
بسم الله
الرحمن
الرحيم

نوآوری کسب و کار از طریق بلاکچین

بنیاد ققنوس
KUKNOS FOUNDATION

راه‌پرداخت

سرشناسه: مورابیتو، وینچنزو. Morabito, Vincenzo / عنوان و نام پدیدآور: نوآوری کسب و کار از طریق بلاکچین؛دیدگاه هیات کسب‌وکار بلاکچین/ وینچنزو مورابیتو ؛ ترجمه حامد حیدری. / مشخصات نشر: تهران: صفحه سفید، ۱۳۹۸. / مشخصات ظاهری: ۲۲٤ ص.؛ ۵/۱٤×۵/۲۱س‌م. / شابک:٦-٤٠-٦٥٩٩-٩٦٤-٩٧٨/ وضعیت فهرست نویسی: فیپا/ یادداشت: عنوان اصلی: Business Innovation Through Blockchain / موضوع: بلاک‌چین/ موضوع: تکنولوژی؛ / شناسه افزوده: حیدری، حامد ۱۳٦٦- مترجم / رده‌بندی کنگره:HG۱۷۱۰؛ رده بندی دیویی: ۳۳۲/۱۷۸

نوآوری کسب و کار از طریق بلاکچین

نویسنده:
وینچنزو مورابیتو

مترجم:
حامد حیدری (مدرس دانشگاه علامه طباطبایی)

بنیاد ققنوس
KUKNOS FOUNDATION

راه پرداخت

نوآوری کسب و کار از طریق بلاکچین، دیدگاه هیات کسب‌وکار بلاکچین / ناشر: صفحه سفید / مؤلف: وینچنزو مورابیتو/ ویراستارمحتوایی: قاسم سرافرازی/ ویراستار: یلدا شایسته‌فر/ صفحه‌آرا: علیرضا کیوان/ نوبت چاپ: اول ۱۳۹۸ / شمارگان: ۱۰۰۰ نسخه / شابک: ۶-۴۰-۶۵۹۹-۹۶۴-۹۷۸ /تمام حقوق این اثر محفوظ و متعلق به موسسه شبکه عصر تراکنش (راه پرداخت) است/ تلفن: ۴۶۰۱۰۵۳۹-۰۲۱ / دورنگار: ۸۹۷۸۴۹۰۲ / پست الکترونیک: mediamanager.ir@gmail.com / پایگاه اینترنتی: Way2Pay.ir نشانی انتشارات و مرکز پخش: تهران، خیابان ولیعصر، بالاتر از عباس‌آباد، برج سرو ساعی، طبقه اول تجاری، واحد ۲. تلفن: ۷۷-۸۸۷۰۲۰۷۶

فهرست

نوآوری یعنی انجام یک کار به شیوه‌ای که قبلا انجام نمی‌شده که این موضوع باعث بهبود کارکرد آن در زوایای مختلف می‌شود. امروزه ما شاهد نوآوری در حوزه‌های مختلف هستیم که نمونه‌های بسیار مشهود و بارز آن را می‌توان در استارت‌آپ‌ها دید. حالا در این شیفت‌های پارادایمی فناوری، نوبت به نوآوری در حوزه فین‌تک رسیده که صرفا محدود به ابزار نمی‌شود؛ بلکه از مدل تفکر تا شیوه اجرا و مدیریت، همگی درگیر این پوست‌اندازی و نوآوری‌ها می‌شوند.

به عقیده فعالان حوزه بلاکچین، این فناوری بیشتر از آنکه یک فناوری تسهیل‌کننده باشد، یک طرز فکر مدرن و یک ایدئولوژی است؛ باورها و اندیشه‌هایی که بر موضوعاتی مثل اعتماد، سرعت و امنیت استوار است، فناوری که با اجرای قراردادهای هوشمند آن، می‌توان از موضوعات کهنه اما تازه‌ای مثل فساد ساختاری جلوگیری کرد، چراکه در این فناوری هر چیزی دارای هویت است و نمی‌توان به‌راحتی در آن دست برد؛ یک ساختار شفاف و آزاد.

حالا در این ساختار جذاب و مدرن، ما می‌خواهیم تا حد ممکن از مزیت‌های آن بهره‌مند شویم و علاوه بر آن نوآوری‌های کسب‌وکاری خود را با بلاکچین گره بزنیم که مستلزم آن است که با این فناوری آشنا شویم. اگر بتوانیم بر فناوری بلاکچین و طرز فکر نهادینه‌شده در آن آشنا شویم، می‌توانیم اکثر پروسه‌های کسب‌وکاری خود را یک قدم ارتقا دهیم و از مزیت‌های بی‌نظیر فضای غیرمتمرکز بهره‌مند شویم که موجب بالا رفتن راندمان کسب‌وکارمان می‌شود.

کسب‌وکاری که بتواند نوآوری از طریق بلاکچین را عملی و اجرا کند، قطعا مزیت رقابتی فوق‌العاده‌ای را برای خود خواهد ساخت.

سیدولی‌الله فاطمی
دبیر بنیاد ققنوس

فصل اول
مدیریت و فناوری بلاکچین

۱

ساختار تغییر پارادایم بلاکچین

چکیده

پیشرفت و نوآوری فناورانه به‌طور پیوسته با سرعتی در حال رشد و تکامل است که لازم است همه با این پیشرفت‌ها و نوآوری‌ها همگام بمانند. تغییر پارادایم بلاکچین نیز از این قاعده مستثنی نیست. مفهوم فناورانه پشت بلاکچین با مفهوم پایگاه‌داده شباهت بسیاری دارد. با این حال، اساسا یکی از مفاهیم کلیدی است که باید برای زندگی در آینده آن را درک کرد. پنج مفهوم کلیدی وجود دارد که نه‌تنها باید آنها را درک کرد؛ بلکه به گونه‌ای باید آنها را بررسی کرد که چگونگی ارتباط آنها را با یکدیگر فرابگیریم؛ قراردادهای هوشمند،[1] اجماع غیر متمرکز،[2] بلاکچین، رایانش اعتمادی[3] و اثبات کار/ اثبات سهام.[4] علت اهمیت حیاتی این پارادایم رایانش جذاب آن است که در آینده به ابزاری برای ساخت نرم‌افزارهای کاربردی غیر متمرکز تبدیل خواهد شد. در این فصل، چهار مفهوم کلیدی از فناوری بلاکچین را بررسی می‌کنیم؛ بلاکچین، اجماع غیر متمرکز در نرم‌افزارهای کاربردی پایگاه‌های داده، اثبات کار/ اثبات سهام و قراردادهای هوشمند. سپس، ساختار تغییر پارادایم بلاکچین را بررسی می‌کنیم.

مقدمه

با توجه به دو دهه آزمایش‌های علمی به‌منظور کشـــف اصول، پیشرفت‌های فنی و نظریات؛ شتاب بسیار زیادی در حوزه شبکه‌سازی رایانش غیر متمرکز (همتا به همتا)[5] و نیز امنیت ارتباطات (رمزنگاری) وجود داشته است. در نتیجه، فناوری جدیدی با نام «بلاکچین» شکل گرفت.

1. smart contracts
2. decentralized consensus
3. trusted computing
4. proof of work/stake
5. peer-to-peer

جای تعجب نیســت که فناوری بلاکچین به لفظ روزمره عصر ما تبدیل شده و توجه بسیاری از کارآفرینان، دولت‌ها، بانک‌ها و نهادهای دیگر را به خود جلب کرده است. به‌نظر می‌رسد که همه آنها بخشی از سرمایه و منابع خود را برای دستیابی سریع به درک روشنی از پارادایم بلاکچین اختصاص داده‌اند و در عین حال، قصد دارند تا از این فناوری کلیدی در آینده استفاده کنند. می‌توان بلاکچین را مرحله بعد در حرکت از سمت مفاهیم معماری رایانش توزیع‌شده[1] به‌سوی پایگاه‌های داده جهانی واسط‌های کاربری دانست که عملکرد دستگاه‌های گوناگون و منابع داده‌ای مختلف را یکپارچه می‌کند.

بلاکچین به پایگاه داده توزیع‌شده رمزی اشاره دارد که مخزنی از اطلاعات است که نمی‌توان آن را بازگشــت داد و غیرقابل دستکاری اســت. به عبارتی دیگر، می‌توان بلاکچین را به‌صورت دفترکل عمومی توزیع‌شده[2] یا پایگاه داده اسناد تمام تراکنش‌هایی تعریف کرد که انجام شده‌اند و بین کاربران شبکه مذکور به اشتراک گذاشته شده‌اند. هر تراکنش یا رویداد دیجیتال در دفترکل عمومی باید از طریق توافق بیش از نیمی از کاربران شبکه مذکور اعتبارسنجی شود. این مطلب نشان می‌دهد که هیچ کاربر یا شرکت‌کننده‌ای به‌صورت انفرادی نمی‌تواند داده‌ای را بدون تفاهم دیگر کاربران (شرکت‌کنندگان) اصلاح و دستکاری کند. کاملا مشخص است که مفهوم فناورانه بلاکچین با مفهوم پایگاه داده شباهت فراوانی دارد.

بلاکچین باعث می‌شود که کاربران در بار اول درباره چگونگی رخداد یک رویداد دیجیتال یا تراکنش خاص، بدون نیاز به هر نوع نهاد کنترل‌کننده، با یکدیگر توافق کنند. این فناوری (فناوری بلاکچین) از این جهت منحصربه‌فرد است که کار واسطه‌ها را کاهش می‌دهد. این مطلب باعث می‌شود که داده‌ای خاص به شیوه‌ای امن و مطمئن به کاربران منتقل شود.

علاوه بر این، فناوری بلاکچین می‌تواند قراردادهای هوشــمند تولید کنــد. این قراردادهای هوشمند را به‌صورت ارزهای دیجیتال تعریف می‌کنند که از نهادهای دولتی مستقل هستند و به آنها «قراردادهای دیجیتال خوداعمال‌کننده»[3] می‌گویند. آنها نیازمند هیچ نوع قانون، مقررات یا دخالت انسانی نیستند.

جای تعجب نیست که فناوری بلاکچین به لفظ روزمره عصر ما تبدیل شده و توجه بسیاری از

1. distributed computing architectural construct
2. distributed public ledger
3. self-enforcing digital contracts

کارآفرینان، دولت‌ها، بانک‌ها و نهادهای دیگر و بسیاری از مردم جهان را به خود جلب کرده است. آنها شاهد ظهور فناوری بلاکچین در اینترنت هستند. همچنین، آنها انتقال قدرت از نهادهای متمرکز در بخش ارتباطات و کسب‌وکار را پیش‌بینی می‌کنند.

فناوری بلاکچین بحث‌برانگیز نیست، چون در بلندمدت بدون اختلال کار کرده و در بخش‌های مالی و غیرمالی با موفقیت از آن استفاده کرده‌اند. این الگوی رایانش جذاب از این جهت مهم است که برای ایجاد نرم‌افزارهای کاربردی غیرمتمرکز ابزاری مفید خواهد بود.

پدیده‌های بلاکچین

در چند سال گذشته، به نظر می‌رسد که یکی از نوآوری‌های فناورانه کلیدی که به آن بلاکچین می‌گویند، نوعی نوآوری فناورانه توزیع‌گر ممکن[1] باشد. اصول بنیادی این فناوری حول‌وحوش نظریه «دفترکل عمومی» ساخته شده که طبق آن این دفتر روی شبکه رایانه‌ای توزیع‌شده‌ای ذخیره و نگهداری می‌شود.

علاوه بر این، دفترکل عمومی باعث شده که شبکه (در حال کلی) به‌طور مشترک تراکنش تولید کند، توسعه دهد و تراکنش‌های قبلی و رویدادهای دیجیتالی آینده را نیز ثبت کند. اخیرا، رمزارز برجسته‌ترین کاربرد فناوری بلاکچین بوده است. نام رمزارز[2] با بیت‌کوین پیوند خورده است. با توجه به محبوبیت و اهمیت بیت‌کوین، در این کتاب از واژه رمزارز برای نمایش جنبه‌های مختلف این دارایی دیجیتال[3] استفاده می‌کنیم.

بیت‌کوین از دفترکل عمومی با نام «بلاکچین» استفاده می‌کند که نام «فناوری بلاکچین» از آن گرفته شده است. با این حال، بیت‌کوین اولین مورد از کاربردهای فراوان فناوری بلاکچین است.

به‌علاوه اینکه، وقتی لازم است چندین کاربر درباره سابقه داده‌های یکسان، مستقل باشند، فناوری بلاکچین به کار می‌آید.

فناوری بلاکچین نوعی ذخیره‌سازی داده است که از جمله ویژگی‌های بارز آن می‌توان به موارد زیر اشاره کرد:

---

1. possible disturbing technological innovation
2. Crypthocurrency
3. digital asset

- در شبکه همتابه‌همتای غیر متمرکز وجود دارد؛
- کاربران خاص می‌توانند آن را بنویسند؛
- از امضای دیجیتال و امنیت ارتباطات (رمزنگاری) برای تایید صلاحیت، سنجش هویت کاربر و اجرای مقررات دسترسی در قالب نوشتاری یا خواندنی استفاده می‌کند؛
- به‌سبب شماتیک فرایند مذکور، تغییر اسناد قدیمی را بسیار دشوار می‌کند؛
- به‌سبب شماتیک فرایند مذکور، افزایش سطح آگاهی کاربران درباره هر نوع اقدام برای تغییر اسناد قدیمی بسیار آسان‌تر می‌شود؛
- تراکنش‌های مالی عموما بخشی از فناوری بلاکچین هستند؛
- کاربران خاص و نیز مخاطبان گسترده می‌توانند آن را بخوانند؛
- به صورت آنی، از طریق چندین سیستم روی شبکه تولید می‌شود.

شکل ۱-۱ و شکل ۲-۱ پایگاه داده متمرکز و پایگاه داده غیر متمرکز را نشان می‌دهد. در پایگاه داده متمرکز، نیاز به واسطه‌ها وجود دارد (گروه ثالث)، در حالی که در پایگاه داده غیر متمرکز، نیاز به واسطه‌ها (گروه ثالث) از میان رفته است.

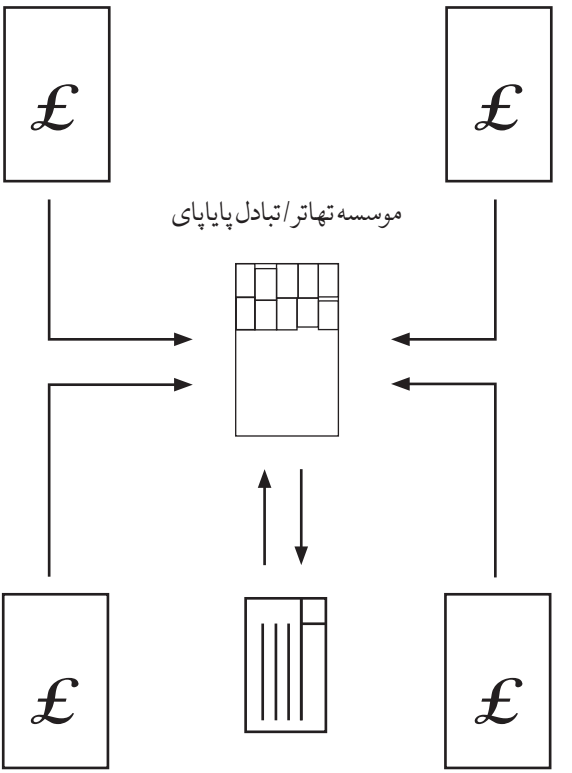
در ادامه چهار مفهوم کلیدی فناوری بلاکچین (بلاکچین، پایگاه داده غیر متمرکز، اثبات کار/اثبات سهام و قراردادهای هوشمند) را بررسی خواهیم کرد.

بلاکچین

بلاکچین در نتیجه بیت‌کوین به وجود آمد، پس می‌توان بلاکچین را بلاکچین بیت‌کوینی نامید. پیش از بحث درباره بلاکچین بیت‌کوین، باید مروری بر بیت‌کوین داشته باشیم.

بیت‌کوین یکی از رایج‌ترین ارزهای دیجیتال مورد استفاده است که در سال ۲۰۰۹ عرضه شد و از آن زمان تاکنون هر روز پیشرفت داشته است. بیت‌کوین نمونه‌ای از ارزهای مجازی است که روی تاریخچه تراکنش‌ها ساخته می‌شود و میان کاربران شرکت‌کننده در آن شبکه دست‌به‌دست می‌شود و از قالب «دفترکل عمومی توزیع‌شده» استفاده می‌کند.

به‌علاوه اینکه، علت طراحی بیت‌کوین اجرای سه هدف و کارکرد اصلی پول سنتی بود. این سه هدف شامل موارد زیر است:



شکل ۱-۱: پایگاه داده غیر متمرکز. برگرفته از لوئیس و همکارانش

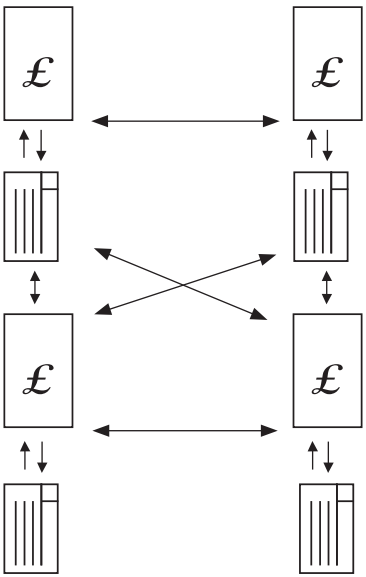
- برای ساده‌شدن تبادل تجاری؛
- برای ذخیره ارزش از سوی کاربران برای اهداف آتی؛
- عمل کردن به‌عنوان واحد پایه برای اندازه‌گیری ارزش کالاهای بازار و خدمات ارائه‌شده.

پیش از اختراع بیت‌کوین و بلاکچین‌اش، کسی تصور نمی‌کرد که ایده ارز دیجیتال عملی و ممکن باشد، زیرا ارزهای دیجیتال به‌راحتی کپی و تکثیر می‌شدند. این معضل را «دوباره خرج کردن»[1] می‌گفتند که طی آن هر تراکنش ریسکی در پی داشت. این ریسک شامل فرستادن یک کپی از تراکنش دیجیتالی به معامله‌گر از سوی دارنده/مالک است؛ درحالیکه، مالک کپی

1. Double spend

اصلی تراکنش دیجیتال را در اختیار نگه می‌دارد. به‌طور مرسوم در مقابل این ریسک از طریق توسعه واسطه‌ای مرکزی و معتمد برای به‌روز ماندن با تراکنش‌های انجام‌شده، خود را محافظت می‌کردند.

با این حال، با ظهور بلاکچین بیت‌کوین که طـی آن تاریخچه تراکنش‌ها و احراز صلاحیت چنین تراکنش‌هایی از سوی شرکت‌کنندگان شبکه انجام می‌شد، اجبار به روزماندن با تراکنش‌ها بر دوش کل سیستم شبکه گذاشته شد. در فصل ۲، یک نمودار مفصل و خوش‌ساخت، سیستم ارزش بلاکچین را به‌خوبی توضیح داده اســت. می‌توان مشــاهده کرد که گره‌هایی وجود دارد (کاربران شبکه) و این گره‌ها بلاکچین را حفظ می‌کنند که از تراکنش‌های تاریخی انجام‌شده در شبکه تشکیل شده است.



شکل ۲-۱: پایگاه‌داده غیرمتمرکز. برگرفته از لوئیس و همکارانش

سیســتم بلاکچین بیت‌کوین به‌واقع سیســتمی چندوجهی اســت که اهــداف زیر را دنبال می‌کند:

- توانایی همه افراد در نوشتن بلاکچین؛
- کنترل متمرکز باید حذف شود؛

- سیستم بلاکچین بیت‌کوین به شیوه‌ای اجرا می‌شود که بسیار شبیه شبکه یا سیستم پایگاه‌های داده رایانه‌ای است و هر کدام شامل تراکنش‌های پیشین بیت‌کوین است.

رویکرد بیت‌کوین در انواع تصمیمات را می‌توان به هفت دسته مختلف تقسیم‌بندی کرد. این موارد شامل: ذخیره‌سازی داده، توزیع داده، مکانیسم اجماع، مکانیسم به‌روزرسانی، معیار مشارکت، مکانیسم دفاعی و طرح تشویقی و انگیزشی است. جدول ۱-۱ به انواع دسته‌ها، پرسش‌ها و روش‌های بیت‌کوین اشاره دارد. مهم‌ترین نکته آن است که مردم می‌خواهند پرسش‌هایی مطرح کنند که به دسته‌بندی‌های اشاره‌شده ربط دارد. با این حال، روش بیت‌کوین در هر دسته پاسخ‌هایی مناسب برای این پرسش‌ها ارائه می‌کند (جدول ۱-۱).

جدول ۱-۱: دسته‌ها، پرسش‌ها و رویکردهای بیت‌کوین

دسته	پرسش	رویکرد بیت‌کوین
ذخیره‌سازی داده	داده‌ها چگونه باید ذخیره شوند؟	داده‌ها باید از طریق فناوری بلاکچین ذخیره شود.
توزیع داده	توزیع داده‌های جدید چگونه باید باشد؟	توزیع داده‌های جدید باید در قالب همتابه‌همتا باشد.
مکانیسم توافق	چگونه باید نزاع حل‌وفصل شود؟	نزاع باید از طریق قانون طولانی‌ترین زنجیره حل‌وفصل شود.
مکانیسم به‌روزرسانی	چگونه قوانین تغییر می‌کنند؟	قوانین از طریق این موارد تغییر می‌کنند: BIP[1] برای نگارش قوانین رای از طریق قدرت پردازش (برای اجرای قوانین)
معیار مشارکت	چه کسی می‌تواند تراکنش را انجام دهد؟	اجرای تراکنش ناشناس و آزاد است.
معیار مشارکت	چه کسی می‌تواند داده را بخواند؟	خواندن داده به‌صورت ناشناس و آزاد انجام می‌شود.

دسته	پرسش	رویکرد بیت‌کوین
معیار مشارکت	چه کسی می‌تواند اعتبار تراکنش را تایید کند؟	احراز صلاحیت و تایید اعتبار تراکنش ناشناس و آزاد است.
مکانیسم دفاعی	چگونه از رفتار خطا پرهیز می‌شود؟	رفتار خطا از طریق اثبات کار پیشگیری و جلوگیری می‌شود.
طرح تشویقی و انگیزشی	بلوک‌سازان چگونه تشویق می‌شوند؟	از طریق بلوک جایزه تشویق می‌شوند و با دستمزد تراکنش جایگزین خواهد شد.
طرح تشویقی و انگیزشی	اعتبارسنج‌های تراکنش چگونه تشویق می‌شوند؟	تشویق اعتبارسنج‌های تراکنش در نظر گرفته نشده است.

منبع: برگرفته از پژوهش لوئیس

بلاکچین‌های عمومی و بلاکچین‌های خصوصی

یکی از نکات برجسته بلاکچین‌های عمومی[1] توانایی بالای این نوآوری در حفظ توافق تراکنشی در شبکه است که امکان نوشتن بلوک‌های تراکنش در بلاکچین (دفترکل عمومی توزیع‌شده)، توسط هر کسی، ایجاد تراکنش‌ها و توانایی در ارسال چنین تراکنش‌هایی فراهم می‌کند. علاوه بر این، این کارها نیازی به تایید گروه ثالث یا واسطه ندارد.

از سویی دیگر، محدودیت کاربران در بلاکچین‌های خصوصی[2] شامل استفاده از دیواره‌های آتش[3] در شبکه خصوصی است. الگوهای سیستمی بلاکچین خصوصی را می‌توان به‌گونه‌ای انجام داد که فقط شرکت‌کنندگان شناخته‌شده بتوانند داده را در بلاکچین وارد کنند.

علاوه بر این، بلاکچین خصوصی به کاربران ناشناس اجازه خواندن یا بازنویسی داده‌ها را نمی‌دهد (جدول ۲-۱).

1. public Blockchains
2. private Blockchains
3. firewalls

جدول ۲-۱: تفاوت‌ها بین بلاکچین عمومی و بلاکچین خصوصی

بلاکچین عمومی	بلاکچین خصوصی
کاربران لزوما شناخته‌شده نیستند.	کاربران مشخص و معتمد هستند.
کاربران لزوما معتمد نیستند.	کاربران معتمد هستند.
هر کسی بدون اجازه نهاد دیگر می‌تواند داده‌ها را بخواند.	فقط کاربران دارای مجوز می‌توانند داده‌ها را بخوانند.
هر کسی بدون اجازه نهادی دیگر می‌تواند داده‌ها را بازنویسی کند.	فقط کابران دارای مجوز می‌توانند داده‌نویسی کنند.

نمونه‌هایی از بلاکچین‌های عمومی و بلاکچین‌های خصوصی بدین شرح است: ریپل (که می‌تواند بین بلاکچین عمومی و بلاکچین خصوصی قرار بگیرد) و اتریوم (که از بلاکچین عمومی استفاده می‌کند). اکنون، به پایگاه داده غیر متمرکز نگاهی می‌اندازیم که در واقع، مفهوم کلیدی دیگری در فناوری بلاکچین است.

پایگاه‌های داده غیر متمرکز

بلاکچین تاثیری عمیق بر شیوه ارتباطات و نیز اشتراک‌گذاری آنلاین داده داشته است. این تاثیر در نتیجه استفاده از پایگاه‌های داده غیر متمرکز در بلاکچین است.

علاوه بر این، با پدیدارشدن پایگاه‌های داده غیر متمرکز، لزوم برقراری ارتباطات یا اشتراک‌گذاری داده‌ها (فیلم و عکس) از طریق شبکه متمرکز یا بسترهای الکترونیکی نظیر گوگل‌درایو، یاهو، جی‌میل و غیره ضرورت کمتری پیدا کرده است. با استفاده از پروتکل‌های ارتباطاتی رمزی و غیر متمرکز، می‌توان پیام‌ها را در هر زمانی و بدون مداخله دولت‌ها انتقال داد، ذخیره ساخت و فراخوانی کرد.

پایگاه‌های داده غیر متمرکز امکان تبادل غیر متمرکز و امن داده را فراهم می‌کند. اگر لازم باشد، می‌توان اطلاعات را نشر داد و در چندین رایانه به شیوه‌ای رمزی توزیع کرد و در نتیجه، توانایی تک‌واحدها را برای سانسور، از بین برد. سیستم ذخیره‌سازی ابری غیر متمرکز ناشناس[1] مثالی از پایگاه داده غیر متمرکز است که از فناوری بلاکچین در مشارکت با دیگر فناوری‌های همتا به همتا

1. Anonymous Decentralized Cloud Storage System

استفاده می‌کند تا استفاده از فضای مازاد روی هاردیسک را برای کاربران ممکن سازد. این حالت شبیه بستر رایانش ابری متمرکز برای کاربران است، اما از لحاظ فناوری و حالت اجرای این بسترها شباهتی با هم ندارند.

در نتیجه فناوری بلاکچین، سازمان‌ها در حال حاضر به‌دنبال شیوه‌هایی برای استفاده از امتیاز پایگاه‌های داده غیر متمرکز هستند. فناوری بلاکچین باعث شـــده که رای‌دهی روی اینترنت یا استفاده از دستگاه‌های موبایل به‌طور ایمن ممکن شـــود. علت این امر توانایی پایگاه‌های داده غیر متمرکز برای به‌کار انداختن اسناد عمومی رمزدار و بازگشت‌ناپذیر توزیع‌شده است که می‌توان بدون زحمت چندان آنها را ممیزی کرد، زیرا هر رای‌دهنده می‌تواند اعتبار شمرده‌شدن رای خود را تایید کند. طبق فرایند رمزگذاری هر سیستم رای‌گیری که بر پایه فناوری بلاکچین است، چنین سیستم رای‌گیری در مقابل هک‌شدن آسیب‌پذیر نیست. سیســـتم‌های پایگاه‌داده غیر متمرکز، جایگزینی فنی برای سیستم نام دامنه (DNS)[1] است که از کل اینترنت پشتیبانی می‌کند.

اثبات کار

دفترکل عمومی غیر متمرکز ســـاختاری بنیادی از پایگاه داده اســـت که برای تراکنش ارزهای دیجیتال، از جمله تراکنش بیت‌کوین، استفاده می‌شود، زیرا به‌صورت مکانی برای ذخیره‌سازی همه تراکنش‌ها عمل می‌کند. لازم به ذکر است که کارکرد فرایند ارز دیجیتال باید شامل ابزارهای ایمن در برابر حملات در بلاکچین باشد. اگر مهاجم تصمیم بگیرد مقدار مشخصی از پول را خرج کند و سپس تلاش کند تا آن تراکنش خاص را معکوس کند، مهاجم می‌تواند نسخه منحصر به‌خود از بلاکچین را منتشر کند که در آن تراکنش مورد نظر وجود ندارد، آنگاه کاربران، پیش از حمله، هیچ نوع آگاهی درباره نسخه معتبر دفترکل عمومی ندارند.

امنیت شبکه بیت‌کوین به پروتکل امنیت شبکه با نام اثبات کار (PoW) وابسته است. در سال ۱۹۹۳، سینتیا دورک و مونی نائور[2] در آغاز این پروتکل امنیت شبکه را پیشنهاد دادند (اثبات کار). این پروتکل امنیت شبکه داده‌ای است که ایجاد آن برای رفع پیش‌نیازهای خاص دشوار است و اعتبارسنجی آن چندان اهمیت ندارد. به‌عبارتی دیگر، به‌منظور اجرای نقشی خاص، این پروتکل هزینه‌ای اضافی اعمال می‌کند. در فصل ۴، درباره این مفهوم بحث می‌کنیم. در آن فصل، جنبه‌های

1. Domain Name System
2. Cynthia Dwork - Moni Naor

امنیت بلاکچین را بررسی می‌کنیم.

با توجه به بیت‌کوین، لازم به ذکر است که در دوره زمانی خاصی، هر تراکنش اجراشده در بلوک بیت‌کوین ثبت و ذخیره می‌شود. سپس، این بلوک به همه گره‌های شرکت‌کننده در شبکه بیت‌کوین مخابره می‌شود. از اثبات هش‌کش کار[1] در این حالت استفاده می‌شود. این نوع اثبات کار در سال ۱۹۹۷ توسط آدام بک[2] معرفی شد. در این اثبات، هر کار بر داده‌ای به نام «نانس»، به بلاکچین اضافه می‌کند تا یک «بلوک+نانس» تشکیل دهد. سپس، این «بلوک+نانس» در الگوریتمی قرار داده می‌شود که به آن «الگوریتم هش»[3] می‌گویند.

این الگوریتم شامل مجموعه‌ای هش اســت که با برخی از پیش‌نیازهای خاص انطباق دارد. سپس، این الگوریتم یک محاســبه پیچیده ریاضی را انجام می‌دهد که طی آن هر گره حاضر در تلاش است تا راه‌حلی برای استفاده از تابع هش SHA 256 پیدا کند (الگوریتم ایمن هش).[4] به‌محض آنکه یک گره راه‌حلی برای محاسبه ریاضی مذکور یافت، پیش‌نیازهای خاص اثبات کار مذکور رفع می‌شوند و حالا به «بلوک+نانس+هش» تبدیل می‌شوند. به محض اینکه این حالت رخ می‌دهد، «بلوک+نانس+هش» در بلاکچین وارد می‌شود و به همه گره‌های شرکت‌کننده در شبکه مخابره می‌شود.

علاوه بر این، پروتکل بیت‌کوین (پروتکل اثبات کار) به شیوه‌ای کار می‌کند که منابع کمیاب فیزیکی به شبکه کمک می‌کنند. این منابع کمیاب فیزیکی به شرح زیر هستند:

- سخت‌افزار مورد نیاز برای اجرای محاسبات ریاضی؛
- توان الکتریکی مورد نیاز برای اجرای سخت‌افزار.

این مطلب نشان می‌دهد که استفاده از پروتکل بیت‌کوین (پروتکل اثبات کار) تا حد زیادی به منابع ربط دارد. در نتیجه این امر، بسیاری از سیستم‌هایی که بر پایه محاسبات پرهزینه نیستند، ساخته شده‌اند و اثبات سهام[5] یکی از آنهاست.

پروتکل اثبات کار، به همان صورتی که در ایمیل‌ها به‌کار رفت، به‌عنوان راهکاری برای بازدید از

---

1. The Hashcash proof of work
2. Adam Back
3. hash algorithm
4. SHA (Secure Hash Algorithm)-256 hash function
5. proof of stake

وب‌سایت‌ها، حفاظت در برابر حملات عدم دسترسی به سرویس،[1] اتصالات TCP[2] محدودساز نرخ و ایجاد انگیزه برای سیستم همتا به همتا توصیه شده است.

اثبات سهام

طرح اثبات سهام (PoS) جایگزینی برای طرح اثبات کار است. اثبات سهام طرحی است که بر پایه پردازش‌های با هزینه کمتر ساخته شده‌است. به‌عبارتی دیگر، طرح اثبات سهام در مقایسه با طرح اثبات کار بر مبنای محاسبات پرهزینه نیست. به جای وابستگی به منابع کمیاب (محاسبات پرهزینه)، طرح اثبات سهام به نهادهایی وابسته است که در شبکه سهیم هستند (این مطلب به دارایی اثبات سهام اشـــاره دارد). به عبارتی دیگر، می‌توان گفت که منبعی که امنیت شبکه به آن وابسته است همان مالکیت سکه/دارایی است که بر اثبات مالکیت[3] دلالت دارد (اثبات مالکیت نیز کمیاب است). برای آنکه احراز هویت و دریافت تراکنش رخ دهد (که دستمزد تراکنش یا سکه جدید است)، ماینر[4] باید مالک چند سکه باشد. امکان اینکه ماینر در ایجاد بلوکی جدید موفق باشد، به مقدار سکه‌ای وابسته است که ماینر مالک آن اســـت و به قدرت محاسباتی در هنگام استفاده از طرح اثبات سهام وابسته نیست. بنابراین، هزینه انرژی در این تراکنش در هر دقیقه است. به‌منظور آسیب رساندن به قابلیت اعتماد سیستم، فرد باید مالک بیش از ۵۰ درصد از سکه موجود باشد که بسیار هزینه‌بر است.

طرح اثبات سهام نسبت به طرح اثبات کار مزایای بسیاری دارد. یکی از مزایای PoS نسبت به PoW، توانایی نهفتگی[5] (تاخیر) کم PoS است. البته، عاری از چالش نیست. همچنین، ثابت شده که در حفاظت در برابر ریسک‌های رمزارز کارآمد نیست.

یکی از چالش‌های طرح اثبات سهم، مساله مرکزیت‌بخشی است، زیرا ذی‌نفعان با سهم‌های بزرگ می‌توانند سطحی از چیرگی را روی شبکه اعمال کنند که دیگران به این سطح قدرت دسترسی ندارند. ترکیبی از طرح اثبات کار و اثبات سهم بعدا اختراع شد. اکنون، درباره طرح ترکیبی اثبات کار و اثبات سهم بحث می‌کنیم.

---

1. denial-of-service
2. Transmission Control Protocol
3. proof-of-ownership
4. miner
5. latency

اثبات ترکیبی سهم و کار

اولین بار، اسکات نادال و ســانی کینگ[1] در مقاله خود با عنوان «پی‌پی‌کوین: رمزارز با اثبات سهم»،[2] اثبات ترکیبی سهم و کار را توصیه کردند و به کار بردند. در اثبات ترکیبی سهم و کار از طرح اثبات کار برای معدن‌کاوی و توزیع در مرحله اولیه استفاده می‌شود و این مطلب نشان می‌دهد که توزیع سکه‌های جدید بین ماینرها از طریق شبکه ممکن می‌شود. طرح اثبات سهم کارآمدی انرژی خوبی برای رمزارز فراهم می‌کند.

جدول ۳-۱: ویژگی‌های اصلی اثبات کار، اثبات سهم و اثبات ترکیبی کار و سهم

طرح	تاخیر پایین/ نهفتگی پایین	اجرای بلندمدت هزینه/ انرژی پایین
اثبات کار (PoW)	خیر	خیر
اثبات سهم (PoS)	بله	بله
اثبات ترکیبی کار و سهم (PoW/PoS)	بله	بله

علاوه بر این، تولید بلوک در طرح ترکیبی به مدلی وابسته است که به آن «مسکوک»[3] (ضرب سکه) می‌گویند و ضریبی از کل سکه‌های یک ماینر است و مالکیت سکه‌های فعلی ماینر را شامل می‌شود. از این رو، تولید بلوک به بلوکی تعلق دارد که بالاترین مسکوکات را داراست. مصرف پایین انرژی از طریق این طرح یکی از ویژگی‌های برجسته این طرح است. جدول ۳-۱ به ویژگی‌های اصلی اثبات کار، اثبات سهم و اثبات ترکیبی کار و سهم اشاره دارد. می‌توان از جدول ۳-۱ مشاهده کرد که اثبات کار تاخیر زیادی دارد و هزینه انرژی در بلندمدت برای اثبات کار بالاست و در عین حال طرح اثبات سهم و نیز اثبات ترکیبی کار و سهم تاخیر اندکی دارد و هزینه انرژی آنها در بلندمدت پایین است.

مزایای فناوری بلاکچین

مزایای بسیاری در فناوری بلاکچین نهفته است. برخی از این مزایا بدین شرح است: اعتماد، آزادی، استقلال، سرعت، انسجام، جهانی بودن و کارآمدی.

1. Scott Nadal - Sunny King
2. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake
3. coinage

پیش از آنکه داده‌ای را به بلاکچین تعریف‌شده‌ای اضافه کنیم، انتظار می‌رود که تعداد زیادی از کاربران سیستم با یکدیگر به توافق برسند. این الگو با الگوی متمرکز که طی آن نهادی متمرکز وجود دارد، متفاوت است. سیستم درست‌کارتر زمانی ایجاد می‌شود که بیشتر کاربران درباره نگارش، ایجاد و تغییر داده‌ها حق نظر و حق رای داشته باشند. این سطح بالای اعتماد از جمله موارد نوآوری بوده که به‌واسطه فناوری بلاکچین ایجاد شده است.

همچنین، استفاده از قراردادهای هوشمند که در حالت آنی با یکدیگر تلفیق می‌شوند، باعث شد که سطح آزادی با پدیدار شدن فناوری بلاکچین به‌شدت بهبود یابد و اینکه، چون داده‌های تجاری روی بستری مشترک نشر یافته، شرکت‌کنندگان می‌توانند آنها را به صورت آنی ببینند. این امر به جلوگیری از هر نوع دستکاری یا تغییر در داده‌ها کمک می‌کند.

طراحی فناوری بلاکچین به شیوه‌ای انجام شـــد که این فناوری به نهادهای مالی نظیر بانک‌ها یا دولت‌ها وابسته نباشد. این امر باعث جذاب‌تر شدن آن و وضع کمتر قوانین دست‌وپاگیر بر آن می‌شود. علاوه بر این، فناوری بلاکچین، سرعت تراکنش‌ها را بهبود داده است؛ چون بلاکچین می‌تواند از طریق افزودن کدهایی با نام «قراردادهای هوشمند» که نیازمند مداخله انسانی نیستند، پیام‌ها را خودکار کند و سرعت پرداخت را بهبود بخشد. این امر نشان می‌دهد که زمان کمتری برای تکمیل تراکنش نیاز است، چون واسطه‌ها حذف شده‌اند، انسجام فناوری بلاکچین امکان ذخیره داده‌ها را روی چندین گره به وجود می‌آورد. هرچقدر تعداد گره‌ها بیشتر باشد، داده‌ها منعطف‌تر هستند. همچنین، توانایی فناوری بلاکچین در ســـرویس‌دهی در سطح محلی و جهانی باعث می‌شود که جذاب‌تر شود. علاوه بر این، فناوری بلاکچین سطح کارآمدی موجود را هنگام تلفیق در بخش مالی بهبود بخشیده است. برای مثال، بانک‌ها معمولا سیستمی را برای تبادل داده‌های تجاری اختصاص می‌دهند تا به امنیت بالاتری دست یابند؛ در نتیجه با افت در تلفیق مواجه می‌شوند. چون فناوری بلاکچین وجود دارد، تلفیق (مغایرت‌گیری)[1] در حالت بلادرنگ انجام می‌شود.

آینده بلاکچین

اگر بلاکچین روی بسترهای متنوع اجرا شود، آینده‌ای درخشان دارد. بلاکچین می‌تواند آینده بخش مالی را دگرگون سازد، زیرا منجر به کاهش فوق‌العاده هزینه‌ها برای همه کاربران بازار می‌شود

1. reconciliation

و در نتیجه، بانکداری جهانی را تغییر می‌دهد.

تا همین اواخر، رئیس اداره بانک ژاپن (هاروهیکو کورودا)[1] به این نکته اشاره کرد که با توسعه فناوری بلاکچین، ممکن است در شیوه طراحی سرویس‌های مالی تغییر و تحولی رخ دهد. وی گفت که هوش مصنوعی[2] و بلاکچین ممکن است اثری عمیق بر بخش سرویس‌های مالی داشته باشد. همچنین، خاطرنشان کرد که دفاتر کل عمومی (زیرساخت اطلاعات پایه) تا حد زیادی از توسعه خدمات مالی پشتیبانی کردند. علاوه بر این، در مه ۲۰۱۶، نایب‌رئیس بانک ژاپن (هیروشی ناکاتو)[3] گفت که توسعه بلاکچین و ارزهای دیجیتال باید توسط بانک‌های مرکزی جدی گرفته شود. در واقع، فناوری بلاکچین را می‌توان در جاهایی به کار گرفت که شامل امور مالی تجاری، بازار سرمایه، پرداخت و میزبانی دیگر حوزه‌ها باشـــد. اکنون درباره این سه حوزه کلیدی بحث می‌کنیم که می‌توان بلاکچین را در آنها به کار برد.

امور مالی تجاری (ترید فاینانس)

این حوزه یکی از حوزه‌های کلیدی است که می‌توان بلاکچین را در آن به کار برد و ظرفیت زیادی دارد. اگر برخی از بانک‌ها تصمیم بگیرند تا از طریق قرار دادن اعتبارنامه‌ها[4] در بلاکچین زنجیره تامین[5] مالی خود را تثبیت کنند، کار دشواری در پیش خواهند داشت، زیرا این اعتبارنامه‌ها جریان پیچیده اطلاعاتی خواهند بود. حتی اگر راهکار بلاکچین توسط تعداد اندکی از کاربران استفاده شود، باز با این پدیده مواجه هستیم.

اخیرا، بانك اچ‌اس‌بی‌سی و بانک آمریکا مریل لینچ[6] و بنگاه فناوری مالی R3، به‌طور جداگانه، گزارش دادند که توانسته‌اند راهی برای استفاده از بلاکچین به منظور ساده‌سازی فرایندهای ترید فاینانس[7] بیابند. علاوه بر این، این دو بانک گفتند که با شرکت اینفوکام دولوپمنت آتوریتی سنگاپور[8] شریک شده‌اند تا در اجرای تراکنش اعتبارنامه (LOC) به برتری برسند. این اعتبارنامه‌ها آنهایی

1. Haruhiko Kuroda
2. artificial intelligence
3. Hiroshi Nakato
4. letters of credit
5. supply chain
6. Bank of America Merrill Lynch
7. trade finance
8. Infocomm Development Authority of Singapor

هستند که عمدتا برای کاهش ریسک بین صادرکننده و واردکننده استفاده می‌شدند. بنابراین، فناوری بلاکچین برای استفاده در حوزه ترید فاینانس مهم است، زیرا راهکارهایی ارائه می‌دهد که شامل توانایی ردیابی است. بلاکچین در زنجیره تامین اصالت محصولات را مشخص می‌کند و همچنین توانایی شفاف‌بودن دارد، زیرا بلاکچین در برابر تراکنش‌های خلاف قانون مقاوم است و در هزینه تلفیق تراکنش صرفه‌جویی می‌کند.

دو حوزه کلیدی ترید فاینانس که می‌توان از فناوری بلاکچین در آنها استفاده کرد شامل انتقال اطلاعات تجاری و امور مالی است. اکنون، به این دو حوزه اشاره می‌کنیم.

امور مالی

هنگامی که از فناوری بلاکچین در تبادل داده طی تجارت استفاده می‌شود، انطباق داده ساده و برگشت‌ناپذیر داده‌ها ممکن می‌شود. همچنین، برای افزایش کارآمدی و سرعت تلفیق عمل می‌کند (این کار به صورت آنی انجام می‌شود) و به افزایش سطح امنیت تراکنش بین گروه‌های درگیر در خریدوفروش و بانک‌هایشان کمک می‌کند.

لازم به ذکر است که با توجه به شرایط انجام امور مالی و مساله انطباق با قوانین، لازم است که به اجماع برسند و این کار باید در دفترکل عمومی توزیع‌شده صورت بگیرد. با این حال، استفاده از دفترکل عمومی توزیع‌شده مشترک می‌تواند برای فعال‌سازی کارهای لازم در اجماع مالی عمل کند.

با توجه به توانایی شفاف‌سازی رویدادها در امتداد زنجیره تامین به‌صورت بلادرنگ و توانایی کاربران غیربانکی نظیر شرکت‌های حمل‌ونقل برای به‌روز نگه‌داشتن داده‌های مربوط به تراکنش‌های تکمیل‌شده، می‌توان اعطای منابع مالی را سریع‌تر انجام داد، بنابراین به بانک‌ها کمک می‌کنیم تا در زمان و منابع صرفه‌جویی کنند و درعین حال پردازش و انطباق دستی داده‌ها را کنار بگذارند. همچنین، این امر به بانک‌ها کمک می‌کند تا زمان و منابع ذخیره‌شده را برای دیگر طرح‌های ارزشی سودده که برای تجارت جهانی و محلی کلیدی‌اند، حفظ کنند.

بازار سرمایه

همان‌طور که پیش‌تر گفتیم، برخی از مزایای فناوری بلاکچین شامل این موارد است: اعتماد، آزادی، استقلال، سرعت، انسجام، جهانی بودن و کارآمدی. این مزایا تاثیری عمیق بر آینده

بازار سرمایه دارند. بازار سرمایه چهار حوزه کلیدی دارد و این حوزه‌ها شامل: پیش‌تجارت،[1] تجارت، پساتجارت[2] و امانت/توقیف[3] و عرضه اوراق بهادار[4] است. در حوزه پیش‌تجارت در بازار سرمایه، منافع فناوری بلاکچین شامل احراز صلاحیت هلدینگ و نیز آزادی این نوع هلدینگ‌ها، دوسویه‌سازی داده‌های استاتیک[5]، کاهش نقص در اعتبار، ابزار آسان‌تر برای شناخت مشتری (KYC)[6] و ابزار آسان‌تر برای شناخت مشتری مشتری (KYCC)[7] از طریق بررسی هلدینگ‌هاست. علاوه بر این، سطح بالاتر آزادی در نظارت بر نهادهای بازار، گزارش‌دهی اتوماتیک، انطباق امن و بلادرنگ تراکنش‌ها، توانایی بازگشت‌پذیر بودن آنی فرایندها و استاندارد بهبودیافته ضد پولشویی از جمله مزایای بلاکچین در حوزه تجارت و بازار سرمایه است. همچنین، کاهش نیاز به وثیقه، کارآمدی بالاتر در پردازش پساتجارت، اجرای خودکار قراردادهای هوشمند و حذف موسسات تهاتر برای تراکنش لحظه‌ای نقدینگی تنها برخی از مزایای فناوری بلاکچین در حوزه پساتجارت در بازار سرمایه است. صدور مستقیم سند روی بلاکچین، توانایی در اختیار داشتن پایگاه‌های غنی‌تر، اتوماسیون و کپی‌زدایی از فرایندهای سرویس‌دهی و در اختیار داشتن داده‌های مرجع مشترک از جمله مزایای فناوری بلاکچین در حوزه امانت/توقیف و عرضه اوراق بهادار در بازار سرمایه است. به‌منظور شکل‌دهی به آینده بازار سرمایه، با توجه به منافع بلاکچین، صنعت باید دیدگاهی جمعی داشته باشد و از این مزایا استفاده کند و در عین حال نقاط قوت اکوسیستم فعلی را حفظ کند.

قراردادهای هوشمند

در فصل ۶، به‌طور کلی قراردادهای هوشمند را تحلیل می‌کنیم؛ در این بخش، به قراردادهای هوشمند نگاهی کلی خواهیم داشت. بلاکچین می‌تواند از طریق افزودن کد اسنیپت‌ها[8]، پیام‌ها را خودکار کند. این کدها را «قرارداد هوشمند» می‌نامند. در قراردادهای هوشمند، از منطق «اگر این

1. pre-trade
2. post-trade
3. custody
4. securities servicing
5. static data mutualisation
6. Know Your Custome
7. Customer's Customer (KYCC)
8. code snippets

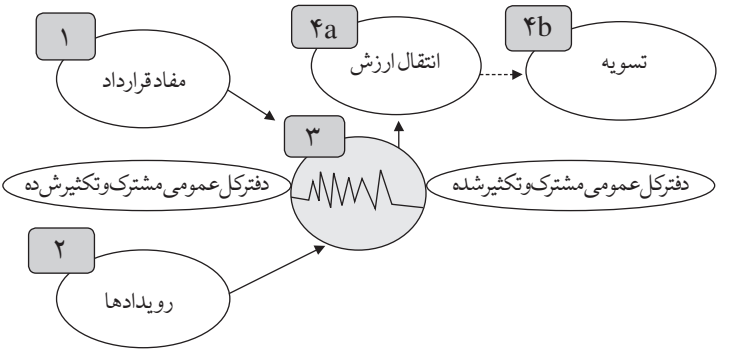
شد، آنگاه آن شود»[1] استفاده می‌کنند. اجرای قرارداد هوشمند نیازمند استفاده از مداخله انسانی نیست. این مطلب نشان می‌دهد که قراردادهای هوشمند غیرمتمرکزند و بدون واسطه یا مقررات گروه ثالث کار می‌کنند. علاوه بر این، آنها از پایگاه داده توزیع‌شده استفاده می‌کنند، به‌طوری که کاربران بتوانند مشـــخص کنند که رویدادی دیجیتال رخ داده است، بدون آنکه به واسطه یا گروه ثالث نیاز باشد. علاوه بر این، قراردادهای هوشمند به زبان قانونی نوشته نشده‌اند، بلکه به‌صورت برنامه‌های رایانه‌ای نوشته شده‌اند و این برنامه‌ها می‌توانند مقررات سفت‌وسختی را تعریف کنند.

علاوه بر این، می‌توان از قراردادهای هوشمند به‌منظور نمایش منطق کسب‌وکار طبق داده‌ها استفاده کرد. این نوع منطق شامل موارد زیر است:

- اولویت‌بخشی به سند ساختاری باز پرداخت؛
- اعطای وام.

رای‌گیری برای یک جایگاه در انجمن

شکل ۳-۱ فلوچارت استفاده از منطق کسب‌وکار را با قراردادهای هوشمند نشان می‌دهد. شکل ۳-۱ را با استفاده از جدول ۴-۱ بیشتر توضیح دادیم. جدول ۴-۱ به اعداد فلوچارت، رویدادهای فلوچارت و تشریح فلوچارت مربوط می‌شود.



شکل ۳-۱: فلوچارت استفاده از منطق کسب‌وکار با قراردادهای هوشمند. برگرفته از مقاله اسکینر

1. if-this-then-that’

جدول ۴-۱: اعداد فلوچارت، رویدادهای فلوچارت و تشریح فلوچارت

اعداد فلوچارت	رویدادهای فلوچارت	تشریح فلوچارت
۱	مفاد قرارداد	طرف‌های قرارداد، تعهدات طرفین و دستورالعمل‌های تسویه را تعیین می‌کنند. دارایی‌ها تحت کنترل شرایط قرارداد هوشمند برای اجرا قرار دارد (اگر... آنگاه...)
۲	رویدادها	رویداد باعث آغاز اجرای قرارداد می‌شود. رویداد به تراکنشی اشاره دارد که آغاز شده یا اطلاعاتی که دریافت شده.
۳	منطق کسب‌وکار	منطق کسب‌وکار (مفاد قرارداد) حرکت ارزش را بر پایه برآوردن شرایط مشخص می‌کند.
a4	انتقال ارزش	ارزش به گیرنده مورد نظر برحسب مفاد قرارداد انتقال می‌یابد. حساب دارایی‌های دیجیتال روی زنجیره (بیت‌کوین) به‌طور خودکار تسویه می‌شوند.
b۴	تسویه	حساب دارایی‌های خارج زنجیره (مثلا اوراق بهادار) با دستورالعمل‌های تسویه تطابق پیدا می‌کنند. تغییرات در حساب‌ها در دفترکل عمومی مشخص می‌شود.

در فلوچارت، عدد ۱ (مفاد قرارداد)، طرف‌های قرارداد، تعهدات طرفین و دستورالعمل‌های تسویه را تعیین می‌کنند، دارایی‌ها تحت نگهداری قرارداد هوشمند قرار می‌گیرند و شرایط اجرا مشخص می‌شود. در فلوچارت، عدد ۲ (رویدادها)، رویدادها می‌توانند به تراکنش آغازشده یا اطلاعات دریافتی و اجرای قرارداد اشاره داشته باشد.

در فلوچارت، عدد ۳ (منطق کسب‌وکار)، حرکت ارزش برحسب مفاد قرارداد مشخص می‌شود. در فلوچارت، عدد a۴ (ارزش انتقال‌یافته)، ارزش طبق مفاد قرارداد به گیرنده مورد نظر انتقال می‌یابد. عدد b۴ (تسویه)، حساب دارایی‌های خارج از زنجیره (مثلا اوراق بهادار)، نوع دستورالعمل تسویه را مشخص می‌کند.

حوزه‌های مرتبط با قراردادهای هوشمند در بخش مالی به این شرح است: حوزه وام، بازار سرمایه، ثبت تجارت و کنترل کیف پول رمزارز. علاوه بر این، رشد قراردادهای هوشمند تاکنون سریع بوده است و ایجاد قراردادهای هوشمند عمدتا برای عرضه اوراق مشتقه و اجرای تهاتر

(پایاپای) صورت گرفته است. چند پروژه منبع‌باز، از جمله کانترپارتی[1] و اتریوم، از لحاظ فناوری پیشرفت داشته‌اند تا زبان برنامه‌نویسی را تولید کنند که به تولید قراردادهای هوشمند پیشرفته منجر می‌شود.

نکته: با این حال، قراردادهای هوشمند با مسائلی مواجه هستند. برخی از این مسائل بدین شرح‌اند: انعطاف‌پذیری (از آنجاکه قراردادهای هوشمند طوری طراحی شده‌اند که در آغاز مذاکره شرکت‌کنندگان بتوانند درباره هر چیزی که وارد مذاکره می‌شود، تصمیم بگیرند و گاهی اوقات این برداشت نادرست است)، اطمینان‌پذیری (در نتیجه نبود واسطه، قانون‌گذار ممکن است با دشواری مواجه شود) و تفویض (اگر در حال حاضر، ساختاردهی با اتکای کامل به قراردادهای هوشمند به همه مفاد تراکنش ممکن نباشد، در آینده دشوار خواهد شد).

یکی از اولین بازارهایی که پیش‌بینی می‌شود از قراردادهای هوشمند استفاده کند، وام‌های صنفی است. این بازار با بیش از چهار تریلیون دلار روی فکس، ایمیل و در قالب صفحه‌گسترده‌های اکسل[2] در حال تبادل است. اموال هوشمند نیازمند کنترل مالکیت یک دارایی (اموال فیزیکی؛ برای مثال یک لپ‌تاپ، خانه و غیره) و اموال غیرفیزیکی نظیر سهام شرکت‌هاست.

موردپژوهی

در این بخش، روی شرکت تبادل دارایی دیجیتال (کوین‌بیس - بلاک‌استریم)[3] تمرکز می‌کنیم که شرکت توسعه‌دهنده نرم‌افزارهای کاربردی بیت‌کوین و دیگر نرم‌افزارهای کاربردی است.

کوین‌بیس به‌دست برایان آرمسترانگ و فرد اهرسام[4] در ۲۰ ژوئن ۲۰۱۲ تاسیس شد. مقر اصلی آن در سان‌فرانسیسکو است. این شرکت به سبب ارائه بستری برای ایجاد کیف پول ارز دیجیتال که می‌توان ارز دیجیتال را با امنیت در آن ذخیره کرد، شناخته شده است. علاوه بر این، در مرورگرهای وب، این کیف پول روی سیستم‌عامل اندروید و آیفون نیز کار می‌کند. کوین‌بیس ابزارهای امن ذخیره‌سازی، حفاظت از بیمه، نگهداری کلیدهای خصوصی و دیگر سرویس‌ها را تضمین می‌کند.

1. Counterparty
2. excel spreadsheets
3. Coinbase - Blockstream
4. Brian Armstrong - Fred Ehrsam

در مارس ۲۰۱۶، کوین‌بیس توسط ریچ‌توپیا[1] (شرکتی واقع در بریتانیا)؛ دومین سازمان بانفوذ بلاکچین معرفی شد. برای ساخت و نیز پذیرش پرداخت با ارز دیجیتال از سوی معامله‌گر و توسعه‌دهنده، واسط کاربری برنامه‌نویسی نرم‌افزار کاربردی (API)[2] ارائه می‌کند.

برخی از کاربردهای کلیدی بستر کوین‌بیس بدین شرح است: کیف پول همراه که به‌صورت بستری برای ارسال بیت‌کوین به دوستان و خرید از معامله‌گرانی عمل می‌کند که بیت‌کوین را می‌پذیرند و حفاظت از بیمه که طی آن بستر کوین‌بیس در برابر هر نوع توافق و دزدی دیجیتال محافظت می‌شود. لازم به ذکر است که ارزش بیت‌کوین و اتریوم در این بستر در دوره زمانی خاصی کمتر از مقدار بیمه‌شده است. یکی دیگر از کاربردهای این بستر ذخیره‌سازی ایمن است. اقدامات مناسبی از سوی کوین‌بیس برای ایجاد امنیت کافی در برابر هر نوع دزدی ارائه شده و این کار از طریق افزودن لایه امنیتی دیگری، جدای از نام کاربری و رمز عبور، محقق شده است.

لازم به ذکر است که نشانگرهای ارزش کاربران در بستر کوین‌بیس با توجه به واسط کاربری و تجربه کاربری مثبت است و تاثیر فرایند بالایی دارد.

موردپژوهی دیگر، فرایندی است که این شرکت آن را بلاک‌استریم می‌نامد و توسط آدام بک و مارک فردن‌بنچ[3] در سال ۲۰۱۴ تاسیس شد و شرکتی است که نرم‌افزارهای کاربردی بیت‌کوین و دیگر نرم‌افزارهای کاربردی را توسعه داده است. یکی از نرم‌افزارهای کاربردی بیت‌کوین سایدچین[4] است که کد منبع‌باز و همچنین توسعه‌دهنده زنجیره‌های فرعی (سایدچین) برای پیشرفت بیت‌کوین محسوب می‌شود. سایدچین حوزه نوآوری اصلی بلاک‌استریم است.

در اکتبر ۲۰۱۵، اولین نرم‌افزار کاربردی تجاری از فناوری سایدچین توسط بلاک‌استریم معرفی شد. این نرم‌افزار تجاری قرار بود به‌صورت بستری برای پردازشگرهای پرداخت بیت‌کوین، تبادل بیت‌کوین و نیز دلالی بیت‌کوین عمل کند.

لازم به ذکر است که هدف از اجرای بلاک‌استریم ایجاد راه‌های جدید نوآوری برای توسعه رمزارز، دارایی‌های آزاد و قراردادهای هوشمند بود. برخی از کاربردهای کلیدی بلاک‌استریم به این شرح هستند: نوآوری بدون نیاز به مجوز و تایید اعتماد که طی آن بستر بلاک استریم قصد دارد

1. Richtopia
2. Application Programming Interface
3. Mark Friedenbach
4. Sidechain

چنین محیطی را برای ایجاد زمینه نوآوری‌های جدید توسعه دهد. همچنین، می‌خواهد این مطلب را تضمین کند که توسعه‌دهندگان، عرضه‌کنندگان دارایی و کاربران به فناوری رایانشی دسترسی دارند؛ این دسترسی، ضمانتی طبیعی و رمزی برای نیازهای مالی آنها فراهم می‌کند. همچنین، انصاف، آزادی و حساب‌پذیری نیز از جمله ویژگی‌های این بستر است که هدف از آنها ایجاد بازارهای منصفانه و حساب‌پذیر است که هدفی مشترک را دنبال می‌کنند.

لازم به ذکر است که نشانگر ارزش کاربران در بستر بلاک‌استریم با توجه به واسط کاربری و تجربه کاربری مثبت است و تاثیر فرایندی بالایی دارد.

خلاصه

در این فصل، به معرفی فناوری بلاکچین پرداختیم. بلاکچین را دفترکل عمومی توزیع‌شده یا پایگاه‌داده اسناد تراکنش‌ها معرفی کردیم که در میان کاربران شبکه مشترک است. همچنین، پدیده بلاکچین را بررسی کردیم که در آن پایگاه‌های داده متمرکز و غیرمتمرکز و بیت‌کوین اولین موارد در فهرست بلندبالای کاربردهای فناورانه بلاکچین بودند. علاوه بر این، درباره چهار مفهوم کلیدی فناوری بلاکچین بحث کردیم؛ بلاکچین، پایگاه داده غیرمتمرکز، اثبات کار (PoW) و اثبات سهام (PoS) و قراردادهای هوشمند.

فناوری بلاکچین شامل توزیع و رمزنگاری پایگاه داده به شیوه‌ای برگشت‌ناپذیر و غیرقابل خرابکاری است. همچنین، چون مزایایی نظیر اعتماد، آزادی، استقلال، سرعت، انسجام، جهانی‌بودن و کارآمدی دارد (که کلید توسعه بازار سرمایه، سیستم‌های پرداخت، ترید فاینانس و دیگر حوزه‌های بخش‌های مالی و غیرمالی‌اند) برای کارآمدی بخش مالی از اهمیت زیادی برخوردار است.

شایان ذکر است که این فناوری در حال گسترش در بخش‌های غیرمالی است. همان‌طور که ایموگن هیپ[1] در رویدادی در لندن در سال ۲۰۱۵ گفته بود: «بزرگ‌ترین مشکل برای یک هنرمند در حال حاضر پرداخت است. بلاکچین می‌تواند بسترها و خدمات بسیاری را به وجود آورد که باعث غنای زندگی ما می‌شوند.» تا حد زیادی، آینده فناوری بلاکچین روشن است، البته اگر از آن استفاده شود.

1. Imogen Heap