



Volume 5, Issue 1, 2024

## Approaches to Employing Smart Contracts in the Digital Currency Market

Fatemeh Kamalinezhad<sup>1\*</sup> Ali Kalantari<sup>2</sup> Yegane Kharat<sup>3</sup> Mehran Bahram arjavand<sup>4</sup>

1. Undergraduate Student of Business Management, Sari Branch, Islamic Azad University, Sari, Iran.

(Corresponding Author) Email: [kamalinezhad80@gmail.com](mailto:kamalinezhad80@gmail.com)

2. Undergraduate Student of Financial Management, Sari Branch, Islamic Azad University, Sari, Iran.

3. Undergraduate Student of Business Management, Sari Branch, Islamic Azad University, Sari, Iran.

4. Undergraduate Student of Financial Management, Sari Branch, Islamic Azad University, Sari, Iran.

### ARTICLE INFORMATION

**Type of Article:**

**Original Research**

**Pages: 84-96**

**Corresponding Author's Info**

**Email:**

[kamalinezhad80@gmail.com](mailto:kamalinezhad80@gmail.com)

**Keywords:**

Smart Contract, Blockchain,  
Cryptocurrency, Security  
Challenges, Internet of Things.

### ABSTRACT

With the rapid and continuous development of cryptocurrencies and advanced blockchain technologies, leading platforms such as Ethereum and Hyperledger have provided the necessary and robust infrastructure to support and execute various smart contracts. This technology, as an automated and enforceable agreement, is rapidly expanding and has successfully found diverse real-world applications, including crowdfunding, financial services, prediction markets, and the Internet of Things. Despite this remarkable growth, numerous critical challenges such as security vulnerabilities, privacy issues, and developmental limitations remain fundamental and significant barriers to widespread adoption. The main objective of this research is to provide a comprehensive and systematic review of blockchain-based smart contracts and to clearly clarify their exact core concept. In this regard, while examining the theoretical foundations, operational mechanisms, and various host platforms, we deeply explore applied scenarios and the challenges faced by developers. The findings of this exploratory study indicate that although smart contracts have high potential in eliminating intermediaries, reducing transaction costs, and automating complex financial and social processes, the lack of powerful debugging tools, programming language limitations, and vulnerabilities such as reentrancy and transaction-ordering dependence require special and urgent attention from researchers. Finally, by outlining future trends, this comprehensive article proposes novel and innovative pathways to enhance security, scalability, and privacy preservation within cyber-physical-social systems.



This is an open access article under the CC BY license.

© 2024 The Authors.

**How to Cite This Article:** Kamalinezhad, F.; Kalantari, A.; Kharat, Y. and Bahram arjavand, M. (2024). Approaches to Employing Smart Contracts in the Digital Currency Market. *Journal of Management, Economics and Entrepreneurship Studies*, 5(1): 84-96. doi: 10.22034/jmek.2024.154707



فصلنامه مطالعات مدیریت، اقتصاد و کارآفرینی

## فصلنامه مطالعات مدیریت، اقتصاد و کارآفرینی

www.JMEK.ir

دوره ۵، شماره ۱، بهار ۱۴۰۳

### روش‌های استفاده از قراردادهای هوشمند در بازار ارزهای دیجیتال

فاطمه کمالی نژاد<sup>۱\*</sup> یگانه خراط<sup>۲</sup> علی کلانتری<sup>۳</sup> مهران بهرام ارجاوند<sup>۴</sup>

۱. دانشجوی کارشناسی مدیریت بازرگانی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

۲. دانشجوی کارشناسی مدیریت مالی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

۳. دانشجوی کارشناسی مدیریت بازرگانی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

۴. دانشجوی کارشناسی مدیریت مالی، واحد ساری، دانشگاه آزاد اسلامی، ساری، ایران.

#### چکیده

با توسعه شتابان ارزهای دیجیتال و فناوری‌های نوین بلاک چین، پلتفرم‌های پیشروی همچون اتریوم و هایپرلجر، بستر لازم را برای پشتیبانی و اجرای انواع قراردادهای هوشمند فراهم آورده‌اند. این فناوری به عنوان یک توافق خودکار و قابل اجرا، به سرعت در حال گسترش است و کاربردهای متنوعی را در دنیای واقعی، از جمله تامین مالی جمعی، خدمات مالی، بازارهای پیش‌بینی و اینترنت اشیا به خود اختصاص داده است. با وجود این رشد چشمگیر، چالش‌های متعددی از جمله آسیب‌پذیری‌های امنیتی، مسائل حریم خصوصی و محدودیت‌های توسعه‌ای همچنان به عنوان موانعی اساسی در مسیر پذیرش گسترده این فناوری باقی مانده‌اند. هدف اصلی این پژوهش، ارائه مروری جامع و نظام‌مند بر قراردادهای هوشمند مبتنی بر بلاک چین و تبیین دقیق مفهوم آن‌هاست. در این راستا، ضمن بررسی مبانی نظری، مکانیزم‌های عملیاتی و پلتفرم‌های مختلف میزبان، به واکاوی سناریوهای کاربردی و چالش‌های پیش‌روی توسعه‌دهندگان پرداخته شده است. یافته‌های این مطالعه اکتشافی نشان می‌دهد که اگرچه قراردادهای هوشمند پتانسیل بالایی در حذف واسطه‌ها، کاهش هزینه‌های مبادله و اتوماسیون فرآیندهای پیچیده مالی و اجتماعی دارند، اما فقدان ابزارهای قدرتمند اشکال‌زدایی، محدودیت‌های زبان‌های برنامه‌نویسی و آسیب‌پذیری‌هایی نظیر ورود مجدد و وابستگی به ترتیب تراکنش‌ها، نیازمند توجه ویژه پژوهشگران است. در نهایت، این مقاله با ترسیم روندهای آتی، مسیرهای نوینی را برای ارتقای امنیت، مقیاس‌پذیری و حفظ حریم خصوصی در بستر سیستم‌های سایبری-فیزیکی-اجتماعی پیشنهاد می‌دهد.

#### اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۸۶-۸۴

اطلاعات نویسنده مسئول

ایمیل:

[kamalinezhad80@gmail.com](mailto:kamalinezhad80@gmail.com)

#### سابقه مقاله:

تاریخ دریافت: ۱۴۰۲/۰۷/۲۶

تاریخ ویرایش: ۱۴۰۲/۱۰/۱۲

تاریخ پذیرش: ۱۴۰۲/۱۲/۲۰

تاریخ انتشار: ۱۴۰۳/۰۱/۰۱

#### واژگان کلیدی:

قرارداد هوشمند، بلاک چین، ارزهای دیجیتال، چالش‌های امنیتی، اینترنت اشیا.



## ۱- مقدمه

در سال‌های اخیر، توسعه شتابان فناوری بلاک چین و ظهور منطق برنامه‌نویسی قابل تنظیم، این امکان را فراهم آورده است که داده‌ها و توافق‌نامه‌های دیجیتال به روشی کاملاً غیرمتمرکز ذخیره و اجرا شوند. این تحول فناورانه، مفهوم «قرارداد هوشمند» را که نخستین بار در سال ۱۹۹۴ توسط نیک سابو مطرح شد، احیا و تسهیل کرده است. قراردادهای هوشمند در واقع توافق‌نامه‌های خوداجرایی هستند که شرایط آن‌ها میان طرف‌های ذی‌نفع تعیین شده و در قالب کدهای برنامه‌نویسی در سراسر یک شبکه بلاک چین غیرمتمرکز توزیع می‌شوند. این فناوری، امکان انجام تراکنش‌های مالی و معاملاتی را میان طرف‌های ناشناس یا غیرقابل اعتماد، بدون نیاز به یک مرجع مرکزی یا واسطه شخص ثالث، فراهم می‌آورد.

کاربردهای قراردادهای هوشمند طیف گسترده‌ای از حوزه‌ها را در بر می‌گیرد؛ از جمله می‌توان به مدیریت دارایی‌های هوشمند (نظیر پلتفرم اسلاک، ایت برای اجاره و فروش بدون واسطه)، سیستم‌های خودمختار، تامین مالی جمعی، بازارهای پیش‌بینی و اینترنت اشیا اشاره کرد. با این حال، محدودیت‌های ذاتی شبکه‌های اولیه مانند بیت‌کوین که تنها از زبان برنامه‌نویسی محدودی پشتیبانی می‌کردند، مانع از پیاده‌سازی قراردادهایی با منطق پیچیده می‌شد. ظهور پلتفرم‌های نوظهوری نظیر اتریوم، با بهره‌گیری از زبان‌های برنامه‌نویسی کامل تورینگ، این محدودیت را برطرف ساخت و مسیر را برای سفارشی‌سازی و توسعه قراردادهای هوشمند پیشرفته هموار کرد. از زمان انتشار بیت‌کوین در سال ۲۰۰۹، ارزهای دیجیتال غیرمتمرکز توانستند با تکیه بر پروتکل‌های اجماع همتابه‌همتا و بدون دخالت مقامات مرکزی، توجه جهانی را به خود جلب کنند و پتانسیل بلاک چین را فراتر از ارزهای رمزنگاری‌شده، به سمت کاربردهایی چون قراردادهای هوشمند گسترش دهند.

در تعریف دقیق‌تر، قرارداد هوشمند به عنوان یک توافق خودکار و قابل اجرا شناخته می‌شود که یا از طریق اجرای حقوقی تعهدات و یا از طریق اجرای بی‌دستکاری کدهای رایانه‌ای بر روی چندین گره از یک دفتر کل توزیع‌شده عملیاتی می‌گردد. ماهیت خوداجرایی این قراردادهای، فرصت بی‌نظیری را برای اتوماسیون فرآیندهای متکی بر داده در حوزه‌های مختلف ایجاد کرده است؛ به طوری که در اوایل سال ۲۰۱۸، بیش از ۱۰ درصد از مشاغل تبلیغ‌شده در پلتفرم‌های فریلنسری بزرگ، مرتبط با توسعه قراردادهای هوشمند و بلاک چین بود.

با وجود افزایش چشمگیر محبوبیت و پذیرش قراردادهای هوشمند، چالش‌های بالقوه‌ای که توسعه‌دهندگان در فرآیند ساخت و استقرار آن‌ها با آن مواجه هستند، همچنان به عنوان یک شکاف تحقیقاتی مهم باقی مانده است. توسعه‌دهندگان ضمن اهمیت فراوانی که برای امنیت کد قائل هستند، اغلب با فقدان راه‌های مؤثر برای اثبات درستی، قابلیت اطمینان و امنیت کدهای خود دست‌وپنج نرم می‌کنند. از سوی دیگر، همان‌طور که توسط بسیاری از توسعه‌دهندگان گزارش شده است، زبان‌های برنامه‌نویسی فعلی و ماشین‌های مجازی که به طور خاص برای قراردادهای هوشمند طراحی شده‌اند، همچنان دارای محدودیت‌های متعددی هستند. به عنوان مثال، فقدان کتابخانه‌های عمومی جامع و پشتیبانی محدود برای اشکال‌زدایی، اغلب بر تجربه توسعه پروژه‌های پیچیده تأثیر منفی می‌گذارد. همچنین، فقدان اسناد پیشرفته و به‌روز و تأخیر در دریافت پاسخ‌های مناسب از سوی جوامع آنلاین توسعه‌دهندگان، از دیگر عواملی هستند که روند توسعه قراردادهای هوشمند را کند کرده‌اند.

لذا با توجه به اهمیت روزافزون این فناوری در بازار ارزهای دیجیتال، بازار سرمایه و سیستم‌های مالی نوین، و همچنین وجود چالش‌های امنیتی، حریم خصوصی و توسعه‌ای حل‌نشده، این پژوهش با هدف ارائه مروری جامع و نظام‌مند بر قراردادهای هوشمند مبتنی بر بلاک چین انجام شده است. در

پیشنهاد شده‌اند که محاسبات پیچیده و اطلاعات خصوصی را خارج از بلاک چین اجرا کرده و تنها نتایج نهایی را جهت حفظ مزایای بلاک چین، در زنجیره ثبت می‌کنند.

پلتفرم‌های میزبان نیز ویژگی‌های متفاوتی ارائه می‌دهند. اتریوم به عنوان محبوب‌ترین پلتفرم عمومی، از یک ماشین مجازی کامل تورینگ برای اجرای بایت‌کدها استفاده می‌کند. در مقابل، هایپرلجر یک چارچوب ماژولار برای راه‌حل‌های سازمانی با تأکید بر محرمانگی و مقیاس‌پذیری ارائه می‌دهد و از کانترینرها برای میزبانی قراردادهای هوشمند (چین‌کد) بهره می‌برد. پلتفرم کوردا نیز به طور خاص برای صنعت خدمات مالی طراحی شده و با ترسیم هویت گره‌ها به هویت‌های قانونی دنیای واقعی، امکان ادغام کد با پروسه‌های حقوقی سنتی را فراهم می‌آورد. از منظر ویژگی‌های ذاتی، قراردادهای هوشمند دارای سه صفت استقلال، خودکفایی و عدم تمرکز هستند. خودمختاری به این معناست که پس از راه‌اندازی، نیاز به تماس بیشتری نیست؛ خودکفایی یعنی توانایی مدیریت منابع (مانند جمع‌آوری سرمایه و پرداخت هزینه پردازش)؛ و عدم تمرکز نیز به دلیل توزیع بر روی گره‌های شبکه است. این ویژگی‌ها، قراردادهای هوشمند را به فعال‌کننده‌های اصلی بلاک چین ۲/۰ و ۳/۰ و پایه‌گذار سیستم‌های مالی و اجتماعی قابل برنامه‌ریزی، از جمله سازمان‌های خودمختار غیرمتمرکز (DAO) تبدیل کرده است.

**۲-۴- پیشینه تحقیق** مرور پیشینه تحقیق نشان می‌دهد که مطالعات متعددی بر کاربردها، چالش‌ها و راهکارهای ارتقای قراردادهای هوشمند متمرکز بوده‌اند. وانگ و همکاران (۲۰۱۸) در پژوهش خود نشان دادند که قراردادهای هوشمند می‌توانند بستر امن و غیرمتمرکزی را برای تراکنش‌های شهری، نظیر تعاملات میان مالک و مستأجر، فراهم آورند. در همین راستا، کلاک و همکاران (۲۰۱۶) مزایای به‌کارگیری این فناوری را در حوزه املاک و مستغلات بررسی کردند و به نتایجی همچون حذف واسطه‌های سنتی، افزایش اعتماد میان

این راستا، ضمن تعریف دقیق مفهوم و واکاوی چارچوب‌های نظری، به بررسی مکانیزم‌های عملیاتی، پلتفرم‌های میزبان (نظیر اتریوم، هایپرلجر و کوردا) و سناریوهای کاربردی متنوع پرداخته شده است. در ادامه، به تحلیل دقیق چالش‌های پیش‌روی توسعه‌دهندگان و آسیب‌پذیری‌های امنیتی رایج پرداخته و در نهایت، روندهای نوین و مسیرهای آتی برای ارتقای امنیت، مقیاس‌پذیری و حفظ حریم خصوصی در این بسترهای غیرمتمرکز تبیین خواهد شد.

## ۲. چارچوب نظری و پیشینه تحقیق

مبانی نظری قراردادهای هوشمند بر پایه فناوری بلاک چین و مفهوم اتوماسیون توافقات حقوقی استوار است. نیک سابو در سال ۱۹۹۴ این مفهوم را با هدف تبدیل بندهای قرارداد به کدهای برنامه‌نویسی جهت کاهش هزینه‌های مبادله و جلوگیری از اقدامات مخرب مطرح کرد. در چارچوب نظری حاضر، قرارداد هوشمند به عنوان یک توافق خودکار و قابل اجرا تعریف می‌شود که یا از طریق اجرای حقوقی تعهدات و یا از طریق اجرای بی‌دستکاری کدهای رایانه‌ای بر روی چندین گره از یک دفتر کل توزیع‌شده عملیاتی می‌گردد. بلاک چین به عنوان زیرساخت اصلی، زنجیره‌ای از رکوردها (بلوک‌ها) است که با استفاده از رمزنگاری به هم متصل شده و در شبکه‌ای از گره‌ها ذخیره می‌شوند. این ماهیت غیرمتمرکز و تغییرناپذیر، امکان انجام تراکنش‌ها را میان طرف‌های غیرقابل اعتماد بدون نیاز به واسطه فراهم می‌آورد.

از منظر مکانیزم‌های عملیاتی، قراردادهای هوشمند مجموعه‌ای از قوانین و منطق رویه‌ای سناریو-پاسخ هستند. طرفین قرارداد پس از توافق بر جزئیات و شرایط نقض، آن را بر روی بلاک چین مستقر می‌کنند. با این حال، به دلیل ماهیت بلاک چین، قراردادهای درون زنجیره‌ای نیازمند اعتبارسنجی توسط تمام گره‌ها هستند که این امر حریم خصوصی را کاهش و هزینه‌های محاسباتی را افزایش می‌دهد. در مقابل، قراردادهای خارج از زنجیره‌ای به عنوان یک راه‌حل جایگزین

اساسی برای تحقق جوامع موازی عمل کرده و با ارائه ساختارهای داده غیرمتمرکز، امکان تبدیل «سیستم‌های مرتون» (دارای عدم قطعیت و پیچیدگی بالا) به «سیستم‌های نیوتن» (قابل پیش‌بینی و کنترل‌پذیر) را از طریق اتوماسیون رفتارهای پیچیده در قالب کدهای قراردادی فراهم می‌آورند.

### ۳. روش تحقیق

پژوهش حاضر از نظر هدف، در زمره تحقیقات بنیادی- کاربردی و از نظر ماهیت و روش، در دسته پژوهش‌های توصیفی-تحلیلی و مروری قرار می‌گیرد. با توجه به ماهیت نوپا، میان‌رشته‌ای و به سرعت در حال تحول حوزه قراردادهای هوشمند و فناوری بلاک چین، طراحی یک چارچوب روش‌شناختی دقیق برای استخراج، طبقه‌بندی و تحلیل دانش موجود از اهمیت بالایی برخوردار است. از این رو، در این پژوهش از ترکیب دو رویکرد «مرور جامع ادبیات» و «مطالعه اکتشافی» استفاده شده است تا ضمن ترسیم دقیق مبانی نظری، شکاف‌های موجود در توسعه و امنیت این فناوری نیز به طور نظام‌مند واکاوی شوند.

در بخش گردآوری داده‌ها، از روش جستجوی نظام‌مند در پایگاه‌های استنادی معتبر علمی نظیر IEEE Xplore، Elsevier، Springer، ACM Digital Library و همچنین مخازن پیش‌چاپ مانند arXiv استفاده شده است. کلیدواژه‌های اصلی مورد جستجو شامل «قرارداد هوشمند»، «بلاک چین»، «تریوم»، «هایپرلجر»، «کودا»، «آسیب‌پذیری‌های امنیتی»، «اینترنت اشیا» و معادل‌های انگلیسی آن‌ها بوده است. بازه زمانی بررسی منابع، از ریشه‌های تاریخی مفهوم قرارداد هوشمند توسط نیک سابو در دهه ۱۹۹۰ و ظهور بیت‌کوین در سال ۲۰۰۹ آغاز شده و تا جدیدترین مقالات و کنفرانس‌های معتبر سال‌های اخیر را در بر می‌گیرد. معیارهای ورود به مطالعه شامل مقالات ژورنالی، مقالات کنفرانسی معتبر و کتب مرجع در حوزه‌های مهندسی نرم‌افزار،

احزاب فاقد سابقه تجاری مشترک، و تفکیک‌پذیری تراکنش‌ها جهت بهبود کارایی فرآیندهای صورت‌حساب دست یافتند. در حوزه کاربردهای مالی، آلیسون (۲۰۱۵) و مزرایی (۲۰۱۶) تأیید کردند که چابکی قراردادهای هوشمند در مدل‌هایی نظیر تامین مالی جمعی و وام‌دهی همتا به همتا، هزینه‌های مبادله را به شدت کاهش داده و از تسویه‌های دست‌وپاگیر جلوگیری می‌کند. همچنین در حوزه اینترنت اشیا، کریستیدیس و همکاران (۲۰۱۶) نشان دادند که ترکیب این فناوری با IoT، امکان اتوماسیون رمزنگاری‌شده گردش‌های کاری زمان‌بر، نظیر قفل‌های هوشمند Slock.it را فراهم می‌آورد.

در خصوص چالش‌های امنیتی و آسیب‌پذیری‌ها، لو و همکاران (۲۰۱۶) و ناتولی و همکاران (۲۰۱۶) به بررسی بحران‌هایی نظیر «آسیب‌پذیری ورود مجدد» و «وابستگی به ترتیب تراکنش‌ها» پرداختند. برای مقابله با مشکل فقدان داده‌های قابل اعتماد، ژانگ و همکاران (۲۰۱۶) راه‌حل «تان کرایر» را پیشنهاد دادند که داده‌های معتبر را از سرورهای وب تأییدشده به قراردادهای هوشمند تغذیه می‌کند. همچنین، کاسبا و همکاران (۲۰۱۶) مدل بلاک چینی «هاک» را توسعه دادند تا با عدم ذخیره صریح تراکنش‌های مالی در زنجیره، حریم خصوصی کاربران را حفظ نماید. با این وجود، ویچین زو و همکاران (۲۰۱۹) در مطالعات اکتشافی خود دریافتند که هنوز هیچ روش پذیرفته‌شده‌ای برای ایمن‌سازی کد وجود ندارد و ابزارهای توسعه از قدرت کافی برخوردار نیستند. الهابری و مورسل نیز شکاف‌های تحقیقاتی مهمی را شناسایی کردند که از آن جمله می‌توان به فقدان مطالعات در زمینه مقیاس‌پذیری، عملکرد و مقابله با فعالیت‌های مجرمانه اشاره کرد.

در نهایت، از منظر روندهای آتی، وانگ و همکاران (۲۰۱۶) و یوان و همکاران (۲۰۱۶) تأکید دارند که توسعه آینده جامعه مدرن نیازمند گذار از سیستم‌های سایبری-فیزیکی به سیستم‌های سایبری-فیزیکی-اجتماعی (CPSS) است. در این پارادایم، بلاک چین و قراردادهای هوشمند به عنوان زیرساخت

رمزنگاری و سیستم‌های توزیع شده بوده است. منابع غیرمرتبط یا فاقد اعتبار علمی کافی از روند تحلیل حذف گردیده‌اند تا روایی داده‌ها تضمین شود.

پس از گردآوری منابع، از روش «تحلیل موضوعی» برای کدگذاری و دسته‌بندی مفاهیم استفاده شده است. بر این اساس، ادبیات پژوهش در پنج محور اصلی سازماندهی شده‌اند: (۱) مبانی نظری و تعاریف هستی‌شناختی؛ (۲) مکانیسم‌های عملیاتی (شامل قراردادهای درون‌زنجیره‌ای و خارج‌زنجیره‌ای)؛ (۳) معماری پلتفرم‌های میزبان؛ (۴) سناریوهای کاربردی در دنیای واقعی؛ و (۵) چالش‌های امنیتی و محدودیت‌های توسعه. همچنین، در این مرحله، مفاهیم کلیدی استخراج شده از هر منبع، با دقت با یکدیگر پیوند داده شده‌اند تا سیر تکاملی فناوری از یک ایده تئوریک برای کاهش هزینه‌های مبادله، به یک زیرساخت اجرایی برای سیستم‌های مالی غیرمتمرکز و سازمان‌های خودمختار به خوبی ترسیم گردد. این رویکرد موضوعی به پژوهشگر اجازه می‌دهد تا از پراکنده‌گویی پرهیز کرده و پیوستگی منطقی میان اجزای مختلف فناوری را تبیین نماید.

یکی از ابزارهای کلیدی در این پژوهش، «روش تحلیل مقایسه‌ای» است. برای درک عمیق‌تر اکوسیستم پلتفرم‌های بلاک چین، سه پلتفرم پیشرو یعنی اتریوم (به عنوان نماینده بلاک چین‌های عمومی و Turing-complete)، هایپرلجر (به عنوان نماینده راهکارهای سازمانی و مازولار) و کوردا (به عنوان پلتفرم تخصصی خدمات مالی) بر اساس معیارهای استاندارد نظیر نوع زبان برنامه‌نویسی، ماشین مجازی، مدل حریم خصوصی، مکانیزم اجماع و نحوه تعامل با هویت‌های دنیای واقعی مورد مقایسه تطبیقی قرار گرفته‌اند. این تحلیل مقایسه‌ای به روشنی نشان می‌دهد که چگونه هر پلتفرم، توازن متفاوتی را میان عدم تمرکز، مقیاس‌پذیری و حریم خصوصی برقرار می‌کند.

علاوه بر این، بخش مهمی از روش‌شناسی این مقاله به «مطالعه اکتشافی چالش‌های توسعه‌دهندگان» اختصاص دارد. همان‌طور که در ادبیات موضوع نیز به آن اشاره شده است، توسعه قراردادهای هوشمند با موانع پیچیده‌ای روبروست. در این بخش، با استفاده از روش استنتاجی و تحلیل ثانویه داده‌های گزارش شده در مطالعات پیشین، آسیب‌پذیری‌های ذاتی کدهای هوشمند نظیر «حمله ورود مجدد» (Reentrancy)، «وابستگی به ترتیب تراکنش‌ها»، «وابستگی به مهر زمانی» و «چالش تأمین داده‌های قابل اعتماد از طریق اوراکل‌ها» شناسایی و طبقه‌بندی شده‌اند. همچنین، راهکارهای پیشنهادی محققان پیشرو مانند استفاده از ابزارهای تحلیل نمادین، سیستم‌های تغذیه داده تأیید شده (مانند Town Crier) و مدل‌های حفظ حریم خصوصی (مانند Hawk) مورد ارزیابی اکتشافی قرار گرفته‌اند تا میزان اثربخشی آن‌ها در مواجهه با چالش‌های امنیتی سنجیده شود.

در نهایت، به منظور تضمین روایی و پایایی پژوهش، از تکنیک «مثلث‌سازی نظری» استفاده شده است. بدین معنا که مفاهیم و چالش‌های استخراج شده، از طریق تقاطع‌گیری نظرات پژوهشگران مختلف اعتبارسنجی شده‌اند تا از هرگونه سوگیری فردی در تفسیر مکانیسم‌های فنی بلاک چین جلوگیری شود. این امر باعث می‌شود تا یافته‌های پژوهش صرفاً بازتاب‌دهنده یک دیدگاه خاص نبوده، بلکه عصاره‌ای از اجماع علمی جامعه پژوهشی در حوزه بلاک چین باشد. در نهایت، خروجی این روش‌شناسی، ساختاری منسجم را برای بخش‌های «یافته‌ها» و «بحث و نتیجه‌گیری» فراهم می‌آورد.

#### ۴. یافته‌ها

۴-۱- ماهیت و معماری بلاک چین و قراردادهای هوشمند  
یافته‌های پژوهش نشان می‌دهد که بلاک چین در ساده‌ترین شکل خود، زنجیره‌ای از رکوردها (بلوک‌ها) است که با استفاده از رمزنگاری به هم متصل و ایمن می‌شوند. هر بلوک شامل داده‌های تراکنش، یک مهر زمانی و مقدار بلوک قبلی خود

قراردادهای خارج از زنجیره‌ای خارج از بلاک چین اجرا می‌شوند و تنها باید توسط شرکت‌کنندگان علاقه‌مند امضا و اجرا شوند. این قراردادها به طور کلی برای توابع شامل محاسبات پرهزینه یا اطلاعات خصوصی طراحی شده‌اند، در حالی که قراردادهای زنجیره‌ای برای وظایف کم‌هزینه و غیرحساس پیشنهاد می‌شوند. برای حفظ مزایای بلاک چین، نتایج قراردادهای خارج از زنجیره‌ای روی زنجیره وارد می‌شود و در صورت اختلاف، می‌توان از یک قرارداد درون‌زنجیره‌ای برای حل آن استفاده کرد.

#### ۴-۳- پلتفرم‌های میزبان و مقایسه تطبیقی

یافته‌های پژوهش نشان می‌دهد که پلتفرم‌های مختلف بلاک چین، پشتیبانی متفاوتی از قراردادهای هوشمند ارائه می‌دهند. اتریوم به عنوان یک پلتفرم بلاک چین عمومی، برنامه‌ها را دقیقاً همان‌طور که برنامه‌ریزی شده است بدون هیچ‌گونه احتمال خرابی، سانسور، تقلب یا دخالت شخص ثالث اجرا می‌کند. این پلتفرم از یک ماشین مجازی کامل تورینگ به نام ماشین مجازی اتریوم (EVM) برای اجرای بایت‌کد قرارداد استفاده می‌کند و برنامه‌های کاربردی بر روی رمزنگاری خاص آن به شکل «اتر» اجرا می‌شوند.

در مقابل، هایپرلجر یک پیاده‌سازی چارچوب بلاک چین است که توسط بنیاد لینوکس حمایت می‌شود و یک پلتفرم برای راه‌حل‌های دفتر کل توزیع‌شده با معماری ماژولار است که درجات بالایی از محرمانگی، انعطاف‌پذیری و مقیاس‌پذیری را ارائه می‌دهد. این پلتفرم از فناوری کانتینر برای میزبانی قراردادهای هوشمند به نام «چین‌کد» استفاده می‌کند که منطق برنامه سیستم را تشکیل می‌دهد.

پلتفرم کوردا نیز یک پلتفرم بلاک چین متن باز است که به صراحت برای در نظر گرفتن محیط تنظیم‌شده صنعت خدمات مالی طراحی شده است. در کوردا، هر گره دارای گواهی است که هویت شبکه آن‌ها را به یک هویت قانونی دنیای واقعی ترسیم می‌کند. ارتباط بین گره‌ها نقطه به نقطه است و تاریخچه

است. این فناوری به عنوان یک دفتر کل عمومی در نظر گرفته می‌شود که در یک مکان واحد ذخیره نمی‌شود، بلکه در شبکه‌ای از گره‌ها تکثیر می‌گردد؛ به طوری که هر گره یک کپی کامل از بلاک چین دارد. این ویژگی باعث می‌شود همه رکوردها عمومی و به راحتی برای همه گره‌های شبکه قابل تأیید باشند و تغییر هر داده‌ای بدون دستیابی به اجماع همه گره‌ها بسیار پرهزینه و تقریباً غیرممکن شود.

قرارداد هوشمند در این بستر، به عنوان یک برنامه در حال اجرا بر روی بلاک چین تعریف می‌شود که شامل داده‌ها (مانند موجودی حساب) و کد اجرایی است. این قراردادها در زنجیره بلوکی ذخیره شده و زمانی که پیش‌شرط خاصی برآورده شد، به طور خودکار اجرا می‌شوند. پس از هر اجرای قرارداد هوشمند، وضعیت آن در بلاک چین به‌روز می‌گردد. این ماهیت خوداجرائی، فرصت فوق‌العاده‌ای را برای استفاده در بسیاری از زمینه‌هایی که به داده‌ها برای هدایت تراکنش‌ها متکی هستند، فراهم می‌آورد.

#### ۴-۲- مکانیزم‌های عملیاتی: قراردادهای درون‌زنجیره‌ای و خارج‌زنجیره‌ای

یافته‌های پژوهش نشان می‌دهد که قراردادهای هوشمند مجموعه‌ای از قوانین و منطق رویه‌ای سناریو-پاسخ هستند. طرفین امضاکننده قرارداد باید در مورد جزئیات، شرایط نقض، مسئولیت نقض و منابع داده‌های تأیید خارجی (اوراکل‌ها) به توافق برسند، سپس آن را بر روی بلاک چین مستقر کنند.

در خصوص مکانیزم‌های عملیاتی، دو رویکرد اصلی شناسایی شده است. قراردادهای هوشمند درون‌زنجیره‌ای به دلیل ماهیت فناوری بلاک چین، باید توسط هر گره اجرا و اعتبارسنجی شوند و تمام تراکنش‌های مربوطه برای کل شبکه قابل مشاهده است. این امر حریم خصوصی قراردادها را کاهش می‌دهد و هزینه تراکنش را به ویژه برای قراردادهای دارای محاسبات پیچیده بالا می‌برد. در مقابل، به عنوان یک راه‌حل جایگزین، ایده قرارداد هوشمند «خارج از زنجیره» پیشنهاد شده است.

تراکنش کاملاً رمزگذاری شده و خصوصی فقط برای طرفین ضروری است. قراردادهای هوشمند در کوردا دارای سه عنصر کلیدی هستند: کد قابل اجرا، استیت آبجکت و دستورات.

#### ۴-۴- سناریوهای کاربردی در دنیای واقعی

یافته‌های پژوهش نشان می‌دهد که قراردادهای هوشمند دارای سه ویژگی اصلی هستند: استقلال، خودکفایی و عدم تمرکز. خودمختاری به این معناست که پس از راه‌اندازی و اجرا، قراردادهای و عوامل آغازگر نیازی به تماس بیشتر ندارند. خودکفایی یعنی توانایی مدیریت منابع (مانند جمع‌آوری سرمایه از طریق ارائه خدمات و خرج کردن آن‌ها در صورت نیاز) و عدم تمرکز نیز به دلیل توزیع بر روی گره‌های شبکه است. این ویژگی‌ها، قراردادهای هوشمند را به فعال‌کننده‌های اصلی بلاک چین ۲/۰ و ۳/۰ و پایه‌گذار سیستم‌های مالی و اجتماعی قابل برنامه‌ریزی تبدیل کرده است.

سناریوهای کاربردی متعددی شناسایی شده‌اند. در حوزه معاملات مالی، قراردادهای هوشمند به ویژه برای مدل‌های کسب‌وکار مانند تأمین مالی جمعی، وام‌دهی هم‌تا به هم‌تا و بیمه آنلاین مناسب هستند.

ویژگی جابکی این قراردادها می‌تواند هزینه‌های مبادله را تا حد زیادی کاهش دهد و از تسویه و تحویل دست‌وپاگیر جلوگیری کند. در حوزه بازارهای پیش‌بینی، پلتفرم‌هایی مانند اگر و گنوسیس با کمک بلاک چین موفق به ایجاد ابزارهای پیش‌بینی دقیق شده‌اند. در حوزه اینترنت اشیا، ترکیب قراردادهای هوشمند و IoT نه تنها می‌تواند به اشتراک‌گذاری اطلاعات بین دستگاه‌ها را تسهیل کند، بلکه به افراد اجازه می‌دهد تا گردش‌های کاری زمان‌بر را به روشی رمزنگاری خودکار تبدیل کنند. وب‌سایت اسلاک اولین قفل مستقلی را پیشنهاد کرد که افراد می‌توانند با توکن باز کنند و کاربران می‌توانند قفل را هر چند وقت یک‌بار که بخواهند باز و بسته کنند.

#### ۴-۵- چالش‌ها و آسیب‌پذیری‌های شناسایی شده

یافته‌های پژوهش نشان می‌دهد که با وجود افزایش محبوبیت قراردادهای هوشمند، چالش‌های بالقوه‌ای وجود دارد. به دلیل ماهیت تغییرناپذیر بلاک چین، قراردادهای پس از استقرار قابل تغییر نیستند و هرکس می‌تواند از این آسیب‌پذیری سوءاستفاده کنند. آسیب‌پذیری‌های اصلی شناسایی شده عبارتند از:

۱. **آسیب‌پذیری ورود مجدد:** این مشکل زمانی رخ می‌دهد که مهاجم از یک تابع فراخوانی بازگشتی برای انجام برداشت‌های مکرر چندگانه استفاده می‌کند، در حالی که موجودی آن‌ها فقط یک بار استنباط می‌شود. بدنام‌ترین مورد این حمله، حمله به DAO است.

۲. **وابستگی به ترتیب تراکنش‌ها:** این حالت زمانی اتفاق می‌افتد که چندین تراکنش وابسته که یک قرارداد را فراخوانی می‌کنند در یک بلوک گنجانده شوند. ماینرها می‌توانند ترتیب دلخواه خود را بین تراکنش‌ها تنظیم کنند و وضعیت نهایی قرارداد را تعیین کنند.

۳. **وابستگی به مهر زمانی:** مهر زمانی روی زمان فعلی سیستم محلی ماینر تنظیم می‌شود و ماینر می‌تواند این مقدار را تغییر دهد. این مشکل امنیتی زمانی ایجاد می‌شود که از مهر زمانی به عنوان یک شرط راه‌اندازی برای انجام اقدامات خاص استفاده می‌شود.

۴. **فقدان داده‌های قابل اعتماد:** قراردادهای هوشمند گاهی به اطلاعاتی از منابع خارجی نیاز دارند، اما قابل اطمینان بودن اطلاعات را نمی‌توان تضمین کرد.

۵. **مسائل حریم خصوصی:** از آنجایی که تمام تاریخچه تراکنش‌ها در زنجیره بلوکی ذخیره می‌شود و برای هر کسی قابل مشاهده است، از نظر تئوری می‌توان اطلاعات خصوصی کاربر را با تجزیه و تحلیل ساختارهای نمودار تراکنش به دست آورد که به این حمله «بینام‌سازی» می‌گویند.

## ۶-۶- پیشرفت‌ها و روندهای آتی

یافته‌های پژوهش نشان می‌دهد که برای مقابله با چالش‌های فوق، محققان راه‌حل‌های متعددی را پیشنهاد کرده‌اند. برای مقابله با آسیب‌پذیری ورود مجدد و وابستگی به ترتیب تراکنش‌ها، استفاده از توابع مبتنی بر اتریوم (مانند send-if-received) و ابزار تحلیل نمادین Oyente برای جستجوی اشکالات امنیتی بالقوه پیشنهاد شده است. همچنین برای حل مشکل فقدان داده‌های قابل اعتماد، راه‌حل Town Crier پیشنهاد شد که داده‌های معتبری را از سرورهای وب قابل تأیید به قراردادهای هوشمند ارائه می‌دهد. برای حفظ حریم خصوصی، مدل بلاک چینی Hawk برنامه‌نویسی شده که تراکنش‌های مالی را به طور صریح در زنجیره بلوکی ذخیره نمی‌کند.

از منظر روندهای آتی، توسعه جامعه آینده منوط به تبدیل از سیستم‌های فیزیکی-سایبری (CPS) به سیستم‌های فیزیکی-اجتماعی-سایبری (CPSS) است که در آن عوامل اجتماعی و انسانی باید در نظر گرفته شوند. بلاک چین و قراردادهای هوشمند آن، زیرساخت اساسی برای تحقق جامعه موازی مبتنی بر CPSS هستند. این فناوری‌ها می‌توانند به تحقق سیستم‌های اجتماعی تعریف‌شده توسط نرم‌افزار کمک کنند و با حذف مقامات متمرکز و استقرار رفتار غیرقابل پیش‌بینی در بلاک چین در قالب کدهای قراردادی، «سیستم مرتون» (دارای عدم قطعیت و پیچیدگی بالا) را به «سیستم نیوتن» (قابل پیش‌بینی و کنترل‌پذیر) تبدیل کنند.

## ۵. بحث و نتیجه‌گیری

پژوهش حاضر با هدف ارائه مروری جامع بر قراردادهای هوشمند مبتنی بر بلاک چین و واکاوی چالش‌های پیش‌روی توسعه آن‌ها انجام شد. یافته‌ها نشان داد که مفهوم قرارداد هوشمند که نخستین بار توسط نیک سابو برای اتوماسیون توافقات حقوقی و کاهش هزینه‌های مبادله مطرح گردید، با

ظهور فناوری بلاک چین و پلتفرم‌هایی نظیر اتریوم، هابیرلجر و کوردا، از یک ایده تئوریک به یک زیرساخت اجرایی و قدرتمند تبدیل شده است. این فناوری با تکیه بر ویژگی‌های بنیادین نظیر عدم تمرکز، تغییرناپذیری و خوداجرایی، امکان مبادله شفاف دارایی‌ها، خدمات مالی، سهام و مالکیت‌های معنوی را بدون نیاز به واسطه‌های سنتی فراهم آورده است.

نتایج این مطالعه اکتشافی تأیید می‌کند که قراردادهای هوشمند در کوتاه‌مدت می‌توانند بر بستر زیرساخت‌های موجود مورد استفاده قرار گیرند و در بلندمدت، به عنوان یک دفتر کل مشترک و قابل برنامه‌ریزی، پایه‌گذار سیستم‌های مالی و اجتماعی نوین خواهند بود. به ویژه در حوزه‌هایی نظیر تامین مالی جمعی، بازارهای پیش‌بینی و اینترنت اشیا، این فناوری پتانسیل بالایی در حذف بروکراسی و افزایش کارایی از خود نشان داده است. با این وجود، بررسی‌ها نشان داد که توسعه قراردادهای هوشمند هنوز در مراحل ابتدایی خود قرار دارد. آسیب‌پذیری‌های ذاتی نظیر حمله ورود مجدد، وابستگی به ترتیب تراکنش‌ها و مهر زمانی، در کنار فقدان ابزارهای قدرتمند اشکال‌زدایی، منابع یادگیری محدود و کمبود پشتیبانی جامعه توسعه‌دهندگان، از مهم‌ترین موانع پذیرش گسترده این فناوری به شمار می‌روند.

از منظر چشم‌انداز کلان، توسعه جوامع مدرن نیازمند گذار از سیستم‌های سایبری-فیزیکی (CPS) به سیستم‌های سایبری-فیزیکی-اجتماعی (CPSS) است. در این پارادایم، بلاک چین و قراردادهای هوشمند به عنوان زیرساخت اساسی برای تحقق جوامع موازی عمل می‌کنند. این فناوری‌ها با حذف مقامات متمرکز و استقرار رفتارهای پیچیده در قالب کدهای قراردادی تغییرناپذیر، امکان تبدیل «سیستم‌های مرتون» (با عدم قطعیت بالا) به «سیستم‌های نیوتن» (قابل پیش‌بینی و کنترل‌پذیر) را فراهم می‌آورند. در نهایت، می‌توان نتیجه گرفت که قراردادهای هوشمند نه تنها یک ابزار فنی، بلکه یک

پیشران اجتماعی برای اتوماسیون و تعریف مجدد اعتماد در عصر دیجیتال هستند.

مانند هر پژوهش علمی دیگری، مطالعه حاضر نیز با محدودیت‌هایی مواجه بود. نخست آنکه این پژوهش از نوع مطالعات مروری و اکتشافی است و بر پایه تحلیل ثانویه منابع و ادبیات موجود استوار بوده است؛ از این رو، فاقد پیاده‌سازی عملی، شبیه‌سازی کدها و ارزیابی کمی عملکرد قراردادهای هوشمند در محیط‌های واقعی است. دوم، به دلیل حجم گسترده و به سرعت در حال تحول اکوسیستم بلاک چین، تمرکز اصلی بر پلتفرم‌های پیشرو و عمومی نظیر اتریوم بوده و بررسی عمیق‌تر پلتفرم‌های سازمانی خاص و مکانیزم‌های اجماع نوین در حوصله این مقاله نمی‌گنجید. سوم، کمبود شدید پژوهش‌های آکادمیک و بومی در زبان فارسی در این حوزه، دسترسی به داده‌های تطبیقی مبتنی بر بستر حقوقی و اقتصادی ایران را با چالش مواجه ساخت و چهارم، محدودیت‌های زمانی و دسترسی به برخی از مقالات پیش‌چاپ و گزارش‌های صنعتی غیررسمی، از دیگر محدودیت‌های این پژوهش بود.

با توجه به شکاف‌های شناسایی‌شده و روندهای نوظهور، مسیرهای متعددی برای پژوهش‌های آتی پیشنهاد می‌گردد. از منظر فنی، توسعه ابزارهای پیشرفته تحلیل نمادین، اثبات رسمی، آزمون کامپایلر سالیدیتی (Solidity) و اشکال‌زدای تعاملی از اهمیت ویژه‌ای برخوردار است. همچنین، طراحی مدل‌های نوین حفظ حریم خصوصی و راهکارهای مقابله با حملات اوراکل‌ها نیازمند توجه بیشتری است. از منظر کاربردی، ادغام عمیق قراردادهای هوشمند با اینترنت اشیا (IoT) و هوش مصنوعی توزیع‌شده برای ایجاد سازمان‌های خودمختار غیرمتمرکز (DAO) می‌تواند موضوع پژوهش‌های میان‌رشته‌ای قرار گیرد.

علاوه بر این، با توجه به نقش پررنگ این فناوری در تامین مالی جمعی و بازارهای مالی، بررسی چالش‌های مقیاس‌پذیری، مصرف انرژی و انطباق قراردادهای هوشمند با چارچوب‌های

حقوقی سنتی (به ویژه در نظام حقوقی ایران) از اولویت‌های پژوهشی آینده است. در نهایت، مطالعات تطبیقی بر روی پلتفرم‌های نسل سوم بلاک چین و مکانیزم‌های اجماع جایگزین برای ارتقای کارایی و امنیت شبکه‌های توزیع‌شده، هم در بعد فنی و هم در بعد تجاری، افق‌های روشن و بکری را پیش روی محققان این حوزه قرار می‌دهد.

**ملاحظات اخلاقی:** کلیه اصول اخلاق در پژوهش، همچنین امانت‌داری علمی در استفاده از منابع، استنادها و ارجاعات موردتوجه قرار گرفته و رعایت شده است.

**تعارض منافع:** نویسندگان اعلام می‌دارند که تدوین و انتشار این مقاله فاقد هرگونه تعارض منافع بوده است.

**سهم نویسندگان:** نگارش و تدوین مقاله به‌صورت مشترک و با مشارکت برابر تمامی نویسندگان انجام شده است.

**تشکر و قدردانی:** بدین‌وسیله از تمامی افرادی که در تهیه و تکمیل این مقاله همکاری و مساعدت داشته‌اند، قدردانی می‌شود.

**تأمین اعتبار پژوهش:** این پژوهش بدون دریافت هرگونه حمایت یا تأمین مالی انجام شده است.

## فهرست منابع

Alharby, M., & van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*.

Allison, I. (2015). *Ethereum-based Slock.it reveals first ever lock opened with money*. IBTimes. Retrieved from <http://www.ibtimes.co.uk>

Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). *Corda: An introduction*. R3 CEV.

- Ethereum smart contracts. In *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (pp. 35–39). IEEE. <https://doi.org/10.1145/3194133.3194137>
- Hertig, A. (2016). *Ethereum prediction market service takes first steps with beta launch*. CoinDesk. Retrieved from <https://www.coindesk.com>
- Kang, M. Z., & Wang, F. Y. (2017). From parallel plants to smart plants: Intelligent control and management for plant growth. *IEEE/CAA Journal of Automatica Sinica*, 4(2), 161-166.
- Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE Symposium on Security and Privacy* (pp. 839-858). IEEE. <https://doi.org/10.1109/SP.2016.55>
- Li, C., Palanisamy, B., & Xu, R. (2019). Scalable and privacy-preserving design of on/off-chain smart contracts. *arXiv preprint arXiv:1902.06359*.
- Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In *Proceedings of the 23rd Conference on Computer and Communications Security* (pp. 254–269). ACM. <https://doi.org/10.1145/2976749.2978309>
- Magazzeni, D., McBurney, P., & Nash, W. (2017). Validation and verification of smart contracts: A research agenda. *Computer*, Buterin, V. (2017). *A next-generation smart contract and decentralized application platform*. Ethereum White Paper. Retrieved from <http://github.com/ethereum/wiki/wiki/White-Paper>
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292-2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- Clack, C. D. (2018). Smart contract templates: Legal semantics and code validation. *Journal of Digital Banking*, 2(4), 338–352.
- Clack, C. D., Bakshi, V. A., & Braine, L. (2016). *Smart contract templates: Foundations, design landscape and research directions*. arXiv:1608.00771.
- Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. In *International Conference on Financial Cryptography and Data Security* (pp. 79-94). Springer. [https://doi.org/10.1007/978-3-662-53357-4\\_6](https://doi.org/10.1007/978-3-662-53357-4_6)
- Eberhardt, J., & Tai, S. (2017). On or off the blockchain? Insights on off-chaining computation and data. In *Proceedings of the 6th European Conference on Service-Oriented and Cloud Computing* (pp. 3–15). Springer.
- Hegedus, P. (2018). Towards analyzing the complexity landscape of Solidity based

- Stark, J. (2016). *Making sense of blockchain smart contracts*. CoinDesk. Retrieved from <https://www.coindesk.com>
- Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.
- Szabo, N. (1996). *Smart contracts: Building blocks for digital markets*. Retrieved from <http://www.fon.hum.uva.nl>
- Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9). <https://doi.org/10.5210/fm.v2i9.548>
- Szabo, N. (1997). *The idea of smart contracts*. Retrieved from <http://szabo.best.vwh.net>
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world*. Portfolio.
- Valenta, M., & Sandner, P. (2017). *Comparison of Ethereum, Hyperledger Fabric and Corda*. Frankfurt School Blockchain Center.
- Wang, F. Y. (2015). Software-defined systems and knowledge automation: A parallel paradigm shift from Newton to Merton. *Acta Automatica Sinica*, 41(1), 1-8.
- Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.-Y. (2018). An overview of smart contract: Architecture, applications, and future trends. In *2018 IEEE Intelligent Vehicles Symposium* (pp. 108-113). IEEE. <https://doi.org/10.1109/IVS.2018.8500488>
- 50(9), 50-57. <https://doi.org/10.1109/MC.2017.3571031>
- Mizrahi, A. (2016). *Everex helps migrant workers send remittance back to Myanmar via Ethereum*. Finance Magnates. Retrieved from <https://www.financemagnates.com>
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- Natoli, C., & Gramoli, V. (2016). The blockchain anomaly. In *2016 IEEE 15th International Symposium on Network Computing and Applications* (pp. 310-317). IEEE. <https://doi.org/10.1109/NCA.2016.7778637>
- R3. (2018). *Corda documents*. Retrieved from <https://docs.corda.net/>
- Ron, D., & Shamir, A. (2013). Quantitative analysis of the full Bitcoin transaction graph. In *Financial Cryptography and Data Security* (pp. 6-24). Springer. [https://doi.org/10.1007/978-3-642-39884-1\\_2](https://doi.org/10.1007/978-3-642-39884-1_2)
- Rutkin, A. (2016). *Blockchain-based microgrid gives power to consumers in New York*. New Scientist. Retrieved from <https://www.newscientist.com>
- Seijas, P. L., Thompson, S. J., & McAdams, D. (2016). *Scripting smart contracts for distributed ledger technology*. IACR Cryptology ePrint Archive, 2016:1156.
- Slock.it. (n.d.). *Decentralized sharing economy*. Retrieved from <https://slock.it/>

Wang, X., Li, L. X., Yuan, Y., Ye, P. J., & Wang, F. Y. (2016). ACP-based social computing and parallel intelligence: Societies 5.0 and beyond. *CAAI Transactions on Intelligence Technology*, 1(4), 377-393. <https://doi.org/10.1016/j.trit.2016.11.008>

Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum Project Yellow Paper.

Yuan, Y., & Wang, F. Y. (2016). Blockchain: The state of the art and future trends. *Acta Automatica Sinica*, 42(4), 481-494.

Zhang, F., Cecchetti, E., Croman, K., Juels, A., & Shi, E. (2016). Town Crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 270-282). ACM. <https://doi.org/10.1145/2976749.2978404>

Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, 6(2), 1594-1605. <https://doi.org/10.1109/JIOT.2018.2844914>

Zou, W., Lo, D., Kochhar, P. P., Xia, X., Li, X., Feng, Z., ... & Chen, G. (2021). Smart contract development: Challenges and opportunities. *IEEE Transactions on Software Engineering*, 47(10), 2084-2106. <https://doi.org/10.1109/TSE.2019.2942301>