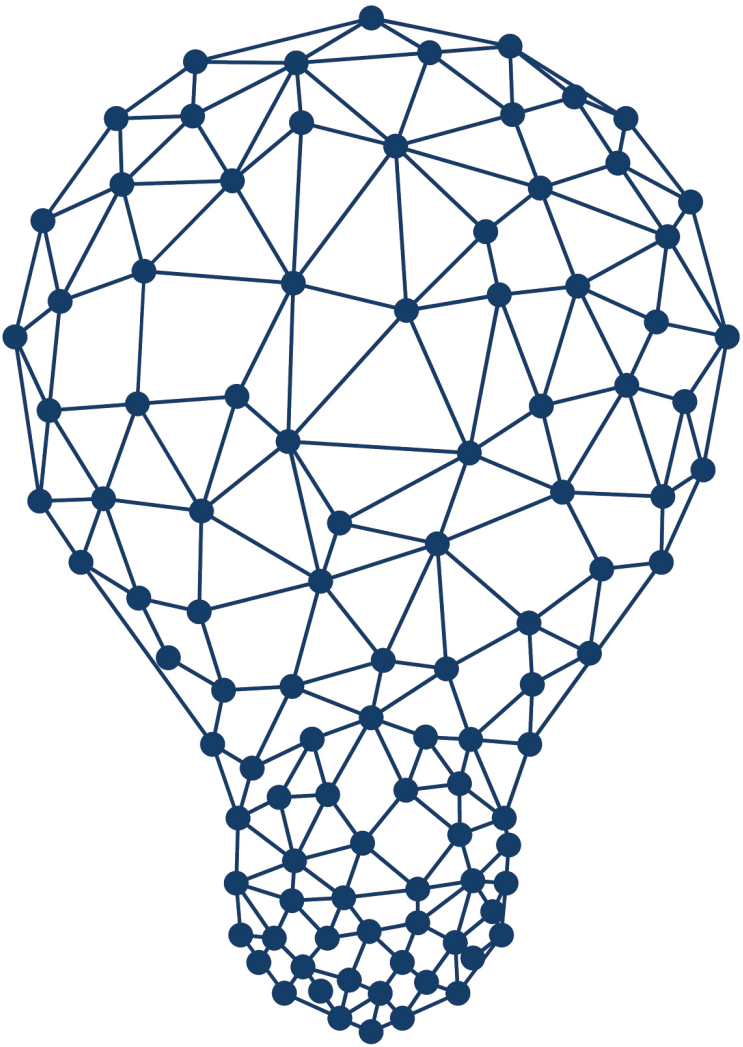
# نوآوری کسب‌وکار از طریق بلاکچین

وینچنزو مورابیتو

مترجم: حامد حیدری

راه پرداخت



فایل نمونه


بسم الله
الرحمن
الرحيم

# نوآوری کسب و کار از طریق بلاکچین

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: ۲۱۸ ص.؛ ۵/۱۴×۵/۲۱س‌م. / شابک:۶-۴۰-۶۵۹۹-۹۶۴-۹۷۸/ وضعیت فهرست نویسی: فیپا/ یادداشت: عنوان اصلی: Business Innovation Through Blockchain / موضوع: بلاک‌چین/ موضوع: تکنولوژی؛ / شناسه افزوده: حیدری، حامد ۱۳۶۶- 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)

راه‌پرداخت

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

# 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.

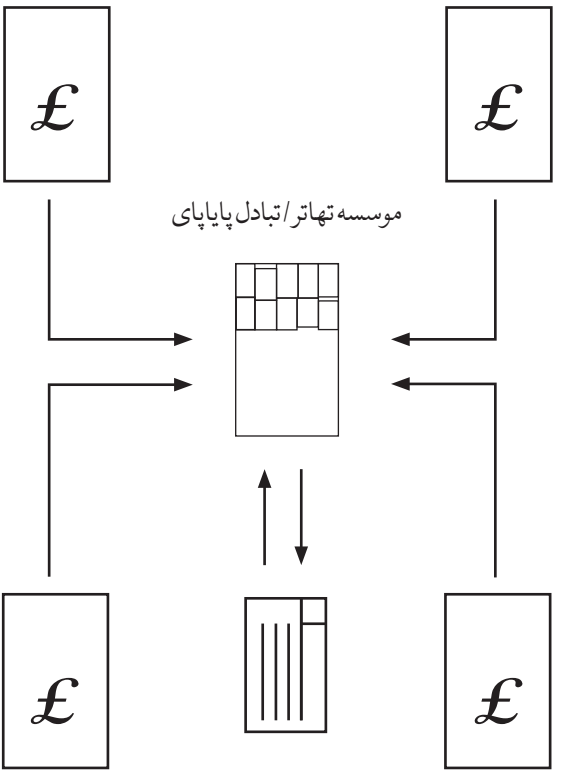
در ادامه چهار مفهوم کلیدی فناوری بلاکچین (بلاکچین، پایگاه داده غیر متمرکز، اثبات کار/اثبات سهام و قراردادهای هوشمند) را بررسی خواهیم کرد.

## 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

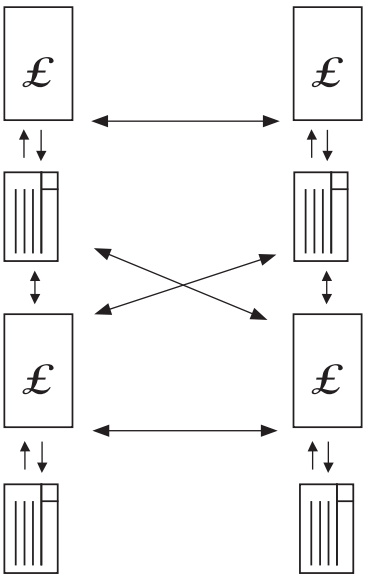
- برای ساده‌شدن تبادل تجاری؛
- برای ذخیره ارزش از سوی کاربران برای اهداف آتی؛
- عمل کردن به‌عنوان واحد پایه برای اندازه‌گیری ارزش کالاهای بازار و خدمات ارائه‌شده.

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:<br>BIP[1] برای نگارش قوانین<br>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

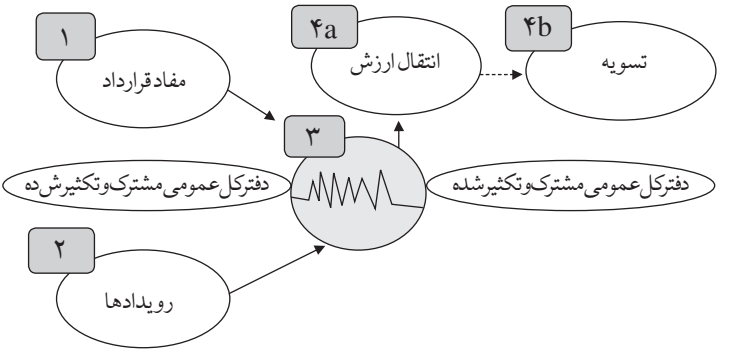
شد، آنگاه آن شود»[1] استفاده می‌کنند. اجرای قرارداد هوشمند نیازمند استفاده از مداخله انسانی نیست. این مطلب نشان می‌دهد که قراردادهای هوشمند غیرمتمرکزند و بدون واسطه یا مقررات گروه ثالث کار می‌کنند. علاوه بر این، آنها از پایگاه داده توزیع‌شده استفاده می‌کنند، به‌طوری که کاربران بتوانند مشـــخص کنند که 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

# ۲

## سیستم ارزش بلاکچین

### چکیده

مدت‌ها پیش از ظهور بلاکچین، نقدینگی دیجیتال به این صورت تعریف شده بود که یک سرور مرکزی معتمد با کمک رمزنگاری کلید عمومی مانع از دوباره خرج کردن می‌شود، در این حالت هر نماینده یک کلید خصوصی دارد (که مثل رمز عبور مخفی نگه داشته می‌شود) و یک کلید عمومی دارد که بین همه نمایندگان مشترک است. با وجود پیشرفت‌های زیاد در رمزنگاری، تضمین سازگارپذیری بین متمرکزسازی، ناشناس‌بودن و جلوگیری از دوباره خرج کردن با شکست مواجه شد و در نهایت قابلیت اطمینان به این پول جدید در هاله‌ای از ابهام باقی ماند. اخیرا، مدل بلاکچین بیت‌کوین به‌صورت ستونی برای طیف وسیعی از اپلیکیشن‌ها معرفی شده است؛ از تجارت دارایی گرفته تا تراکنش املاک واقعی، از خدمات سند تضمینی تا سیستم توزیع درآمد ملی. سیستم ارزش یکی از مجموعه‌های همدیس/متجانس ارزش است که سازمان‌ها یا جوامع می‌توانند آن را استانداردی برای هدایت رفتار خود در همه شرایط در نظر بگیرند. در این فصل، درباره بلاکچین در مقام سیستم ارزشی بحث می‌کنیم و اصول اصلی بنیادی این فناوری، شیوه کار آن، مزایا، محدودیت‌ها و چالش‌های بلاکچین را شرح می‌دهیم. در نهایت، برخی از اپلیکیشن‌های پیشرفته آن را نیز معرفی می‌کنیم.

### مقدمه

فناوری‌های مدرن به مردم امکان ارتباط مستقیم را می‌دهند. تماس‌های صوتی و تصویری، ایمیل، تصاویر و پیام‌های لحظه‌ای مستقیما از فرستنده به گیرنده، در اینترنت، منتقل می‌شوند، در حالی که اعتماد بین افراد حفظ می‌شود و اصلا مهم نیست که چقدر با یکدیگر فاصله داشته باشند. با این حال، وقتی نوبت به پول می‌رسد، مردم باید به طرف سوم اعتماد کنند تا تراکنش را تکمیل کنند؛ بنابراین طی

دهه گذشته، بلاکچین به‌آرامی در اینترنت نفوذ کرده و الگوی دیجیتالی جایگزین و امنی به حساب می‌آید. با استفاده از ریاضی و رمزنگاری، پایگاه داده غیر متمرکزی از هر نوع تراکنش ارزشی خواهیم داشت که شامل پول، کالا، اموال، کار یا حتی رای می‌شود. به عبارتی دیگر، بلاکچین یک ساختار داده‌ای است که خلق، اشتراک‌گذاری و ذخیره‌سازی دفترکل عمومی دیجیتال تراکنش‌ها را میان شبکه رایانه‌ای توزیع‌شده تسهیل می‌کند و آن را غیر متمرکز و توزیع‌شده می‌گرداند. این حالت امکان ایجاد سندی را به وجود می‌آورد که می‌توان اعتبار آن را از طریق کل جامعه تایید کرد و بلاکچین را فناوری «بی‌نیاز از اعتماد» می‌کند. در این مورد، «بی‌نیاز از اعتماد» یعنی «ارزش» روی شبکه‌ای رایانه‌ای را می‌توان تایید کرد، رصد کرد و بدون نیاز به طرف سوم معتمد یا نهاد متمرکز اجرا کرد. پس، سازمان اعتماد طرف سوم نظیر وری‌ساین[1] ممکن است دیگر لازم نباشد.

در نتیجه، اقتصاد آینده به سوی یکی از اموال و اعتمادهای توزیع‌شده می‌رود که در آن هر کسی که به اینترنت دسترسی داشته باشد، می‌تواند وارد تراکنش‌های مبتنی بر بلاکچین شود. می‌توان بلاکچین را وصیت‌نامه و قراردادی در نظر گرفت که خودش مسئول اجرای خودش است؛ منبع غیر متمرکز جهانی اعتماد می‌شود. بر همین اساس، مالکیت سیستم به یک شرکت یا شخص خاص تعلق ندارد، بلکه هر کسی می‌تواند از آن استفاده و آن را راه‌اندازی کند. در نتیجه، تا وقتی یکی از رایانه‌ها یا گره‌ها در شبکه امن باشد، دفترکل عمومی دیجیتال امن است.

کاربردهای فناوری بلاکچین بی‌پایان است. برخی پیش‌بینی می‌کنند که در کمتر از ۱۰ سال، از آن برای جمع‌آوری مالیات استفاده شود. همچنین، چون هر تراکنش روی یک دفترکل توزیع‌شده و عمومی ثبت می‌شود، انتقال پول به نواحی مختلف جغرافیایی که دسترسی به نهادهای مالی در آنجا محدود است، آسان‌تر می‌شود و همین امر باعث کاهش چشم‌گیر کلاهبرداری مالی می‌شود. بخش بزرگی از سرویس‌های اعتماد که از بانکداری تا دفاتر اسناد رسمی را شامل می‌شود، با چالش‌هایی درباره قیمت و حجم مواجه می‌شوند و در برخی موارد بقای آنها با چالش مواجه می‌شود. ممکن است نهادهای دولتی مقررات مالی سنتی را به سبب امکانات جدیدی که بلاکچین به آنها ارائه می‌کند، اجرا کنند تا دیگر نیازی به واسطه‌های مالی فناور نداشته باشند. سازمان‌هایی نیز که خود را با روند جدید فناوری سازگار نکنند، دچار اختلال یا فروپاشی می‌شوند، زیرا موفقیت آنها به انتخاب استراتژیکی که درباره پذیرش فناوری‌های جدید انجام می‌دهند، بستگی دارد. با این حال، قضاوت

1. VeriSign

در این‌باره که آیا دولت‌ها و نهادهای مالی و قانونی از بلاکچین استفاده خواهند کرد یا خیر، هنوز زود است. می‌توان پیش‌بینی کرد که همه آماده استفاده از ویژگی‌ها و مشخصه‌های این فناوری نیستند.

## اصول بنیادی

همان‌طور که در فصل اول گفتیم، بلاکچین به‌صورت فناوری اعتبارسنجی و احراز هویت و صلاحیت برای بیت‌کوین توسعه یافت؛ اولین ارز دیجیتال رمزی غیرمتمرکز. در بیت‌کوین، تراکنش زمانی آغاز شده که مالک آینده سکه‌ها (یا توکن‌های دیجیتال) کلید عمومی خود را به مالک اصلی بفرستد. سکه‌ها از طریق امضای دیجیتال[1] به‌صورت هش منتقل شده‌اند. کلیدهای عمومی از لحاظ رمزنگاری آدرس‌های تولیدشده‌ای هستند که در بلاکچین ذخیره شده‌اند. هر سکه با یک آدرس در ارتباط است و یک تراکنش در اقتصاد رمزی[2] صرفا تبادل سکه از یک آدرس به آدرس دیگر است. در بلاکچین، داده‌های مورد استفاده در تراکنش در سند عمومی غیرقابل تقلیدی یا صفحه‌گسترده عظیمی ذخیره می‌شود که اعضای حاضر در شبکه همتابه‌همتا از آن محافظت می‌کنند و مانند اعتبارسنج‌های صلاحیت و اعتبار خود عمل می‌کنند. فناوری بلاکچین مکانیسمی برای ایجاد تراکنش‌های «بدون نیاز به اعتماد» است که نیازی به اعتبارسنجی یا مانیتورینگ یکپارچگی ارزش تبادل‌شده بین شبکه‌های رایانه‌ای از سوی نهادهای واسطه ندارند. به بیان ساده، بلاکچین به کسب‌وکارها اجازه می‌دهد تا در میان دیگران تراکنش داشته باشند، بدون آنکه به نهاد مالی متمرکزی نظیر بانک نیاز باشد.

تراکنش بلاکچین بین دو گروه زمانی آغاز می‌شود که یکی از کاربران پیامی به شبکه در خصوص مفاد و شرایط حاکم بر تراکنش بین دو ذی‌نفع بفرستد. سپس، کاربر دیگر پذیرش خود را در شبکه اعلام می‌کند که به‌طور پیش‌فرض درخواست کاربران شبکه برای احراز هویت و تایید تراکنش را فعال می‌سازد. در نتیجه، اعضای شبکه به‌طور خودکار نقش اعتبارسنج‌ها را بازی می‌کنند که از تراکنش مذکور در برابر دوباره خرج‌کردن در سیستم اعتبارسنجی جلوگیری می‌کند (اثبات کار) و نشان‌دهنده رقابت بین اعضای شبکه برای اعتبارسنجی تراکنش است. در این نقطه، وقتی تراکنش تایید شد، دفترکل عمومی (سند بلاکچین) و نیز کاربران شبکه به‌طور جمعی جایگاه تراکنش‌هایی را که اخیرا افزوده شده، به‌روزرسانی می‌کنند. این مکانیسم با استفاده از دفترکل عمومی غیرمتمرکز و

1. digital signature
2. crypto-economy

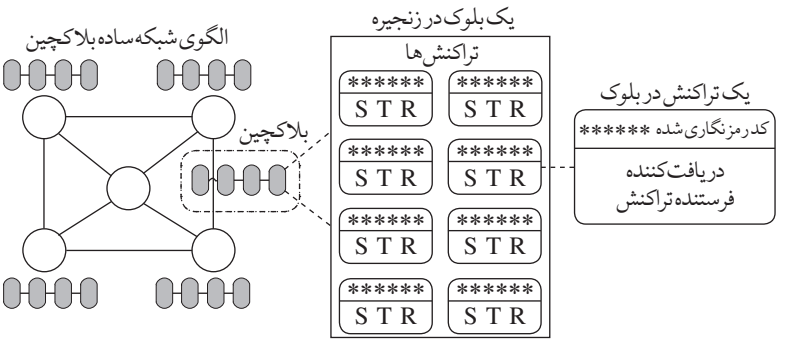
نیز الگوریتم‌های رمزی به ایجاد اعتماد بین ذی‌نفعان کمک می‌کند. الگوریتم‌های رمزی می‌توانند تراکنش‌های تاییدشده‌ای را تضمین کنند که نمی‌توان پس از اعتبارسنجی آنها را تغییر داد. نکات زیر به‌طور خلاصه ویژگی‌های کلیدی بلاکچین را شرح می‌دهد:

**غیرمتمرکز:** یکی از ویژگی‌های اصلی بلاکچین غیرمتمرکز بودن آن است که کاربران در آن به یکدیگر وصل می‌شوند و در بازار می‌توانند تراکنش انجام دهند و مالکیت دارایی‌های ارزش‌دار را میان خود به شیوه‌ای شفاف و بدون کمک واسطه و میانجی انتقال دهند، در نتیجه، نام شبکه ارزش[1] به آن می‌دهند؛

**اعتماد و سرمنشأ:** بلاکچین مکانیسم انکارناپذیری برای تایید داده‌های تراکنش ایجاد می‌کند که در بلوک مورد نظر در زمانی خاص رخ داده است. علاوه بر این، چون هر بلوک در زنجیره، حاوی اطلاعاتی درباره بلوک قبلی است، پس تاریخچه، مکان و مالکیت هر بلوک به‌طور خودکار احراز صلاحیت می‌شود و نمی‌توان آن را تغییر داد.

**ارتجاع و برگشت‌ناپذیری:** خاصیت ارتجاع بلاکچین ناشی از ساختار آن است، چون به‌صورت شبکه‌ای توزیع‌شده از گره‌ها (رایانه‌ها) طراحی شده که هر گره یک کپی از کل زنجیره را دارد. از این رو، وقتی تراکنش تایید می‌شود و توسط گره‌های شرکت‌کننده احراز صلاحیت می‌شود، تغییر یا دستکاری داده‌های تراکنش غیرممکن می‌شود.

این بخش، کارکرد بلاکچین را توضیح می‌دهیم. شکل ۱-۲ اجزای ابتدایی بلاکچین را نشان می‌دهد.




شکل ۱-۲: اجزای ابتدایی بلاکچین

1. Value network

در شکل ۱-۲، تراکنش متشکل از فرستنده، اطلاعات تراکنش و گیرنده است و به‌واسطه کد رمز حفاظت می‌شود. این بلوک حاوی چندین تراکنش است و بلاکچین از چندین بلوک ساخته شده است. شکل ۱-۲ نشان می‌دهد که این تراکنش چگونه تایید اعتبار می‌شود و چگونه بلوک ساخته می‌شود، زنجیره‌ای می‌شود و اعتبارسنجی می‌شود.

نکات زیر به مراحل شکل ۲-۲ مربوط است:

**تعریف تراکنش:** اولین گام است که طی آن فرستنده تراکنشی را به وجود می‌آورد که اطلاعاتی درباره آدرس عمومی گیرنده، ارزش تراکنش و امضای دیجیتال رمزنگاری دارد که اعتبار و صحت تراکنش را تایید می‌کند.

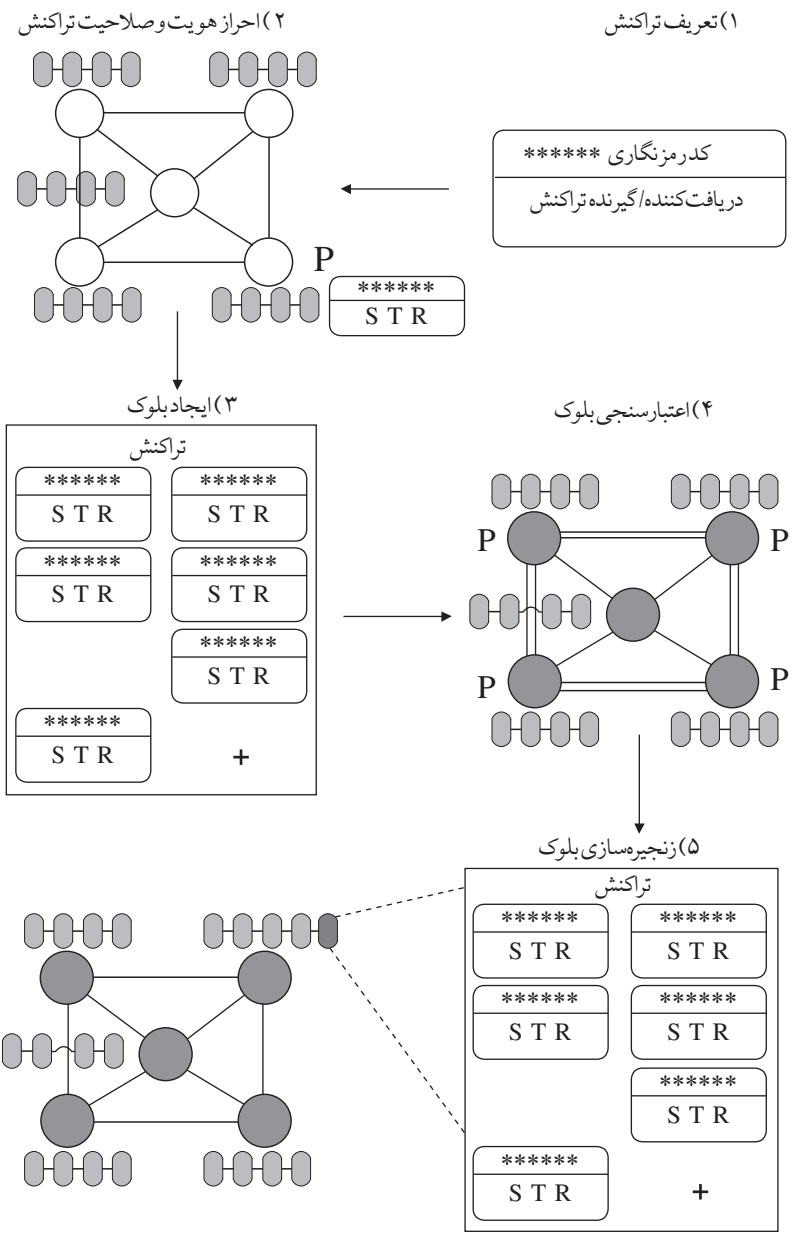
**احراز صلاحیت و اعتبار تراکنش:** وقتی گره‌های شبکه، تراکنش را دریافت می‌کند، در ابتدا پیام را از طریق رمزگشایی امضای دیجیتال اعتبارسنجی می‌کند و سپس پیام به‌طور موقت حفظ می‌شود تا آنکه در ایجاد بلوک مورد استفاده قرار بگیرد.

**ایجاد بلوک:** یکی از گره‌ها در شبکه از تراکنش‌های معلق استفاده می‌کند تا دفترکل یا بلوک را به‌روزرسانی کند. سپس، در بازه‌های زمانی خاص، بلوک به‌روزشده به گره‌های دیگر مخابره می‌شود که منتظر تایید اعتبار هستند.

**اعتبارسنجی بلاکچین:** وقتی گره مسئول اعتبارسنجی در شبکه درخواست اعتبارسنجی یک بلوک به‌روزشده را دریافت می‌کند، از فرایند تکرارشونده‌ای عبور می‌کند که نیازمند تفاهم از جانب دیگر گره‌هاست تا صلاحیت بلوک سنجیده شود.

**زنجیره‌سازی بلوک:** وقتی همه تراکنش‌های بلوک تایید شدند، آنگاه بلوک جدید به‌صورت زنجیره به بلاکچین فعلی وصل می‌شود و همین موضوع به مخابره حالت جدید بلوک به باقی شبکه منجر می‌شود.

ممکن است تکمیل این مراحل ۳ تا ۱۰ ثانیه طول بکشد و همین مطلب باعث شده که بلاکچین به فناوری بسیار سریعی برای تسویه تراکنش‌های مالی مبدل شود.




شکل ۲-۲: مرور تعمیم‌یافته از تراکنش بلاکچین

## چالش‌های بلاکچین

پذیرش بلاکچین به‌صورت روشـــی واحد برای اجرای تراکنش‌های مالی در اینترنت، نیازمند بازطراحی وظیفه برای شبکه سازمان‌های شرکت‌کننده و نیز فرایندهای مالی کسب‌وکار است و با چالش‌های بسیاری مواجه است. اول آنکه، سازمان‌ها باید به توافق برسند که مقررات بنیادی شبکه جدید را مدیریت کنند. با این حال، چنین توافق‌هایی ممکن است فرایند بسیار طاقت‌فرسایی باشد، زیرا سازمان‌ها و کسب‌وکارهای متفاوت، سیاست‌ها و پروتکل‌های اجرایی متنوعی دارند و ممکن است تعیین بهترین رویه به مذاکراتی طولانی و بادقت نیاز داشته باشد. علاوه بر این، مسائل امنیت و حریم خصوصی دغدغه بزرگی در پی دارد، چون سازمان‌های همکار باید از سطح امنیت موجود در برابر حملات و نیز اطلاعات تجاری که باید برای هر تراکنش مالی شـــناخته شود، تا در شبکه سنجش‌پذیر باشد، مطمئن و راضی شوند. به‌منظور غلبه بر چالش‌های ذکرشده، استانداردها نقطه شروع خوبی برای همگام‌کردن نهادها در صنعت مورد نظر هستند. استانداردها حیطه رقابتی برابری ایجاد می‌کنند و از زمان ورود فناوری‌های جدید به بازار می‌کاهند. بنابراین، تمرکز اجرای بلاکچین بیشتر بر استانداردسازی جریان داده و زبان واسطه مورد استفاده برای برقراری ارتباط در بلاکچین است تا فناوری‌ای که از بستر آن پشتیبانی می‌کند.

## مزایا و محدودیت‌های بلاکچین

فناوری بلاکچین بر پایه ایده توزیع پایگاه داده تراکنش بین چندین گره اســـت که همان رایانه‌ها هستند. این گره‌ها در کنار یکدیگر به‌صورت یک سیســـتم کار می‌کنند و توالی رمزدار تراکنش‌ها را به‌صورت یک زنجیره یا بلوک واحد ذخیره می‌کنند. همان‌طور که پیش‌تر گفتیم، با اســـتفاده از بلاکچین، گروه‌ها می‌توانند بدون وابستگی به واسطه یا میانجی برای تامین اعتماد و سنجش اعتبار تراکنش، تبادل را انجام دهند. با این حال، این مزیت تنها امتیاز بلاکچین نیســـت. فهرست زیر به مهم‌ترین مزایای بلاکچین اشاره می‌کند که می‌تواند وارد دنیای کسب‌وکار شود:

- **کاربران مختار:** بلاکچین کاربران را قادر می‌سازد تا اطلاعات و نیز تراکنشی را کنترل کنند که خود بخشی از آن هستند.
- **دوام، اعتمادپذیری و طول عمر:** بلاکچین به معماری رایانشی متمرکز وابسته نیست. بنابراین به سبب شکست یک نهاد دچار اختلال نمی‌شود.

- **پردازش با یکپارچگی، شفافیت و تقلیدناپذیری:** تراکنشی که با استفاده از بلاکچین انجام شده، در معرض دید عموم است و نمی‌توان آن را تغییر داد، بنابراین یکپارچگی، شفافیت و انکارناپذیری تضمین می‌شود.
- **تراکنش سریع‌تر و کم‌هزینه‌تر:** بلاکچین ظرفیت کاهش فوق‌العاده زمان و هزینه را در تراکنش‌ها از طریق حذف واسطه‌ها یا گروه‌های ثالث دارد. با این حال، معرفی فناوری نوپایی نظیر بلاکچین به دنیای کسب‌وکار، به سبب اصولی که بر آن استوار است، با چالش‌های متعددی مواجه است. بنابراین حل‌وفصل مشکلات مربوط به فرایند اعتبارسنجی تراکنش و محدودیت داده به ازای هر تراکنش در پذیرش این فناوری جدید در بخش‌های حیاتی کسب‌وکار نظیر خدمات مالی بسیار مهم است. علاوه بر این، در فهرست زیر درباره دیگر چالش‌ها بحث می‌کنیم که اجرای بلاکچین را با اختلال مواجه ساخته‌اند.
- **قوانین حاکم بر وضعیت مقرراتی:** ارزهایی که در حال حاضر در تراکنش مالی استفاده می‌شوند، از سوی دولت‌ها کنترل می‌شوند و برای آنکه بلاکچین از سوی نهادهای مالی به‌طور گسترده پذیرفته شود، باید دولت‌ها برای وضع مقررات استفاده از بلاکچین با یکدیگر به توافق برسند، در غیر این صورت، وضعیت آن نامشخص باقی می‌ماند.
- **دغدغه‌های امنیتی و حریم خصوصی:** با وجود راهکار امنیتی مربوط به الگوریتم رمزنگاری قوی، دغدغه‌های امنیتی سایبری را یکی از عوامل مهم در نظر می‌گیرند که بر تصمیم عموم درباره اشتراک‌گذاری داده‌های شخصی با استفاده از بلاکچین تاثیر می‌گذارد. سیستم امنیت بلاکچین در فصل ۴ بررسی می‌شود.
- **آسیب‌پذیری نرم‌افزاری:** ایرادات نرم‌افزاری همیشه وجود دارد و نرم‌افزارهای ضعیف به‌طور ویژه در برابر فعالیت‌های خرابکارانه آسیب‌پذیرند. همان‌طور که نرم‌افزار پیچیده‌تر و به‌هم متصل‌تر می‌شود، اطمینان‌پذیری آن کاهش می‌یابد و در عین حال تعداد ایرادات بیشتر می‌شود. گرچه پیشرفت‌های بزرگی در فناوری داشتیم، اما به دلیل اینکه نرم‌افزار را انسان می‌نویسد، بنابراین همیشه ناقص است. علاوه بر این، یکپارچگی نرم‌افزار و شبکه از لحاظ بنیادی در ارزش‌یابی بلاکچین مهم است، زیرا فناوری زیرساختی است. اگر فناوری در تمامی ابعاد سیستم مالی در سطح جهان نفوذ کند، اثرات هک یا ایراد نرم‌افزاری فاجعه‌بار خواهد بود.
- **دغدغه‌های یکپارچه‌سازی:** وقتی سازمان‌ها از فناوری‌های جدید برای پربازده کردن فرایند

کسب‌وکار خود استفاده می‌کنند، با چالش تغییر مدیریت و یکپارچه‌سازی سیستم‌های جدید با سیستم‌های قدیمی مواجه می‌شوند. در این وضعیت، استفاده از بلاکچین مستثنی نیست. چون چنین پروژه‌هایی وظیفه بزرگ و دشواری برای راهبردی کردن انتقال خواهند داشت.

- **درک فناوری:** یکی از بزرگ‌ترین ریسک‌های عملیاتی در بلاکچین آن است که افراد نسبتاً کمتری کارکرد آن را درک می‌کنند. کدنویسان و هکرها که در نوشتن نرم‌افزار تخصص دارند، وظایف ابتدایی و کارکرد آن را درک می‌کنند. با این حال، باید زمانی نگران استقرار نرم‌افزار باشیم که از ناشناخته‌ها آگاهی نداریم. برای مثال، اخیراً فولکس‌واگن، خودروساز آلمانی، اقرار کرده نرم‌افزاری که توسط کدنویسان برنامه‌نویسی شده‌اند، میزان گسیل آلاینده از خودروهای آنها را اشتباه ذکر می‌کردند. در نتیجه، خشم بین‌المللی در برابر این شرکت به وجود آمد که منجر شد رئیس اجرایی این شرکت استعفا دهد. اگر چنین اتفاقی در بلاکچین رخ می‌داد، تاثیرات بزرگ‌تری بر دنیای مالی داشت.
- **ذات غیرمتمرکز بلاکچین:** درست است که بلاکچین غیرمتمرکز است و همین مطلب باعث می‌شود حمله همزمان به همه کاربران دشوارتر شـــود، اما با این حال، اگر حمله از سوی یکی از توسعه‌دهندگان صورت بگیرد که تجربه توپولوژی شبکه دارد، آنگاه ممکن است خرابی بزرگی برای شبکه به همراه داشته باشد.
- **پذیرش فرهنگی:** پذیرش عمومی به منظور استفاده از بلاکچین برای موفقیت در پروژه‌های اجرای بلاکچین مهم است.
- **هزینه اولیه اجرا:** صرفه‌جویی حاصل استفاده از بلاکچین جذاب است، با این حال، هزینه‌های اولیه اجرا را عاملی مهم می‌دانند که نمی‌توان از آن غافل شد.

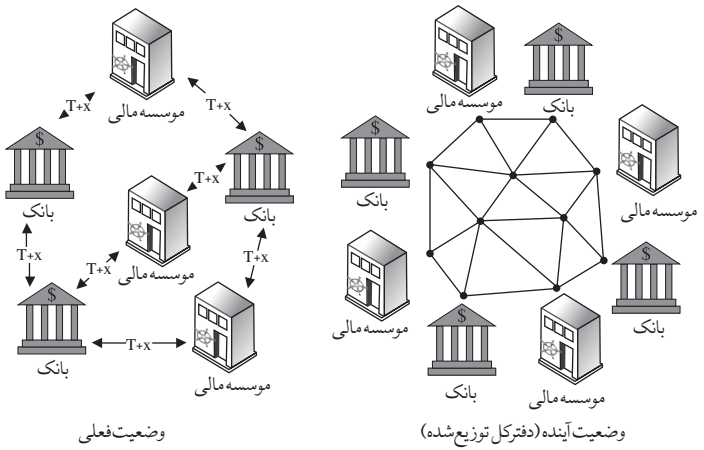
## استفاده بالقوه از فناوری بلاکچین

فناوری بلاکچین فرصت‌های بسیاری برای صرفه‌جویی در هزینه‌ها و زمان و نیز افزایش امنیت برای انواع تراکنش آنلاین پدید می‌آورد. در این بخش، دربـــاره برخی از کاربردهای بلاکچین در خدمات مالی، بخش بهداشت و درمان و نیز پژوهش‌های علمی بحث می‌کنیم.

### اجرای بلاکچین در خدمات مالی

علاقه به بلاکچین به‌سرعت در حال رشد است، زیرا عوامل بسیاری نظیر عدم کفایت طرف

سوم، زمان پردازش تدارکات، افزایش بازده و نیز شبکه‌های هزینه‌بر و پرریسک مخاطبان در این امر دخیل‌اند؛ بنابراین نهادهای بخش خدمات مالی در حال نشان‌دادن علاقه به این فناوری به‌عنوان جایگزینی برای رویکرد فعلی در اجرای تراکنش بین سازمان‌ها هستند. فهرست چنین نهادهایی شامل بانک‌های بزرگ نظیر جی‌پی مورگان و گلدمن ساکس است که برای سرمایه‌گذاری در بلاکچین و توسعه آن طبق نیازها، استانداردها و انتظارات‌شان با یکدیگر شریک شده‌اند. چنین سرمایه‌گذاری برای نهادهای مالی حیاتی است، زیرا بانک سانتاندر برآورد کرده که بلاکچین ظرفیت صرفه‌جویی ۲۰ میلیارد دلار در نتیجه حذف نهادهای متمرکز و غلبه بر دلایل ذکرشده در سرمایه‌گذاری در بخش بلاکچین را دارد. علاوه بر این، وقتی نوبت به ارزیابی عملکرد می‌رسد، بلاکچین باعث تسهیل بررسی ارزش اعتبار چک‌ها می‌شود و در نتیجه کاهش اصطکاک و افزایش شفافیت را در پی خواهد داشت. به‌طور مشابه، نهادهای مالی می‌توانند از توانایی بلاکچین در کاهش زمان تسویه مورد نیاز در تبادلات مالی نفع ببرند که در آن تهاتر پساتجارت و تسویه بخشی از فرایند است. دومین مورد استفاده به تکثیر دفترکل در خدمات مالی مربوط می‌شود، چون هر نهاد مالی ثبت‌کننده‌های منحصربه‌خود را در اختیار دارد. فرایند تلفیق این ادارات هزینه‌بر است، به‌ویژه در مورد بانک‌های بزرگ که صدها اداره کل دارند.




شکل ۳-۲: تاثیر بلاکچین بر خدمات مالی

همچنین، این فرایند با اســتفاده از ابزارهای ناامن و ابتدایی نظیر زبان برنامه‌نویسی ویژوال بیسیک انجام می‌شــود که فرایندی پرخطر خواهد بود. در نتیجه، نیاز به فناوری نظیر بلاکچین برای رفع تاخیر ناشی از معماری گسسته احساس شد. بلاکچین می‌تواند دفترکل واحدی برای تراکنش بین موسسات مالی شرکت‌کننده باشــد که این امر به تراکنش‌های تاییدشده به صورت تقریبا آنی منجر می‌شود (شکل ۳-۲).

استفاده از بلاکچین در بخش خدمات مالی می‌تواند مزایایی داشته باشد:

**کاهش هزینه:** در نتیجه حذف تکثیر و کاهش پردازش پســاتجارت نظیر تســویه و تلفیق (مغایرت‌گیری)، برآورد می‌شود که بانک‌ها می‌توانند بین ۱۵ تا ۲۰ میلیارد دلار طی هفت سال صرفه‌جویی داشته باشند.

**قراردادهای هوشمند:** قراردادهای هوشــمند یکی دیگر از مزایای بلاکچین است، چون اکثریت دارایی‌های مالی موجود به شکل الکترونیکی هستند و قرارداد هوشمند می‌تواند منطق موجود را خودکار ســازد و در نتیجه از هزینه رمیتنس (انتقال پول بین‌المللی) و اولیه کاســته می‌شود. قراردادهای هوشمند در فصل ۶ بررسی می‌شود.

**مدیریت ریسک:** می‌توان از بلاکچین در این حوزه نیز استفاده کرد، زیرا سرعت تسویه بالایی دارد که به افزایش نقدینگی و کاهش ریسک ترازنامه منجر می‌شود.

**انطباق بهتر با قوانین:** از طریق در اختیار داشــتن قانون‌گذاری ذی‌صلاح برای تایید اینکه دفترکل عمومی شفاف بین ســازمان‌های مالی توزیع شده اســت. این مطلب می‌تواند هزینه فرایندهای ضدپولشویی و مبارزه علیه تروریسم را کاهش دهد.

### اجرای بلاکچین در بخش بهداشت و درمان

درک منافع بلاکچین برای صنعت بهداشــت و درمان رشد داشته اســت، زیرا فرصت‌های بسیاری برای این بخش حیاتی دارد.

مدل‌های جدید مدیریت و اشتراک‌گذاری پرونده‌های پزشکی با استفاده از ظرفیت بلاکچین در تامین اعتماد و امنیت و کاهش هزینه‌ها، زمان و منابع مورد نیاز در زیرساخت مدیریت سنتی بهداشت و درمان به وجود آمده است.

در نتیجه، سیستم‌هایی نظیر تبادل اطلاعات سلامت (HIE)[1] و پایگاه داده غرامت تمام‌عاملی (APCD)[2] بی استفاده شده‌اند. برای مثال، مشارکت بین دولت استونی و شرکت امنیت سایبری با نام گاردتایم (guardtime.com) در سال ۲۰۰۷ باعث شد تا سیستم‌های مبتنی بر بلاکچین جایگزین HIE و سیستم‌های APCD شوند. برنامه این بود که از زیرساخت امضای بدون‌کلید بلاکچین (KSI)[3] به‌منظور احراز هویت و تایید اعتبار یکپارچگی داده‌های عمومی پزشکی استفاده کنند.

علاوه بر این، فناوری‌های سرمایه‌گذاری‌شده در پوشاک خاص، منابع داده‌ای غنی برای جمع‌آوری داده‌های مرتبط با سلامت بیمار فراهم آورده است (PGHD). با این حال، چون این داده‌ها از لحاظ امنیتی در دسترس نیست، هنوز از ظرفیت آن به‌طور کامل استفاده نشده است؛ بنابراین نوآوران عرصه سلامت دیجیتال نظیر هلث‌بنک (healthbank.coop) و نت‌سترا (netcetera.com) در سوئیس و نیز نوسر (noser.com) در آلمان طرح ابتکاری را برای اشتراک امن داده‌های شخصی پزشکی آغاز کرده‌اند. آنها در استفاده از فناوری بلاکچین سرمایه‌گذاری کردند. هدف از این سرمایه‌گذاری توانمندسازی اشخاص برای کنترل داده‌های خودشان است.

## بلاکچین به‌صورت ابزاری برای بهبود اعتماد در پژوهش‌های علمی

اعتماد در پژوهش علمی یکی از عوامل مهم برای سنجش اعتبار خروجی، به‌ویژه در حوزه‌های حیاتی نظیر علوم پزشکی است. با این حال، این عامل دچار مشکلات اعتماد است که ناشی از دستکاری داده‌های علمی نظیر سوئیچینگ خروجی،[4] پاک‌کردن داده و نشر نتایج گزینشی است.

بنابراین مطالعه کارلیسل در سال ۲۰۱۴ اثبات کرد که بلاکچین می‌تواند هزینه کمی در پی داشته باشد، روش اعتبارسنجی مستقلی برای ممیزی باشد و اطمینان‌پذیری نتایج مطالعات علمی را با استفاده از پروتکل بلاکچین تایم‌استمپ‌شده[5] تایید کند. مطالعه کارلیسل نشان

1. Health Information Exchange
2. All-Player Claim Database
3. Keyless Signature Infrastructure
4. outcome switching
5. blockchain-timestamped protocols

می‌دهد که بلاکچین چگونه پرونده‌ای تغییرناپذیر از ماهیت، یکپارچگی و مالکیت پروتکل خاص آزمایش پزشکی ارائه می‌کند.

## کاربرد در صنایع گوناگون

علاوه بر این، فناوری بلاکچین در صنایع مختلف کاربردهایی دارد. این کاربردها به شرح زیر است:

- **رمز ارز:** اصالتا برای انتقال و پرداخت ارزش استفاده می‌شود، این کاربرد بلاکچین از طریق ارائه مجوز به چندین گروه برای تراکنش با یکدیگر به‌شیوه‌ای قابل اعتماد بدون نیاز به واسطه عمل می‌کند. علاوه بر این، سازمان‌هایی که به استفاده از دفترکل عمومی توزیع‌شده علاقه دارند، تلاش می‌کنند تا از این فرایند برای فعالیت‌های پساتجارت استفاده کنند، نظیر وصول‌کردن، امانت/وثیقه‌دادن و مدیریت نقدینگی؛
- **اثبات خدمات:** توانایی بلاکچین در ذخیره ارزش با جزئیات بسیار (هویت، مالکیت، عضویت و غیره) باعث می‌شود که دولت‌ها بتوانند خدماتی برای شهروندان در ارتباط با گواهی تولد و فوت ارائه و مجوزهای کسب‌وکار و مالکیت اموال را صادر کنند. یکی از مثال‌های واقعی این پروژه، بیت‌نیشن (bitnation.co) است و هدف از آن آغاز دولت غیرمتمرکز در مقیاس جهانی نظیر کارت شناسایی شهروند جهانی[1] است.
- **قراردادهای هوشمند:** قراردادهای هوشمند می‌توانند بدون دخالت طرف سوم با استفاده از اطلاعات جداسازی‌شده نظیر مفاد و شرایط از پیش‌تعیین‌شده و قوانین، اجرای خودکار تراکنش‌ها را ممکن سازند. برخی از پروژه‌های مبتنی بر بلاکچین شرکت‌های نوپا، از کلیه قابلیت‌های قراردادهای هوشمند استفاده کرده‌اند (نظیر پروژه اتریوم). در فصل ۶، قراردادهای هوشمند به‌طور کامل تحلیل می‌شوند.
- **سیستم‌ها/سرویس‌های خودمختار غیرمتمرکز:** ممکن است این مورد برجسته‌ترین نقش بلاکچین باشد که به ایجاد مکانیسم‌های اعتماد بین انسان و رایانه مربوط می‌شود. به این حالت، سازمان‌های خودمختار غیرمتمرکز (DAO)[2] می‌گویند و می‌تواند به‌طور خودمختار عواملی روی اینترنت برای اجرای وظایف تخصصی اجرا کند. با این حال، قابل درک است

1. World Citizenship ID
2. Decentralized Autonomous Organizations

که ایجاد DAO خودمحور و خودسازمان‌ده ماموریت آسانی نیست، اما اگر به‌درستی انجام شود، می‌تواند اثری قابل توجه روی بخش‌های صنعتی گوناگون نظیر حمل‌ونقل، بهداشت و درمان و ذخیره‌سازی ابری داشته باشد.

جدول ۱-۲ گروه‌بندی کاربردهای کلیدی فناوری بلاکچین را برای کاربران فناوری نشان می‌دهد.

علاوه بر این، شـــکل ۴-۲ گروه‌بندی کاربردهای کلیدی بلاکچین را برای زیرداامنه‌های فناوری و نشانگرهای زمان تحویل نمایش می‌دهد.

## پذیرش بلاکچین

معرفی بلاکچین به دنیای کسب‌وکار تغییر گسترده‌ای برای زیرساخت فناوری اطلاعات سازمان‌ها و نیز شیوه تراکنش و اجرای کسب‌وکار آنها در پی داشت.

در این بخش، ظرفیت فناوری بلاکچین و نیز منافع و موانعی را که در راه پذیرش آن پیش رو دارد، بررسی می‌کنیم.

## ظرفیت بلاکچین به‌صورت جایگزینی برای سوئیفت

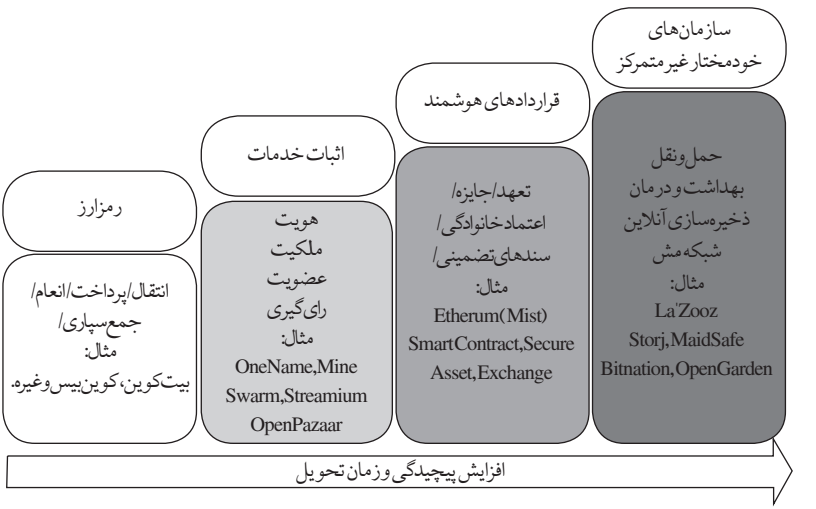
سوئیفت[1] مخفف جامعه ارتباطات مالی بین‌بانکی جهانی[2] است و مهم‌ترین جنبه صنعت بانکداری از دهه ۷۰ میلادی تاکنون محسوب می‌شود. سیستمی جهانی است که نهادهای مالی را قادر می‌ســـازد تا به‌طور امن اطلاعات مربوط به تراکنش مالی خـــود را تبادل کنند. سوئیفت در سطح جهان توســـط بیش از ۹۰۰۰ نهاد مالی در ۲۰۹ کشـــور برای تبادل پنج تریلیون در روز استفاده می‌شود.

به این دلایل، جایگزین‌کردن ســـوئیفت با بلاکچین برای بانک‌ها و دیگر ســـازمان‌های مالی دشوار است و در شـــرایطی که بانکداران و مدیران اجرایی فاقد درک کاملی از ماهیت بلاکچین، نحوه کارکرد یا ظرفیت‌های آن هستند، حتی رخداد این انتقال نیز دشوارتر می‌شود. توانمندی‌های بلاکچین شامل ثبت تبادل ارزش دیجیتال نظیر پرداخت یا ثبت ازدواج و ثبت تسویه اوراق بهادار است.

1. SWIFT
2. Society for Worldwide Interbank Financial Telecommunication

جدول۱-۲: دسته‌بندی کاربردهای کلیدی بلاکچین بر اساس کاربران این فناوری

| موسسات | قانون‌گذاران | عملیات‌ها | افراد |
|---|---|---|---|
| تسویه FX | گزارش‌دهی تطبیق | وارد کردن مشتری | جمع‌سپاری |
| تلفیق تجاری | ترسیم ریسک | تسویه بین‌شرکتی | هویت تصویری |
| پرداخت بین‌مرزی | تطبیق با قانون بازل۳ | نرمال‌کردن داده‌های مرجع | امتیازدهی به اعتبار |
| بازده اعتبار | شفافیت کلاهبرداری مشتری | تایم استمپینگ | حواله بین‌مرزی |
| تسویه وام | شناخت مشتری/ مبارزه با پولشویی | قابلیت جابه‌جایی حساب | خدمات سند تضمینی/ امانات بهادار/خزانه |
| وصول اوراق مشتقه OTC | گزارش تجاری | شناسایی کلاهبرداری کارگزار | هزینه واریز مشتری |
| مدیریت وثیقه‌ای | | توافق اوراق بهادار به‌عنوان قراردادهای هوشمند | وام‌دهی همتابه‌همتا |




شکل ۴-۲: گروه‌بندی کاربردهای کلیدی بلاکچین طبق فناوری زیرحوزه‌ها

## پذیرش بلاکچین توسط سازمان‌ها

بسیاری از سازمان‌ها مزایای بالقوه بلاکچین را درک کرده‌اند. برای مثال IBM در حال سرمایه‌گذاری در این فناوری است تا قواعدی را شکل دهد که در اداره عملیات‌هایش از آن استفاده کند و نیز محصولاتی را توسعه دهد که کسب‌وکارهای مرتبط بتوانند از آنها استفاده کنند.

علاوه بر این، IBM به مجمع تجارت دیجیتال[1] پیوسته که این مجمع خود توسط گروهی از شرکت‌های نوپای بلاکچین، بنگاه‌های نرم‌افزاری، نهادهای مالی و سرمایه‌گذاران علاقه‌مند در سال ۲۰۱۴ تاسیس شده است؛ اقدامی که با دولت آمریکا همکاری نزدیک دارد تا برای توسعه بلاکچین و استفاده از آن و نیز توسعه چارچوبی قانونی که بتواند پذیرش آن را هدایت کند، استانداردهایی وضع کند.

ایده شرکت IBM، در مشارکت با شرکت‌های دیجیتال اسست هلدینگز و لینوکس فاندیشن[2]، این بود که نرم‌افزارهای مبتنی بر بلاکچین منبع‌باز را توسعه دهد که بتواند به قاعده‌ای برای هر نوع اجرای بلاکچین از سوی سازمان‌های ذی‌نفع تبدیل شود. شرکت‌های اصلی نظیر جی‌پی مورگان چیس، ای‌ان‌زی بانک، سیسکو، اکسنچر، اینتل، لاندن استاک اکسچنج گروپ، میتسوبیشی یواف‌جی فاینانس گروپ، IC3 و وی‌ام‌ویر از مدت‌ها قبل سرمایه‌گذاری در این بخش را آغاز کرده‌اند. علاوه بر این، دیلویت، مثال دیگری از سازمان‌های بزرگ است که ظرفیت بلاکچین را درک کرد، زیرا با پنج شرکت تخصصی بلاکچین مشارکت کرد تا از فناوری نوظهور به‌طور موثر در امر کسب‌وکار مشاوره‌ای استفاده کند. دیلویت از طریق توسعه نرم‌افزارهای کاربردی مبتنی بر بلاکچین نظیر هویت دیجیتال، بانکداری دیجیتال، پرداخت بین‌مرزی و نیز وفاداری و جایزه قصد دارد تا به اهداف خود برسد.

علاوه بر این، بازارهای سرمایه بخش مهمی از سیستم مالی هستند که از سهم، اوراق قرضه و دیگر سرمایه‌گذاری‌های بلندمدت برای تولید و افزایش سرمایه شرکت‌ها استفاده می‌کنند. شکل ۵-۲ مزایای پذیرش بلاکچین را در مراحل مختلف تجارت در بازارهای مالی نشان می‌دهد. این مراحل شامل: پیش‌تجارت، تجارت، پساتجارت و در نهایت امانت/وثیقه و اعطای خدمات اوراق بهادار است.

---

1. Chamber of Digital Commerce,
2. Digital Asset Holdings - the Linux Foundation


شکل ۵-۲: مزایای پذیرش بلاکچین در بازارهای سرمایه

البته، با در نظر گرفتن اثر پذیرش بلاکچین در بازارهای سرمایه، در نظر گرفتن موانعی که ممکن است بر موفقیت بلاکچین تاثیر بگذارند، ضرورت می‌یابد؛ بنابراین فناوری بلاکچین نیازمند سرمایه‌گذاری بیشتر به‌منظور داشتن توافق روی استانداردهای مشترک و داشتن فناوری مقیاس‌پذیر کافی است. در بخش زیر، ترتیب زمانی اجرایی مناسب را بررسی می‌کنیم که باید پیش از امکان‌پذیری اتخاذ گسترده بررسی شود.

## ترتیب زمانی پیاده‌سازی بلاکچین

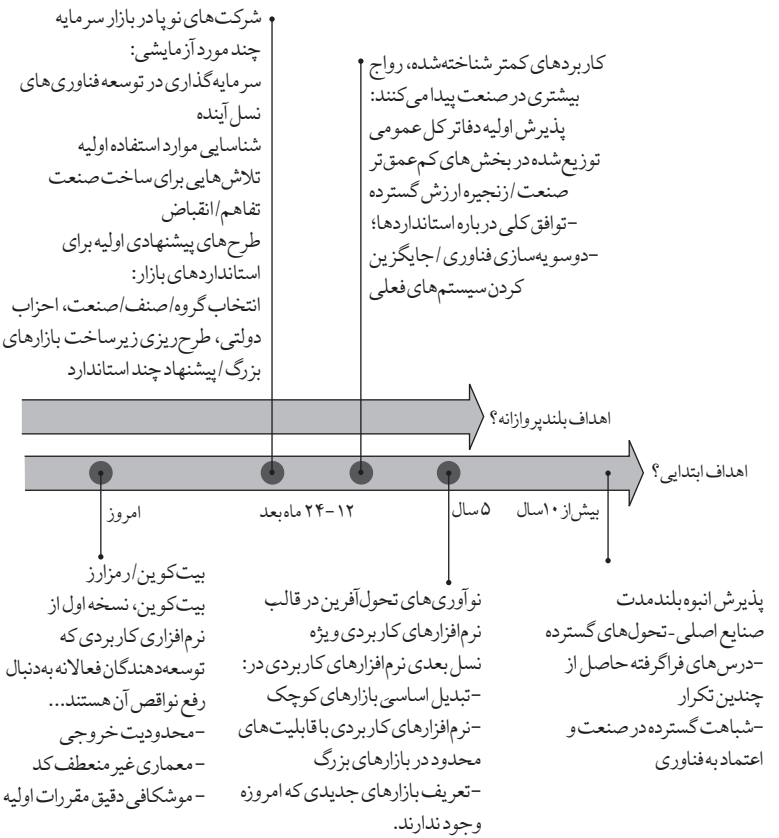
از نظر توسعه‌دهندگان فناوری‌های جدید نظیر بلاکچین مهم است که نرم‌افزارهای کاربردی عملی و راهکارهایی تولید کنند تا سرمایه‌گذاری جاری را تضمین کند و بتوانند فناوری را در محیط‌های واقعی عملیاتی کنند. شکل ۶-۲ خط زمانی برای استفاده و توسعه از نرم‌افزارهای مبتنی بر بلاکچین نشان می‌دهد.

با توجه به ترتیب زمانی برای انجام کارها (خط زمانی)[1]، درک اهمیت به‌روز ماندن با فناوری‌های نوظهور برای سازمان‌ها حیاتی است، زیرا عقب‌افتادن در این مسیر ممکن است به از دست رفتن سهم مهم در بازار یا حتی ترک بازار منجر شود؛ بنابراین در نکات زیر به چند پرسش متداول درباره استفاده از بلاکچین برای اجرای موفقیت‌آمیز پروژه‌ها اشاره می‌کنیم:

1. Timeline

**اثبات مفهوم باید قابل اعتماد و متقاعدکننده باشد:** توسعه‌دهندگان فناوری و نوآوران باید از طریق تشریح چگونگی تاثیرگذاری دفاتر کل عمومی توزیع‌شده بر صنعت و مشتریان، موارد استفاده مناسبی را تعریف کنند.

**درک جایگاه کنونی و تاثیر در آینده:** توسعه‌دهندگان یا استفاده‌کنندگان علاقه‌مند به بلاکچین باید وضعیت کنونی و راهکارهای فناورانه فعلی را درک کنند و چالش‌ها، هزینه‌ها و منافع حاصل از پذیرش بلاکچین در سازمان را تجزیه‌وتحلیل کنند.




شکل ۶-۲: پذیرش بلاکچین و ترتیب زمانی پیاده‌سازی آن

فناوری‌های جدید برای موفقیت به زمان بیشتری نیاز دارند: نوآوری‌ها در حوزه فناوری از اولین نسخه‌های خود به موفقیت نمی‌رسند، در نظر داشتن نسخه‌های ابتدایی (مثلا نمونه‌های آزمایشی) برای کشف حیطه‌هایی که نیاز به بهبود دارند حائز اهمیت است.

- **اهمیت پر کردن خلاء بین فناوری و صنعت:** درک کامل دامنه دانشی که برای توسعه فناوری جدید از آن استفاده خواهد شد و نیز عدم جداسازی فرایند توسعه از تخصص کسب‌وکار بسیار مهم است.
- **اهمیت نقش قانون‌گذاران:** توسعه فناوری باید با استانداردها و نقش نهادهای ذی‌صلاح در تطابق باشد. اطلاع‌رسانی به ذی‌نفعان ذی‌صلاح درباره فرایند توسعه به‌منظور رفع نگرانی ایشان در خصوص امنیت، حریم خصوصی و اقدامات قانونی حائز اهمیت است.
- **مقیاس‌پذیری فناوری:** بسیار مهم است که در فناوری‌های جدید نظیر بلاکچین بتوانیم پایگاه‌های داده بازارهای مالی بزرگ را مدیریت کنیم و در عین حال به حل‌وفصل مشکلات مرتبط با امنیت، انسجام و عملکرد بپردازیم. این مساله به‌ویژه به‌منظور مدیریت ریسک‌های عملیاتی در مرحله انتقال به فناوری جدید مهم می‌شود.
- **توافق بر سر استانداردهای مشترک:** صنایع باید درباره مشکلات طراحی بلاکچین با یکدیگر توافق داشته باشند (مثلا دسترسی آزاد به سیستم‌ها یا دسترسی با مجوز؟). علاوه بر این، باید عقاید مشترکی درباره چگونگی عملیاتی کردن و مدیریت زیرساخت بلاکچین داشته باشند که شامل اداره آن، به‌روزرسانی آن و مسئولیت‌پذیری می‌شود.

## موردپژوهی

در این بخش، دو موردپژوهی خواهیم داشت که اجرای بلاکچین در محیط کاری را نشان می‌دهد. همچنین نقش بلاکچین برای موفقیت کسب‌وکار را توضیح می‌دهیم. با این حال، از آنجا که دنیای کسب‌وکار همچنان به‌دنبال کشف ظرفیت‌های فناوری‌های نوپا (مثل بلاکچین) است، موارد استفاده زیر در حال توسعه هستند.

اولین موردپژوهی درباره برنامه آینده‌گرا یا چشم‌اندازی به نام «اتحادیه انرژی»[1] است که در سند استراتژی اتحادیه انرژی کمیسیون اروپا[2] در سال ۲۰۱۴ تعریف شد. هدف از این طرح،

1. Energy union
2. European Commission Energy Union Framework Strategy

ارائه اختیار به شهروندان اتحادیه اروپا برای اســتفاده از اشکال دیگر انرژی به‌منظور کاهش هزینه‌ها، داشتن گزینه‌های بیشتر، مشارکت فعال در بازار انرژی و مهم‌تر از همه، حفاظت از مصرف‌کننده است. با این حال، چنین چشم‌اندازی نیازمند مواجهه با مسائلی بحرانی است که به برخی از آنها اشاره می‌کنیم:

- **ارائه اطلاعات دقیق:** با توجه به هزینه‌های صرف‌شده و مصرف انرژی و برای آنکه مشترکان فرصت‌های ممکن را در بازار انرژی کاملا یکپارچه قاره اروپا درک کنند.
- **شیوه‌های مقتضی برای پاداش‌دهی به شرکت‌کنندگان فعال:** مثلا استفاده از قراردادهای تشویقی و مدیریت تقاضا و پاسخگویی طبق قیمت‌های کنونی؛
- **تضمین عملیات‌پذیری بین حوزه‌ای در بازار:** تضمین عملیات‌پذیری بین حوزه‌ای در بازار و در عین حال، در نظر داشتن جنبه‌های مختلف نظیر تامین‌کنندگان سرویس‌های انرژی به منازل مسکونی و گزینه‌های موجود برای مصرف‌کنندگان و نیز دستیابی به منافع ممکن با تولید انرژی در مقیاس خرد و خودکفایی در تولید انرژی.

این عوامل باعث شد که کمیسیون اروپا در فناوری‌های جدیدی سرمایه‌گذاری کند که انتظارات آنها را برطرف می‌کند. از ایــن رو، توجه به بلاکچین و دفترکل عمومی توزیع‌شــده آن به‌صورت فناوری‌ای که بتواند سطح یکپارچه‌سازی و توسعه بازار خرده‌فروشی انرژی را بهبود بخشد، مهم است؛ بنابراین یکی از کمیسیون‌های اتحادیه اروپا با نام مرکز تحقیقات مشترک (JRC)[1] در بخش سرویس‌های پژوهش که به سیاســت‌گذاران اتحادیه اروپا مشاوره علمی می‌دهد، عملا در حال بررسی کاربردهای بلاکچین نظیر بازار خرده‌فروشــی انرژی و دفترکل قراردادهای انرژی[2] است. مورد اول درباره مصرف‌کنندگانی است که می‌توانند به‌طور محلی انرژی تولید کرده و آن را با بازار محلی تبادل کنند. دفاتر کل توزیع‌شده و سنجش‌های هوشمند می‌توانند تولیدکنندگان محلی را قادر سازند تا به بازارهای انرژی وارد شوند. تاکنون، این مورد فقط جزء اختیارات تامین‌کنندگان اصلی انرژی بوده است. مورد دوم، دفترکل قراردادهای انرژی، کاربرد دیگری است که دفترکل توزیع‌شده در آن می‌تواند پیچیدگی‌های مرتبط با تغییر تامین‌کننده انرژی را بهتر مدیریت کند؛ مثلا، فســخ قراردادهای کنونی، انعقاد قراردادهای جدید با تامین‌کننده بعدی و بحث درباره مفاد جدید. دفاترکل

1. Joint Research Centre
2. energy contract ledger

توزیع‌شده می‌توانند از طریق ارائه اختیار به مصرف‌کنندگان برای نهایی‌ساختن آسان انتقال روی اینترنت، این فرایند را بهبود دهند. علاوه بر این، تامین‌کنندگان انرژی می‌توانند در هزینه‌های مربوط به عملیات‌های مدیریتی صرفه‌جویی کنند.

**نکته:** این مطالعه موردی نشان می‌دهد که چگونه می‌توان از دفاتر کل عمومی توزیع‌شده برای توسعه بازارهای رقابتی‌تر خرده‌فروشـــی انرژی از طریق ارائه اطلاعات بیشتر به مصرف‌کنندگان بهره‌برداری کرد. اطلاعات بیشتر به مصرف‌کنندگان می‌تواند آنها را قادر سازد تا آزادی عمل بیشتری داشته باشند. منافع چنین چشم‌اندازی نویدبخش است، از این رو، به بررسی‌های بیشتری نیاز داریم. با این حال، همچنان پرسش‌هایی درباره مقیاس‌پذیری، امنیت و پایداری چنین کاربردهایی مطرح است که باید به آنها پاسخ داد.

در دومین موردپژوهی، درباره استفاده از فناوری دفاتر کل توزیع‌شده در حالتی بحث می‌کنیم که با هدف اصلی آن، بیت‌کوین، فرق دارد؛ چون این مفاهیم و ساختارها که برای دفاتر کل توزیع‌شده توسعه یافته‌اند، به‌شدت قابل تعمیم به دیگر حوزه‌های اقتصاد و تعاملات اجتماعی‌اند. موضوع این موردپژوهی درباره توانایی دولت‌ها در استفاده از دفاتر کل عمومی برای اشتراک‌گذاری اطلاعات بین واحدهای اقتصادی است که به کاهش اصطکاک بازار کمک می‌کند و شکل‌های جدید ادغام نوآوری را ممکن می‌سازد. در نتیجه، کسب‌وکارهای کوچک و متوسط[1] (SME) می‌توانند از کاهش در هزینه‌های تراکنش بهره ببرند تا در بـــازار آزادانه‌تر حرکت کنند و به کاهش کل مخارج عملیاتی کمک کنند. علاوه بر این، با اســـتفاده از DLT (دفتر کل توزیع شـــده) برای ثبت پتنت شرکت‌ها و مالکیت فکری (IP)[2]، امکان کاهش تعداد قراردادهای فسخ‌شـــده ممکن می‌شود. حدود ۵۷ درصد از دادخواهی‌ها در مراجع قضایی بریتانیا به فسخ قراردادها مربوط می‌شود که بیشتر از دیگر دعوی‌های قانونی است.

**نکته:** این موردپژوهی نشان می‌دهد که چگونه دفاتر کل توزیع‌شده می‌توانند به کاهش هزینه‌های تراکنش در SMEها و افزایش بازده هزینه صرف‌شده عملیات‌ها به دولت‌های محلی و ملی کمک کنند. به‌علاوه اینکه، با اختیار داشتن اثبات درستکاری مالک دارایی‌های دیجیتال نظیر IP، از احتمال دادخواهی کاسته می‌شود و منافع اجتماعی بسیاری برای جامعه بریتانیا در پی خواهد داشت.

---

1. Small to medium-sized enterprise
2. Intellectual Property

می‌توان از DLT برای ثبت قراردادها و دارایی‌ها اســتفاده کرد که روشی منسجم و درست برای اثبات مالکیت تجاری دارایی است، (به‌عنوان مثال مالکیت فکری و ثبت اختراعات) علاوه بر این، دفتر کل توزیع شــده می‌تواند ریز پرداخت‌ها، تبادل و انتقال ارزش غیر متمرکز، دستیابی و خرج توکن‌ها را مدیریت کنند؛ بنابراین DLT به دولت‌ها کمک می‌کند تا راه کسب‌وکار را به شیوه‌های گوناگون بهبود دهند. این راه‌ها شامل موارد زیر است:

- اعطای مجوز کسب‌وکار؛
- ثبت (مثلا اموال، وصیت‌نامه، مالکیت فکری، خدمات دفاتر اسناد رسمی، داده‌های پزشکی و غیره)؛
- تراکنش‌های بیمه‌ای؛
- مدیریت مالیات در سطح شهری و مقرراتی؛
- داده‌های مرتبط با حقوق بازنشستگی.

دفاتر کل توزیع‌شده فرصتی برای دولت‌ها فراهم می‌کنند تا هزینه‌های کاری را کاهش دهند، از احتمال کلاهبرداری و خطا بکاهند و هزینه‌های ارائه سرویس را برای کاربران محروم کم کنند. از طریق کاهش هزینه‌های تراکنش، SMEها می‌توانند از این لحاظ به سود برسند.

## خلاصه

بلاکچین فناوری‌ای است که به احتمال بسیار زیاد شیوه کسب‌وکار را در آینده‌ای نزدیک تغییر خواهد داد، درست مانند کاری که اینترنت در دهه ۹۰ انجام داد. همچنین یك فناوری نوظهور است و درک ظرفیت‌های آن برای غلبه بر معضلات موجود در شیوه تراکنش کسب‌وکارها با یکدیگر و نیز بهبود رویه‌های کنونی کسب‌وکار باعث شده که سازمان‌های بزرگی چون IBM و بانک‌های بزرگ به‌دنبال سرمایه‌گذاری عظیم در این فناوری باشند. با این حال، کاربران بلاکچین باید با چالش‌های متعددی نظیر مقررات دولتی، مشکلات امنیت و حریم خصوصی، مسائل یکپارچه‌سازی و پذیرش فرهنگی مواجه شــوند. اگر این دغدغه‌ها به‌طور مناسب پاسخ داده شــوند، آنگاه از ظرفیت‌های بلاکچین، به‌عنوان سیستم ارزشی، اســتفاده فراوانی خواهد شد و مزایای ممکن رجوع به فناوری بلاکچین برای سازمان‌های مصرف‌کننده نویدبخش خواهد بود.

در این فصل، توصیف جامعی از بلاکچین و ویژگی‌های آن ارائه شد. علاوه بر این، درباره

# نوآوری کسب‌وکار از طریق بلاکچین

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 پایگاه داده 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، اجماع غیرمتمرکز، بلاکچین، رایانش اعتمادی و اثبات کار / اثبات سهام. علت اهمیت حیاتی این پارادایم رایانش جذاب آن است که در آینده به ابزاری برای ساخت نرم‌افزارهای کاربردی غیرمتمرکز تبدیل خواهد شد.

ISBN 978-964-6599-4-06
۴۹۵۰۰ تومان
راه‌پرداخت