساس آن به نگارش درآمده است و پروتکل‌های قرارداد هوشمندی که سامانه از آنها پشتیبانی می‌کند.

ـ **تعامل‌پذیری:** توانایی سامانه در برقراری ارتباط با دیگر انواع دفاتر کل توزیع شده و انتقال واحد ارزش از یک سامانه دفتر کل توزیع شده به سامانه دیگر به‌صورت خودکار (Epstein, 2017).

ـ **توانایی مدیریت عدم نیاز به مجوز ورود:** سامانه‌های پیشنهادی به‌ویژه در مرحله آزمایشی ممکن است تنها به افرادی اجازه دهند که واجد شرایط باشند. در این‌صورت برخی ملاحظات امنیتی دیگر وجود نخواهد داشت و سرعت می‌تواند بسیار بالاتر باشد. اما زمانی عیار واقعی یک سامانه مشخص می‌شود که بتواند شرایط جهانی را مدیریت کند (Thompson, 2016). یعنی شرایطی که هر فردی بتواند با نصب نرم‌افزار تبدیل به عضوی از شبکه شود.

ـ قابلیت حکمرانی: هر سامانه دفتر کل توزیع شده یک پروژه نرم‌افزاری است و رفع ایراد و اصلاح سامانه در طول زمان نیاز خواهد بود. در یک شبکه توزیع شده همه امضا باید همزمان نرم‌افزارهای خود را به‌روزرسانی کنند. در صورتی‌که تفاهم به‌وجود نیاید شبکه به دو شبکه مستقل تبدیل می‌شود. هرچه جزئیات مربوط به حکمرانی بهتر تبیین شده باشد قابلیت حکمرانی سامانه افزایش پیدا می‌کند.

۲-۴. مقایسه و رتبه‌بندی ارزهای دیجیتالی توسط مؤسسه اعتبارسنجی وایس

مؤسسه اعتبارسنجی وایس[1] بررسی و رتبه‌بندی بیش از ۷۴ ارز رمزپایه که حدود ۸۰ درصد اندازه بازار ارزهای رمزپایه را شکل می‌دهند را انجام داده است. این مؤسسه، ارزهای رمزپایه را بین بازه‌های A+ به معنای بسیار خوب و D- به معنای ضعیف طبقه‌بندی می‌کند. طبق آخرین گزارش این مؤسسه،[2] هیچ ارز رمزپایه‌ای شرایط لازم برای اخذ رتبه A را کسب نکرده است. بالاترین رتبه توسط ارزهای دیجیتالی اتریوم، ایی‌اواس[3] و کاردانو[4] کسب شده است که رتبه آنها B است. ارز رمزپایه بیتکوین رتبه C+ یا معمولی را کسب کرده است. مؤسسه اعتبارسنجی وایس براساس مدل زیر با چهار شاخص، ارزهای رمزپایه را رتبه‌بندی می‌کند:

۱. شاخص مخاطره ارز رمزپایه: این شاخص براساس الف) نوسانات نسبی و مطلق قیمت در طول بازه‌های زمانی مختلف ب) افول از اوج در واحد توالی و اندازه، پ) ترجیح

1. Weiss

۲. مورخ ۲۴ ژانویه ۲۰۱۸

3. EOS
4. Cardano

بازار به سمت بالا و پایین و دیگر عوامل، تهیه شده است.

۲. شاخص پاداش ارز رمزپایه: این شاخص الف) بازده در مقایسه با میانگین‌های متحرک[1] ب) بازده سرمایه مطلق در مقایسه با (ارز رمزپایه) محک،[2] بازده هموار شده[3] و دیگر عوامل را می‌سنجد.

۳. شاخص فناوری ارز رمزپایه: سطح حفظ حریم شخصی و ناشناسی، قابلیت‌های حکمرانی، توانایی به‌روزرسانی، بهینگی مصرف انرژی در حین تراکنش، راهکارهای افزایش مقیاس، قابلیت تعامل با دیگر زنجیره‌های بلوکی و دفاتر کل توزیع شده، به‌علاوه دیگر نقاط قوت و ضعف فناورانه را می‌سنجد.

۴. شاخص بنیادین ارزهای رمزپایه: این شاخص سرعت تراکنش و مقیاس‌پذیری، رسوخ در بازار، امنیت شبکه، توزیع‌شدگی تولید ارز، ظرفیت شبکه، مشارکت توسعه‌دهندگان، پذیرش عمومی و نظایر آن را می‌سنجد.

این مؤسسه هدف خود را رتبه‌بندی شفاف و بدون غرض‌ورزی از گزینه‌های سرمایه‌گذاری اعلام کرده، اما سوابق قبلی (SEC, 2006) نشان می‌دهند صحت و دقت بررسی‌های این مؤسسه باید حداقل در یک بازه زمانی مشخص بررسی شود.

1. Moving Average
2. Benchmark
3. Smoothed Returns

جمع‌بندی

ماهیت و معنای فناوری هنگامی شکل می‌گیرد که با زندگی روزمره بشری درهم می‌آمیزد (Reijers, 2016). فناوری دفاتر کل توزیع شده نیز هنگامی که در مصداق بیتکوین به جهان معرفی شد، هنوز ماهیت بالفعل خود را نشان نداده بود. اما پس از نزدیک به ۱۰ سال از معرفی فناوری دفاتر کل توزیع شده و استفاده و همچنین اقبال جهانی به این فناوری‌ها و ایجاد مصادیق دیگری از فناوری دفاتر کل توزیع شده اکنون برخی جلوه‌های این فناوری قابل درک شده است. فناوری دفاتر کل توزیع شده در مسیر تحول نهادهای مهم همچون بانکداری، بورس اوراق بهادار، ثبت اسناد و املاک و خدمات زیرساختی چشم‌اندازهای جدیدی ترسیم کرده است. البته هنوز راه زیادی برای نفوذ کامل این فناوری در زندگی بشری باقی مانده است، اما تجربه کاربری ۱۰ سال اخیر نشان می‌دهد که استفاده انحصاری از سازوکار اثبات کار موجب می‌شود که شبکه از آرمان عدم انحصار به انحصار دارندگان زیرساخت‌های فنی سوق داده شود. مثلاً شبکه بیتکوین درحال حاضر در انحصار چند مجموعه معدن‌کاوی اصلی است. گرچه تکیه محض به سازوکار اثبات سهم نیز بازتولید انحصار سنتی صاحبان منابع مالی همچون بانک‌ها را نتیجه خواهد داد. امضای دیجیتالی راهبردی‌ترین جزء یک سامانه دفاتر کل توزیع شده است و استفاده از سازوکارهایی که از نظر امنیتی ضعیف هستند می‌تواند کل سامانه را در معرض خطر قرار دهد.

برای تحقق اهداف مختلف باید انواع مختلفی از معماری‌های داده سامانه‌های دفاتر کل توزیع شده، مورد استفاده قرار گیرد. هنوز هیچ‌کدام از معماری‌های داده یا سازوکارهای حصول تفاهم نتوانسته‌اند کاملاً موفقیت خود را تضمین کنند و سرعت پیشرفت فناوری از طریق تسهیل سرمایه‌گذاری با کمک همین فناوری‌ها به‌شدت افزایش

پیدا کرده است. ورود به این بازار تنها نیازمند خلاقیت و نوآوری بیشتر است. دولت‌ها نمی‌توانند مانع از مشارکت شهروندانشان در این بازارها شوند اما می‌توانند با اتخاذ نقش حمایتی فعال، بازار را به‌گونه‌ای شکل دهند که منافع کشور تأمین شود. اگر بازار به‌گونه‌ای شکل بگیرد که با منافع کشور سازگار نباشد اصلاح آن در آینده به‌سادگی امکان‌پذیر نخواهد بود.

قراردادهای هوشمند یکی از مهمترین مزایای دفاتر کل توزیع شده است و تدوین مقررات الزام انتشار داده‌ها براساس استانداردهای داده باز یکی از مهمترین گام‌ها در ایجاد زیرساخت‌های لازم برای استفاده از مزایای قرارداد هوشمند است.

تدوین قوانین و مقررات در زمینه کفایت ذخیره اطلاعات مربوط به سهام در دفاتر کل توزیع شده می‌تواند روند استفاده از این فناوری‌ها را تسریع کند. تسهیل مقررات برای امکان‌پذیر ساختن تولید ژتون‌های خدماتی برای ایده‌های کارآفرینانه در زمینه عرضه اولیه سکه می‌تواند در دستور کار قرار گیرد.

منابع و مآخذ

۱. رجبی، ابوالقاسم و روح‌الله فریور. *آشنایی با فناوری راهبردی زنجیره بلوکی و کاربردهای آن*. تهران، مرکز پژوهش‌های مجلس، ۱۳۹۶.

۲. رجبی، ابولقاسم. *بیتکوین؛ ابزاری نوین در نظام پرداخت‌های الکترونیکی*، مرکز پژوهش‌های مجلس، ۱۳۹۳.

3. Hall, Timothy A., and Sharon S. Keller. 2014. *The FIPS 186- 4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS).* NIST. https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Algorithm-Validation-Program/documents/dss2/ecdsa2

vs.pdf.
4. Percival, C., and S. Josefsson. 2016. *The scrypt Password-Based Key Derivation Function.* IETF. doi:10.17487/RFC7914 .
5. Aggarwal, Divesh , Gavin K. Brennen, and Troy Lee Miklo. 2017. " Quantum attacks on Bitcoin, and how to protect against them."
6. Apodaca, Rich. 2017. *Six Things Bitcoin Users Should Know about Private Keys.* https://bitzuma.com/posts/six-things-bitcoin-users-should-know-about-private-keys/.
7. Aste, Tomaso. 2016. "The Fair Cost of Bitcoin Proof of Work." (SSRN).
8. Boyen, Xavier, Christopher Carr, and Thomas Haines. 2016. "Blockchain-free cryptocurrencies: A framework for truly decentralised fast transactions." *Cryptology* .
9. Buntinx, JP. 2017 . *Scrypt vs X11 vs SHA-256.* https://themerkle.com/scrypt-vs-x11-vs-sha-256/.
10.Business dictionary. 2017. http://www.businessdictionary.com/definition/data-architecture.html.
11. Buterin, Vitalik. 2017. "Vitalik Buterin: Sharding and…f Stake Protocols in Ethereum." https://fac.weblecture.nus.edu.sg/Panopto/Pages/Viewer.aspx?id=14a86a43-95ff-4443-b717-56392bd1ef03.
12. Buterin, Vitalik. 2013. *Ethereum white paper.* GitHub repository.
13. Cachin, Christian. 2017. *ITU Workshop on "Security Aspects of Blockchain".* ITU .
14. Cachin, Christian, and Marko Vukolić. 2017. *"Blockchains Consensus Protocols in the Wild.* arXiv preprint .
15. D'Anconia, Frisco. 2017. *Future of Digital Currency May Not Involve Blockchains.* https://cointelegraph.com/news/future-of-digital-currency-may-not-involve-blockchains.
16. De la Rosa, Josep Lluis, Victor Torres-Padrosa, Andrés el-Fakdi, Denisa Gibovic, O. Hornyák, Lutz Maicher, and Francesc Miralles. 2017. "A SURVEY OF BLOCKCHAIN TECHNOLOGIES FOR OPEN INNOVATION." *In 4rd Annual World Open Innovation Conf. WOIC, .*
17. Epstein, Jeremy. 2017. *How Blockchain Interoperability Opens the Mainstream Adoption Floodgates.* https://medium.com/@jer979/how-

blockchain-interoperability-opens-the-mainstream-adoption-floodgates -22f86fba38c.
18. Gervais, Arthur, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. "On the security and performance of Proof of Work blockchains." *" In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security.* ACM.
19. Hülsing, A. 2015. "Hash-based Signatures:An Outline for a New Standard."
20. I Anshel, D Atkins, D Goldfeld, PE Gunnells. 2017. "WalnutDSATM: A Quantum-Resistant Digital Signature Algorithm."
21. IETF. 2017. "Edwards-Curve Digital Signature Algorithm (EdDSA)." https://tools.ietf.org/html/rfc8032.
22. Ittay Eyal, Emin Gün Sirer. 2014 . *How A Mining Monopoly Can Attack Bitcoin.* http://hackingdistributed.com/2014/06/16/how-a-mining-monopoly-can-attack-bitcoin/.
23. Kampanakis, P. 2017. "LMS vs XMSS: Comparion of two Hash-Based Signature Standards." https://eprint.iacr.org/2017/349.pdf.
24. Konstantopoulos, Georgios. 2017. *Understanding Blockchain Fundamentals, Part 1: Byzantine Fault Tolerance.* https://medium.com/loom-network/understanding-blockchain-fundamentals-part-1-byzantine-fault-tolerance-245f46fe8419.
25. KOTESKA, BOJANA, ELENA KARAFILOSKI, and ANASTAS MISHEV. 2017. "Blockchain Implementation Quality Challenges: A Literature Review." *roceedings of the SQAMIA 2017: 6th Workshop of Software Quality, Analysis, Monitoring, Improvement, and Applications.*
26. Lee, Sherman. 2018. *Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0.* https://www.forbes.com/sites/shermanlee /2018/01/22/ explaining-directed-acylic-graph-dag-the-real-blockchain -3-0/.
27. LeMahieu, Colin. 2017. "RaiBlocks: A Feeless Distributed Cryptocurrency Network." raiblocks. net/media/RaiBlocks-Whitepaper -English. pdf .

28. Marc, Kaplan, Leurent Gaëtan , Leverrier Anthony , and Naya-Plasencia María . 2016 . "Breaking Symmetric Cryptosystems using Quantum Period Finding." *Quantum Physics.*
29. Mengerian. 2017. *Bringing Stability to Bitcoin Cash Difficulty Adjustments.* https://medium.com/@Mengerian/bringing-stability-to-bitcoin-cash-difficulty-adjustments-eae8def0efa4.
30. Nakamoto, Satoshi. 2008. *Re: Bitcoin P2P e-cash paper.* https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html.
31. Neto, Moritz. 2017. *How to issue your own token on Ethereum in less than 20 minutes.* https://medium.com/bitfwd/how-to-issue-your-own-token-on-ethereum-in-less-than-20-minutes-ac1f8f022793.
32. Poelstra, Andrew. 2015. "On Stake and Consensus." public domain.
33. Ray, Shaan. 2018. *What are Sidechains?* https://hackernoon.com/what-are-sidechains-1c45ea2daf3.
34. Reijers, Wessel, and Mark Coeckelbergh. 2016. "The blockchain as a narrative technology: investigating the social ontology and normative configurations of cryptocurrencies." *Philosophy & Technology.*
35. Ripple. 2017. *Signing Algorithms.* https://ripple.com/build/cryptographic-keys/#signing-algorithms.
36. Rosic, Ameer. 2017. *Proof of Work vs Proof of Stake: Basic Mining Guide.* https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.
37. Ryszkiewicz, Peter. 2018. *IOTA vs NANO (RaiBlocks).* https://hackernoon.com/iota-vs-raiblocks-413679bb4c3e.
38. SEC. 2006. "WEISS RESEARCH, INC., MARTIN WEISS, AND LAWRENCE EDELSON ." https://www.sec.gov/litigation/admin/2006/ia-2525.pdf.
39. Swan, Melanie. 2015. *Blockchain: Blueprint for a new economy.* O'Reilly Media, Inc.
40. Szabo, Nick. 1997. *The idea of smart contracts.* Nick Szabo's Papers and Concise Tutorials.
41. Tayo, Andrew. 2017. *Proof of work, or proof of waste?* https://hackernoon.com/proof-of-work-or-proof-of-waste-

9c1710b7f025.
42. The Royal Fork. 2014. *Layman's Guide to Elliptic Curve Digital Signatures.* http://royalforkblog.github.io/2014/09/04/ecc/.
43. Thompson, Collin. 2016. *Private Blockchain or Database?* https://medium.com/blockchain-review/private-blockchain-or-database-whats-the-difference-523e7d42edc.
44.Verify.as. 2017. *Why Dagger-Hashimoto for Ethereum?* https://medium.com/verifyas/why-dagger-hashimoto-for-ethereum-773f0792a689.
45. Vukolić, Marko. 2015. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." *Workshop on Open Problems in Network Security.* Springer.
46. Wattenhofer, Roger. 2016. *The science of the blockchain.* CreateSpace Independent Publishing Platform.
47. Wilmoth, Josiah. 2018. *3 Types of ICO Tokens.* http://strategiccoin.com/3-types-ico-tokens/.
48. Xu, Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. 2017 . " A taxonomy of blockchain-based systems for architecture design." *2017 IEEE International Conference on* . IEEE.

مرکز پژوهش‌ها
مجلس شورای اسلامی

شناسنامه گزارش	شماره مسلسل: ۱۵۹۲۰

عنوان گزارش: فناوری دفاتر کل توزیع شده فراتر از فناوری زنجیره بلوکی

نام دفتر: مطالعات ارتباطات و فناوری‌های نوین (گروه فناوری اطلاعات و ارتباطات)

تهیه‌کننده: ابوالقاسم رجبی

مدیر مطالعه: حسن پوراسماعیل

ناظران علمی: مهدی فقیهی، حسین افشین

متقاضی: معاونت پژوهش‌های زیربنایی و امور تولیدی

واژه‌های کلیدی:

زنجیره بلوکی، بلاکچین، فراتر از بلاکچین، بیتکوین، اتریوم، گراف جهتدار بی‌دور، گراف جهتدار غیرمدور، دگ، سازوکارهای حصول تفاهم، سازوکار اثبات کار، سازوکار اثبات سهم، معماری داده، امضای دیجیتالی، الگوریتم برهم‌ریزی، هش، رمزنگاری منحنی بیضوی، کلید عمومی و خصوصی، نقد بیتکوین، نقد زنجیره بلوکی، رتبه‌بندی وایس، قرارداد هوشمند، عرضه اولیه سکه، توکن، ژتون سهام، ژتون اوراق بهادار، ژتون خدماتی، ارزیابی فناوری، دولت الکترونیکی، درخت مرکل، گواه اثبات کار.

تاریخ انتشار: ۱۳۹۷/۴/۱۲