سیستم‌های فازی و کاربردها
سال پنجم، شماره اول (بهار و تابستان ۱۴۰۱)
صص. ۲۹۵ تا ۳۳۴
شاپای چاپی: ۲۷۱۷-۴۴۰۹
شاپای الکترونیکی: ۲۷۱۷-۳۹۸۴
DOI:10.22034/JFSA.2022.353946.1140

زنجیره بلوکی: معرفی و کاربردها

مهرزاد میرزاصادقی* **و حسین نظام آبادی پور**

گروه مهندسی برق،دانشگاه شهید باهنر کرمان، کرمان، ایران

تاریخ دریافت: ۱۴۰۱/۵/۸ تاریخ پذیرش: ۱۴۰۱/۶/۱۵

نوع مقاله: علمی-مروری دعوت شده

چکیده

زنجیره‌بلوکی را می‌توان یک دفتر دیجیتال جهانی خطاناپذیر معرفی کرد که برای هر گونه عملیات ثبت داده یا به بیانی دیگر ذخیره‌سازی تراکنش‌ها به کار می‌رود. غیرمتمرکز بودن، توزیع پذیری، امنیت، شفافیت، تغییرناپذیری و گمنامی از ویژگی‌های اصلی این فناوری نوظهور می‌باشند. رمزارزها و به طور خاص بیت‌کوین مهم‌ترین و موفق‌ترین کاربرد فناوری زنجیره‌بلوکی هستند و بیت‌کوین اولین پیاده‌سازی عملی و موفق زنجیره‌بلوکی است. نوآوری خالق بیت‌کوین در این بود که راهی برای غیرمتمرکزسازی تراکنش‌های مالی با استفاده از زنجیره‌بلوکی ایجاد کرد و پس از آن هزاران رمزارز دیگر با تغییراتی در این ساختار پایه، بر بستر زنجیره‌بلوکی بوجود آمد. با استفاده از این فناوری، امکان تقلب، دوبار خرج کردن پول و برگشت تراکنش‌های مالی ثبت شده در شبکه از بین می‌رود. با پیشرفت دنیای رمزارزها، اتریوم که آن را نسل دوم زنجیره‌بلوکی می‌نامند، ظهور کرد. هدف اصلی اتریوم این بود که بتواند همه عملیات و فرآیندها را غیرمتمرکز کند. قراردادهای هوشمند نیز یکی از فناوری‌های حاصل از شبکه اتریوم است. هدف طراح آن، این بود که برای نگهداری از قراردادها از یک دفترکل توزیع شده استفاده کند.

عبارات و کلمات کلیدی: زنجیره بلوکی، ثبت تراکنش، بیت‌کوین، اتریوم، دفترکل توزیع شده، قراردادهای هوشمند

Email(s): mmirzasadeghi@eng.uk.ac.ir and nezam@uk.ac.ir.

Mathematics Subject Classification:

۱ سرآغاز

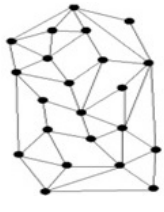
قرن بیست و یکم، قرن فناوری اطلاعات و ارتباطات است. دسترسی به داده، مساله‌ای که در دنیای امروز بسیار تسهیل شده است. بنابراین، امکان انتقال، کپی‌برداری و ویرایش اطلاعات به سهولت ایجاد شده است. فرآیندهایی که در گذشته تقریبا غیرممکن بوده است اکنون در کسری از ثانیه در حال انجام است اما مشابه هر پیشرفتی، این حالت نیز همراه مشکلاتی می‌باشد. از اساسی‌ترین مشکلاتی که دنیای دیجیتال با خود دارد کپی غیرمجاز و جعل اطلاعات است. این در حالی است که مساله مالکیت در برخی موارد به صورت جدی درنظر گرفته نمی‌شود و داده که یک کالای دیجیتال به حساب می‌آید به دلیل سهولت در دسترسی و انجام عملیات مخصوص آنها نادیده گرفته می‌شود. از طرفی دیگر اطلاعات جعل می‌شوند و امکان تشخیص اطلاعات درست از نادرست فرآیندی دشوار خواهد بود. اگر تا دهه‌ی ۶۰ میلادی نبودن اطلاعات یکی ازچالش‌های بزرگ علم در آن زمان بوده است، امروزه انفجار اطلاعات و تشخیص اطلاعات غلط و صحیح از یکدیگر یکی از چالش‌های دنیای امروز در این حوزه است. بشر ده‌ها هزار سال برای بهبود و توسعه شرایط زندگی خود کوشیده است و جوامع بشری سه مرحله تکامل را پشت سر گذاشته‌اند: جامعه سنتی، جامعه صنعتی و جامعه فراصنعتی یا جامعه اطلاعاتی. در جامعه اطلاعاتی ما سه انقلاب را پشت سرگذاشته‌ایم: انقلاب اول، انقلاب دیجیتال بود که با خلق ترانزیستورها ایجاد شد. انقلاب دوم، انقلاب اینترنت بود که در سال ۱۹۹۰ صورت گرفت و انقلاب بعدی انقلاب کارآفرینی بود که بر بستر فناری اطلاعات شکل گرفت. شاید بتوان گفت که اینترنت نسل سوم که بر بستر زنجیره‌بلوکی می‌باشد و با ظهور بیت‌کوین آشکار شده است، تبدیل به انقلاب جدیدی بشود که با استفاده از متاورس‌ها و دیگر فناوری‌های ایجاد شده در این حوزه محقق شود [۴۷]. در سال ۲۰۰۸ و به دنبال بحران مالی جهانی و سقوط بازارهای بورس، مردم تا حدی اعتماد خود را به مؤسسات مالی از دست دادند و ایده استفاده از سیستم‌های غیرمتمرکز به جای بانک‌ها که اساسا سیستم‌های متمرکزی هستند برای انجام تراکنش‌های مالی مطرح شد. در سال ۲۰۰۹، ساتوشی ناکاماتو بیت‌کوین را به دنیا معرفی کرد. در شبکه بیت‌کوین با استفاده از یک فناوری پایه به نام زنجیره‌بلوکی، می‌توان به یک سیستم غیرمتمرکز اعتماد کرد و تمام معاملات مالی را با استفاده از آن انجام داد [۲۳]. فناوری زنجیره‌بلوکی در خدمات مختلف مالی از جمله

دارایی‌های دیجیتال، انتقال پول و پرداخت‌های برخط می‌تواند کارایی مفیدی داشته باشد. علاوه بر این از این فناوری در زمینه‌هایی از جمله رسانه‌ها، خدمات عمومی، اینترنت اشیا، سیستم‌های امنیتی، انرژی، منابع انسانی و غیره به دلیل عملکرد بسیار مورد استفاده قرار گرفته است [۱۹]. تولد اتریوم نیز با قابلیت‌های بیشتر در مقایسه با بیت‌کوین، یکی از رویدادهای مهم در تاریخچه زنجیره‌بلوکی است. شبکه اتریوم با توجه به توانایی آن در پشتیبانی از قراردادهای هوشمند، تبدیل به یکی از بزرگ‌ترین کاربردهای فناوری زنجیره‌بلوکی شد [۱۳]. تاریخچه زنجیره‌بلوکی و تکامل آن به بیت‌کوین و اتریوم محدود نمی‌شود. در سال‌های اخیر پروژه‌های جدید بسیاری پیشنهاد شده‌اند که به دنبال استفاده از همه قابلیت‌های زنجیره‌بلوکی و رفع نقایص موجود در بیت‌کوین و اتریوم هستند. چند نمونه از این پروژه‌ها عبارتند از: NEO است که به عنوان اولین پلتفرم متن‌باز غیرمتمرکز، در چین معرفی شده است و در حال حاضر از حمایت مدیرعامل Alibaba برخوردار است [۵۰]. در رقابت برای سرعت بخشیدن به اینترنت اشیاء، برخی از توسعه‌دهندگان استفاده از زنجیره‌بلوکی را پیشنهاد کرده‌اند که موجب بوجود آمدن IOTA شد. هزینه انجام تراکنش در شبکه را به صفر رسانده و فرآیندهای تأیید منحصر به فردی را ارائه دهد. همچنین در IOTA تلاش شده است که مشکل مقیاس‌پذیری در بیت‌کوین نیز حل شود [۵۱]. علاوه بر NEO و IOTA، پلتفرم‌های دیگری همچون Monero [۵۲]، [۵۳]، و [۵۴]، به عنوان راه‌حلی برای مشکلات مربوط به امنیت و مقیاس‌پذیری زنجیره‌های‌بلوکی نسل اول و دوم پیشنهاد شدند. این سه پلتفرم زنجیره‌بلوکی در هنگام انجام معاملات به دنبال حفظ سطح بالای امنیت و حریم خصوصی هستند. ادامه این مقاله اینگونه سازمان‌دهی شده که در بخش دوم مفاهیم اساسی زنجیره‌بلوکی بیان خواهند شد. در بخش سوم زنجیره‌بلوکی نسل سوم و مباحث مربوط به آن توضیح داده شده‌اند. در بخش چهارم کاربردهای زنجیره‌بلوکی و معرفی چندین پروژه پیاده‌سازی شده در قالب پایان‌نامه‌های دوره کارشناسی ارشد در آزمایشگاه پردازش هوشمند داده، آورده شده است. در بخش پنجم به بیان مخاطرات و معایب اینگونه شبکه‌ها با ذکر چند نمونه اشاره شده است و در نهایت در بخش ششم مقاله جمع‌بندی می‌شود.

۲ مفاهیم اساسی

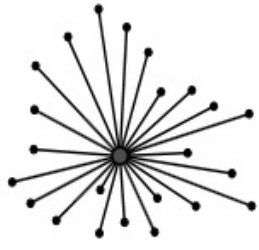
۱.۲ شبکه زنجیره بلوکی

زنجیره‌بلوکی چیست؟ پرسشی است که با پاسخ به آن تا حدودی می توانیم به دلایل اهمیت آن و کاربرد زیادش در حوزه‌های مختلف پی برد. وجود دارایی‌های دیجیتال و حفظ و نگهداری از آنها نیازمند بستری است که بتوان بر روی آن مبادله ارزش داشته باشیم، اعتماد را تا حد مطلوبی بدست آوریم و این فرآیندها را بر روی شبکه‌ای انجام دهیم که ذاتاً اعتماد را درون خود ایجاد کند و مکانیزم‌های اعتماد، درونش وجود داشته باشد و از درستی و صحت اطلاعات اطمینان لازم حاصل شود. محقق ساختن تمام این فاکتورها نیازمند استفاده از شبکه زنجیره‌بلوکی می‌باشد که دنیای غیرمتمرکزی را بوجود می‌آورد که سه خصوصیت ارزش، اعتماد و صحت درستی اطلاعات را فراهم خواهد کرد. نیازمندی به پایگاه داده در بسیاری از حوزه‌های موجود، بسیار روشن است. زیرا وظیفه آن ذخیره‌سازی و ثبت تمام اطلاعات و تراکنش‌های مهم می‌باشد. در خصوص پایگاه داده چند نکته حائز اهمیت است. پایگاه داده‌های سنتی از نوع متمرکز بوده و در آنها یک واحد مرکزی قوانین را کنترل می‌کند و برمبنای قوانین کنترلی توسط آن واحد (فرد)، ثبت و ضبط داده‌ها در پایگاه انجام می‌شود. نکته حائز اهمیت در این نوع از پایگاه‌های داده این است که واحد مرکزی می‌تواند با توافق‌های غیرمجاز قوانین را تغییر دهد و در اطلاعات ذخیره شده، تغییرات دلخواهی را ایجاد کند. همچنین، ایجاد اینگونه تغییرات می‌تواند هرگز آشکار نشود و در صورت آشکار شدن توانایی برای اثبات و اصلاح آن برای دیگران وجود نداشته باشد؛ زیرا در این نوع پایگاه داده قدرت به طور کامل در اختیار واحد مرکزی است. این در حالی است که زنجیره‌بلوکی پایگاه داده توزیع‌شده است (شکل ۱). با به چالش کشیدن پایگاه داده سنتی، زنجیره‌بلوکی می‌تواند جایگزین بسیار

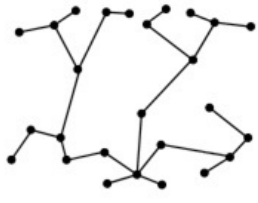


شکل ۱: *ساختار شبکه توزیع شده*

مناسبی برای آن باشد. به عبارتی زنجیره‌بلوکی، پایگاه داده توزیع‌شده است و تلاش می‌کند مشکلات پایگاه داده سنتی را برطرف کند. از جمله تفاوت‌های آن با پایگاه داده متمرکز می‌توان به حذف قدرت واحد مرکزی اشاره کرد. پایگاه داده‌ای توزیع‌شده است که تمام گره‌هایی که عضو شبکه می‌شوند می‌توانند یک نسخه از اطلاعات را در اختیار داشته باشند و این ساختار امکان ایجاد تغییرات در شبکه را از بین خواهد برد. از طرفی دیگر در طراحی زنجیره‌بلوکی دو نوع مکانیزم تعریف شده‌اند که مکانیزم اول مربوط به تایید اطلاعات است که باعث ایجاد اطمینان و اعتماد در شبکه می‌شود و نیازمندی به قدرت کنترل‌کننده مرکزی را از بین می‌برد. اعضای شبکه با کنترل‌هایی که بر روی شبکه انجام می‌دهند، می‌توانند صحت اطلاعات را بررسی کنند. مکانیزم دوم، مربوط به رمزنگاری و زمان‌بندی می‌باشد. از این طریق امکان هک، تغییر و حذف اطلاعات ثبت شده تقریبا از بین می‌رود. مطابق شکل‌های ۲ و ۳ در راستای بیان تفاوت‌های سیستم‌های متمرکز و



شکل ۲: *گراف سیستم متمرکز*



شکل ۳: *گراف سیستم غیرمتمرکز*

غیرمتمرکز می‌توان عنوان کرد که سیستم‌های متمرکز دارای چالش‌های بوده و دارای یک نقطه شکست هستند. به عبارتی امکان تبانی در آنها وجود دارد و هزینه‌های غیرقابل قبولی برای ساخت شبکه متمرکز صرف می‌شود. اما در زنجیره‌بلوکی که غیرمتمرکز بودن از مهم‌ترین ویژگی آن است، گره‌های مختلف می‌توانند با یکدیگر تبادل اطلاعات را انجام

دهند و اختیاراتی مشابه یکدیگر دارند. همچنین قدرت مرکزی از بین رفته و به واسطه غیرمتمرکز بودن، شفافیت در شبکه وجود دارد به طوریکه اطلاعات به واسطه‌ی آن مدیریت شده و ضعف‌های سیستم‌های متمرکز حذف خواهند شد. غیرمتمرکز بودن نسبت به متمرکز بودن دارای مزایایی است که برخی از آنها عبارتند از:

(آ) مقاومت در برابر خرابی به خاطر افزونگی ایجاد خواهد شد. این بدان معنی است که اگر چندین گره در شبکه از بین بروند عملکرد شبکه مختل نخواهد شد.

(ب) مقاومت در برابر حملات و تبانی افزایش خواهد یافت. زمانی یک حمله در سیستم زنجیره‌بلوکی می‌تواند موفق باشد که حمله‌کنندگان به سیستم حداقل ۵۱ درصد از شبکه را از آن خود کنند و بتوانند یک تبانی بزرگ را در سطح ۵۱ درصد شبکه یا بیشتر بوجود آورند و این یک قابلیت بسیار مطلوب برای این نوع شبکه است. به دلیل اینکه بدست آوردن حداقل ۵۱ درصد توان پردازشی شبکه در عمل غیرممکن است و احتمال آن نزدیک صفر است تبانی در این نوع شبکه‌ها امری غیرممکن است.

(پ) عدم نیاز به مکانیزم متمرکز اعتماد و در نتیجه کاهش هزینه‌ها. به دلیل نوع ساختار زنجیره‌بلوکی ایجاد یک واحد مرکزی نظارتی خارج از شبکه وجود ندارد. مکانیزم آن را به گونه‌ای طراحی کرده‌اند که می‌توان به داده‌هایی که شبکه غیرمتمرکز ثبت می‌کند، اعتماد کرد و چون در این مکانیزم، واحد مرکزی وجود ندارد کاهش هزینه‌ها را به همراه دارد.

مزایای بیان شده برای سیستم‌های غیرمتمرکز طراحان و توسعه‌دهندگان را به طراحی سیستم‌های غیرمتمرکز ترغیب خواهد کرد. به همین منظور به بیان توضیح مختصری در مورد انواع این سیستم‌ها پرداخته شده است. سیستم‌های غیرمتمرکز را می‌توانیم به دو دسته تقسیم کنیم. دسته اول سیستم‌های غیرمتمرکز از نظر معماری و ساختاری هستند. این در حالی است که این نوع از سیستم‌های غیرمتمرکز از نظر مدیریت، متمرکز هستند مانند گوگل که در سرتاسر جهان سرورهایش وجود دارند اما قدرت نظارتی و مرکزی آن یکسان است. در مقابل دسته دوم سیستم‌هایی هستند که از نظر مدیریت و کنترل غیرمتمرکز بوده و موجودیت کنترل‌کننده سیستم بیش از یک کاربر است که زنجیره‌بلوکی در

این دسته قرار دارد [۱۱].

۲.۲ تاریخچه زنجیره‌بلوکی

ایده‌ی اولیه زنجیره‌بلوکی در شبکه بیت تورنت مطرح شد و در واقع این ایده در رابطه با انتقال فایل بدون سرور بود که تاریخچه آن به اوایل دهه ۱۹۹۰ برمی‌گردد [۲۴]. بعد از آن با پیاده‌سازی همین ایده در بیت‌کوین و انتقال پول بدون بانک، فناوری زنجیره‌بلوکی به شکل کاربردی مورد استفاده قرار گرفت. در این حالت از طریق یک شبکه غیرمتمرکز، بدون ناظر و دخالت بانک‌ها که خود نوعی سیاست‌گذار مالی به شمار می‌آیند، می‌توان انتقال پول را همراه با اعتماد کافی به آن شبکه انجام داد [۴۷]. اما برای بیان جزئی‌تر تاریخچه زنجیره‌بلوکی می‌توان گفت در سال ۱۹۹۱ یک مقاله کنفرانسی توسط افرادی به نام استورات هابر و اسکات استورنتا تحت عنوان "چگونه می‌توان مانع جعل اطلاعات دیجیتال شد؟" ارائه شد و در این مقاله فناوری زنجیره‌بلوکی معرفی شد. [۴۹]. اولین کار آنها شامل یک زنجیره‌بلوکی دارای رمزنگاری امن بود که به موجب آن هیچ کس نمی‌توانست در زمان‌بندی اسناد دست‌کاری کند. در این نسخه پیشنهادی، اطلاعات به شکل بلوک‌های رمزنگاری شده به یکدیگر متصل می‌شدند. افزودن اطلاعات جدید در یک قالب ایجاد یک بلوک جدید انجام می‌شد که از طریق پیوندهای رمزنگاری شده به اطلاعات قبلی متصل بود و این پیوند از هرگونه تغییری در اطلاعات گذشته جلوگیری می‌کرد. به طورکلی زنجیره‌بلوکی یک دفترکل توزیع‌شده است که در یک شبکه همتابه همتا فعالیت می‌کند و هدف کلی آن ثبت تراکنش‌ها می‌باشد. محتویات دفترکل با افزودن یک بلوک جدید که به بلوک قبلی مرتبط است به‌روزرسانی می‌شود. زنجیره‌بلوکی، زنجیره‌ای از بلوک‌های رمزنگاری شده برای حفاظت از اطلاعات می‌باشد.

۳.۲ ظهور بیت کوین

در سال ۲۰۰۸ فردی با نام مستعار ساتوشی ناکاماتو با استفاده از فناوری زنجیره‌بلوکی، پول دیجیتال امروزی به نام بیت‌کوین را ارائه کرد. بیت‌کوین اولین فناوری است که با ظهورش زنجیره‌بلوکی را که تاکنون سه نسل از آن ظهور کرده را به کار گرفت و باعث شناخته شدن این فناوری شد. بیت‌کوین اولین رمزارز شناخته شده دنیا می‌باشد که با ارائه

مقاله‌ای در سال ۲۰۰۹ با عنوان "بیت‌کوین یک سیستم نقدی الکترونیکی همتا به همتا" به دنیا معرفی شد [۴۷]. می‌توان گفت بیت‌کوین واحد پولی است که با وعده رهایی از سیستم‌های بحران‌ساز متمرکز مالی متولد شده است. دلیل اصلی ظهور بیت‌کوین را می‌توان با داشتن نگاه اجمالی به تاریخچه پول شفاف‌سازی کرد. در ابتدای تاریخچه پول مبادلات براساس قوانین غیررسمی صورت می‌گرفت. بعد از آن براساس سکه‌هایی که به وجود آمده انجام پذیرفت و سپس براساس پول‌های کاغذی. سیستم‌های مرکزی برای تضمین مبادلات مالی ایجاد شدند که جعلی نبودن، دارای پشتوانه بودن، رسمیت داشتن و معتبر بودن پول‌های موجود را بررسی کنند به طوریکه این موسسات رسمی به مرور زمان بانک‌ها نام گرفتند. به مرور زمان و با پیشرفت فناوری در نهایت تجارت برخط بوجود آمد که امروزه بسیار پرکاربرد است. تجارت برخط نیز زیرنظر بانک‌ها و موسسات مالی صورت می‌گیرد و آنها تمام تراکنش‌ها و مبادلات مالی را کنترل خواهند کرد. در تمام این موارد یک سیستم مرکزی وجود دارد که کنترل سیستم مالی را برعهده دارد و همچنین می‌تواند بر بسیاری از نوسانات مالی نیز تاثیرگذار باشد. حال می‌توان به راحتی به این سوال پاسخ داد که چرا بیت‌کوین بوجود آمد؟ دلیل اصلی ظهور بیت‌کوین را می‌توان به عنوان راه‌حلی برای رفع مشکلات موجود در آن زمان بیان کرد. اینکه افراد جامعه به عنوان سرمایه‌گذاران سیستم مالی اطلاعی از اینکه قرار است چه اتفاقی برای سرمایه هایشان رخ دهد، ندارند. همچنین سیستم نظارت‌کننده مرکزی آنها را با یک عدم قطعیت روبرو کرده است. خلق یک سیستم که واسطه‌ها را حذف کند و عدم قطعیت را به حداقل برساند می‌تواند یک راه‌حل مناسب برای رفع این مشکل باشد که در نتیجه قدرت مرکزی یا همان بانک‌ها را به عنوان واسطه‌ها حذف خواهد کرد. بیت‌کوین خلق شد تا با ایجاد یک شبکه غیرمتمرکز، قدرت متمرکز سیستم‌های رسمی را به چالش بکشد و واسطه‌ها را حذف کند. اینکار نیازمند وجود یک مکانیزم نظارتی مناسب است که بتواند اعتماد ایجاد کند، مبادلات مربوط به داده‌ها و تراکنش‌ها بتوانند توسط آن به خوبی ثبت شوند و همچنین دارایی‌های سرمایه‌گذاران به چالش کشیده نشود. در اینجا چه اتفاقاتی ممکن است پیش آید؟ جعل کردن و چندبار خرج کردن پول از دسته اتفاقات غیرقانونی است که ممکن است در این سیستم رخ دهد. این در حالی است که در سیستم‌های متمرکز به وقوع پیوستن این رخدادها غیرممکن می‌باشند. برای مثال اگر در یک کارت بانکی مبلغ

مشخصی وجود دارد تمام آن مبلغ را نمی‌توان در دو محل مختلف خرج کرد. اما در دنیای دیجیتال این اتفاق ممکن است و سیستم بیت‌کوین شبکه را از این قبیل اتفاقات ایمن نگه خواهد داشت. در نتیجه ایجاد امنیت ویژگی مهمی در اینگونه سیستم‌ها می‌باشد که در سیستم‌های متمرکز از طریق بانک مرکزی محقق می‌شود. این در حالی است که در سیستم‌های غیرمتمرکز هدف دستیابی به سیستمی است که با حذف بانک‌ها همچنان بتوان به امنیت قابل قبولی دست یافت. ایجاد تورم و چالش‌های اقتصادی از دسته مشکلاتی است که بانک‌ها می‌توانند ایجاد کنند و به همین دلیل جوامع درصدد حذف آنها برآمدند [۱۸]. به بیانی دیگر بیت‌کوین را می‌توان یک نظام بانکی بدون بانک تعریف کرد. به بیت‌کوین نباید فقط از دیدگاه یک رمز ارز نگاه کرد بلکه یک سیستم بانکی بدون بانک است. این شبکه تمام فعالیت‌های یک نظام بانکی را برعهده می‌گیرد بدون اینکه بانک مرکزی وجود داشته باشد. در این شبکه مکانیزمی وجود دارد که می‌تواند امنیت، شفافیت، اعتماد و نظارت را به طور همزمان و هر آنچه که در یک نظام پولی نیاز است را به همراه داشته باشد. بیت‌کوین بر بستر زنجیره‌بلوکی می‌باشد و با آن یکی نمی‌باشد بلکه فقط از فناوری آن استفاده کرده است. خصوصیت‌های کلیدی بیت‌کوین را می‌توان به شرح زیر نام برد:

(آ) عدم نیاز به اعتماد به شخص سوم در شبکه همتا به همتا.

(ب) عرضه محدود بدون تورم. در سیستم بیت‌کوین تعداد ۲۱ میلیون سکه تعریف شده است که این تعداد ثابت می‌تواند ضد تورم باشد.

(پ) عدم امکان تقلب و انتشار پول جعلی.

(ت) دفترکل شفاف همراه با حفظ محرمانگی. در زنجیره‌بلوکی شبکه همتابه همتا، به گروهی از دستگاه‌ها یا گره‌ها گفته می‌شود که از طریق اینترنت به یکدیگر متصل هستند و ساختاری توزیع‌شده دارند. همچنین در این شبکه، سرور مرکزی وجود ندارد و هر گره یک نسخه کامل از تمام فایل‌های به اشتراک گذاشته شده در اختیار دارد [۸].

۴.۲ اتریوم

نسل اول زنجیره‌بلوکی از سال ۲۰۰۹ با انتشار مقاله سفیدش به همگان معرفی شد و تا سال ۲۰۱۳ تکامل پیدا کرد. بعد از آن در خلال سال‌های ۲۰۱۳ تا ۲۰۱۵ نسل دوم زنجیره‌بلوکی در قالب شبکه اتریوم بوجود آمد. اتریوم فراتر از یک رمزارز است. می‌توان گفت مانند یک کامپیوتر توزیع شده عمل می‌کند و امکان انجام برخی عملیات از جمله نوشتن برنامه و اجرای آن را بر روی شبکه اتریوم فراهم می‌کند. تولد اتریوم با قابلیت‌های بیشتر در مقایسه با بیت‌کوین در سال ۲۰۱۳، یکی از رویدادهای مهم در تاریخچه زنجیره‌بلوکی است [۹].

۵.۲ دفترکل توزیع شده

در حالت کلی برای بیان فناوری زنجیره‌بلوکی باید به سه سوال اساسی پاسخ داده شود که با پاسخ به آنها می‌توان این فناوری را شفاف‌تر معرفی کرد و بتواند جایگزین سیستم‌های سنتی شود. سه پرسش اساسی عبارتند از:

- چگونه این فناوری واسطه‌ها را حذف می‌کند؟
- اعتماد چگونه در این بستر بوجود می‌آورد؟
- چگونه این فناوری دنیا را غیرمتمرکز می‌کند؟

معرفی دفترکل توزیع‌شده می‌تواند مقدمه‌ای برای پاسخ به این سوالات باشد. دفترکل توزیع‌شده در سیستم‌های سنتی در فایل اکسل موجود می‌باشد و دارای اطلاعات لازم می‌باشد که به آن دفترکل دیجیتال یا همان پایگاه داده گفته می‌شود. مشکل سیستم‌هایی از جمله بانک این است که به دلیل اینکه دارای قدرت مرکزی هستند به اطلاعات دسترسی کامل دارند و می‌توانند قدرت را از مشترکین بانک بگیرند و از آنها بهره‌گیری کرده و در نهایت هر گونه درخواستی را از آنها داشته باشند. در سیستم بانکی دفترکل متمرکز بانک، مرجع حل اختلافات است و هر اطلاعات و قوانینی را که بانک‌ها ثبت کنند همه اعضا می‌بایست از آن تبعیت کنند. یکی از راهکارها برای حذف بانک و سیستم‌هایی که دفترکل آن‌ها متمرکز است استفاده از زنجیره‌بلوکی و تبدیل دفترکل آنها به دفترکل توزیع

شده است. در این راستا لازم است که هر کدام از گره‌ها و اعضای شبکه یک نسخه از دفترکل را برای خودشان داشته باشند و همه‌ی اعضا تمام تراکنش‌های انجام شده در شبکه را ثبت کنند. اما ممکن است اختلاف حساب‌هایی بوجود بیاید که در این صورت برای حل اختلافات مربوط به تراکنش‌ها از مکانیزم اجماع استفاده می‌شود. مکانیزم اجماع در حالت کلی، براساس رای بیش از پنجاه درصد از اعضای شبکه است. برای رفع هر گونه اختلاف، رای‌ی که بیش از نیمی از اعضا در مورد آن اتفاق نظر داشته باشند، رای نهایی خواهد بود. از این رو، هر تراکنشی که بخواهد در شبکه ثبت شود باید حداقل توسط ۵۱ درصد از کل اعضای شبکه تایید شود. در این صورت آن تراکنش می‌تواند در بلوک‌های جدید ایجاد شده در زنجیره‌بلوکی ذخیره شوند [۵۵].

۶.۲ اجماع

سازوکار اجماع، زیربنای اعتماد در زنجیره بلوکی است. این در حالی است که در این نوع از سیستم‌ها واسطه‌ها حذف شده و با به کاربردن مکانیزم اجماع می‌توان اعتماد را ایجاد کرد. به زبان ساده می‌توان گفت اجماع یعنی همه کسانی که یک نسخه از زنجیره‌بلوکی را دارند، در مورد تراکنش‌های موجود در شبکه به توافق برسند. تمام دفترکل‌هایی که در گره‌های شبکه وجود دارند باید دارای اطلاعات یکسانی باشند. یکی از مواردی که در این راستا نقش مهمی دارد، گواهی انجام کار است. گواهی انجام کار شامل حل کردن معماهای پیچیده‌ای است که یکی از اهداف آن کنترل زمان است. اینکار با طراحی مساله‌ای سخت یا همان معمای پیچیده انجام می‌شود و هر فردی که آن مساله را حل کند، این مجوز را دارد که بلوکی جدید را به زنجیره‌بلوکی اضافه کند. در ضمن این فرآیند، اطلاعات تراکنش‌های شبکه به صورت رمزنگاری شده به یکدیگر متصل شده و تغییر یا حذف آنها در عمل غیرممکن خواهد بود. هر گره با حل مساله ریاضی اثبات می‌کند که چه مقدار کار انجام داده و با این کار تعهد خود را به سیستم و گره‌های دیگر نشان می‌دهد و از این طریق، دیگران به او اعتماد می‌کنند. در حالت کلی مکانیزم اجماع شامل سه رکن اساسی رمزنگاری، ساختار همتا به همتا و اثبات کار می‌باشد. ساختار همتابه همتا به گروهی از دستگاه‌ها گفته می‌شود که از طریق اینترنت به یکدیگر متصل هستند و ساختاری توزیع‌شده دارند و در چنین شبکه‌هایی سرور مرکزی وجود ندارد. اثبات کار نیز در واقع

مکانیزمی است که به شبکه‌ای غیرمتمرکز اجازه می‌دهد تا به اجماع و توافق برسند [۹].

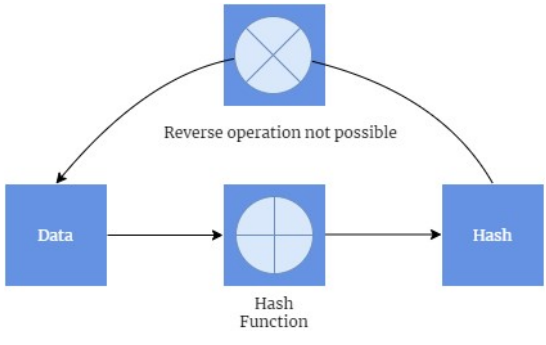
۷.۲ دفترکل‌های توزیع شده چگونه کار می‌کنند

زنجیره‌بلوکی از بلوک‌های متعددی تشکیل شده است که هر کدام از آنها حجم مشخصی از اطلاعات را در خود جای داده و دارای یک هش مخصوص به خود می‌باشند که شامل اطلاعات بلوک به همراه هش بلوک قبلی است. به دلیل اینکه در محاسبه‌ی هر هش، هش بلوک قبلی نیز دخالت دارد بلوک‌های شبکه به یکدیگر زنجیر خواهند شد و زنجیره‌بلوکی شکل خواهد گرفت. همچنین بلوک اول که به آن بلوک جنسیس یا بلوک آفرینش گفته می‌شود هش بلوک قبلی برای آن صفر درنظرگرفته می‌شود چون بلوکی قبل از آن وجود ندارد. یکی از اصلی‌ترین خصوصیت‌های زنجیره‌بلوکی عدم امکان تغییر در اطلاعات ذخیره شده در آن می‌باشد. دلیل اصلی آن این است که اگر فردی بخواهد اطلاعات بلوکی را تغییر دهد هش آن بلوک نیز تغییر خواهد کرد و در نتیجه به دلیل زنجیره بودن بلوک‌ها به یکدیگر باید بتواند هش بلوک بعدی را نیز تغییر دهد و به همین ترتیب تا انتهای زنجیره هش بلوک‌ها باید تغییر داده شوند. این در حالی است که به دلیل حل مساله ریاضی سخت و تعداد زیاد بلوک‌های شبکه، این کار بسیار زمان‌بر بوده و عملاً میسر است. در شبکه بیت‌کوین میانگین مدت زمانی که طول می‌کشد تا مساله ریاضی مورد نظر حل شود، حدود ده دقیقه است و کاربری که قصد تغییر اطلاعات بلوکی را دارد باید بتواند تا قبل از ایجاد بلوک جدید در انتهای زنجیره‌بلوکی، تمام هش‌های بعد از بلوکی که میخواهد اطلاعاتش را تغییر دهد را دوباره ایجاد کرده تا هش‌های ایجاد شده با یکدگیر مطابقت داشته باشند. این فعالیت در واقع غیرممکن است زیرا مدت زمانی که برای ایجاد هش‌های بعد از بلوک موردنظر نیاز است بسیار بیشتر از ده دقیقه است و این در حالی است که به دلیل رشد دائمی زنجیره فقط ده دقیقه برای اینکار فرصت باقی است.

۸.۲ توابع هش

توابع هش یا توابع درهم ساز، توابعی یکطرفه هستند که اطلاعاتی را که به آنها داده می‌شود را با استفاده از تابعی پیچیده به یک خروجی خاص تبدیل می‌کنند. همانطور که در شکل ۴ آورده شده است نکات مهم در خصوص این توابع، دارا بودن طول ثابت در

خروجی و یک‌طرفه بودن آن‌ها است. یک‌طرفه بودن به این معنی است که خروجی‌های متفاوت حتما دارای ورودی‌های متفاوت می‌باشند. این توابع همچنین برگشت‌ناپذیراند. بدان معنی که از روی خروجی نمی‌توان به ورودی رسید. همچنین این توابع شبه اتفاقی هستند، به طوریکه با ایجاد یک تغییر کوچک در ورودی کل ساختار خروجی نیز تغییر خواهد کرد. برای رمزنگاری در شبکه‌های زنجیره‌بلوکی عموماً از توابع هش بسیار سریع که دارای محاسبه سریع هستند، استفاده می‌شود. زیرا تابع درهم‌ساز باید بتواند رشته درهم‌سازی شده را به سرعت تولید کند تا در کارایی سیستم اختلالی ایجاد نشود. یکتابودن خروجی نیز یکی دیگر از ویژگی‌های توابع هش می‌باشد به طوریکه به خروجی تابع هش اصطلاحاً اثر انگشت گفته می‌شود. زیرا برای هر ورودی، خروجی یکتا است. در ساختار زنجیره‌بلوکی، اطلاعات بلوک‌ها با استفاده از این توابع هش رمزنگاری شده و اگر کاربر مخربی بخواهد اطلاعات بلوک‌ها را تغییر دهد، مقدار تابع هش در خروجی تغییر خواهد کرد و به دلیل تاثیر مقدار هش بلوک‌ها در محاسبه هش یکدیگر، تمام بلوک‌های بعدی نامعتبر خواهند شد [۸].



شکل ۴: *عملکرد توابع هش*

۹.۲ اعتبار بلوک‌ها

همه‌ی بلوک‌های تولید شده توسط اعضای شبکه، معتبر نیستند. اعتبار یک بلوک، برمبنای قوانین زنجیره‌بلوکی تعیین می‌شود. یافتن بلوک معتبر کار سختی است که برعهده استخراج کنندگان شبکه است. استخراج‌کنندگان در واقع اثبات کار را انجام می‌دهند. برای یافتن بلوک معتبر، باید یک مساله سخت ریاضی حل شود. به عنوان مثال در شبکه

بیت‌کوین سختی این مساله به گونه‌ای تعیین می‌شود که به طور میانگین هر ده دقیقه، فقط یک بلوک معتبر استخراج شود. استخراج‌کنندگان در ازای این کار سخت، پاداش بلوک را دریافت می‌کنند.

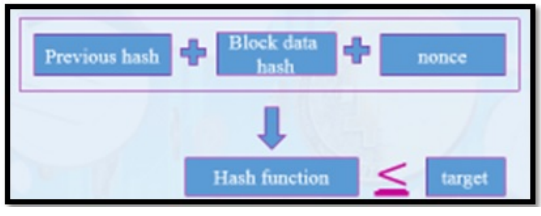
۱۰.۲ استخراج

به طور مختصر می‌توان گفت دستگاه‌هایی که عمل اثبات کار را انجام می‌دهند، دستگاه‌های استخراج نامیده می‌شوند. به آن دسته از اعضای شبکه که اثبات کار را انجام می‌دهند، استخراج‌کننده گفته می‌شود و وظیفه اصلی آنها تایید تراکنش‌ها می‌باشد. با حذف واسطه‌ها ایجاد اعتماد در زنجیره‌بلوکی وظیفه استخراج‌کنندگان است. به طوریکه بررسی وضعیت یک تراکنش بستگی به رای حداقل پنجاه و یک درصد از آنها دارد و نقش بسیار مهمی در شبکه‌های توزیع‌شده دارند. استخراج بیت‌کوین مشابه با استخراج طلاست با این تفاوت که طلا در معدن قرار دارد و بیت‌کوین در پروتکل شبکه. استخراج‌کنندگان با تولید بلوک‌هایی از تراکنش‌های معتبر و اتصال آنها به شبکه زنجیره‌بلوکی تعداد مشخصی بیت‌کوین به عنوان پاداش دریافت می‌کنند. در حال حاضر این تعداد ۲۵.۶ بیت‌کوین به ازای استخراج هر بلوک است. به طور کلی فرآیند استخراج، دو هدف را دنبال می‌کند: استخراج بیت‌کوین‌های (سکه‌های) و ایجاد اعتماد. فرآیند اعتماد به کاربران این اطمینان را می‌دهد که در این شبکه قدرت محاسباتی کافی برای استخراج بلوک‌ها و همچنین تایید تراکنش‌هایی صرف شده است. زمانی که برای تایید یک تراکنش در یک شبکه انرژی و زمان قابل توجهی صرف شود می‌تواند این اطمینان را به کاربران شبکه بدهد که هر تراکنشی در شبکه تایید نمی‌شود و اطلاعاتی که در بلوک‌های شبکه ذخیره شده‌اند صحیح می‌باشند و برای تایید آنها توسط استخراج‌کنندگان پردازش قابل توجهی انجام شده است [۲۰].

۱۱.۲ حل پازل استخراج

هر بلوک در شبکه زنجیره‌بلوکی دارای چندین پارامتر است که یکی از آنها نانس می‌باشد. در بلوک‌های استخراج نشده یافتن عدد نانس برعهده استخراج‌کنندگان است. خروجی هش هر بلوک نتیجه‌ی اعمال تابع هش بر روی مجموع اطلاعاتی از جمله تراکنش‌ها، عدد

نانس و هش بلوک قبلی است. این در حالی است که اطلاعات تراکنش‌ها و هش بلوک قبلی از مولفه‌های معلوم بوده و عدد نانس یک پارامتر نامعلوم است. مطابق شکل ۵ استخراج‌کنندگان شبکه برای استخراج بلوک جدید باید عدد نانس را به گونه‌ای بیابند که در نهایت هش خروجی از مقدار مشخصی کوچکتر باشد. به بیان دیگر می‌توان گفت براساس سختی تعریف شده در شبکه، یافتن نانسی قابل قبول است که بتواند تعداد مشخصی صفر را در ابتدای هش خروجی ایجاد کند. به دلیل اینکه تابع هش یکطرفه است یافتن چنین عددی کار بسیار دشوار و زمانبری است. به همین دلیل نیازمند قدرت پردازشی بالایی است و استخراج‌کنندگان برای یافتن عدد نانس انرژی بسیار زیادی را صرف خواهند کرد. ساختار زنجیره‌بلوکی در بیت‌کوین به گونه‌ای طراحی شده است



شکل ۵: *یافتن نانس قابل قبول*

که سختی شبکه به نحوی تنظیم شود که هر ده دقیقه یکبار عدد نانس صحیح توسط استخراج‌کنندگان یافت شود. این کار با انجام نوعی سعی و خطا و تغییر عددهای مختلف برای نانس انجام می‌شود و به همین دلیل به قدرت پردازشی بالایی نیاز است. این در حالی است که استخراج‌کنندگانی که دستگاه‌های آنها در اختیار شبکه هستند در صورتی که قیمت انرژی بالا رود و قیمت بیت‌کوین کاهش یابد ترجیح می‌دهند عملیات استخراج را برای مدتی متوقف کرده و دستگاه‌های خود را خاموش کنند. در این وضعیت مقدار سختی شبکه کاهش یافته و میزان پاداش تقسیمی بین استخراج‌کنندگان ناشی از استخراج بلوک افرایش می یابد. به این صورت است که شبکه به یک حالت تعادل خواهد رسید.

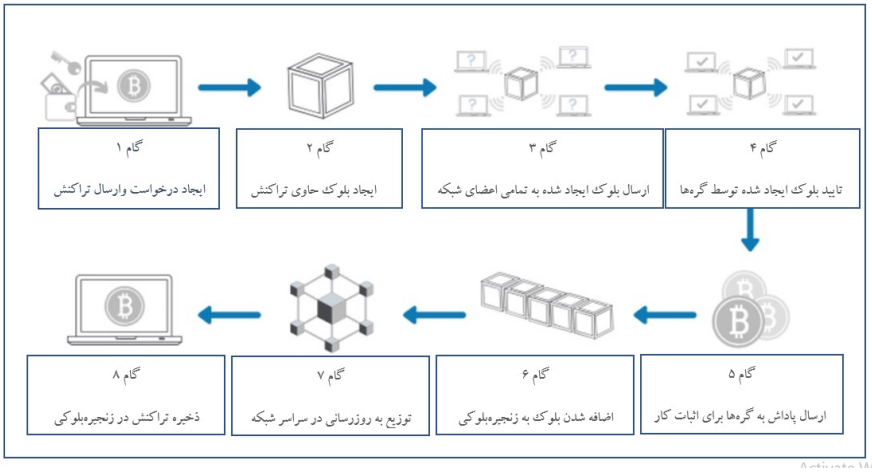
۱۲.۲ اثبات کار

مکانیزم‌های توافق، زیربنای اعتماد در شبکه‌های زنجیره‌بلوکی می‌باشند. راه‌حل اثبات کار دارای دو مرحله اصلی است. مرحله اول استخراج بلوک‌ها و تایید تراکنش‌ها که مساله

اصلی در شبکه‌های زنجیره‌بلوکی به حساب می‌آید را سخت می‌کند تا هر فردی که قصد تقلب را دارد این امکان برایش فراهم نباشد. مرحله دوم استفاده از علم رمزنگاری در زنجیره‌بلوکی است. به طوریکه در طراحی زنجیره‌بلوکی یکی از پارامترهای بلوک جدید هش بلوک قبلی تعریف شده است. مرحله سوم کنترل زمان است و به دلیل اینکه زمان زیادی در اختیار کاربران شبکه نیست، امکان تغییر بلوک‌های قبلی عملاً غیرممکن خواهد بود. با این سه مرحله می‌توان مساله اعتماد را در شبکه‌های زنجیره‌بلوکی ایجاد کرد. به طور خلاصه می‌توان گفت هر گره با حل مساله ریاضی یا همان اجرای اثبات کار این نکته را اثبات می‌کند که چه مقدار کار انجام داده است و در نتیجه با این فرآیند تعهد خود را نسبت به سیستم زنجیره‌بلوکی نشان داده و بنابراین دیگر اعضای شبکه به او اعتماد می‌کنند [۲۰].

۱۳.۲ ساختار فناوری زنجیره‌بلوکی

به طور مختصر می‌توان گفت فناوری زنجیره‌بلوکی زنجیر شدن اطلاعات است و در بیت‌کوین به عنوان اولین کاربرد عملی استفاده شده است. تمامی مراحل فرآیند ذخیره یک تراکنش در زنجیره‌بلوکی در شکل ۶ آورده شده است. مطابق این شکل در گام اول یک تراکنش توسط کاربری از شبکه ایجاد شده و به شبکه ارسال می‌شود. در این مرحله هنوز تراکنش در شبکه ذخیره نشده است. برای مثال، این تراکنش می‌تواند ارسال تعدادی بیت‌کوین به یک کاربر دیگر شبکه باشد. تراکنشی که به شبکه ارسال شد توسط استخراج‌کنندگان درون یک بلوک قرار می‌گیرد و بلوکی حاوی این تراکنش ایجاد خواهد شد این عملیات در گام دوم صورت می‌گیرد. در گام سوم بلوک ایجاد شده به تمامی اعضای شبکه ارسال می‌شود تا وضعیت آن براساس قوانین شبکه بررسی شود. ادامه این فرآیند در گام چهارم برای حالتی درنظر گرفته می‌شود که بلوک ایجاد شده توسط تعداد پنجاه درصد گره‌ها به اضافه یک گره تایید شود. گره‌های استخراج‌کننده‌ای که توان پردازشی خود را برای تایید بلوک و اطلاعات آن صرف می‌کنند این عملیات را به انگیزه‌ی خاصی انجام می‌دهند. انگیزه‌ی آنها پاداشی است که توسط شبکه به دلیل تایید بلوک به آنها داده می‌شود. در نتیجه در گام پنجم به گره‌های استخراج‌کننده از طرف شبکه پاداش معینی ارسال خواهد شد. بعد از آن در گام ششم هر بلوک به یک بلوک قبل و بعد از خود



شکل ۶: *فلوچارت یک تراکنش در زنجیره‌بلوکی*

متصل شده و در یک زنجیره تغییرناپذیر قرار می‌گیرد. به این صورت تراکنش‌ها به یکدیگر زنجیر شده و این شبکه زنجیره‌ای از بلوک‌ها یا زنجیره‌بلوکی نام می‌گیرد. بعد از اضافه شدن هر بلوکی به زنجیره‌بلوکی باید اطلاعات شبکه در که همه گره‌ها توزیع شده است به‌روزرسانی شود این عملیات نیز در گام هفتم صورت خواهد گرفت. و در نهایت بعد از این مراحل تراکنش در بلوکی از شبکه ذخیره خواهد شد و امکان تغییر و حذف آن در هیچ صورتی امکانپذیر نخواهد بود.

۱۴.۲ شرایط لازم برای استفاده از زنجیره‌بلوکی

استفاده از زنجیره‌بلوکی فقط محدود به استفاده در رمزارزها نیست، بلکه برای بررسی اینکه آیا در یک کاربرد خاص می‌توان از فناوری زنجیره‌بلوکی استفاده کرد یا خیر نیاز است که به چندین سوال پاسخ داده شود که به ترتیب مطرح خواهند شد. سوال اول اینکه: آیا به پایگاه داده نیاز داریم یا خیر؟ پاسخ به این سوال از آن جهت اهمیت دارد که در کاربردی که به پایگاه داده نیاز نباشد استفاده از زنجیره‌بلوکی معنایی نخواهد داشت. سوال دوم اینکه: آیا چندین نفر اجازه نوشتن در پایگاه داده را دارند؟ اگر در کاربردی نیاز به یک نفر باشد که اطلاعات را در پایگاه داده ثبت کند خود آن شخص تمام فعالیت‌ها و کنترل‌های لازم را انجام می‌دهد. اما اگر این وظیفه برعهده چندین نفر باشد باید به این سوال پاسخ

دهیم که سوال سوم خواهد بود که آیا نویسندگان ناشناس غیرقابل اعتماد هستند یا با هم تضاد منافع دارند؟ در صورت مثبت بودن پاسخ سوال چهارم مطرح می‌شود که آیا به شخص سوم اعتماد نداریم؟ در صورت اعتماد داشتن به شخص سوم نیازی به استفاده از زنجیره‌بلوکی نمی‌باشد اما در صورت مثبت بودن پاسخ به سراغ سوال پنجم خواهیم رفت که آیا سطح دسترسی کاربران بدون محدودیت است؟ در صورتی که دارای محدودیت باشد استفاده از این سیستم مفید نخواهد بود. در صورتی که بدون محدودیت باشد سوال ششم مطرح می‌شود که آیا در این کاربرد تغییرناپذیری و غیرقابل جعل بودن از کارایی مهم‌تر است؟ در ادامه روند پاسخ به سوالات مربوطه باید به این نکته دقت کرد که با جایگزینی یک پایگاه داده متمرکز با یک پایگاه داده غیرمتمرکز کارایی سیستم افت پیدا می‌کند. زیرا سیستم‌های متمرکز بسیار سریع‌تر هستند در حالیکه در سیستم‌های غیرمتمرکز فرایند گواهی اثبات کار را داریم که زمانبر بوده و می‌توان گفت نوعی کنترل‌کننده زمان می‌باشند. در نتیجه در صورت دارای اهمیت بودن تغییرناپذیری و غیرقابل جعل بودن نسبت به کارایی باید در نهایت به سوال آخر پاسخ دهیم که آیا تراکنش‌ها می‌توانند شفاف و عمومی باشند؟ که این یکی از ویژگی‌های اصلی زنجیره‌بلوکی است و در صورتی که نمی‌خواهیم تراکنش‌ها شفاف باشند به کاربردن زنجیره‌بلوکی مفید نخواهد بود اما در صورت مثبت بودن پاسخ می‌توانیم از آن در کاربرد مربوطه استفاده کنیم [۴۵].

۳ زنجیره بلوکی نسل دوم

اتریوم را می‌توان یکی از رقبای اصلی بیت‌کوین معرفی کرد و براساس شاخص اندازه بازار، بعد از بیت‌کوین به عنوان دومین رمزارز بزرگ دنیا شناخته شده است. اتریوم به عنوان ملکه ارزهای دیجیتال شهرت دارد و آن را نسل دوم زنجیره‌بلوکی معرفی می‌کنند. این در حالی است که بیت‌کوین به عنوان پادشاه رمزارزها و نسل اول آنها شناخته می‌شود. هدف اصلی اتریوم این بود که بتواند همه عملیات و فرایندها را غیرمتمرکز کند.

۱.۳ اتریوم چیست؟

در سال ۲۰۱۳ فردی به نام ویتالیک بوترین با ارائه مقاله سفیدی رمزارز اتریوم و پلتفرم آن را معرفی کرد [۴۴] و در سال ۲۰۱۴ برای رمزارز خود یک ICO یا به بیانی عرضه اولیه سهام را برگزار کرد [۳۰] برای برگزاری ICO اتریوم، از رمزارز بیت‌کوین استفاده شد و مبلغی حدود هجده و نیم میلیون دلار سرمایه اولیه جمع‌آوری شد. اتریوم را از یک منظر می‌توان یک رمزارز به شمار آورد که می‌توان آن را مورد مبادله قرار داد. از سویی دیگر یک پلتفرم برای ایجاد قراردادهای هوشمند و برنامه‌های غیرمتمرکز است که می‌توان آن را به عنوان پروژه‌ای برای ارائه‌ی یک سیستم کاملا یکپارچه و غیرمتمرکز به منظور توسعه نرم‌افزارهای کاربردی و انجام مبادلات معرفی کرد. واحد پول اصلی اتریوم، Ether است و کاربرد اصلی این دارایی در شبکه اتریوم در پرداخت هزینه تراکنش‌هاست. کوچکترین واحد اتریوم wei می‌باشد و هزینه تراکنش در شبکه اتریوم Gas نام دارد. شبکه اتریوم را همچنین ”یک کامپیوتر جهانی“ نیز نام‌گذاری کرده‌اند. این بدان معنی است که اتریوم یک کامپیوتر در مقیاس جهانی است و گره‌های پراکنده از سراسر دنیا منابع خود را در اختیار این کامپیوتر جهانی قرار می‌دهند تا قابلیت این را داشته باشد که بتواند کدهای قرارداد هوشمند را اجرا کند. در این مکانیزم به جای یک سرور متمرکز، یک سرور غیرمتمرکز وجود دارد که هر نوع برنامه‌ای را می‌توان بر روی آن اجرا کرد [۹].

۲.۳ تفاوت بیت کوین و اتریوم

بیت‌کوین یک پول مجازی همتا به همتا می‌باشد که هدف اصلی آن تسهیل فرآیند انتقال پول میان افراد مختلف بدون نیاز به واسطه است. در حالی که اتریوم یک کامپیوتر جهانی است که هدف آن حذف واسطه‌گری در زندگی بشر به پشتوانه هزاران کامپیوتر داوطلب در سراسر دنیاست. هدف طراح شبکه بیت‌کوین این بود که افراد بتوانند با استفاده از یک تنها CPU و به صورت غیرمتمرکز بیت‌کوین را در تمام دنیا استخراج کنند. این ساختار در راستای محقق ساختن هدف اصلی ساتوشی ناکاماتو خالق بیت‌کوین که”یک CPU در برابر یک حق رای ”است، طراحی شده بود. اما با آمدن دستگاه‌های ASIC برای استخراج، این هدف زیرپا گذاشته شد و در حال حاضر تقریبا فقط افرادی قادر به استخراج بیت‌کوین هستند که دارنده‌ی اینگونه دستگاه‌ها باشند. این نکته برای دنیای

رمزارزها یک خطر محسوب می‌شود و زنجیره‌بلوکی را به سمت متمرکزشدن پیش می‌برد و در نهایت تعداد زیادی بیت‌کوین را خواهیم داشت که به دست گروه خاصی می‌باشند که قدرت پردازشی سیستم آنها بیشتر از دیگر افراد شبکه است. این گونه کاربران شبکه قادرند هر زمان تمایل دارند تعداد زیادی بیت‌کوین را بفروشند و قیمت‌ها را کاهش دهند و هر زمان که تمایل دارند حجم زیادی بیت‌کوین را بخرند و قیمت‌ها را افزایش دهند. این عمل با هدف ساتوشی ناکاماتو در تعارض است. نحوه استخراج بیت‌کوین و اتریوم نیز با یکدیگر تفاوت دارد به گونه‌ای که بیت‌کوین قابل استخراج با دستگاه‌های ASIC می‌باشد در حالی‌که اتریوم غیرقابل استخراج با اینگونه دستگاه‌هاست و اصطلاحا proof-ASIC است و در بیشتر موارد با کارت گرافیک استخراج می‌شوند. تفاوت دیگر بیت‌کوین و اتریوم در اندازه بلوک آنهاست. در بیت‌کوین اندازه بلوک ثابت و در حدود یک مگابایت است و تقریبا هر ده دقیقه یکبار یک بلوک استخراج می‌شود اما در اتریوم اندازه بلوک متغیر است و تقریبا هر پانزده ثانیه یکبار یک بلوک استخراج می‌شود. در زنجیره‌بلوکی مفهومی به نام مقیاس‌پذیری وجود دارد که سرعت شبکه را مشخص می‌کند. شبکه بیت‌کوین دارای مقیاس‌پذیری پایینی است، زیرا سرعت اجرای تراکنش‌ها و ثبت آنها در شبکه پایین است. ولی در شبکه اتریوم این مقیاس مقداری افزایش پیدا کرده است. این توسعه را ویتالیک بوترین با استفاده از بیان مفهومی به نام سه راهی مقیاس‌پذیری انجام داده است که برای اولین بار توسط خود این فرد مطرح شد. در این مفهوم سه ویژگی مقیاس‌پذیری، امنیت و عدم تمرکز وجود دارند که به طور همزمان فقط دو ویژگی محقق خواهند شد. در صورتی که شبکه بخواهد دو ویژگی عدم تمرکز و امنیت را بیشتر داشته باشد، مانند شبکه بیت‌کوین دارای سرعت پایینی خواهد بود و مقیاس‌پذیری را تا حدودی از دست خواهد داد. ویتالیک بوترین با استفاده از روشی به نام "شاردینگ" قصد داشت با حفظ امنیت و عدم تمرکز، مقیاس‌پذیری سیستم را نیز افزایش دهد. با تولد شاردینگ گویی راهی پیش روی توسعه‌دهندگان شبکه‌های زنجیره‌بلوکی باز شد تا همزمان با حفظ امنیت و تمرکززدایی، مقیاس‌پذیری پروژه‌های خود را نیز افزایش دهند. به بیان ساده شاردینگ به معنی تقسیم یک پردازش بزرگ به پردازش کوچکتر است. این روش راهکاری است که بار پردازشی را به قسمت‌های کوچکتر تقسیم می‌کند و به این طریق، ظرفیت و سرعت شبکه را افزایش می‌دهد. همچنین به لحاظ تِئوری می‌تواند با

کمترین هزینه، به چالش‌های مقیاس‌پذیری زنجیره‌بلوکی غلبه کند. در اتریوم نسل دوم از این فناوری استفاده خواهد شد و در این صورت سرعت تراکنش‌ها در آن افزایش می‌یابند. افزایش سرعت به گونه‌ای خواهد بود که شبکه اتریوم بتواند جایگزین شبکه‌های پرداختی فعلی مانند شبکه ویزا شود. شبکه ویزا شبکه‌ای است جهانی که ارائه دهنده‌ی خدمات مالی است و در حالت عادی پنج هزار تراکنش را در روز انجام می‌دهد [۵۶].

۳.۳ قرارداد هوشمند

مفهوم قرارداد هوشمند برای اولین بار در سال ۱۹۷۷ توسط فردی به نام نیک زابو دانشمند علوم کامپیوتر، حقوقدان و رمزنگار معرفی شد. هدف نیک زابو این بود که برای نگهداری از قراردادها از یک دفترکل توزیع‌شده استفاده کند [۳۴]. قراردادهای هوشمند مشابه با قراردادهای فیزیکی تعریف می‌شوند، با این تفاوت که دیگر به وجود واسطه و نقش آن در این نوع از قراردادها نیازی نیست. برای مثال، برای اجاره دادن یک منزل که دارای دو مالک است اگر از قرارداد هوشمند استفاده شود به صورت خودکار بعد از واریز اجاره منزل آن مبلغ به صورت خودکار به دو قسمت تقسیم شده و به حساب مالکان واریز خواهد شد و هیچ نیازی به وجود واسطه و اعتماد خاص بین اعضای آن نیست. این در حالی است که در قراردادهای سنتی به وجود یک واسطه قابل اعتماد مانند املاک نیاز است و فرآیند واریز اجاره بها و تقسیم شدن آن بین دو مالک زمان‌برتر از حالت قبل خواهد بود.

۴.۳ مزایای استفاده از قرارداد هوشمند

مشابه ویژگی‌های بیان شده برای زنجیره‌بلوکی، حذف واسطه یکی از ویژگی‌های کاربردی برای قراردادهای هوشمند است. در بسیاری از کاربردها از جمله قراردادهای پیمانکاری با حذف واسطه‌ها از بروز بسیاری از مشکلات ممانعت خواهد شد. عدم نیاز به اعتماد نیز دومین خصوصیت کاربردی و مهم مربوط به این دسته از قراردادها می‌باشد. قراردادهای هوشمند به دلیل اینکه بر روی زنجیره‌بلوکی اجرا می‌شوند، بسیاری از خصوصیت‌های این نوع از شبکه‌ها را به ارث می‌برند؛ شفافیت نیز یکی از این ویژگی‌هاست به گونه‌ای تمام اعضای شبکه می‌توانند مفاد قرارداد را بر روی شبکه مشاهده کنند. زمانی که برنامه یک قرارداد هوشمند نوشته می‌شود و بر روی زنجیره‌بلوکی منتشر می‌شود، این قرارداد غیرقابل

تغییر خواهد شد. این خصوصیت می‌تواند به طور همزمان یک مزیت و یک عیب برای قراردادهای هوشمند به شمار آید. برای مثال در صورتی که یک حفره امنیتی درون برنامه وجود داشته باشد امکان متوقف کردن و اصلاح آن وجود نخواهد داشت و تا همیشه بر روی زنجیره‌بلوکی باقی خواهد ماند [۳۹].

۵.۳ مراحل طراحی قرارداد هوشمند

در این بخش در رابطه با چگونگی نگارش قرارداد هوشمند و نحوه‌ی اجرای آن‌ها توضیح داده خواهد شد. همچنین در رابطه با اینکه شبکه اتریوم چگونه قراردادهای هوشمند را اجرا خواهد کرد و اینکه نقش استخراج‌کنندگان در اجرای یک قرارداد هوشمند چیست، مطالبی بیان خواهد شد. در این راستا، اولین قدم این است که طراح قراداد هوشمند به عنوان یک برنامه‌نویس به این نتیجه رسیده است که بستر شبکه اتریوم برای نوشتن و اجرای قرارداد هوشمند مربوطه مناسب است. برای ایجاد یک قرارداد هوشمند سه مرحله وجود دارد که عبارتند از :الف) نوشتن قرارداد هوشمند. ب) انتشار قرارداد هوشمند در شبکه اتریوم. ج) اجرای قرارداد هوشمند.

۱.۵.۳ نوشتن قرارداد هوشمند

در این مرحله در قدم اول برای نوشتن قرارداد هوشمند لازم است یک زبان برنامه‌نویسی انتخاب شود. زبان برنامه‌نویسی سالیدیتی معروف‌ترین و پرکاربردترین زبان برنامه‌نویسی در شبکه اتریوم و برای طراحی قراردادهای هوشمند به شمار می‌آید. با استفاده از این زبان برنامه‌نویسی قوانین به زبان کد بیان خواهند شد. هر قانونی که قرار است در قرارداد هوشمند اجرا شود به صورت توابعی به زبان کد در خواهند آمد. برای نمونه در مثال بخش قبل تقسیم شدن و واریز شدن اجاره منزل به حساب مالکان به توابعی از قرارداد هوشمند تبدیل خواهند شد که با استفاده از زبان برنامه‌نویسی سالیدیتی نگارش شده‌اند [۴۲].

۲.۵.۳ انتشار یک قرارداد هوشمند در شبکه اتریوم

در مرحله دوم قرارداد هوشمند نوشته شده در مرحله قبل باید در شبکه اتریوم منتشر شود. در شبکه اتریوم مفهومی از تراکنش که در شبکه بیت‌کوین نیز تعریف شده است به صورت

گسترده‌تر وجود دارد. در بیت‌کوین یک فرستنده و یک گیرنده وجود دارند که به همراه مبلغی رمزارز که انتقال داده خواهد شد در یک تراکنش آورده شده و مهم‌ترین اجزای یک تراکنش به حساب می‌آیند. اما در شبکه اتریوم اجزای اصلی عبارتند از یک ارسال کننده قرارداد هوشمند که همان نویسنده قرارداد هوشمند است و یک قرارداد هوشمند که باید بر روی شبکه اتریوم قرار بگیرد. در این شبکه فرستنده باید یک تراکنش را ایجاد کند و این تراکنش را به صورت کد قرارداد هوشمند که یک فایل می‌باشد داخل یک بلوک قرار داده و آن را به شبکه اعلام کند و شبکه نیز طبق همان مکانیزمی که در شبکه بیت‌کوین وجود دارد آن را از نظر اعتبار بررسی کند و اگر از طرف شبکه تایید شود در زنجیره‌بلوکی اتریوم ثبت خواهد شد. مشابه شبکه بیت‌کوین که یک تراکنش بر روی شبکه قرار می‌گیرد در شبکه اتریوم نیز یک قرارداد هوشمند بر روی شبکه قرار می‌گیرد. شبکه اتریوم نیز به این قرارداد هوشمند یک آدرس را نسبت می‌دهد و برای برقراری ارتباط با قرارداد هوشمند باید با آدرس آن تعامل برقرار کرد. علاوه بر تعریف آدرس برای یک قرارداد هوشمند مفهوم حافظه نیز در شبکه اتریوم برای اینگونه قراردادها تعریف شده است. اطلاعات مرتبط با قرارداد هوشمندی که در یک بلوک ثبت شده است باید در فضای حافظه ای که در همان بلوک تعریف شده ذخیره شود و این فضای حافظه به قرارداد هوشمند متصل خواهد شد. برای ثبت یک قرارداد هوشمند در شبکه اتریوم باید استخراج‌کنندگان بلوک مربوطه را استخراج کرده و در نتیجه قرارداد هوشمند در شبکه ثبت خواهد شد [۳۹].

۳.۵.۳ اجرای قرارداد هوشمند

در مرحله سوم باید به افراد مختلف اجازه داده شود که بتوانند کد قرارداد هوشمند و توابع مختلف تعریف شده در آن را اجرا کنند. با اجرای توابع قراداد هوشمند توسط کاربران، تراکنش‌هایی ایجاد شده و بر روی شبکه ارسال خواهند شد. این تراکنش‌ها در بلوک‌های بعد از بلوکی که قرارداد هوشمند در آن ثبت شده است قرار می‌گیرند و استخراج‌کنندگان تا زمانی که تراکنش‌های مربوط به این قرارداد هوشمند وجود داشته باشند برای استخراج آنها تلاش خواهند کرد. به طور کلی اجرای یک قرارداد هوشمند دارای مراحل زیر می‌باشند: الف) استخراج‌کنندگان کد قرارداد هوشمند را اجرا کرده و کاربران با اجرای توابع موجود در قرارداد هوشمند، تراکنش‌ها را ایجاد می‌کنند. ب)

استخراج‌کنندگان پایگاه داده و حافظه مرتبط با هر قرارداد را به روزرسانی می‌کنند. ج) استخراج‌کنندگان برای اجرای این کد قرارداد هوشمند کارمزد دریافت می‌کنند که در شبکه اتریوم به آن GAS گفته می‌شود [۳۹].

۶.۳ شبکه اتریوم

در شبکه اتریوم چندین مفهوم کلیدی و مهم وجود دارند که برای درک بهتر عملکرد شبکه اتریوم به بیان توضیحات مربوط به آنها پرداخته شده است.

۱.۶.۳ ماشین مجازی اتریوم EVM

ماشین مجازی(VM) برنامه‌ای است که به عنوان یک رایانه مجازی عمل می‌کند و می‌توان آن را یک رایانه فیزیکی واقعی معرفی کرد. عملکرد کلی آن به این صورت است که بر روی یک کامپیوتر چندین کامپیوتر مجازی ایجاد می‌کند و منابع آن را میان این ماشین‌های مجازی تقسیم می‌کند به صورتی‌که ماشین‌های مجازی به طور مستقل از یکدیگر عمل خواهند کرد [۴۲]. ماشین مجازی اتریوم [۱] نیز عملکردی مشابه دارد و به طورکلی می‌توان آن را یک نرم‌افزار معرفی کرد که قراردادهای هوشمند را اجرا می‌کند. در شبکه اتریوم نیاز به یک بستر برای اجرای کدهای قرارداد هوشمند است زیرا برای اجرای کدهای سالیدیتی به حافظه زیادی نیاز می‌باشد که باید به زنجیره‌بلوکی اتریوم اختصاص داده شود و امکان اجرای آنها بر روی فقط یک کامپیوتر وجود ندارد. در نتیجه به یک محیط مجزا به نام EVM که به صورت یک نرم‌افزار می‌باشد، نیاز است که کدهای قرارداد هوشمند را اجرا کرده و تغییرات لازم را در زنجیره‌بلوکی ذخیره کند. این بدان معنی است که نیاز است هر استخراج‌کننده یک نسخه از نرم‌افزار EVM را نصب نموده و بعد از آن کدهای سالیدیتی را اجرا کند [۱۱].

۲.۶.۳ حساب ها

در شبکه اتریوم دو نوع حساب با عنوان "با مالکیت خارجی" و "حساب قرارداد" تعریف می‌شوند. حساب‌های با مالکیت خارجی برای ذخیره و انتقال ارزش بکار می‌روند

[1] Ethereum Virtual Machine (EVM)

و همچنین با استفاده از کلیدهای خصوصی و عمومی قابل کنترل هستند و یک نهاد خارجی و فردی خاص صاحب آن حساب‌ها می‌باشد. اما برخی حساب‌ها برپایه قرارداد هوشمند هستند و با یک کد قرارداد منطبق هستند و برخلاف نوع حساب با مالکیت خارجی بوسیله کد کنترل خواهند شد نه کلیدهای خصوصی و عمومی کاربر [۲۵].

۳.۶.۳ حالت شبکه اتریوم

به مقدار تمام متغیرهای سیستم کامپیوتری که همه گره‌های شبکه بر روی آن توافق نظر دارند حالت شبکه گفته می‌شود. این مقادیر شامل موجودی حساب‌ها، کدهای قرارداد هوشمند و داده‌های مربوط به آن قراردادها می‌باشند. هر تراکنش که توسط یک کاربر با یک قرارداد هوشمند ایجاد می‌شود، حالت شبکه را تغییر می‌دهد. همچنین استخراج‌کنندگان همیشه آخرین حالت شبکه را ذخیره می‌کنند. سیر مراحل مربوط به تغییر حالت شبکه به گونه ای است که با انتقال پول از حساب فرستنده به حساب گیرنده یک تراکنش صورت می‌گیرد. بعد از آن EVM با اجرای برنامه‌ها بر روی شبکه اتریوم حالت شبکه را تغییر می‌دهد. در این مرحله کد سالیدیتی بعد از کامپایل شدن به بایت کدهای اتریوم تبدیل می‌شود و توسط ماشین مجازی اتریوم اجرا می‌شود [۳۹].

۴.۶.۳ گس

انجام محاسبات موجود در قراردادهای هوشمند هزینه‌بر است. همانطور که در شبکه بیت‌کوین با مصرف انرژی برق الگوریتم اثبات کار توسط استخراج‌کنندگان شبکه اجرا می‌شود و برای انجام آن کارمزد دریافت می‌کنند، در شبکه اتریوم نیز عملکردی مشابه صورت خواهد گرفت. گس برای انجام محاسبات و حافظه‌ای است که استخراج‌کنندگان شبکه در حال استفاده از آن هستند. این در حالی است که اگر EVM به عنوان موتور محرک اتریوم درنظرگرفته شود گس را می‌توان به عنوان سوخت آن موتور محرک درنظر گرفت که باعث حرکت موتور یا همان اجرای قراردادهای هوشمند خواهد شد. استفاده از گس یک سری مزایا دارد که برخی از مهم‌ترین آنها عبارتند از: پرداخت کارمزد استخراج‌کنندگان، کاهش خطر حمله اسپم، جلوگیری از اجرای کدهای مخرب شبکه. حمله اسپم ارسال حجم انبوهی از تراکنش‌های بی‌فایده بر روی شبکه را گویند تا گره‌های

شبکه مشغول اجرای آنها شده و نتوانند برنامه‌های مفید شبکه را اجرا کنند. پرداخت هزینه یا همان گس برای هر تراکنش مانع از ایجاد اینگونه حملات توسط هر گره مخرب بر روی شبکه خواهد شد [۳۲].

۵.۶.۳ هک DAO

به عنوان یکی از مهم‌ترین پیشامدهایی که برای پروژه اتریوم به وقوع پیوسته است می‌توان به هک DAO اشاره کرد. ارائه ICO مربوط به پروژه اتریوم که در سال ۲۰۱۵ اتفاق افتاد، توانست مبلغ صد و پنجاه میلیون دلار سرمایه را جذب کند. اما قرارداد هوشمند نوشته شده دارای یک حفره برنامه‌نویسی بود که از طریق آن حدود یک سوم سرمایه‌های جمع‌آوری شده که مبلغ پنجاه میلیون دلار بود، به حساب کاربر مخرب انتقال داده شد. بعد از آن کاربران شبکه دو دسته شدند گروهی از کاربران بر این نظر بودند که پول سرقت شده باید برگردانده شود که این راه‌حل برخلاف قوانین حاکم بر شبکه‌های زنجیره‌بلوکی و ویژگی‌های ساختاری آن بود. در مقابل گروه دیگری از کاربران بر این نقطه نظر بودند که "کد قانون است" و شبکه باید به همین شکل به کار خود ادامه دهد. به دلیل همین اختلاف نظرها، کاربران شبکه اتریوم به دو دسته تقسیم شدند. عده‌ای از کاربرن فعالیت خود را در همان شبکه اتریوم قبلی ادامه دادند و آن شبکه اتریوم کلاسیک نام گرفت. این در حالی است که دیگر کاربران "کد قانون است" را قبول نداشتند و در نتیجه شبکه اتریوم فعلی را پذیرفتند [۱۷].

۴ کاربردهای زنجیره‌بلوکی

۱.۴ عرضه اولیه سکه

به عنوان یک نمونه از کاربردهای قرارداد هوشمند می‌توان به عرضه اولیه سکه یا ICO اشاره کرد. برای جمع‌آوری سرمایه در شروع استارت آپ‌ها، جمع سپاری را می‌توان به عنوان یک راه‌حل متمرکز معرفی کرد. این روش تمام ایرادات سیستم‌های متمرکز را دارا می‌باشند به همین منظور راه‌حلی برای غیرمتمرکز شدن جمع سپاری پیشنهاد شده است که برپایه استفاده از فناوری زنجیره‌بلوکی می‌باشد و ICO نیز در واقع نتیجه استفاده از این

فناوری است. به طور کلی ICO را می توان عرضه اولیه سکه بیان کرد به این صورت که بعد از ارائه پروژه یک رمزارز جدید و انتشار مقاله سفید مربوط به آن، توسعه‌دهندگان آن تاریخ مشخصی را برای ارائه سهام مربوط به آن پروژه اعلام کرده و آن را عرضه خواهند کرد. عرضه سهام اولیه پروژه جدید در قالب یک قرارداد هوشمند اجرا می‌شود به صورتی که این قرارداد در یک آدرس خاص نوشته شده و در زنجیره‌بلوکی ثبت می‌شود و سهام خود را به ازای تعداد مشخصی رمزارز به کاربران اختصاص خواهد داد. برای مثال اتریوم نیز با جمع‌آوری رمزارز از طریق بیت‌کوین سهام اولیه خود را عرضه کرد و توانست پروژه خود را توسعه دهد. بدون مرز بودن به منظور شرکت در پروژه‌های سرمایه‌گذاری، محدویت کمتر نسبت به ساختارهای متمرکز و نوآوری بیشتر به دلیل عدم وجود محدودیت‌ها را می‌توان از مزایای جمع سپاری غیرمتمرکز برشمرد [۴۰].

۲.۴ برنامه‌های غیرمتمرکز

یکی دیگر از کاربردهای قراردادهای هوشمند برنامه‌های غیرمتمرکز[۲] می‌باشند که بر بستر زنجیره‌بلوکی اجرا خواهند شد. اینگونه از برنامه‌ها کاربردهای زیادی در حوزه‌های مختلف دارند از جمله در انتخابات، موسسات مالی و بانک‌ها، بیمه‌ها، دولت‌ها، املاک، رسانه، خدمات سلامت، انجام مبادلات و غیره می‌توان از فناوری آنها استفاده کرد [۳۰]. برخی از این کاربردها در آزمایشگاه پردازش هوشمند داده پیاده‌سازی و اجرا شدند. برگزاری انتخابات یکی از این پروژه‌ها است که به هدف رفع مشکلات برگزاری رای‌گیری به شیوه سنتی پیاده‌سازی شد. شفافیت در آرا، هزینه کمتر، سادگی، اعتماد، امنیت بالا و حذف واسطه‌ها از فوائد سیستم‌های رای‌گیری مبتنی بر زنجیره‌بلوکی است. برگزاری انتخابات هیات ممیزه دانشگاه شهید باهنر کرمان در سال ۹۸ با استفاده از قراردادهای هوشمند بر روی شبکه‌های اتریوم نیز جز سوابق استفاده از این فناوری است. از دیگر پروژه‌های انجام شده با استفاده از فناوری زنجیره‌بلوکی در آزمایشگاه پردازش هوشمند داده می‌توان به استفاده از این فناوری در حوزه انرژی خورشید، خدمات سلامت و مدیریت و احراز هویت دیجیتالی اشاره کرد که در ادامه به بیان توضیحاتی در این رابطه پرداخته شده است.

[2] Decentralized Application (DAPP)

۱.۲.۴ انرژی خورشیدی

تولید برق از انرژی خورشیدی در اولویت‌های اصلی وزارت نیرو قرار دارد. نرخ خرید تضمینی برق از نیروگاههای خورشیدی بالاترین نرخ خریداری برق را در میان انواع نیروگاه‌ها به خود اختصاص داده است و سرمایه‌گذاری در این حوزه را توجیه‌پذیر نموده است. برای توسعه ملی در این حوزه، باید دانش و فناوری ساخت این نیروگاه‌ها در کشور بومی‌سازی شود. این موضوع تنها در صورتی ممکن خواهد بود که سرمایه‌گذار داخلی در پروژه تصمیم گیرنده باشد و رویکرد انتقال فناوری در آن وجود داشته باشد. یکی از بخش‌های اصلی در قرارداد بین وزارت نیرو و سرمایه‌گذاران نیروگاه‌های خورشیدی، بخش تعیین دانش فنی است و این بخش از عوامل موثر بر روی تعیین نرخ برق تولیدی است [۵۷]. در حال حاضر، فرآیندهایی که برای تعیین ضریب تشویق حاصل از دانش فنی استفاده شده در نیروگاه‌های خورشیدی به کار می‌روند، پرهزینه، زمانبر و دارای یک پایگاه داده متمرکز هستند. در این پروژه که به نگارش یک پایان‌نامه انجامید، اطلاعات و مدارک مربوط به تجهیزات فناوری و نیروگاه‌های انرژی خورشیدی مشمول ضریب تشویق به صورت غیرمتمرکز، امن و شفاف در شبکه زنجیره‌بلوکی ذخیره می‌شوند که قابل دستکاری نیستند. زنجیره‌بلوکی یک دفتر توزیع‌شده و غیرمتمرکز است که کار فرآیند ثبت تراکنش‌ها و ردگیري دارايي ها را براي يك شبكه‌ي كسب‌وكار ساده‌تر مي‌كند و در آن همه‌ی تراکنش‌ها به صورت برخط ثبت می شوند و برقراری ارتباط، ارسال یا تأیید تراکنش‌ها برای همه افراد امکان پذیر است [۲۲]، [۳۵]، [۴۳]. همچنین یک توکن غیرقابل تعویض بر اساس استاندارد ERC شماره ۷۲۱ رای امتیاز فناوری و ضریب تشویق تعیین شده برای تجهیزات فناوری و نیروگاه‌های خورشیدی ایجاد شده است. توکن مربوط به استاندارد ERC شماره ۷۲۱ را می‌توان به عنوان استانداردی تعریف کرد که نحوه ایجاد توکن‌های منحصر به فرد در زنجیره‌بلوکی اتریوم را توضیح می‌دهد [۲۱]. رابط استاندارد تعریف شده توسط استاندارد ERC شماره ۷۲۱، پیاده‌سازی قراردادهای هوشمند را قادر می‌سازد تا توکن‌ها را به شیوه‌ای منحصر به فرد، متناسب با دارایی رمزنگاری شده، مدیریت، مالکیت و معامله کنند. به استاندارد ERC شماره ۷۲۱ توکن‌های غیرقابل تعویض می‌گویند [۴۶]. پژوهشگاه نیرو برای صاحب فناوری و یا نیروگاه انرژی خورشیدی یک شناسه توکن منحصربه فرد را به همراه اطلاعات مورد نیاز برای ردیابی به

توکن پیوست می‌کند و توسط ساتبا اعلام می‌شود که باعث کاهش در هزینه‌ها، تسریع روند قراردادها، شفافیت و اطمینان، حذف واسطه می‌شود در نتیجه باعث تشویق بیشتر استفاده از دانش فنی در نیروگاه‌ها، افزایش تولیدات داخلی و اشتغال می‌شود [۳].

۲.۲.۴ خدمات سلامت

با توسعه فناوری زنجیره‌بلوکی و ویژگی‌های منحصر به فرد آن، این فناوری در بسیاری از بخش‌های تجارت، صنعت، معدن، بهداشت و غیره جایگاه ویژه‌ای پیدا کرده است. با توجه به حساسیت داده‌ها و سوابق پزشکی و اهمیت آن برای داشتن جامعه‌ای سالم، ما ملزم به مدیریت و نگهداری این داده‌ها به بهترین و مطمئن‌ترین شکل ممکن هستیم. فناوری زنجیره بلوکی تا حد زیادی به ما این امکان را می‌دهد که سامانه‌ای کامل، دارای امنیت و مناسب را برای بهداشت و درمان کشور داشته باشیم. سوابق پزشکی بیماران در مراکز بهداشت و درمان به صورت متمرکز و گاهی ناقص نگهداری میشوند. حدود ۸۶ درصد بیماران نگران امنیت سوابق پزشکی خود هستند. حدود یک چهارم آنها به دلیل احتمال افشای اطلاعات پزشکی خود این اطلاعات را در اختیار پزشکان قرار نمیدهند. با افزایش جرائم اینترنتی، سوابق پزشکی باید بیشتر محافظت شوند چراکه حاوی اطلاعات شخصی بیماران هستند [۳۶].

طبق تحقیقات انجام شده در مرجع [۲۶]، نشان داده شده است که ما هرساله شاهد افشای شمار زیادی از اطلاعات پزشکی هستیم. از طرفی دسترسی سریع و آسان به این سوابق در مواقع ضروری یا در کشوری دیگر امکان پذیر نیست [۳۱]. نگرانی عمده، مدیریت داده‌های پزشکی کلان است که هزینه‌ی گزافی به همراه دارد. از این رو پیش‌بینی شده است که در سال ۲۰۲۴ این هزینه به ۴۰ میلیارد دلار خواهد رسید [۵۸]. از طرفی حوادث و بلایای طبیعی نظیر (انفجار، سقوط هواپیما، سونامی و ...) در هر جای جهان و در هرلحظه امکان رخ دادن دارد و شمار زیادی قربانی به همراه خواهد داشت. لذا گروه مدیریت بحران پزشکی قانونی نیازمند دسترسی سریع به سوابق دندان‌پزشکی و آزمایشگاهی افراد برای شناسایی قربانیان است، چراکه شناسایی قربانیان حوادث یکی از مسائلی است که در حوزه حقوق بشر قرار می‌گیرد [۶]. بحث دیگر خود بیماران هستند. هر فرد حق دارد از اطلاعات پزشکی و روند معالجه خود اطلاع داشته باشد و خود او

تعیین کند که چه کسی اجازه‌ی دسترسی به این اطلاعات را داشته باشد. استفاده از فناوری زنجیره‌بلوکی این امکان را می‌دهد که یک سیستم مراقبت بهداشتی کامل داشته باشیم که توسط مرجع مرکزی مدیریت نمی‌شود و ضمن حفظ یکپارچگی داده‌ها، امنیت و شفافیت را تضمین کند. چنین سامانه‌ای برای یک جامعه سالم ضروری است ، بنابراین استفاده از فناوری زنجیره‌بلوکی برای ثبت اطلاعات پزشکی می‌تواند سیستم مراقبت‌های بهداشتی کشور را بهبود بخشد. در مرجع [۱] سیستمی مبتنی بر ذخیره غیرمتمرکز و یکپارچه سوابق پزشکی بیماران با استفاده از سیستم توزیع فایل همتابه‌همتا در شبکه زنجیره‌بلوکی به‌منظور دسترسی آسان و امن به این سوابق ارائه شده است. همچنین، دسترسی به سوابق پزشکی هر فرد و تبادل صحیح اطلاعات مابین افراد ذیربط (پزشکان، دندانپزشکان، آزمایشگاه‌ها، و مراکز پزشکی قانونی) با استفاده از قرارداد هوشمند اتریوم کنترل می‌شود. به‌علاوه، این سیستم پزشکی بیمار را قادر میسازد ضمن دسترسی سریع به اطلاعات پزشکی، نظر خود را به صورت امتیازدهی در خصوص هر یک از ارائه‌دهندگان خدمت (پزشک، دندانپزشک، آزمایشگاه) ثبت کند. این کار موجب رقابت سازنده و بهبود عملکرد خدمت میگردد. در این سیستم به منظور خدمات‌رسانی به بیمار، برای ارائه‌دهندگان خدمت در صورت تمایل ارائه‌دهنده، نوبت‌دهی برخط ایجاد شده است. در این سیستم بارگذاری سوابق پزشکی بیماران توسط ارائه‌دهنده خدمت و همچنین دسترسی به سوابق پزشکی و تعیین اجازه دسترسی افراد انتخاب شده توسط بیمار، برای ۵۰ بیمار آزمایش گردید. نتایج حاصله نشان میدهد در سیستم پیشنهادی بارگذاری سوابق پزشکی بیماران، همچنین دسترسی بیمار به این سوابق و بهره‌مندی از سایر خدمات طراحی شده برای بیمار، حدود چند ثانیه زمان میبرد. به علاوه، هزینه موردنیاز نیز بسیارکم خواهد بود.

۳.۲.۴ مدیریت و احراز هویت دیجیتالی

امروزه احراز هویت و مدیریت آن به جزء جدایی‌ناپذیری از زندگی افراد تبدیل‌شده است. هویت دیجیتالی تقریباً در همه‌ی سیستم‌های اطلاعاتی ویژه تأیید اعتبار و مجوز دادن ضروری است [۷]. درواقع هویت دیجیتالی را به‌عنوان اطلاعات الکترونیکی مرتبط با یک فرد در یک سیستم هویت خاص تعریف می‌کنند و از این سیستم‌های هویتی می‌توان برای احراز هویت و صدور مجوز استفاده کرد [۱۲]. در پایان‌نامه نگارش شده در این

حوزه، یک سیستم مدیریت و احراز هویت غیرمتمرکز مبتنی بر زنجیره‌بلوکی با استفاده از قراردادهای هوشمند ارائه شده است که شامل دو روش احراز هویت است. در روش اول، لایه اعتبارسنجی دوم برای امنیت بیشتر با کمک سیستم تشخیص چهره ایجاد شده است. در روش دوم با مقایسه خودکار اطلاعات مدارک کاربران نقش اشخاص ثالث کاهش و سرعت اعتبارسنجی افزایش داده شده است. همچنین در این روش به دلیل انتقال پایگاه‌های داده سازمانهای اعتبارسنج هویت به شبکه زنجیره‌بلوکی امنیت این پایگاه‌ها افزایش یافته است. همچنین طرح پیشنهادی به کاربران امکان می‌دهد هویت خودمختار داشته باشند، بطوریکه خود کاربر رضایت برای دسترسی و زمان دسترسی را برای به اشتراک‌گذاری برخی از اطلاعات مربوط به هویت خود را به سازمان‌های دولتی و خصوصی می‌دهد. نتایج حاصل از سیستم پیشنهادی نشان می‌دهد که کاربران و ارائه‌دهندگان خدمات می‌توانند مدیریت و احراز هویتی ایمن، قابل‌اعتماد، شفاف و با زمان و هزینهای کم را داشته باشند [۴].

۴.۲.۴ ثبت مدارک دانشگاهی

گواهی فارغ‌التحصیلی که بطور سنتی به شکل یک سند مبتنی بر کاغذ است به عنوان یک سند الکترونیکی می تواند به طور موثر جایگزین یک گواهینامه فیزیکی شود [۴۱]. با این حال، با توجه به تکنولوژی‌های پیشرفته و ارزان اسکن و چاپ، جعل گواهینامه‌ها افزایش یافته است [۳۸].

بنابراین، اعتبارسنجی و تأیید صحت اسناد، وظایف مهمی است. لازم است تأیید شود که گواهی فارغ التحصیلی که توسط فارغ التحصیل ارائه شده است، واقعی و دارنده صاحب قانونی آن اثر است. علاوه بر این، یک گواهی فارغ التحصیلی باید تأیید شود تا اطمینان حاصل شود که محتوای آن صحیح است و گواهی از یک منبع معتبر است [۱۰]. در طول فرآیند، زمان زیادی برای تأیید یک گواهینامه از دانشگاه یا در انتظار پاسخی از دانشگاه برای تایید اینکه یک گواهی معتبر است و اطلاعات دقیق است، صرف می‌شود. در راستای ارائه راهکاری برای این مساله استفاده از زنجیره‌بلوکی می‌تواند برای صرفه‌جویی در زمان، صرفه‌جویی در هزینه‌ها و امنیت مفید واقع شود. زنجیره‌بلوکی مانع از بروز تقلب شده و عملا تغییر اطلاعات ذخیره شده در بلوک‌های آن غیرممکن است

[۱۵]. از این رو، در این پیاده‌سازی یک مدل نظری برای تایید گواهینامه دانشگاهی با استفاده از فناوری زنجیره‌بلوکی ارائه شده است. زنجیره‌بلوکی برای هر تراکنش منحصر به فردی که ایجاد شده باشد، اطلاعات قطعی و قابل بازبینی را ثبت می‌کند [۱۶]. هدف از پیاده‌سازی در این پایان نامه، طراحی و اجرای یک سیستم مبتنی بر زنجیره‌بلوکی اتریوم برای ثبت گواهینامه و مدارک دانشگاهی با استفاده از سیستم توزیع فایل همتابه‌همتا یا IPFS است. در این پایان‌نامه سه نوع مختلف از قراردادهای هوشمند توسعه‌یافته، برای قسمت‌های سرویس کنترل، صدور گواهینامه و مدیریت ورود، ارائه شده است. سیستم گواهینامه کلی شامل چهار مولفه است که ذخیره‌سازی گواهی زنجیره‌بلوکی در قالب تصویر دیجیتالی، رویکرد اصلی توسعه این نمونه اولیه است. زنجیره‌بلوکی گواهینامه‌های آموزشی را به بلوک‌های خود اختصاص می‌دهد و اطمینان حاصل می‌کند که این اطلاعات تأییدشده و تغییرناپذیر هستند. در سیستم پیشنهادی، زمان و هزینه مورد بررسی قرار گرفت و با توجه به نتایج به دست آمده، مشخص شدکه با هزینه بسیارکم و سرعت بالا می توان مدارک دانشگاهی را روی شبکه زنجیره‌بلوکی اتریوم ثبت و تایید کرد [۲].

۵ مخاطرات و معایب

زنجیره‌بلوکی مانند هر فناوری، دارای معایبی است که کاربران اینگونه شبکه‌ها علی‌رغم کارایی مفید آن با آن روبرو هستند. براساس مطالعات انجام شده در رابطه با به کار بردن زنجیره‌بلوکی در حوزه‌های مختلف، در این بخش به بیان برخی از ایرادات آن پرداخته شده است. بیت‌کوین به عنوان اولین رمزارزی که از شبکه‌های زنجیره‌بلوکی استفاده کرده است، دارای ایراداتی نیز می‌باشد. از جمله این مشکلات می‌توان به طولانی بودن مدت زمان تأیید تراکنش‌ها که هر ده دقیقه یکبار است وکارمزدهای بعضاً گران آن اشاره کرد [۳۳]. یکی دیگر از مشکلات بیت‌کوین، مصرف بالای انرژی توسط شبکه آن است که همواره یکی از موارد انتقاد به این فناوری بوده است. برای استفاده از زنجیره‌بلوکی در برخی از کاربردها لازم است که تمامی گره‌ها دفترکل توزیع شده را ذخیره کنند که در این صورت هر گره نیازمند فضای ذخیره‌سازی با حجم زیادی است [۵]. این ویژگی در کاربرد [۴۸] حجم لازم برای اجرای نرم‌افزار را نیز افزایش داده است و کاربران را ملزم به داشتن فضای اجرایی زیادی کرده است. مقیاس‌پذیری یکی از مشکلات مشترک شبکه‌های زنجیره‌بلوکی

است که در انواع مختلف اینگونه شبکه‌ها از جمله بیت‌کوین تاحدودی برای رفع آن تلاش شده است برای مثال توسعه‌دهندگان در شبکه بیت‌کوین کش تا حدودی توانسته‌اند برای مقیاس‌پذیری بهبود حاصل کنند [۱۴]. وجود تاخیر در مواردی که از شبکه‌های زنجیره‌بلوکی استفاده شده است یک ویژگی مشترک برای آنهاست به طوریکه در کاربرد [۳۷] بین عرضه و تقاضا فاصله زمانی وجود دارد. همچنین یکی دیگر از معایب این شبکه‌ها، عدم بررسی تاثیر سرمایه‌گذاری در الگوی پیشنهادی برای مبادلات انرژی است که در کاربرد [۲۷] بیان شده است. در این طرح فناوری زنجیره‌بلوکی راه‌حل‌های توزیع شده و غیرمتمرکزی را برای انجام تراکنش‌های انرژی ارائه می‌دهد. توسعه‌دهندگان برای رفع مشکل تاخیر به طور مثال در شبکه بیت‌کوین، شبکه لایتنینگ را ارائه کردند که در آن تراکنش‌ها بسیار سریع‌تر تایید می‌شوند [۲۸]. در برخی از کاربردهایی که از زنجیره‌بلوکی خصوصی استفاده می‌کنند علاوه بر کارایی بسیار بالای آنها در پیاده‌سازی و عملکرد، پیچیدگی در اجرای بخش‌های مختلف را نیز به همراه دارد که در کاربرد [۲۹] ذکر شده است.

۶ نتیجه‌گیری

فناوری زنجیره‌بلوکی به عنوان بستر شبکه بیت‌کوین به شهرت رسید و توانست به دنیای فناوری‌های جهانی ورود پیدا کند. این فناوری با شعار تغییر جهان مورد توجه قرار گرفت، اما علاوه بر اینکه قادر است اینترنت را به یک ابزار فوق‌العاده اثربخش تبدیل کند، بلکه انقلابی در اقتصاد، سیاست و قدرت جهانی نیز پدید آورد. زنجیره‌بلوکی همچنین توانایی و ظرفیت خود را برای تغییر سیستم‌های سنتی با استفاده از ویژگی‌های کلیدی خود از جمله غیرمتمرکز بودن، توزیع‌پذیری، امنیت، شفافیت، تغییرناپذیری و گمنامی نشان داده است. در این مقاله مروری کامل بر مباحث اساسی و مهم زنجیره‌بلوکی انجام شده است. در ابتدا در بخش اول به بیان مفاهیم اساسی از جمله: شبکه زنجیره‌بلوکی و تاریخچه آن، تولید بیت‌کوین، اتریوم، دفترکل توزیع شده و توضیحات مربوط به آن، اجماع و چگونگی عملکرد آن، توابع هش، اعتبار بلوک‌ها، استخراج و حل پازل آن، اثبات کار، ساختار کلی زنجیره‌بلوکی وشرایط لازم برای استفاده از زنجیره‌بلوکی پرداخته شده است. در ادامه و در بخش دوم توضیحاتی در رابطه با شبکه اتریوم، تفاوت اتریوم و بیت‌کوین، قرارداد

هوشمند و نمونه‌ای از آن، مزایای استفاده از آن، مراحل طراحی قرارداد هوشمند، ماشین مجازی اتریوم، حساب‌ها، حالات شبکه اتریوم،گس و هک DAO آورده شده است. در نهایت نیز در بخش سوم مقاله به بیان کاربردهای زنجیره‌بلوکی پرداخته است. عرضه اولیه سکه، برنامه‌های غیرمتمرکز و همچنین استفاده از این فناوری در پیاده‌سازی پروژه‌هایی در حوزه‌هایی از جمله انرژی خورشیدی، خدمات سلامت، مدیریت و احراز هویت دیجیتالي و ثبت مدارک دانشگاهی از دیگر مواردی است که در این بخش توضیح داده شده است . در حال حاضر نیز این فناوری در بسیاری از حوزه‌ها کاربرد دارد و توانسته است تحولات وسیعی را در دنیای علم و فناوری به همراه داشته باشد.

تشکر و قدردانی

- بدینوسیله از تمامی اعضای تیم ”نهمین کنگره مشترک سیستم های فازی و هوشمند” که در اسفند ۱۴۰۰ و در شهرستان بم برگزار شد کمال تشکر را دارم زیرا این مقاله براساس سخنرانی کلیدی در این کنگره آماده شده است.

- بدینوسیله از سرکار خانم محدثه رضایی تشکر و قدردانی می‌نمایم.

- در اینجا قصد دارم از اعضای تیم بلاک چین آزمایشگاه پردازش هوشمند داده دانشگاه شهید باهنر کرمان تشکر و قدردانی نمایم.

مراجع

[۱] روحانی یزدی، ف. (۱۴۰۰) ثبت اطلاعات پزشکی روی شبکه بلاک‌چین. پایاننامه کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه شهیدباهنر کرمان.

[۲] شاه کرمی پور، ش. (۱۴۰۰) ثبت و تأیید مدارک دانشگاهي روی شبکه بلاک‌چین. پایاننامه کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه شهیدباهنر کرمان.

[۳] شایگان، پ. (۱۴۰۰) طراحي واحد دانش فني نیروگاه های خورشیدی با استفاده از فناوری قراردادهای هوشمند بر بستر زنجیره بلوکی پایان نامه کارشناسي ارشد، دانشکده فني و مهندسي، دانشگاه شهیدباهنر کرمان.

[۴] شجاعی باغینی، م. (۱۴۰۰) مدیریت و احرازهویت دیجیتالی با استفاده از فناوری بلاک چین" پایان¬نامه کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه شهیدباهنر کرمان.

[5] Aitzhan, N. Z. and Svetinovic, D. (2016). Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 15(5), 840-852.

[6] AlQahtani, S., Alsalamah, S., Alimam, A., AlAdullatif, A., AlAmri, M., Al-Thaqeb, M., ... and Aschheim, K. (2019). Towards a unified blockchain-based dental record ecosystem for disaster victims identification. In Proceedings of the 5th International Conference on Health Informatics and Medical Systems.

[7] Angelov, A. and Sørensen, M. (2018). Decentralized Identity Management System for Self-Sovereign Identity, M.Sc. In Engineering of Inovative Communication Technologies and Entrepreneurship, Aalborg University Copenhagen.

[8] Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc.

[9] Antonopoulos, A. M., and Wood, G. (2018). Mastering ethereum: building smart contracts and dapps. O'reilly Media.

[10] Balsubramanian, S., Prashanth, I. R., and Ravishankar, S. (2009). Mark sheet verification. In 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, 359-362, IEEE.

[11] Bashir, I. (2017). Mastering blockchain. Packt Publishing Ltd.

[12] Bhargav-Spantzel, A., Squicciarini, A. C., and Bertino, E. (2006). Establishing and protecting digital identity in federation systems. Journal of Computer Security, 14(3), 269-300.

[13] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

[14] Cash, B. (2019). Bitcoin cash. Development, 2.

[15] Chen, Z., and Zhu, Y. (2017, June). Personal archive service system using blockchain technology: Case study, promising and challenging. In 2017 IEEE International Conference on AI and Mobile Services (AIMS), 93-99, IEEE.

[16] Cheng, J. C., Lee, N. Y., Chi, C., and Chen, Y. H. (2018). Blockchain and smart contract for digital certificate. In 2018 IEEE international conference on applied system invention (ICASI), 1046-1051, IEEE.

[17] Dhillon, V., Metcalf, D., and Hooper, M. (2017). The DAO hacked. In Blockchain Enabled Applications, 67-78. Apress, Berkeley, CA.

[18] Franco, P. (2014). Understanding Bitcoin: Cryptography, engineering and economics. John Wiley and Sons.

[19] Bhaskar, P., Tiwari, C. K., and Joshi, A. (2020). Blockchain in education management: present and future applications. Interactive Technology and Smart Education.

[20] Goutte, S., Guesmi, K., and Saadi, S. (2019). Cryptofinance and Mechanisms of Exchange. Springer International Publishing.

[21] Goyal, S., Sanjith, K., Sisodia, A., Suhaas, N. M., and Akram, S. (2020). Transactions Process in Advanced Applications on Ethereum Blockchain Network. In

2020 International Conference on Recent Trends on Electronics, Information, Communication and Technology (RTEICT), 275-281, IEEE.

[22] Gupta, M. (2018). Blockchain for Dummies (2nd IBM Li).

[23] Hileman, G. (2016). State of blockchain q1 2016: Blockchain funding overtakes bitcoin. CoinDesk, New York, NY, May, 11.

[24] Haber, S., and Stornetta, W. S. (1990). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography, 437-455. Springer, Berlin, Heidelberg.

[25] Iyer, K., and Dannen, C. (2018). The ethereum development environment. In Building games with ethereum smart contracts, 19-36. Apress, Berkeley, CA.

[26] Jin, H., Luo, Y., Li, P., and Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. IEEE Access, 7, 61656-61669.

[27] Kang, E. S., Pee, S. J., Song, J. G., and Jang, J. W. (2018). A blockchain-based energy trading platform for smart homes in a microgrid. In 2018 3rd international conference on computer and communication systems (ICCCS), pp. 472-476, IEEE.

[28] Khan, N. (2019). Lightning network: A comparative review of transaction fees and data analysis. In International Congress on Blockchain and Applications, 11-18. Springer, Cham.

[29] Laszka, A., Eisele, S., Dubey, A., Karsai, G., and Kvaternik, K. (2018). TRANSAX: A blockchain-based decentralized forward-trading energy exchanged for transactive microgrids. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), 918-927, IEEE.

[30] Metcalfe, W. (2020). Ethereum, smart contracts, DApps. Blockchain and Crypt Currency, 77.

[31] Miller, A. R., and Tucker, C. (2014). Health information exchange, system size and information silos. Journal of health economics, 33, 28-42.

[32] Mohanty, D. (2018). Basic solidity programming. In Ethereum for Architects and Developers, 55-103. Apress, Berkeley, CA.

[33] Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., and Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2 C. Nature Climate Change, 8(11), 931-933.

[34] Ozer R., (2017). Ethereum-The Insider Guide to Blockchain Technology, Cryptocurrency and Mining Ethereum, Stat. F. Theor, 50.

[35] Pee, S. J., Kang, E. S., Song, J. G., and Jang, J. W. (2019). Blockchain based smart energy trading platform using smart contract. In 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 322-325). IEEE.

[36] Ramachandran, S., Kiruthika, O. O., Ramasamy, A., Vanaja, R., and Mukherjee, S. (2020). A review on blockchain-based strategies for management of electronic health records (EHRs). In 2020 International Conference on Smart Electronics and Communication (ICOSEC) , 341-346. IEEE.

[37] Sabounchi, M., and Wei, J. (2017). Towards resilient networked microgrids: Blockchain-enabled peer-to-peer electricity trading mechanism. In 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 1-5, IEEE.

[38] Sheng, C. A. O., Zheng, C., a nd Xuandong, S. (2007). Anti-counterfeit Authentication System of Printed Information Based on A Logic Signing Tehinique. In In-

ternational Conference on Intelligent Systems and Knowledge Engineering 2007, 1254-1259. Atlantis Press.

[39] Szabo N. Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16), 18(2):28.

[40] Venegas, P. (2017). Initial coin offering (ICO) risk, value and cost in blockchain trustless crypto markets. Value and Cost in Blockchain Trustless Crypto Markets.

[41] Warasart M, Kuacharoen P. (2012) based document authentication using digital signature and QR code. In4TH International Conference on Computer Engineering and Technology (ICCET 2012).

[42] Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F. Y. (2019). Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277.

[43] Wang S, Taha AF, Wang J, Kvaternik K, Hahn A. (2019). Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. IEEE Transactions on Systems, Man, and Cybernetics: Systems.4;49(8):1612-23.

[44] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.

[45] Wüst, K., and Gervais, A. (2018). Do you need a blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), 45-54, IEEE.

[46] Wu, X. B., Zou, Z., and Song, D. (2019). Learn ethereum: build your own decentralized applications with ethereum and smart contracts. Packt Publishing Ltd.

[47] Nakamoto, S. (2009). Nakamoto, S, Bitcoin: A peer-to-peer electronic cash system.

[48] Zhou, Z., Tan, L., and Xu, G. (2018). Blockchain and edge computing based vehicle-to-grid energy trading in energy internet. In 2018 2nd IEEE conference on energy internet and energy system integration (EI2), 1-5, IEEE.

[49] Available at: https://101blockchains.com/.

[50] Available at: https://www.allcryptowhitepapers.com/neo-whitepaper/.

[51] Available at: https://iota.org/IOTA-Whitepaper/.

[52] https://www.allcryptowhitepapers.com/monero-whitepaper/.

[53] https://www.allcryptowhitepapers.com/zcash-whitepaper/.

[54] https://www.allcryptowhitepapers.com/dash-whitepaper/.

[55] https://arzdigital.com/.

[56] http://bitinfocharts.com/.

[57] https://www.satba.gov.ir/.

[58] https://www.statista.com/.