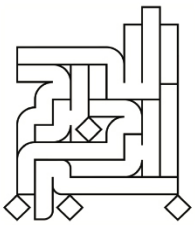


سرشناسه: ناصرعامری، محمد، ۱۳۵۸-، گردآورنده
عنوان و نام پدیدآور: کاربردهای بلاک‌چین در امنیت سایبری / تالیف و گردآوری محمد ناصرعامری.
مشخصات نشر: تهران: انتشارات دانشگاهی کیان، ۱۴۰۲.
مشخصات ظاهری: ۳۰۴ ص. : مصور(بخشی رنگی)، جدول، نمودار(بخشی رنگی).
شابک: ۹۷۸-۶۰۰-۳۰۷-۳۰۰-۵
وضعیت فهرست نویسی: فیپا
یادداشت: کتابنامه: ص. ۳۰۴.
موضوع: بلاک‌چین (پایگاه‌های اطلاعاتی) -- مقاله‌ها و خطابه‌ها
Blockchains (Databases) -- *Addresses, essays, lectures
پایگاه‌های اطلاعاتی -- امنیت-- مقاله‌ها و خطابه‌ها
Database security-- *Addresses, essays, lectures
بلاک‌چین(پایگاه‌های‌اطلاعاتی)–تدابیرایمنی–مقاله‌هاوخطابه‌ها
Blockchains (Databases) -- Security measures -- *Addresses, essays, lectures
شبکه‌های کامپیوتری -- تدابیر ایمنی -- مقاله‌ها و خطابه‌ها
Computer networks -- Security measures -- *Addresses, essays, lectures
کامپیوترها--ایمنی‌اطلاعات--تدابیرایمنی--مقاله‌هاوخطابه‌ها
Computer security -- Security measures -- *Addresses, essays, lectures
رده بندی کنگره: HQ۱۷۱۰
رده بندی دیویی: ۳۳۲/۱۷۸
شماره کتابشناسی ملی: ۹۴۰۹۲۷۹
اطلاعات رکورد کتابشناسی: فیپا

نام کتاب : کاربردهای بلاک‌چین در امنیت سایبری
تألیف و گردآوری : محمد ناصرعامری
ویراستار : فاطمه علی‌اکبری
صفحه‌آرا : فرزانه گلچین
طراحی گرافیک : معراج قنبری و علیرضا غفوری
چاپ اول : ۱۴۰۲
تیراژ : ۵۰۰ نسخه
چاپ : لوح‌آیین
صحافی : آذین

شابک : ۹۷۸-۶۰۰-۳۰۷-۳۰۰-۵

کاربردهای بلاک‌چین در امنیت سایبری

تألیف و گردآوری: محمد ناصرعامری

نشر دانشگاهی کیان

سخنی با خوانندگان

حمد و سپاس بی‌پایان خدایی را سزاست که عالم را در منتهای کمال آفرید و آدمی را بر بلندای قله‌ی هستی گماشت و او را جلوه‌گاه جمال، مخاطب کلام و وارث قلم گردانید و «کتاب» را به‌عنوان بزرگ‌ترین معجزه‌ی جاودان خویش در اختیار انسان قرار داد. آیین و فرهنگ کهن ما انس و الفتی دیرین با کتاب داشته‌اند و همواره انسان‌های وارسته، سعادت و آرامش را در کتاب جست‌وجو کرده‌اند؛ چنان‌که به تعبیر امیر مؤمنان علی علیه‌السلام، «کسی که با کتاب آرامش یابد، هرگز آسایش از او سلب نمی‌شود».

کتاب حافظه‌ی بشریت است و در ساحت اندیشه، هیچ وسیله‌ای همچون کتاب واجد ژرفا و کارایی لازم نیست؛ ازاین‌رو ترویج و نشر کتاب، نهادینه‌سازی فرهنگ کتاب‌خوانی، ارضای حس کنجکاوی و پرسشگری دانشجویان و تربیت علمی و فرهنگی نسلی شایسته و درخور، رسالتی مسلم بر دوش ارباب فرهنگ و دانش است. این رسالت ما را نیز بر آن داشت که به‌عنوان عضو کوچکی از جامعه‌ی علمی و فرهنگی ایران، پای به میدان نهیم و در تحقق این هدف ارزنده و انسانی، نقشی هرچند اندک ایفا کنیم.

باعث تأسف است که در شرایط کنونی، معضلات اجتماعی و مشکلات روزمره‌ی زندگی اشتیاق مطالعه را کاسته و با توسعه‌ی سریع دنیای مجازی و شبکه‌های اجتماعی، مطالب کوتاه، سطحی و کم‌محتوا جایگزین کتاب‌های عمیق، مفید و اندیشه‌ساز گردیده و در این میان، مشکلات نشر، همچون هزینه‌های رو به افزایش کاغذ و چاپ و به تبع آن عدم اقبال عمومی به کتاب، مزید بر علت شده‌است. اگرچه این تصور که با پدید آمدن وسایل نوظهور ارتباط جمعی کتاب به انزوا خواهد رفت، تصوری خلاف واقع است، اما از این نکته نیز نباید غافل بود که امتیاز ابزارهای جدید دنیای مجازی سهولت کاربری آن‌هاست. ولی به هر حال، این ابزارها هرگز از جهت عمق، تحلیل و سازندگی فکر و ذهن، جای کتاب را نخواهند گرفت.

انتشارات دانشگاهی کیان با بیش از یک دهه سابقه‌ی فعالیت در تولید و نشر کتاب‌های دانشگاهی و نیز فنی و مهندسی، می‌کوشد رسالت‌های خود را در سایه‌ی لطف پروردگار و حمایت‌های مخاطبان خود، به بهترین نحو ممکن به‌انجام رساند. در این راستا، تلاش بر آن است که آنچه در این نشر به‌چاپ می‌رسد، حائز معیارهای استاندارد کیفی کتاب باشد و بر همین اساس است که کتاب‌ها در مسیر تولید، با حوصله و دقت تحت نظارت همه‌جانبه‌ی محتوایی - معنایی شامل چندین مرحله ویرایش علمی و نیز صوری قرار می‌گیرند تا در نهایت متنی روان و ساده براساس اصول آموزشی تهیه و تدوین شود. همچنین برای همه‌ی آثار به لحاظ بصری و زیبایی‌شناسی از منظر صفحه‌آرایی و طراحی جلد، سطح کیفی مناسبی درنظر گرفته شده‌است.

همه‌ی تلاش انتشارات دانشگاهی کیان بر این بوده است که همگام با خواست مخاطبان خود حرکت و کتاب‌ها را با بالاترین کیفیت منتشر کند، اما به حتم، این اثر خالی از اشکال نیست و از تمام مخاطبان فهیم آن و سایر آثار نشر خواهشمند است نقدها و نظرهای ارزشمند و سازنده‌ی خود را جهت بهبود در کتاب‌های آتی مطرح فرمایند.

انتشارات دانشگاهی کیان
www.kianpub.com
info@kianpub.com

پیش‌گفتار

مجموعه مقالات در این نوشتار، جزئیاتی درباره‌ی پیاده‌سازی بلاک‌چین در زمینه‌های بین‌رشته‌ای و تکنولوژیکی نظیر علوم پزشکی، ریاضیات کاربردی، علوم محیطی، مدیریت کسب‌وکار و علوم کامپیوتر ارائه می‌دهد. این کتاب همچنین دانشی عمیق از فناوری بلاک‌چین جهت کاربرد در تکنولوژی‌های پیشرفته و در حال ظهور در آینده را ارائه می‌دهد و بر اهمیت آن‌ها تمرکز می‌کند. در همین راستا، بر مطالعات موصوف زمینه (مقیاس و تناوب)، ریسک (امنیت، قابلیت اطمینان و درستی) و زمان (تأخیرات و جدول زمانی، بهره‌وری و جزئیات پیاده‌سازی تکنولوژی‌های بلاک‌چین) متمرکز خواهیم شد. بیت‌کوین و ارز دیجیتال اولین موارد استفاده از تکنولوژی بلاک‌چین هستند، اما امروزه بلاک‌چین کاربردهای بسیار گسترده‌تری یافته‌است. درحقیقت، بلاک‌چین تقریباً در هر صنعتی انقلابی به‌پا کرده‌است. بلاک‌چین در عصر جدید، یک تکنولوژی تحول‌گرا و مبنایی برای ظهور تمام ارزهای دیجیتال و به‌عنوان راه‌حل مفید در سایر حوزه‌های فناوری معرفی می‌شود. ازجمله ویژگی‌های تکنولوژی بلاک‌چین دفترهای کل ایمن توزیع‌شده و متمرکز است که تراکنش‌ها را در یک شبکه‌ی نظیربه‌نظیر ثبت می‌کنند و پتانسیلی برای حذف خطاهای ناخواسته با شفافیت و نیز پاسخ‌گویی فراهم می‌سازند. این موضوع نه‌تنها بخش فناوری‌های مالی (ارزهای دیجیتال) بلکه سایر حوزه‌ها مانند موارد زیر را نیز تحت تأثیر قرار داده‌است:

- اقتصاد رمزنگاری[1]؛
- بلاک‌چین سازمانی؛
- صنعت سفر با استفاده از بلاک‌چین؛
- حریم خصوصی تعبیه‌شده با استفاده از بلاک‌چین؛
- انقلاب صنعتی چهارم با استفاده از بلاک‌چین؛
- پیاده‌سازی شهرهای هوشمند به کمک بلاک‌چین؛
- فناوری‌های آتی بلاک‌چین؛
- تشخیص اخبار جعلی با استفاده از بلاک‌چین؛
- فناوری بلاک‌چین و کاربردهای آتی آن؛
- پیامدهای فناوری بلاک‌چین؛
- حریم خصوصی بلاک‌چین؛
- موارد استفاده و استخراج بلاک‌چین؛

---

۱. به زبان ساده، اقتصاد کریپتویی با ترکیب رمزنگاری و اقتصاد، راهی برای هماهنگی رفتار شرکت‌کنندگان در شبکه فراهم می‌کند. به‌طور خاص، اقتصاد کریپتویی حوزه‌ای از علوم کامپیوتر است که سعی می‌کند مشکلات هماهنگی شرکت‌کنندگان در اکوسیستم‌های دیجیتال را از طریق رمزنگاری و مشوق‌های اقتصادی برطرف کند.

- برنامه‌های کاربردی شبکه‌ی بلاک‌چین؛
- قرارداد هوشمند بلاک‌چین؛
- معماری بلاک‌چین؛
- مدل‌های کسب‌وکار بلاک‌چین؛
- اجماع بلاک‌چین؛
- بیت‌کوین و ارزهای دیجیتال و زمینه‌های مرتبط با آن.

ابتکارات و ابداعاتی که در آن فناوری بلاک‌چین برای توزیع و پیگیری نقطه‌ی شروع ارتباطات به‌کار می‌رود، حریم خصوصی را فراهم و آن را مدیریت می‌کند و به این ترتیب، محیط قابل‌اعتمادی ایجاد خواهد کرد. تنها چند مورد از کاربردهای تکنولوژی بلاک‌چین هستند که خطراتی مانند حفاظت از حریم خصوصی را برجسته می‌کنند. نظرات متفاوتی درباره‌ی کاربرد تکنولوژی بلاک‌چین وجود دارد. بعضی علاقه‌مند و مشتاق به آن هستند و بعضی معتقدند که بلاک‌چین صرفاً یک پدیده‌ی تبلیغاتی است. همچنین بلاک‌چین وارد حوزه‌ی کمک‌های بشردوستانه و توسعه‌ای همانند مدیریت زنجیره‌ی تأمین، هویت دیجیتال، قراردادهای هوشمند و بسیاری موارد دیگر شده‌است. در مجموعه مطالعات حاضر، مفاهیم و کاربردهای تکنولوژی بلاک‌چین به‌طور شفاف ارائه شده‌است و از کارشناسان مراکز تحقیقاتی، استادان دانشگاه، صنایع و دولت در این راستا دعوت به همکاری می‌شود.

فهرست مطالب

مقدمه‌ای بر تکنولوژی بلاک‌چین

چکیده

در سال‌های اخیر، تکنولوژی‌های متعددی درنتیجه‌ی نوآوری‌های تکنولوژیکی ظهور کرده‌اند. در چند سال گذشته، تکنولوژی بلاک‌چین یا تکنولوژی دفتر کل ایمن توجه زیادی را به خود جلب کرده‌است. در زمینه‌ی محاسبات، تکنولوژی بلاک‌چین به‌عنوان پنجمین نوآوری تحول‌آفرین شناخته شده‌است. از طرف دیگر، می‌توان گفت که بلاک‌چین یک دفتر کل توزیع‌شده از رکوردهاست که مطلق و قابل‌تأیید است. به بیان دیگر، فناوری بلاک‌چین (دفتر کل) اساساً رکوردی از پایگاه داده‌ی توزیع‌شده و یا یک دفتر کل عمومی از تمام معاملات، اقدامات و جریاناتی است که به‌طور دیجیتال انجام و با سایر موجودیت‌های مشارکت‌کننده به اشتراک گذاشته می‌شوند. هر تراکنش انجام‌شده در دفتر کل عمومی با توافق متقابل تمام شرکت‌کنندگان تأیید می‌شود. وقتی اطلاعات وارد می‌شود، دیگر هرگز پاک نمی‌گردد. هر تراکنش انجام‌شده در سیستم به‌سادگی می‌تواند تأیید و در بلاک‌چین ثبت شود. پس از ظهور تکنولوژی بلاک‌چین در سال ۲۰۰۸، این مفهوم به روش‌های مختلفی به‌کار گرفته شد. علاقه‌مندی به این تکنولوژی به دلیل ویژگی‌ها و خاصیت‌های منحصربه‌فردش نظیر حفظ امنیت، رازداری و یکپارچگی داده‌ها بدون مداخله‌ی شخص ثالث کنترل‌کننده‌ی تراکنش افزایش یافته‌است. بنابراین بسیاری از محققان را برانگیخته‌است که با چالش‌ها، کاربردها و محدودیت‌های این تکنولوژی آشنا شوند. بارزترین تأثیر تکنولوژی بلاک‌چین را می‌توان در ظهور ارزهای دیجیتال متعدد مشاهده کرد. به‌علاوه، کاملاً واضح است که کاربرد تکنولوژی بلاک‌چین بسیار فراتر از ارز دیجیتال و بسیار عمیق‌تر از ذخیره‌سازی در دفتر کل توزیع‌شده است. این تکنولوژی توسط بخش‌های مختلف مانند اقتصاد، تولید، آموزش و پزشکی برای بهره‌مندی از منافع و مزایای منحصربه‌فرد آن به‌کار گرفته شده‌است، مزایای منحصربه‌فردی نظیر قابلیت اعتماد، همکاری، سازمان‌دهی، تأیید، اعتبارسنجی و شفافیت.

به‌علاوه، تکنولوژی بلاک‌چین در حوزه‌ی اقتصاد و بانکداری بیشترین استفاده را دارد و همچنین آزمایش‌های متعددی توسط شرکت‌های بزرگ در حوزه‌های دیگر نیز انجام شده‌است. این تحقیق بر حوزه‌ها و بخش‌های متعددی که در آن‌ها تکنولوژی بلاک‌چین تأثیرگذار بوده‌است تمرکز دارد و استفاده از آن در بخش‌های مختلف در آینده را نیز مورد بحث قرار می‌دهد.

کلمات کلیدی: تکنولوژی بلاک‌چین، چالش‌ها، کاربردهای آتی، محدودیت‌ها

۱. مقدمه

بلاک‌چین فناوری‌ای است که دارای رکوردی از پایگاه داده‌ی عمومی یا دفتر کل عمومی شامل تمام جریانات مختلف و تمام موارد دخیل در این جریانات می‌باشد. تراکنشی که رخ می‌دهد توسط اغلب شرکت‌کنندگان از طریق توافق، احراز هویت می‌شود. وقتی اطلاعات وارد سیستم شد، دیگر قابل‌تغییر نیست. این تکنولوژی متشکل از رکوردهای هر تراکنش است که تاکنون در سیستم انجام شده‌اند.

شناخته‌شده‌ترین و معروف‌ترین تکنولوژی بلاک‌چین تحت عنوان بیت‌کوین است که ذاتاً پیچیده است. اخیراً بیت‌کوین یکی از بحث‌برانگیزترین پدیده‌ها نیز بوده‌است، چراکه تراکنش‌های مولتی بیلیون دلاری بازار جهانی را بدون محدودیت دولتی آسان کرده‌است. به همین دلیل مسایل مقرراتی متعددی وجود دارد که دولت در سطح ملی و سایر مؤسسات مالی را درگیر می‌کند.

اما در چند سال اخیر، مفهوم تکنولوژی بلاک‌چین پدیده‌ای کاملاً بحث‌برانگیز بوده و در دنیای اقتصاد و غیراقتصادی، به‌طور مؤثر اجرا شده‌است. بنابر گفته‌ی مارک اندرسن، رهبر سرمایه‌داران سیلیکون والی، مدل اجماع توزیع‌شده‌ی بلاک‌چین به‌عنوان مهم‌ترین مداخله در حوزه‌ی اینترنت به‌شمار می‌رود. این اقتصاد توسط سیستم دیجیتال هدایت می‌شود و متکی بر بعضی قدرت‌های قابل‌اعتماد است. وقتی تراکنش توسط یک فرد انجام می‌شود، باید به سیستم اعتماد کند، به‌عنوان مثال خدمات ایمیل که اطلاعات ایمیل‌شده را ارائه می‌دهد یا فیس‌بوک که اطلاعات پست‌شده و به‌اشتراک گذاشته‌شده با دیگران را نشان می‌دهد یا تراکنش مالی از طریق بانک که در آن تأیید می‌شود پول به گیرنده‌ای در هرجایی از دنیا منتقل شود.

می‌توان گفت ما در دنیای دیجیتال زندگی می‌کنیم که در آن مجبوریم به‌منظور مسایل امنیتی و حفظ حریم خصوصی بر شخص ثالث تکیه کنیم. اما حقیقت این است که این منبع سوم می‌تواند کارساز باشد و یا هک شود. اینجاست که نقش تکنولوژی بلاک‌چین وارد صحنه می‌شود. در حال حاضر، سیستم تراکنش میان دو فرد و دو شرکت اغلب ماهیتی متمرکز دارد و توسط شخص ثالث کنترل می‌شود. هرگاه یک پرداخت دیجیتال انجام می‌دهیم، همیشه باید یک شخص ثالث دخیل باشد تا تراکنش تکمیل شود. به‌علاوه، بعضی هزینه‌های اضافی از طرف بانک‌ها یا شرکت کارت اعتباری تحمیل می‌شود. الگوی مشابهی در حوزه‌های دیگر نظیر بازی‌ها، موزیک، نرم‌افزار و ... دنبال می‌شود. این مسئله با ابداع تکنولوژی بلاک‌چین حل شده‌است. تأکید اصلی این تکنولوژی ایجاد محیطی است که ماهیتی غیرمتمرکز دارد و نیازمند دخالت شخص ثالث در تراکنش‌ها و داده‌ها نیست [۱].

این تکنولوژی دارای خاصیتی است که به ما امکان می‌دهد هر تراکنش انجام‌شده در گذشته و حال را که می‌تواند در آینده تأیید شود به کمک اجماع توزیع‌شده پیگیری کنیم. این موضوع حتی بدون درنظرگرفتن محرمانگی دارایی‌های دیجیتال و پیچیده‌ی شخص ثالث انجام می‌شود. ویژگی‌های اصلی تکنولوژی بلاک‌چین اجماع توزیع‌شده و گمنامی است.

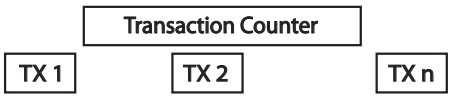
رکورد داده‌هایی که پیوسته در حال افزایش است و توسط گره‌های مختلف دخیل در آن با کمک پایگاه داده‌ی توزیع‌شده انجام می‌شود توسط بلاک‌چین نگهداری می‌گردد. هر تراکنش که تکمیل می‌شود در یک دفتر کل عمومی ذخیره می‌گردد. تکنولوژی بلاک‌چین راه‌حلی ارائه می‌دهد که ماهیتی غیرمتمرکز دارد و نیازمند دخالت شخص ثالث نیست. به‌علاوه، تمام گره‌ها در بلاک‌چین گمنام هستند که باعث می‌شود تراکنش در مقابل سایر گره‌ها امنیت بیشتری داشته باشد. کاربرد اولیه‌ی معرفی‌شده در تکنولوژی بلاک‌چین بیت‌کوین بوده‌است. بیت‌کوین پلتفرمی است که در آن اجناس و کالاها به کمک پرداخت دیجیتال در محیطی غیرمتمرکز خرید‌وفروش و مبادله می‌شوند [۲].

هرچند به‌نظر می‌رسد این تکنولوژی برای انجام تراکنش به کمک ارزهای دیجیتال بسیار مناسب است، اما هنوز با مشکلات فنی و محدودیت‌هایی دست به گریبان است که نیازمند تحلیل عمیق می‌باشد. گره‌ها در بلاک‌چین باید به‌صورت خصوصی نگه داشته شوند تا در مقابل حملات از آن‌ها محافظت شود و سطح بالایی از امنیت و تراکنش را حفظ کنند [۳]. به‌علاوه، برای تأیید تراکنش بلاک‌چین، نیازمند قدرت محاسباتی نیز هستیم.

با توجه به آنچه گفته شد، در این مقاله، درک موضوعاتی که توسط نویسندگان مختلف مورد مطالعه قرار گرفته‌اند و حوزه‌هایی که نیازمند توجه بیشتر به تهدیدها و چالش‌ها در مطالعات آتی هستند حائز اهمیت است. برای کشف و درک این موضوعات، از نقشه‌ای سیستماتیک برای درک فرایند مطالعه [۴] جهت مرور مطالعات مختلف مرتبط با حوزه‌ی بلاک‌چین استفاده می‌شود. شکل ۱ ساختار بلوکی بلاک‌چین را نشان می‌دهد.

محتوای موجود در پایگاه داده‌ی علمی می‌تواند به کمک پروتکل تحقیقاتی با طراحی مناسب در یک مطالعه‌ی نگاشتی سسیستماتیک جست‌وجو شود. براساس تحقیقات فعلی در حوزه‌ی بلاک‌چین، یک نقشه‌ی راه تهیه شده‌است و بدین منظور سایر محققان از درک موضوع تحقیقات آتی و سؤالات آینده بهره‌مند می‌شوند. با این‌که تحقیقات بسیاری در حوزه‌ی ارزهای دیجیتال در مطالعات اقتصاد و مدیریت انجام شده‌است، اما قصد داریم روی چشم‌انداز فنی و تکنیکی بلاک‌چین تمرکز کنیم. درواقع، تمرکز اصلی این مقاله درک چشم‌انداز فنی بلاک‌چین است. بنابراین توجه ما معطوف موضوعاتی مرتبط با چشم‌انداز فنی بلاک‌چین مشتمل بر امنیت، کارایی، یکپارچگی داده‌ها، حریم خصوصی و پایداری خواهد بود.

Block Version	02000000
Parent Block Hash	B6ff0b2b1680a2862a30ca44d346d9e8910d334beb48ca0000000000000000
Merkle Tree Root	9d10aa52ee949386ca9385695f04ede270dda20810decd12bc9b048aaab31471
Timestamp	24d95a54
nBits	30c31b18
Nonce	Fe9f0864



شکل ۱. ساختار بلوک

این مقاله دارای چندین بخش مختلف است. بخش اول شامل مقدمه است و بخش دوم به بلاک‌چین و بیت‌کوین می‌پردازد. به‌علاوه، نویسندگان در تلاش‌اند که چالش‌ها و محدودیت‌های فنی معدود تکنولوژی بلاک‌چین را مورد بحث و بررسی قرار دهند. بخش سوم این نوشته بر روش‌شناسی مورداستفاده و جمع‌آوری مقالات تحقیقاتی مناسب تمرکز دارد. براساس تحلیل انجام‌شده در مقالات تحقیقاتی قبلی، نتایج در بخش چهارم و الگوهای طبقه‌بندی در بخش پنجم ارائه شده‌اند. در بخش آخر نیز نتایج و حوزه‌ی دیگری از موضوع تحقیق آورده شده و نتیجه‌گیری انجام شده‌است.

۲. پیشینه

تکنولوژی بلاک‌چین اولین بار در قالب بیت‌کوین معرفی شد و تکنولوژی‌ای است که ارز دیجیتال بیت‌کوین را اجرا و مدیریت می‌کند. یکپارچگی تراکنش داده‌ها به کمک یک سیستم دفتر کل انجام می‌شود [۳]. حتی در حال حاضر هم بیشترین مورد استفاده‌ی تکنولوژی بلاک‌چین بیت‌کوین است [۶]. ویژگی اصلی بیت‌کوین این است که یک درگاه پرداخت با ماهیتی غیرمتمرکز و شامل یک دفتر کل تراکنش عمومی است [۷]. کیفیت اصلی بیت‌کوین این است که می‌تواند مقدار ارز را بدون دخالت هیچ سازمان یا مؤسسه‌ی دولتی نگهداری کند. تعداد کسانی که به‌طور ثابت از بیت‌کوین استفاده می‌کنند به‌تدریج در حال افزایش است و تعداد تراکنش‌ها نیز روزبه‌روز افزایش می‌یابد [۸]. به‌علاوه، این امر منجر به تبدیل ارزهای مشتریان به KRW، EUR و USD[1] و همچنین منجر به تبدیل ارز فعلی موجود

۱. دلار آمریکا، یورو و وون کره‌جنوبی

در بازار می‌شود [۹ و ۱۰]. ازاین‌رو این ارز دیجیتال در میان مجموعه افراد مختلف در سراسر دنیا توجه بسیاری را به خود جلب کرده و موفق به اجرای آن شده‌است [۹].

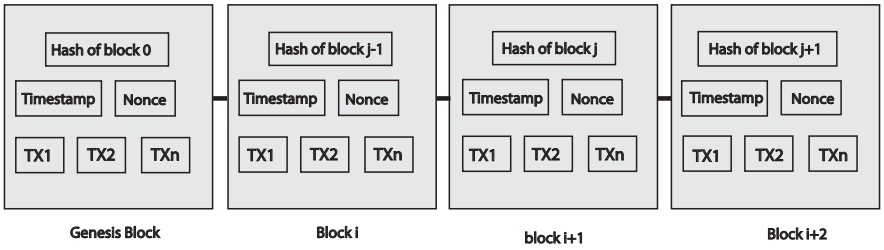
براساس آنچه گفته شد، یک مکانیزم زیرساخت کلید عمومی (PKI) درباره‌ی بیت‌کوین به‌کار می‌رود [۱۱]. مکانیزم PKI دارای یک کلید عمومی و خصوصی است. در کیف پول بیت‌کوین، کلید عمومی جهت تعامل و کلید خصوصی جهت احراز هویت به‌کار می‌روند. به‌طور کلی سه مؤلفه‌ی اصلی در هر تراکنش شامل کلیدهای عمومی متعدد گیرنده، کلید عمومی فرستنده و ارزشی است که مبادله شده‌است. در بازه‌ی زمانی ده‌روزه، این تراکنش در بلوک اطلاع‌رسانی می‌شود. اطلاعات مربوط به تمام تراکنش‌ها در تمام بلوک‌های مربوطه در دیسک ذخیره‌سازی کاربران ذخیره می‌شود. بنابراین اطلاعاتِ هر آنچه در تراکنش انجام شود در شبکه‌ی بیت‌کوین ذخیره می‌شود و همچنین تراکنش انجام‌شده توسط بلوک‌های قبلی احراز هویت می‌شود. تمام تراکنش‌های انجام‌شده تأیید می‌شوند و بنابراین تمام گره‌ها پاداش دریافت می‌کنند. این فرایند را می‌توان ماینینگ (استخراج و کاوش) نامید و می‌تواند با اثبات کار[1] که یکی از تکنولوژی‌های حیاتی در بلاک‌چین است انجام شود. هنگامی که تمام تراکنش‌ها به‌طور موفق تکمیل شوند، تمام گره‌ها به اجماع می‌رسند. با ایجاد ارتباط میان بلوک‌های جدید و بلوک‌های قبلی، زنجیره‌ای میان تمام گره‌ها ایجاد می‌شود. این را روش دفتر کل عمومی در بیت‌کوین می‌نامند که بلاک‌چین نیز نامیده می‌شود و در آن بلوکی از زنجیره‌ها وجود دارد.

بیت‌کوین فناوری بلاک‌چین است که ماهیتی غیرمتمرکز دارد و به‌طور خاص برای توزیع و انتقال ارز برای اپراتورهای بیت‌کوین طراحی شده‌است. در این فناوری، بدون مداخله‌ی شخص ثالث، دفتر کل عمومی که قبلاً اجرا نشده می‌تواند پشتیبانی شود [۳]. مزیت اصلی تکنولوژی بلاک‌چین این است که هرگاه داده‌ها توسط تمام گره‌ها پذیرفته شوند، داده‌های ذخیره‌شده در دفتر کل عمومی تغییر نمی‌کنند و یا حذف نمی‌شوند. یکی از دلایل اصلی شهرت تکنولوژی بلاک‌چین ویژگی‌های امنیتی و یکپارچگی داده‌ها در آن است. برای مثال، در خدمات ابری[2]، محیطی را برای انجام تراکنش دیجیتال و اشتراک داده روی شبکه‌ی نظیربه‌نظیر می‌توان ایجاد کرد [۳]. ویژگی منحصربه‌فرد تکنولوژی بلاک‌چین یکپارچگی داده‌هاست که همین عامل اصلی موفقیت بسیار بلاک‌چین و کاربرد آن در سایر خدمات و اپلیکیشن‌ها نیز هست. شکل ۲ معماری پایه‌ای سیستم بلاک‌چین را نشان می‌دهد.

1. Proof of work
2. Cloud services

در مقابل، محدودیت‌های فنی و چالش‌هایی نیز در تکنولوژی بلاک‌چین وجود دارد. سوان [۳] چالش‌ها و محدودیت‌های فنی‌ای را ارائه کرده‌است که در آینده‌ی این تکنولوژی باید درنظر گرفته شوند:

توان عملیاتی: مشکل اصلی در تکنولوژی بلاک‌چین توان عملیاتی بالقوه است که در حال حاضر به 7tps (تراکنش در ثانیه) بسط داده شده‌است. سایر شبکه‌های پیش‌رو VISA (۲۰۰۰ تراکنش در ثانیه) و توییتر (۵۰۰۰ تراکنش در ثانیه) هستند. وقتی فرکانس در شبکه به سطح مشخصی افزایش می‌یابد، توان عملیاتی باید حفظ شود.



شکل ۲. معماری بلاک‌چین که شامل بلوک‌های مختلف ترتیبی است.

تأخیر: برای تکمیل یک تراکنش تقریباً ده دقیقه زمان لازم است و این زمان جهت ایمنیِ بلوک تراکنش که در بیت‌کوین می‌تواند ایجاد شود کافی است. اما زمان بیشتری باید به یک بلوک اختصاص داده شود تا کارایی در امنیت حاصل گردد، زیرا باید هزینه‌ی حملات مضاعف را جبران کند. وقتی پول بیش از یک بار پرداخت شود، آنگاه دو بار خرج کردن[1] رخ می‌دهد. با احراز هویت، هر تراکنش که به بلوک اضافه می‌شود، بیت‌کوین می‌تواند به کاربر برای اجتناب از دو بار خرج کردن کمک و تضمین کند که هیچ ورودی قبلی در تراکنش‌های قبلی پرداخت نشده‌است [۱۲]. بنابراین در شرایط فعلی، تأخیر یک مشکل بزرگ تلقی می‌شود. در حالی که امنیت تأمین می‌شود، در عرض چند ثانیه تراکنش باید با ایجاد بلوک‌ها تکمیل شود. برای مثال، در VISA، تراکنش می‌تواند در عرض چند ثانیه تکمیل گردد که در مقایسه با بلاک‌چین مفید است.

اندازه و پهنای باند: در فوریه‌ی ۲۰۱۶، اندازه‌ی شبکه‌ی بیت‌کوین بیش از ۵۰۰۰۰ MB بوده‌است. وقتی بازدهی به سطح VISA برسد، در هر سال، ظرفیت بلاک‌چین ۲۱۴ مگابایت رشد خواهد داشت. جامعه‌ی بلاک‌چین فرض می‌کند که اندازه‌ی یک بلوک ۱MB است و هر ده دقیقه یک بلوک ایجاد می‌شود [۱۳] که به‌واسطه‌ی آن، تعداد تراکنش‌هایی

1. Double - spending

که می‌تواند در هر لحظه کنترل شود با محدودیت مواجه می‌شود (۵۰۰ عملیات در یک بلوک به‌طور میانگین) [۱۴]. اگر تکنولوژی بلاک‌چین بخواهد تعداد بیشتری تراکنش را مدیریت کند، مشکلات اندازه و پهنای باند باید حل شوند.

امنیت: در حال حاضر، امکان حمله به بلاک‌چین تقریباً ۵۱ درصد است. در حالت ۵۱ درصد، حمله به کل شبکه‌ی نرخ هش ماینینگ با یک موجودیت کاملاً قابل‌کنترل خواهد بود و بنابراین می‌تواند بلاک‌چین را تحت تأثیر قرار دهد. ازاین‌رو حل مشکل امنیت نیازمند مطالعه و تحقیق بیشتری است [۱۵].

منابع تلف‌شده: مقدار انرژی بسیار زیادی (۱۵ میلیون دلار در روز) هنگام استخراج بیت‌کوین تلف می‌شود. اثبات کار (POW) منجر به اتلاف انرژی درمورد بیت‌کوین می‌شود. در زمینه‌ی صنعت، جایگزین‌هایی مانند اثبات سهام[1] وجود دارد. به کمک اثبات کار، می‌توان تعیین کرد که استخراج‌کننده چقدر کار انجام داده‌است [۱۶]. برای مثال، اگر فردی ۱ درصد بلاک‌چین داشته باشد، می‌تواند تقریباً ۱ درصد از بلاک‌چین اثبات سهام را استخراج کند [۱۶]. برای استخراج هرچه مؤثرتر، باید مشکل اتلاف منابع حل شود.

کاربردپذیری: در توسعه‌ی برنامه‌نویسی کاربردی (API) بیت‌کوین، ارائه‌ی خدمات بسیار دشوار است. در بلاک‌چین، باید API مناسب‌تری ارائه شود که می‌تواند مشابه با APIهای REST باشد.

نسخه‌بندی و زنجیره‌های چندگانه: وقتی زنجیره‌ی کوچک متشکل از گره‌های کم است، امکان حمله تقریباً ۵۱ درصد بیشتر است. مشکل دیگر زمانی بروز می‌کند که زنجیره‌ی هدف نسخه‌سازی یا مدیر تقسیم می‌شود.

به‌طور کلی، این تکنولوژی به گونه‌ای که روزانه به‌صورت آزمایشی اجرا شود، قابلیت تغییر تراکنش را دارد. به‌علاوه، کاربرد بلاک‌چین نه‌تنها محدود به ارزهای دیجیتال نیست، بلکه می‌تواند در سایر زمینه‌های مختلف که در آن تراکنش انجام می‌شود به‌کار رود. در همین راستا، کاملاً گنجکاویم که ابعاد مختلف بلاک‌چین را بررسی کنیم، اما در حال حاضر بلاک‌چین با محدودیت‌ها و تهدیدهایی همراه است.

سه ویژگی ناشناس ماندن، یکپارچگی داده‌ها و ویژگی‌های امنیتی چالش‌های زیادی را به‌دنبال دارد و در این خصوص، باید ضمن بررسی و ارزیابی‌های زیاد پاسخ شفاف ارائه شود. مسئله‌ی دیگری که باید در تحقیقات آتی مدنظر قرار گیرد مقیاس‌پذیری است. ازاین‌رو درک و بررسی تحقیقات انجام‌شده در زمینه‌ی بلاک‌چین بسیار حائز اهمیت است و برای این منظور، باید تمام مقالات مهم و تحقیقات مرتبط موجود در این زمینه جمع‌آوری شوند. بنابراین براساس تحقیقات انجام‌شده، می‌توانیم چالش‌ها و محدودیت‌های ارائه‌شده و حل‌شده را بدانیم و زمینه‌های مختلفی که در بلاک‌چین نیازمند توجه هستند را بشناسیم [۱۷].

1. Proof of stake

در گذشته، اغلب تراکنش‌ها برای تأیید تراکنش‌های آنلاین دارایی‌های دیجیتال روی شخص ثالث تمرکز داشتند، اما در حال حاضر، بازار موجود در تکنولوژی بلاک‌چین می‌تواند در زمینه‌ی تراکنش‌های مالی و غیرمالی به‌کار رود. در سال ۱۹۹۴، کاربرد دیگری به نام «قراردادهای هوشمند» توسط نیک سابو[1] معرفی شد و بیشتر یک ایده‌ی شگفت‌انگیز بود که در آن شرکت‌کنندگان می‌توانستند به‌طور خودکار قراردادی را بین خودشان اجرا کنند. تا زمانی که ایده‌ی ارز دیجیتال معرفی نشده بود، این ایده خیلی کاربردی و مورد استفاده نبود. اما وقتی شرایط لازم برای برنامه‌نویسی یک توافق قراردادی فراهم شد، بلاک‌چین و قرارداد هوشمند توانستند به‌طور هم‌زمان کار کنند. قراردادهای هوشمند درواقع پروتکل‌های مشخصی هستند که به‌طور خودکار توسط کامپیوترها اعمال می‌شوند.

به کمک تکنولوژی بلاک‌چین، وظیفه‌ی ثبت، احراز هویت و اجرای قراردادهای هوشمند راحت‌تر انجام می‌شود. شرکت‌های بسیاری نظیر اتریوم و کودیس[2] که قراردادهای هوشمند در آن‌ها از تکنولوژی بلاک‌چین استفاده می‌کنند دارای ماهیتی منبع باز هستند. بسیاری از شرکت‌ها در حال حاضر، روی تکنولوژی‌های بیت‌کوین و بلاک‌چینی کار می‌کنند که از قراردادهای هوشمند پشتیبانی می‌نمایند [۱۸].

موارد متعددی وجود دارد که در آن‌ها دارایی‌ها تنها زمانی می‌توانند منتقل شوند که شرط‌های مشخصی برآورده شود و این نیازمند آن است که وکیلان توافق‌نامه‌ای تنظیم کنند و بانک‌ها خدمات امانی را که می‌تواند جایگزین قراردادهای هوشمند شود ارائه دهند. اتریوم به‌علت داشتن پلتفرم قابل‌برنامه‌نویسی، توانست حس کنجکاوی را برانگیزد. ارز دیجیتال اتریوم می‌تواند توسط هرکسی ایجاد شود و برای پرداخت قراردادهای هوشمند به‌کار رود. برای پرداخت سایر خدمات یا خدمات اضافی، اتر[3] خود ارز دیجیتال اتریوم است. دامنه‌ی گسترده‌ای از کاربردها درمورد اتریوم وجود دارد که شامل کاربردهای دولتی، بانک‌های مستقل، دسترسی بدون کلید، سرمایه‌گذاری جمعی، تجارت مشتقات مالی و مخارج با استفاده از قراردادهای هوشمند است. نه‌تنها ارزهای دیجیتال در دسترس هستند، بلکه بلاک‌چین‌های بسیاری موجودند که دامنه‌ی گسترده‌ای از کاربردها را پشتیبانی می‌کنند. در حال حاضر، سه رویکرد در صنعت وجود دارد که می‌توانند سایر کاربردها را پشتیبانی و به غلبه بر محدودیت تخمینی بلاک‌چین بیت‌کوین کمک کنند [۱۹]. در یک دارایی دیجیتال خاص، برای رسیدن به یک اتفاق‌نظر در سطح توزیع‌شده،

1. Nick Szabo
2. Codius
3. Ether

سیستمی از الگوریتم بلاک‌چین به‌کار می‌رود که به آن بلاک‌چین جایگزین[1] گفته می‌شود. استخراج ترکیبی[2] فرایندی است که در آن ماینرها می‌توانند با شبکه‌ی والد اشتراک داشته باشند. ازجمله کاربردهای متعدد پیشنهادی بلاک‌چین می‌توان به DNS، مرجع صدور گواهی دیجیتال SSL، ذخیره‌ی فایل و رأی‌گیری اشاره کرد.

در رأس تکنولوژی بلاک‌چین با اعمال قابلیت‌هایی فراتر از ایجاد دارایی‌های دیجیتال، یک منبع باز به نام سکه‌های رنگی[3] وجود دارد که روش‌های مختلفی در اختیار توسعه‌دهندگان جهت ایجاد دارایی‌های دیجیتال قرار می‌دهد. زنجیره‌های جانبی[4] بلاک‌چین‌های جایگزینی هستند که توسط بیت‌کوین‌ها از طریق قرارداد بیت‌کوین پشتیبانی می‌شوند (مانند طلا که بعضی دلارها و پوندها را هک می‌کند).

امکان داشتن هزاران زنجیره‌ی جانبی متصل به بیت‌کوین که هریک ویژگی‌ها و اهداف مختلفی دارند وجود دارد که تمام آن‌ها از مزیت کمیابی و انعطاف‌پذیری تضمین‌شده توسط بلاک‌چین بیت‌کوین بهره‌مند هستند.

۳. کاربردهای تکنولوژیکی

۳-۱. حوزه‌ی مالی

الف اوراق بهادار خصوصی[5]

می‌دانیم تبدیل یک شرکت به سهامی عام بسیار پرهزینه است. در این راستا، فرایندهای بسیاری باید توسط اتحادیه‌های صنفی بانکی انجام شود که شامل فرایندهای پذیره‌نویسی و جذب سرمایه‌گذاران مختلف است. شرکت‌هایی که در دسته‌ی شرکت‌های سهامی عام قرار می‌گیرند با بازار ثانویه شریک می‌شوند تا در صورت وقوع معاملات، عملکرد درست و به‌موقعی داشته باشند. با استفاده از تکنولوژی بلاک‌چین، شرکت‌ها می‌توانند بی‌وقفه سهام را عرضه کنند. بعضی سهام‌هایی که در رأس بلاک‌چین قرار دارند می‌توانند به‌طور مستقیم در بازار ثانویه خرید‌وفروش شوند. مواردی از این دست در ادامه بیان می‌شود.

سهام خصوصی NASDAQ: در سال ۲۰۱۴، NASDAQ سهام خصوصی خود را راه‌اندازی کرد. NASDAQ برای بعضی شرکت‌های عرضه‌ی سهام اولیه[6] و خصوصی جهت نظارت

---

1. Alternative blockchain
2. Merged mining
۳. سکه‌های رنگی یا colored coins روشی برای نمایش و مدیریت دارایی‌های دنیای واقعی در بلاک‌چین بیت‌کوین هستند.
4. Side chain
5. Private Securities
6. Pre-IPO

بر عملکردهای حیاتی نظیر جدول سهام‌داری[1] و مدیریت روابط سرمایه‌گذار راه‌اندازی شده‌است. از آنجا که چندین شخص ثالث در رویکرد خریدوفروش سهام در فرایند تبادل حضور دارند، این فرایند بسیار کند و ناکارامد است [۲۰]. یک همکاری مشترک بین NASDAQ و یک استارت‌آپ جدید به نام chain.com برای تبادل سهام خصوصی در بلاک‌چین وجود دارد. برای پیاده‌سازی تبادل، chain.com از قراردادهای هوشمند مبتنی بر بلاک‌چین استفاده می‌کند. پیش‌بینی می‌شود که عملکرد این تبادل سریع، قابل‌توجه و کارامد باشد. با استفاده از بلاک‌چین به‌عنوان طرف قرارداد در پیاده‌سازی، مدیچی[2] به‌عنوان یک تبادل سهام توسعه داده شده‌است. تمرکز اصلی معطوف به ایجاد بازار سهامی است که نهایت تکنولوژی باشد. به‌واسطه‌ی پروتکل طرف قرارداد، ابزار مالی سنتی می‌تواند به‌صورت قراردادهای هوشمندِ خوداجرا پیاده‌سازی شود. بنابراین شرایط قرارداد فیزیکی به‌واسطه‌ی این قراردادهای هوشمند حذف می‌شود. قراردادهای مختلف می‌توانند مورد مذاکره قرار گیرند، آسان و اجرا شوند و همچنین شرایط شخص ثالث واسطه شامل کارگزار، صرافی یا بانک را حذف کنند.

برای پرداختن به مشکلات مختلف مرتبط با ارزهای دیجیتال جایگزین، مانند تکه‌تکه‌شدگی و امنیت، یک پروژه‌ی منبع باز با تأکید بر زنجیره‌ی جانبی معرفی می‌شود که موارد استفاده از آن می‌تواند شامل تسهیل در ثبت قراردادهای مختلف و اجرای آن و همچنین حذف الزام شخص ثالث به‌عنوان واسطه مشتمل بر کارگزار، صرافی یا بانک باشد. از دیگر موارد استفاده‌ی آن می‌توان به ثبت اوراق بهادار همچون سهام، اوراق قرضه و امثال آن برای حصول اطمینان از امنیت موجودی بانکی و وام مسکن اشاره کرد.

یک صرافی جدید بیت‌کوین مستقر در نیویورک به نام کوین‌استارتر[3] وجود دارد که در حال کار برروی پروژه‌ای تحت عنوان های‌لاین[4] است. به‌واسطه‌ی این پروژه و به کمک تکنولوژی بلاک‌چین، تراکنش مالی برخلاف T+3 یا T+2 روز، در عرض T+10 دقیقه تسویه می‌شود.

بازارهای دیگری ازجمله آگر[5] با ماهیتی غیرمتمرکز وجود دارد که در آن کاربران می‌توانند سهام را با پیش‌بینی احتمال وقوع کانال‌ها در آینده خریدوفروش کنند. بنابراین براساس «خرد جمعی» می‌توانند برای انجام تراکنش‌های مالی و پیش‌بینی اقتصادی نیز به‌کار روند.

1. Cap table
2. Medici
3. CoinStarter
4. Highline
5. Augur

توکن‌های دیجیتالی به نام بیت شیر[1] نیز وجود دارد که در بلاک‌چین و دارایی‌های خاص - مرجع نظیر ارز دیجیتال یا کالاها قرار می‌گیرند که ویژگی‌های منحصربه‌فردی به صاحبان توکن علاقه‌مند به کالاهایی مانند طلا و نفت و همچنین دلار، یورو و ابزارهای ارزی ارائه می‌کند.

ب بیمه

بلاک‌چین می‌تواند دارایی‌های منحصربه‌فرد را ثبت کند. این دارایی‌ها توسط یک یا چند شناسه مشخص می‌شود و حذف یا تکرار آن‌ها چالش‌برانگیز است. این موضوع می‌تواند در احراز هویت پیشینه‌ی مالکیت، تراکنش‌های گذشته و همچنین مکان‌یابی به‌کار رود. هر مالکیتی (مادی یا دیجیتالی مانند املاک و مستغلات، اتومبیل، دارایی‌های فیزیکی، لپ‌تاپ و سایر اشیای باارزش) می‌تواند توسط بیمه‌گذار تأیید شود و همچنین توسط بلاک‌چین ثبت گردد و یا به مالکیت بلاک‌چین درآید [۲۱].

دفتر کل دائمی گواهی‌نامه‌ی الماس توسط شرکتی به نام اورلجر[2] تهیه شده‌است که در آن پیشینه‌ی تراکنش‌ها نیز قابل‌پیگیری است. ویژگی‌های منحصربه‌فرد الماس که آن را از سایرین متمایز می‌کند ارتفاع، عرض، وزن، عمق و رنگ هستند که در بلاک‌چین ثبت و بخشی از آن می‌شوند. این الماس‌ها می‌توانند توسط شرکت‌های بیمه با اجرای قوانین مختلف از طریق سازمان‌های اجرایی، مالکان و مطالبه‌کنندگان تأیید شوند. API خدمات وب می‌تواند به‌سادگی در اورلجر به‌منظور تأیید الماس، بررسی و به‌روزرسانی ادعاهای شرکت‌های بیمه و در گزارش‌هایی مشابه گزارش‌های پلیس به‌کار رود.

۳-۲. حوزه‌ی غیرمالی

الف دفتر اسناد رسمی

بلاک‌چین می‌تواند هویت اسناد مختلف را تأیید کند و شرایط لازم برای اختیار متمرکز را حذف نماید. خدمات تأیید سند در اثبات مالکیت (چه کسی مالک است)، اثبات موجودیت (در یک زمان مشخص) و اثبات یکپارچگی (دست‌کاری نشدن) اسناد قطعاً مفید خواهد بود. این خدمات از نظر قانونی محدود شده‌اند، زیرا می‌توانند توسط شخص ثالث احراز هویت شوند و تقلبی بودن آن‌ها نیز اثبات گردد.

فناوری بلاک‌چین را می‌توان برای تأیید آن‌گونه اسناد رسمی به‌کار برد که به حصول اطمینان از حفظ حریم خصوصی سند کمک می‌کند. با کمک رمزنگاری فایل‌های مختلف در بلاک‌چین، می‌توان زمان ثبت اسناد رسمی را به سطح بالاتر بعدی برد. تکنولوژی بلاک‌چین همچنین می‌تواند در حذف هزینه‌های اسناد رسمی که بسیار گران هستند و روش‌های نامناسب انتقال سند مفید واقع شود [۲۲].

1. Bit share
2. Everledger

یک شرکت بلاک‌چین به نام استمپری[1] فایل‌های متعددی را از طریق ایمیل ارسال می‌کند. هر ایمیل توسط فردی که پست الکترونیکی انفرادی و خاص ایجاد کرده‌است از طریق ارسال ایمیل ویژه به او تأیید می‌شود. شرکت‌ها و سازمان‌های حاکمیتی متعددی وجود دارد که از تکنولوژی استمپری جهت احراز هویت اسناد به روشی مقرون‌به‌صرفه استفاده می‌کنند.

برای خدمات دفتر اسناد رسمی، شرکتی تحت عنوان ویاکوین[2] برای تسهیل پروتکل به‌کار می‌رود. با استفاده از شبکه‌ی بیت‌کوین TestNet3 یا شبکه‌ی بیت‌کوین، اثبات وجود می‌تواند با اپلیکیشن iOS به نام بلوک نوتری[3] ایجاد شود. اسناد می‌توانند به کمک تعداد کمی بیت‌کوین تأیید شوند، به طوری که بتوانند در بلاک‌چین عمومی و برای اسناد رسمی عمومی رمزنگاری‌شده ثبت گردند.

خدمات دیگری تحت عنوان اثبات موجودیت وجود دارد که جهت استفاده از بلاک‌چین در اسناد SHA256 خلاصه‌شده کاربرد دارد.

با کمک بلاک‌چین، شرکتی به نام اسکرایب[4] در زمینه‌ی تأیید تألیف فعالیت می‌کند. با انتساب به نویسنده‌ی اصلی، مالکیت سرویس قابل‌انتقال است.

ب کاربردهای بلاک‌چین در صنعت موسیقی

در چند دهه‌ی اخیر، تحولات عظیمی در صنعت موسیقی به‌واسطه‌ی دیجیتالی شدن رخ داده‌است؛ خدمات جاری[5] به سطح بعدی رفته و آگاهی درباره‌ی خدمات اینترنتی افزایش یافته‌است. این تحول تمام افراد فعال در صنعت موسیقی ازجمله هنرمندان، ناشران، ترانه‌سراها و سایر ذینفعان که خدمات جریانی ارائه می‌دهند را تحت تأثیر قرار داده‌است. به‌علت ظهور اینترنت، فرایند تعیین حق امتیاز پیچیده‌تر شده و نیاز به شفافیت بیشتر درباره‌ی پرداخت حق امتیاز هنرمندان و ترانه‌سراها ایجاد شده‌است [۲۳].

صنعت موسیقی یکی از حوزه‌هایی است که در آن بلاک‌چین نقش مهمی ایفا می‌کند. به کمک این تکنولوژی، یک پایگاه داده‌ی توزیع‌شده‌ی جامع و دقیق را می‌توان ایجاد کرد که حق مالکیت را در یک دفتر کل عمومی ثبت می‌کند. قراردادهای هوشمند نیز می‌توانند حق مالکیت و سایر حقوق مربوطه را تعیین کنند. رابطه میان سهام‌داران مختلف تعیین شده‌است و تعاملات میان آن‌ها به کمک قراردادهای هوشمند به‌طور خودکار اعمال خواهد شد.

---

1. Stampery
2. Viacoin
3. Block notary
4. Ascribe

۵. رسانه‌ی جاری یا استریمینگ به آن دسته از محتوای چندرسانه‌ای گفته می‌شود که هم‌زمان با ارسالش از طرف فرستنده‌ی محتوا، توسط گیرنده‌ی محتوا قابل‌نمایش است. به بیان دیگر، گیرنده‌ی محتوا نیاز ندارد که ابتدا تمام محتوا را دانلود کند تا بتواند آن را ببیند، بلکه فرستنده می‌تواند محتوا را به‌صورت جاری ارسال یا به‌اصطلاح استریم کند.

۴. اثبات غیرمتمرکز وجود اسناد

در هر راه‌حل قانونی، تأیید وجود مرحله‌ی بعدی (نشست بعدی)[1] اسناد امضاشده بسیار حیاتی است [۲۴]. بعضی چالش‌های امنیتی در مدل سنتی اعتبارسنجی اسناد وجود دارد که از مقامات مرکزی برای ذخیره‌سازی و تأیید اسناد استفاده می‌کند. هرچه اسناد قدیمی‌تر باشد، این کار دشوارتر است.

تکنولوژی بیت‌کوین مدل جایگزینی برای اثبات موجودیت[2] و همچنین مالکیت شرکت‌های قانونی ارائه می‌دهد. اثبات آنلاین اسناد مختلف می‌تواند به کمک خدماتی تحت عنوان اثبات موجودیت به‌طور گمنام ایمن شود. وقتی کاربر سندی را ثبت می‌کند، خدمات اثبات موجودیت خلاصه‌ی رمزنگاری‌شده‌ی فایل را ذخیره می‌کند. باید درنظر داشت که صرفاً خلاصه‌ی رمزنگاری‌شده یا اثرانگشت ذخیره می‌شود و سند واقعی ذخیره نمی‌گردد. در این زمینه، کاربر نباید نگران حفظ حریم خصوصی و امنیت اطلاعات باشد. بعد از یک مدت‌زمان مشخص، تأیید وجود سند مجاز است. امضا و مهرِ زمانی مربوط به سند قانونی را می‌توان به‌راحتی با استفاده از فناوری بلاک‌چین ذخیره کرد و توسط مکانیزم‌های بلاک‌چین احراز هویت نمود [۲۵].

مزایای اصلی اثبات موجودیت این است که به کاربر اجازه می‌دهد امنیت و حریم خصوصی خود را حفظ کند و به کنترل‌کننده نیز امکان نگهداری مدارک متفرقه‌ی سند را می‌دهد. بنابراین وجود سند با به‌کارگیری تکنولوژی بلاک‌چین تأیید می‌شود بدون این‌که به یک موجودیت متمرکز واحد متکی باشد.

۴-۱. ذخیره‌سازی غیرمتمرکز

برای ذخیره‌ی انواع مختلف فایل‌ها مانند عکس، فیلم و موسیقی، انواع مختلفی از خدمات ابری ذخیره‌سازی فایل مانند دراپ باکس[3]، گوگل درایو[4] یا وان درایو[5] وجود دارد که توجه زیادی را به خود جلب کرده‌اند. اما علی‌رغم این جلب‌توجه و علاقه، ذخیره‌سازی فایل‌ها در ابر با محدودیت‌های امنیتی، حفظ حریم خصوصی و کنترل داده همراه است. مهم‌ترین مشکل این است که حتی در مورد فایل‌های محرمانه، فرد مجبور است به شخص ثالث اعتماد کند.

پلتفرم‌های ذخیره‌سازی ابری توزیع‌شده‌ی نظیربه‌نظیر را می‌توان توسط فناوری بلاک‌چین معروف به استورج[6] ارائه کرد که به کاربر در تبادل و انتقال داده‌ها بدون

1. Post-session
2. Proof of existence
3. Dropbox
4. Google drive
5. One drive
6. Storj

وابستگی به شخص ثالث کمک می‌کند. در چنین مواردی می‌توان از پهنای باند غیرعادی استفاده کرد و همچنین فضای اختصاصی در کامپیوترهای شخصی را می‌توان برای میکروپرداخت‌های مبتنی بر بیت‌کوین به‌کار برد [۲۶].

در صورت فقدان کنترل مرکزی، امنیت، حریم خصوصی و کنترل داده‌ها به میزان قابل‌توجهی افزایش می‌یابد و همچنین محافظه‌کارانه‌ترین خرابی‌ها و قطعی‌ها را حذف می‌کند. پلتفرم استورج در راستای مشارکت مناسب در شبکه استفاده می‌شود و برای ایجاد انگیزه به الگوریتمی چالشی متکی است. بنابراین در این سبک، یکپارچگی و دسترس‌پذیری فایل‌ها می‌تواند به‌صورت رمزنگاری‌شده و با کمک استورج بررسی شود و به روشی مستقیم به کسانی که در نگهداری فایل‌ها سهیم هستند پاداش داد. در مثالی مشابه، می‌توان دید که انگیزه و روش پرداخت هردو می‌تواند توسط میکروپرداخت‌های مبتنی بر بیت‌کوین انجام شود. از طرف دیگر، بلاک‌چینی مجزا برای فایل‌های متاداده به‌کار می‌رود.

۲-۴. اینترنت اشیای غیرمتمرکز

اینترنت اشیا[1] (IoT) توجه زیادی را به خود جلب کرده و به تکنولوژی متداولی در هر دو حوزه‌ی فضای مشتری و فضای سازمانی بدل شده‌است [۲۷ و ۲۸]. پلتفرم‌های IoT متعددی وجود دارد که مبتنی بر مدل متمرکز هستند و در آن کنترل و هماهنگی میان وسایل توسط هاب یا کارگزار کنترل می‌شود. اما موارد گوناگونی وجود دارد که در آن‌ها این روش کاملاً غیرعملی و غیرکاربردی است، چراکه وسایل هوشمند باید داده‌ها را میان خودشان به‌طور مستقل تغییر دهند. این نیاز خاص منجر به ارائه‌ی پلتفرم‌های IoT غیرمتمرکز شده‌است. پیاده‌سازی پلتفرم‌های IoT غیرمتمرکز می‌تواند به کمک تکنولوژی بلاک‌چین آسان شود که شامل ثبت رکوردها و تبادل داده‌ی ایمن و قابل‌اعتماد است. در این سبک معماری، دفتر کل عمومی توسط تکنولوژی بلاک‌چین فراهم می‌شود و تمام پیام‌های ارسال‌شده در توپولوژی غیرمتمرکز میان وسایل هوشمند را به‌طور قابل‌اعتماد ثبت می‌کند.

ADEPT (تله‌متری[2] نظیربه‌نظیر غیرمتمرکز مستقل) پلتفرمی است که توسط IBM و سامسونگ به‌طور مشترک معرفی شده‌است و در صورتی که بیت‌کوین‌ها و شبکه‌های توزیع‌شده‌ی وسایل و یا اینترنت اشیای غیرمتمرکز ساخته شده باشد، از این طرح استفاده

1. Internet of things

۲. Telemetry یا دوری‌سنجی به معنای ضبط اطلاعات اندازه‌گیری‌شده و ارسال آن‌ها با استفاده از خطوط ارتباطی یا از طریق ارتباط بی‌سیم است.

می‌شود. سه پروتکل وجود دارد که در ADEPT به‌کار می‌رود: بیت‌تورنت[1] (اشتراک فایل)، اتریوم[2] (قراردادهای هوشمند) و تله‌هش[3] (ارسال پیام نظیربه‌نظیر).

فیلامنت[4] استارت‌آپی است که یک دسته نرم‌افزار IoT غیرمتمرکز ارائه می‌دهد که از بلاک‌چین بیت‌کوین استفاده می‌کند تا توسط آن وسایل قادر به نگهداری هویت‌های منحصربه‌فرد روی یک دفتر کل عمومی باشند.

۴-۳. بلاک‌چین مبتنی بر شرایط ضدجعل

در کسب‌وکارهای معاصر، یکی از چالش‌های متداول و به‌ویژه یکی از بزرگ‌ترین مشکلاتی که تجارت دیجیتال در سناریوی امروز با آن دست‌وپنجه نرم می‌کند مشکل جعل است. راه‌حل این مشکل وابسته به شخص ثالثی است که حساسیت منطقی را بین فروشندگان و مشتریان در این سناریو اعمال می‌کند.

مسئله‌ی مکانیزم جعل می‌تواند با تکنولوژی بلاک‌چین از طریق پیاده‌سازی‌های غیرمتمرکز و قابلیت‌های امنیتی آن مدیریت شود. شرایطی را فرض کنید که در آن تمام فروشندگان، برندهای معروف و بازارها سیستم بلاک‌چین گره‌های مختلفی را به‌اشتراک می‌گذارند که در آن‌ها مستندات می‌تواند ذخیره شود و صحت و اعتبار محصول تأیید گردد. با استفاده از تکنولوژی بلاک‌چین، ذینفعان زنجیره‌ی تأمین به موجودیتی متمرکز برای تأیید محصولات انحصاری وابسته نیستند.

راه‌حل‌های ضدجعل را می‌توان به کمک تکنولوژی بلاک‌چین با استفاده از تأیید بلوک ارائه کرد که منجر به شفافیت در زنجیره‌ی تأمین می‌شود. کاربردهای مختلفی در حوزه‌های گوناگون مانند حوزه‌های دارویی، اقلام لوکس، الماس و صنایع الکترونیک وجود دارد.

۵. بلاک‌چین در حوزه‌ی اینترنت

یک تکنولوژی بلاک‌چین دیگر به نام نیم‌کوین[5] وجود دارد که دارای تغییرات اندک است و به کمک آن نسخه‌ی غیرمتمرکز DNS[6] را می‌توان پیاده‌سازی کرد که قابلیت از بین رفتن ندارد. در حال حاضر، سرورهای DNS عمدتاً توسط سازمان‌ها و شرکت‌های بزرگ سفارش داده می‌شوند؛ در صورت استفاده‌ی مشتری از اینترنت، امکان سانسور، سرقت یا جاسوسی وجود دارد. با استفاده از تکنولوژی بلاک‌چین، دفترتلفن یا DNS اینترنت می‌تواند به روشی غیرمتمرکز نگهداری شود و کاربران مربوطه می‌توانند رکوردهای دفترتلفن مشابهی را در محیط کاری خود نگهداری کنند.

1. BitTorrent
2. Ethereum
3. Telehash
4. Filament
5. Namecoin
6. Domain Name System

برای مدیریت دیجیتال گواهی‌نامه‌ها و به‌منظور توزیع متمرکز، تکنولوژی زیرساخت کلید عمومی کاربرد گسترده‌ای دارد. برای تأیید گواهی‌نامه‌ی دیجیتال، هر دستگاه باید دارای اعتبار اصل مرجع صدور گواهی دیجیتال (CA) باشد [۲۹]. با این‌که تکنولوژی PKI کاربرد بسیار زیادی دارد و بسیار موفق است، اما مسئله‌ی مقیاس‌پذیری آن به CA وابسته است. ویژگی‌های بلاک‌چین می‌توانند بعضی مشکلات PKI را با استفاده از ویژگی زیرساخت امنیت بدون کلید (KSI[1]) آسان و حل کنند.

تابع هش رمزنگاری درمورد KPI[2] استفاده می‌شود که مجوز تأیید وابسته به ایمنی توابع هش و همچنین در دسترس بودن بلاک‌چین را صادر می‌کند.

۵-۱. ریسک‌های استفاده

تکنولوژی بلاک‌چین امیدوارکننده و موفقیت‌آمیز است. همان‌طور که قبلاً گفته شد، برخی از برنامه‌ها یا مشکلات متعدد را می‌توان با کمک فناوری بلاک‌چین حل کرد و مسایل مالی (حواله‌جات بانکی و سرمایه‌گذاری) را در حوزه‌ی برنامه‌های کاربردی غیرمالی مانند خدمات اسناد رسمی وارد نمود.

۵-۲. تغییر رفتار

تغییر جزء جدانشدنی زندگی بشر است و مقاومت در برابر آن کاملا بدیهی است. مشتریان باید بدانند که انتقال الکترونیکی که انجام می‌دهند در شرایط فعلی ایمن و کامل است. همچنین در نقش‌ها و مسئولیت‌های واسطه‌ها مانند Visa یا Mastercard (برای کارت‌های اعتباری) تغییراتی ایجاد خواهد شد و به‌طور حتم این شرکت‌ها در بلاک‌چین سرمایه‌گذاری خواهند کرد و تمام پلتفرم‌های آن‌ها نیز به سمت پلتفرم‌های مبتنی بر این فناوری حرکت خواهند نمود، چراکه برای حفظ روابط مشتری، شرکت‌های کارت اعتباری به ارائه‌ی این قبیل خدمات نیازمند خواهند بود.

۵-۳. مقیاس‌پذیری

موضوع مقیاس‌پذیری به‌عنوان چالش در ارائه‌ی خدمات مبتنی بر فناوری بلاک‌چین در مرحله‌ی ابتدایی وجود دارد. بیایید فرض کنیم که برای اولین بار تراکنش‌های بلاک‌چین را انجام می‌دهیم. در این حالت، شخص باید کل مجموعه‌ی بلاک‌چین را دانلود کند و قبل از انجام اولین فعالیت تجاری، باید آن را احراز هویت نماید. این امر می‌تواند مدت‌زمان زیادی طول بکشد، زیرا تعداد بلوک‌ها به‌طور تصاعدی افزایش می‌یابد [۳۰].

---

۱. یک فناوری بلاک‌چین است که در استونی طراحی شده و در سطح جهانی استفاده می‌شود تا اطمینان حاصل شود که شبکه‌ها، سیستم‌ها و داده‌ها همگی با حفظ صددرصد حریم خصوصی داده‌ها عاری از هرگونه خطری هستند.

2. Key Public Infrastructure

۴-۵. بوت‌استرپینگ[1] (خودراه‌اندازی)

اگر مجبور باشیم چهارچوب اسناد تجاری یا اسناد موجود را به روش جدید بلاک‌چین منتقل کنیم، مجموعه‌ی مهمی از وظایف مرتبط با این جابه‌جایی باید انجام شود. برای مثال، اگر مالکیت املاک و مستغلات را درنظر بگیریم، اسناد موجود که هنوز در دفترهای اسناد رسمی قرار دارند باید به شکل معادل در بلاک‌چین منتقل شوند. این فرایند می‌تواند زمان و هزینه‌ی بسیار زیادی را دربر گیرد [۳۱].

۵-۵. قوانین دولتی

کمیسیون تجارت فدرال ایالات متحده‌ی آمریکا (FTC[2]) و کمیسیون بورس و اوراق بهادار (SEC[3]) سازمان‌های دولتی هستند که می‌توانند با معرفی قوانین جدید، نظارت و تأسیس سازمان‌های مختلف جهت پذیرش و موافقت در راستای تسریع در فرایند ایجاد نهادهای نوظهور و مبتنی بر تکنولوژی بلاک‌چین اقدام کنند [۲۷]. بنابراین شرایط پذیرش نهادهای مبتنی بر بلاک‌چین در ایالات متحده‌ی آمریکا به دلیل جلب اعتماد اکثر مشتریان و نمایندگان آن‌ها قابل‌قبول است. هرچند در اقتصادهایی مانند چین که بیشتر کنترل می‌شوند، روند پذیرش با چالش‌های مهمی همراه خواهد بود.

۶-۵. فعالیت‌های کلاه‌بردارانه

هرچند تکنولوژی بلاک‌چین ویژگی‌های مثبت، قابلیت‌ها و مزایای بسیار زیادی دارد، اما همین ویژگی‌ها می‌توانند توسط بعضی افراد به‌منظور کلاه‌برداری‌هایی مانند قاچاق پول به‌کار روند. بنابراین برای جلوگیری از چنین اقداماتی و به حداقل رساندن فعالیت‌های کلاه‌بردارانه، باید قوانین و مقررات قوی و پشتیبانی‌های تکنولوژیکی وضع شود و بازرسان با اعمال قوانینی بر نظارت و بازبینی خود بیفزایند [۳۲].

۷-۵. محاسبات کوانتومی

فناوری بلاک‌چین به جهت محاسبات پیچیده‌ی ریاضی به قدرت رایانه‌ای بسیار بالایی نیاز دارد. به کمک روش کورکورانه‌ی محض[4] و به‌واسطه‌ی پیشرفت‌های آتی در کوانتوم کامپیوترها، کلیدهای رمزنگاری می‌توانند به‌سادگی کرک شوند. به همین دلیل، کل سیستم به زانو در خواهد آمد. در مقابل نیز توافقی وجود دارد که می‌گوید این کلیدهای رمزنگاری قوی‌تر و کرک کردن آن‌ها سخت‌تر می‌شود [۲۸].

1. Bootstrapping
2. Federal Trade Commission
3. Securities and Exchange Commission
4. Sheer brute force

۵-۸. تأمین بودجه‌ی شرکتی و بهره

در سپتامبر و اکتبر سال ۲۰۱۵، ارز بیت‌کوین به بالاترین سطح معاملاتی از لحاظ قیمت و حجم رسید. این دوره‌ی جدید ارز دیجیتال منجر به جنبشی آنی در زمینه‌هایی شامل خواستگاه بازار و اوراق بهادار قابل‌خریدوفروش به همراه قانون‌گذاری‌های جدید و متفاوت شد. افراد برای تزریق هرچه بیشتر سرمایه به زیرساخت دیجیتال اشتیاق نشان دادند. سطح این هیجان به‌تدریج برای بیت‌کوین و بلاک‌چین به‌عنوان مجموعه‌هایی که تقریباً یک بیلیون دلار سرمایه‌ی ثبت‌شده در سال ۲۰۱۵ داشتند افزایش یافت. شرکت‌های متعددی نظیر امریکن اکسپرس[1]، برین کپیتال[2]، دیلویت[3]، گلدمن ساکس[4]، مسترکارت[5] و شرکت بیمه زندگی نیویورک[6] اخیراً میلیون‌ها دلار در بیت‌کوین سرمایه‌گذاری کرده‌اند [۳۳].

براساس تحلیل‌های انجام‌شده، بسیاری از صنایع و خانه‌های شرکتی[7] به تکنولوژی بلاک‌چین و زیرساخت بیت‌کوین در بخش‌های مختلف علاقه نشان داده‌اند. برای ایجاد سیستمی ایمن‌تر و کارامدتر برای خریدوفروش سهام، NASDAQ تکنولوژی تاپینگ[8] را در حوزه‌ی بلاک‌چین ارائه می‌دهد. شرکتی تحت عنوان DocuSign، متخصص در بازارهای الکترونیکی، از بلاک‌چین برای پیگیری اجاره‌ی ماشین و همچنین به‌حداقل‌رساندن کاغذبازی استفاده کرده‌است [۲۴]. مایکروسافت همچنین از ایده‌ی سرمایه‌گذاری خود با استفاده از قراردادهای هوشمندی که از فناوری بلاک‌چین استفاده می‌کنند پرده برداشته‌است. در عین حال، میزان کنجکاوی درباره‌ی تکنولوژی بلاک‌چین به حدی رسیده‌است که بسیاری از شرکت‌ها با ایجاد بلاک‌چین خصوصی کوچک‌تر در محل دفتر خود از آن به‌طور آزمایشی استفاده می‌کنند. برای مثال، بسیاری از مجموعه‌ها شرکت‌های مختلفی نظیر بلوک سایبر[9] را استخدام می‌کنند که یک استارت‌آپ در شهر رد وود کالیفرنیاست و در حوزه‌ی ایجاد تکنولوژی بلاک‌چین در دفتر و محل تجاری خود فعالیت می‌کند [۳۴].

---

1. American express
2. Brain capital
3. Deloitte
4. Goldman Sachs
5. MasterCard
6. New York Life Insurance

۷. corporate houses اصطلاحی در صنعت جابه‌جایی است که به اجاره‌ی یک آپارتمان مبله، کاندو یا خانه به‌صورت موقت به افراد، کارکنان نظامی، گروه‌های کارآموز یا شرکت‌ها به‌عنوان جایگزینی برای هتل سنتی یا اقامت طولانی‌مدت در هتل اشاره دارد.

۸. Tapping یا تپ شبکه‌ی سیستمی است که رویدادهای یک شبکه‌ی محلی را رصد می‌کند. تپ معمولاً یک دستگاه سخت‌افزاری اختصاصی است که راهی برای دسترسی به داده‌های جاری در یک شبکه رایانه‌ای فراهم می‌کند.

9. Block Cypher

۶. نتیجه‌گیری

ارز دیجیتال بیت‌کوین توسط تکنولوژی بلاک‌چین ارائه می‌شود. این فناوری پلتفرم و محیطی با ماهیتی غیرمتمرکز است که در سیستم دفتر کل عمومی تمام تراکنش‌ها ثبت شده و توسط تمام شرکت‌کنندگان قابل مشاهده است. تمرکز اصلی تکنولوژی بلاک‌چین معطوف به فراهم ساختن گمنامی (ناشناس ماندن)، امنیت، حریم خصوصی و شفافیت برای تمام افرادی است که از آن استفاده می‌کنند. اما علی‌رغم این ویژگی‌ها، چالش‌ها و محدودیت‌های متعددی نیز وجود دارد که باید بررسی شوند [۴]. هدف اصلی این نوشته‌ی سیستماتیک، بررسی وضعیت موجود تکنولوژی بلاک‌چین و حوزه‌های مختلف آن در تحقیقات آتی است. در این مقاله، تنها چشم‌اندازهای تکنیکی و فنی پرداخته شده و چشم‌اندازهای اقتصادی، قانونی، تجاری و قوانین در نظر گرفته نشده‌اند. مقاله‌های متعددی از پایگاه داده‌ی علمی استخراج شده‌است و نویسندگان با استفاده از آن‌ها تلاش کرده‌اند داده‌ها را تجزیه و تحلیل کنند. با توجه به مطالعه‌ی مقاله‌های مختلف، نویسندگان با درک وضعیت فعلی تکنولوژی بلاک‌چین، مسیرهای جدیدی برای تحقیقات آتی در این حوزه براساس موارد زیر پیشنهاد کرده‌اند:

- تشخیص و شناسایی مشکلات و چالش‌های موجود در تکنولوژی بلاک‌چین و پیشنهاد راه‌حل‌هایی برای حل این مشکلات. از سال ۲۰۱۳، تکنولوژی بلاک‌چین منجر به تغییرات و جنب‌وجوش زیادی شده‌است و کاربرد آن در هر حوزه‌ای در حال افزایش است. تحقیقات مختلفی در این زمینه انجام شده و هرساله تعداد مقاله‌ها و تحقیقات انجام‌شده در این حوزه افزایش می‌یابد. از میان تحقیقات انجام‌شده در این زمینه، اغلب مقاله‌ها بر چالش‌ها و محدودیت‌ها تأکید داشته‌اند، اما هنوز مسایل زیادی هست که مورد توجه قرار نگرفته‌اند.
- تحقیقات بیشتری باید درباره‌ی مشکل مقیاس‌پذیری بلاک‌چین انجام شود. بعد از تجزیه، تحلیل و استخراج اطلاعات از مقاله‌های تحقیقاتی مختلف، مشخص شد که اغلب تحقیقات فعلی به مسایل امنیتی و حفظ حریم خصوصی پرداخته‌اند. اگر تکنولوژی بلاک‌چین به شیوه‌ای فراگیر پیاده‌سازی شود، مشکل مقیاس‌پذیری که شامل عملکرد و تأخیر است باید حل گردد.
- کاربردهای بیشتر بلاک‌چین فراتر از بیت‌کوین و ارز دیجیتال باید توسعه داده شوند.

این مقاله عمدتاً بر یکی از کاربردهای بلاک‌چین یعنی بیت‌کوین تمرکز دارد. به‌علاوه، سایر کاربردهای تکنولوژی بلاک‌چین نظیر قراردادهای هوشمند نیز مورد بحث قرار گرفته‌اند. برای نشان دادن چالش‌ها و محدودیت‌های مختلف در زمینه‌ی تکنولوژی بلاک‌چین، محققان زیادی تنها به ارائه‌ی راه‌حلی مختصر بسنده کرده‌اند، اما این راه‌حل‌ها از نظر کارایی و اثربخشی در ارزیابی عینی دچار نقص‌هایی هستند.

منابع

1. Lerner J (2006) The new new financial thing: The origins of financial innovations. J Financial Econ 79(2):223–255, 2006, [online]Available: http://search.proquest.com.ezproxy.lib.usf.edu/docview/231721046?accountid=14745
2. Frame W, White L (2004) Empirical studies of financial innovation: Lots of talk little action?J Econ Literature 42(1):116–144. [online] Available: http://www.jstor.org/stable/3217038
3. Swan M (2015) Blockchain: blueprint for a new economy. O'Reilly Media, Inc.
4. Kitchenham B, Charters S (2007) Guidelines for performing systematic literature reviews in software engineering
5. Wiesche M, Jurisch MC, Yetton PW, Krcmar H (2017) Grounded theory methodology in information systems research. MIS Quart 41(3):685–701
6. Coinmarketcap, Crypto-Currency Market Capitalizations (2016) Accessed 24 Mar 2016. https://coinmarketcap.com/
7. Bitcoin NS (2012) A peer-to-peer electronic cash system. Consulted 2008(1):28
8. Kondor D, Pósfai M, Csabai I, Vattay G (2014) Do the rich get richer? An empirical analysis of the Bitcoin transaction network. PloS one. 9(2):e86197. pmid:24505257
9. Herrera-Joancomart J, Research and challenges on bitcoin anonymity. In: Garcia-Alfaro J, Herrera-Joancomart J, Lupu E, Posegga J, Aldini A, Martinelli F, et al (eds) Data privacy management, autonomous spontaneous security, and security assurance, vol 8872 of Lecture Notes in Computer Science. Springer International Publishing, pp 3–16. Available from: http:// dx.doi.org/10.1007/978-3-319-17016-9_1
10. Judmayer A, Stifter N, Krombholz K, Weippl E, Bertino E, Sandhu R (2017) Blocks and chains: introduction to bitcoin, cryptocurrencies, and their consensus mechanisms. Morgan &Claypool

11. Bitcoincharts (2016) Accessed 24 MAr 2016. https://bitcoincharts.com
12. Housley R (2004) In: Public key infrastructure (PKI). Wiley&Sons, Inc. Available from: http://dx.doi.org/10.1002/047148296X.tie149
13. Double-spending (2016). Accessed: 24 Mar 2016. https://en.bitcoin.it/wiki/Double-spending
14. Bitcoin wiki (2015) Accessed 24 Mar 2016. https://en.bitcoin.it
15. WangY, Hugh Han J,Davies PB(2018) Understanding blockchain technology for future supply chains: a systematic literature review and research agenda, vol 24, pp 62–84
16. Antonopoulos AM (2014) Mastering Bitcoin: unlocking digital cryptocurrencies. O'Reilly Media, Inc.
17. Proof-of-Stake (2016) Accessed 24 Mar 2016. https://en.bitcoin.it/wiki/Proof_of_Stake
18. Mingxiao D, Xiaofeng M, ZheZ,XiangweiW, QijunC(2017)Areviewon consensus algorithm of blockchain. In: 2017 IEEE international conference on systems man and cybernetics
19. Borenstein J (2016) A risk-based view of why banks are experimenting with bitcoin and the Blockchain. SpotlightonRisk Technology, 18 Sept 2015. Web. 03 May 2016
20. Barski C, Wilmer C (2014) The blockchain lottery: how miners are rewarded—CoinDesk. CoinDeskRSS. CoinDesk, 23 Nov 2014. Web. 03 May 2016
21. Wild, Jane, Martin Arnold, and Philip Stafford."Technology: Banks Seek theKey to Blockchain -FT.com."FinancialTimes.N.p.,1 Nov. 2015. Web. 03 May 2016
22. Driscoll S (2013) How bitcoin works under the hood. Imponderable Things, 14 July 2013.Web. 03 May 2016
23. Kelly J (2015) Nine of world's biggest banks join to form block-chain partnership. Reuters. Thomson Reuters, 15 Sept 2015. Web. 03 May 2016
24. Kalra V, Rashmi A (2019) Challenges of text analytics in opinion mining. In: Extracting knowledge from opinion mining. IGI Global, pp 268–282

25. Why NASDAQ Private Market. Nasdaq Private Market |. N.p., n.d. Web. 03 May 2016
26. Chain | Enterprise Blockchain Infrastructure. N.p., n.d. Web. 03 May 2016
27. Bhushan D, Rashmi A (2020) Security challenges for designing wearable and IoT solutions. In: A handbook of internet of things in biomedical and cyber physical system. Springer, Cham,pp 109–138
28. Bhushan D, Rashmi A (2020) The Internet of Things: looking beyond the hype. An industrial IoT approach for pharmaceutical industry growth, vol 2, p 231
29. Infante A (2014) Quantum computers: the end of cryptography?—Make Use Of. N.p., 16 Nov 2014. Web. 03 May 2016
30. Lee TB (2015) Bitcoin's value is surging. Here are 5 charts on the growing bitcoin economy. Vox. N.p., 03 Nov 2015. Web. 03 May 2016
31. Rivera J (2015) Gartner's 2015 hype cycle for emerging technologies identifies the computing innovations that organizations should monitor. N.p., 18 Aug 2015. Web. 03 May 2016
32. Gupta N, Rashmi A (2018) NoSQL security. In: Advances in computers, vol 109. Elsevier, pp101–132
33. Gupta V (2017) A brief history of blockchain. Harvard Bus Rev. [online] Available: https:// hbr.org/2017/02/a-brief-history-of-blockchain
34. Nærland K, Müller-Bloch C, Beck R, Palmund S (2017) Blockchain to rule the waves—Nascent design principles for reducing risk and uncertainty in decentralized environments. In: Proceedings of 38th International Conference on Information System. [online] Available: https://aisel.aisnet.org/icis2017/HCI/Presentations/12/