

# Designing a Conceptual Model for Fraud Detection in Banking Payments Using a Blockchain Approach

1. Hamid Dehghani<sup>ID</sup>: Department of Management, Deh.C., Islamic Azad University, Dehaghan, Iran

2. Mohammad Reza Sharifi Qazvini<sup>ID\*</sup>: Department of Industrial Engineering, Deh.C., Islamic Azad University, Isfahan, Iran. Email: Mo.sharifi@iau.ac.ir (Corresponding Author)

3. Saeid Aghasi<sup>ID</sup>: Department of Management, Deh.C., Islamic Azad University, Dehaghan, Iran

## Article history



Received: 21 June 2025

Revised: 23 October 2025

Accepted: 29 October 2025

Initial Publish: 11 June 2026

Final Publish: 22 June 2026

## Abstract:

The main objective of this study is to design a conceptual model for detecting and preventing fraud in banking payment systems through blockchain technology. This research is applied–developmental in purpose, interpretivist in philosophy, inductive in approach, and qualitative in strategy. Data were collected through a literature review, semi-structured interviews with ten banking and blockchain experts, and a questionnaire. Thematic analysis and meta-synthesis were employed to identify categories and components. Inter-coder reliability (81% and 83%) confirmed the consistency of coding across researchers. The results revealed that fraud detection in blockchain-based payment systems is influenced by four major categories: technological, internal organizational, external organizational, and financial–technical factors. The final model indicates that blockchain enhances fraud detection efficiency by eliminating intermediaries, improving data transparency, increasing transaction security, and reducing operational costs. Moreover, technology transfer, legal frameworks, information infrastructure, management capabilities, and financial capacities play critical roles in the effective implementation of blockchain in the banking sector. The proposed model demonstrates that blockchain technology can serve as a reliable and transparent infrastructure for fraud detection and prevention in Iran’s banking industry. By ensuring data integrity and accountability, blockchain provides a transformative framework that strengthens trust and operational performance in digital financial systems.

**Keywords:** Fraud detection; Banking; Blockchain; Thematic analysis; Meta-synthesis



**Extended Abstract****Introduction**

In recent years, the banking sector has undergone a fundamental transformation under the influence of digitalization and disruptive financial technologies. The increasing prevalence of online banking, the diversification of digital payment channels, and the expansion of financial transactions in cyberspace have made banks more vulnerable to financial fraud and cybercrime. Conventional fraud detection systems—often dependent on centralized architectures and human monitoring—struggle to detect complex, adaptive, and large-scale fraudulent activities in real time (Motie & Raahemi, 2024).

Blockchain technology has emerged as one of the most promising solutions for enhancing transparency, traceability, and security in digital financial ecosystems. Unlike traditional databases, blockchain operates as a distributed ledger, recording transactions across a network of decentralized nodes that cannot be easily altered or deleted (Kumar et al., 2024). This immutability feature ensures the integrity of data and enables stakeholders to verify transactions without relying on centralized authorities (Spsychiger et al., 2023). In the banking industry, blockchain provides an opportunity to reconstruct the architecture of payment systems and enhance mechanisms for fraud detection and prevention (Salimi, 2023).

Early studies described blockchain primarily as a technological innovation for cryptocurrencies; however, its potential in financial transparency, auditing, and fraud management has since been widely recognized (Amirshakari & Latifi, 2017). For instance, the decentralized autonomous organization (DAO) model proposed by Kumar et al. (2024) offers a new governance framework that enhances accountability and prevents manipulation by distributing decision-making power (Kumar et al., 2024). Similarly, Bettini de Miranda et al. (2024) developed a blockchain-based voting system for inter-organizational collaboration, showing how distributed architectures can reduce data opacity and manipulation in corporate environments (Bettini de Miranda et al., 2024).

In the field of fraud detection, blockchain can act as both a preventive and detective mechanism. Liu and Lee (2022) introduced the CFLedger model, which prevents chargeback fraud by validating transactions through immutable distributed ledgers (Liu & Lee, 2022). In a related context, Mahtani (2022) argued that blockchain-based accounting systems reduce fraudulent practices by providing a transparent and tamper-proof financial data structure (Mahtani, 2022). Empirical evidence also suggests that blockchain reduces risks associated with information asymmetry and moral hazard in financial reporting (Salimi, 2023).

Beyond banking, blockchain applications extend to risk management, insurance, and supply chain finance. Huang et al. (2023) demonstrated how blockchain-assisted insurance systems preserve privacy and resist fraud, while simultaneously improving operational efficiency (Huang et al., 2023). Similarly, Zhang et al. (2025) developed a blockchain-based decision support system for intelligent risk management in supply chain financing, showing that distributed networks enhance predictive accuracy and control over financial anomalies (Zhang et al., 2025).

In Iran, preliminary efforts to integrate blockchain into financial services have focused on fraud prevention and regulatory compliance. Sepanloo et al. (2019) proposed a blockchain-based system to mitigate fraud in issuing letters of credit, reducing transaction delays and increasing traceability (Sepanloo et al., 2019). Likewise, Hamidi and Karbasian (2024) highlighted that blockchain, combined with smart analytical tools, can detect fraudulent banking behaviors by integrating transaction history, customer identity verification, and risk profiling (Hamidi & Karbasian, 2024).

Nevertheless, the adoption of blockchain in banking remains limited due to barriers such as insufficient technological infrastructure, high implementation costs, and uncertain regulatory frameworks (Akinbowale et al., 2024). The complexity of blockchain's technical design, along with resistance to organizational change, hinders its large-scale implementation (Spsychiger et al., 2023). Additionally, studies emphasize the necessity of human capital development and digital literacy among banking personnel to ensure proper utilization of blockchain solutions (Fitriana et al., 2024).

In summary, prior research underscores that blockchain's decentralized, transparent, and secure architecture can transform fraud detection processes in the banking sector. However, existing studies are fragmented and context-dependent, lacking an integrated conceptual framework that considers both internal and external organizational factors. Addressing this gap, the present study aims to design a comprehensive conceptual model for fraud detection in banking payments using a blockchain-based approach, combining technological, organizational, and regulatory dimensions.

### Methods and Materials

This study employed a qualitative research design with an applied-developmental objective and an interpretivist philosophical foundation. The methodological approach was inductive, emphasizing theory-building through data synthesis rather than hypothesis testing.

The research was conducted in two major phases. The first phase involved a meta-synthesis (meta-aggregation) of existing qualitative and conceptual studies related to blockchain applications in financial systems and fraud detection. Using defined keywords across major academic databases (IEEE, Scopus, Springer, and ScienceDirect), 3742 articles were initially retrieved. After systematic screening and relevance evaluation, 52 high-quality studies were selected for inclusion in the synthesis.

The second phase involved semi-structured interviews with ten subject-matter experts specializing in digital banking, payment systems, and blockchain technology. Interview participants were selected using purposive sampling and engaged until theoretical saturation was achieved. Interview transcripts were coded using open, axial, and selective coding techniques. To ensure reliability, inter-coder agreement was calculated at 83% and 81%, exceeding the accepted threshold of 60%.

The results from both the meta-synthesis and expert interviews were integrated through thematic analysis to construct a multi-layered conceptual model. Data triangulation enhanced the validity of the results.

### Findings

The data analysis identified four main categories influencing the adoption and effectiveness of blockchain-based fraud detection in banking payments:

1. Technological Factors
2. Internal Organizational Factors
3. External Environmental Factors
4. Financial and Technical Factors

Within these four dimensions, 54 sub-factors were extracted from the coding process.

**1. Technological Factors** included the complexity of blockchain architecture, scalability, interoperability with existing systems, data encryption mechanisms, and automation capacity. Banks with advanced IT infrastructure and robust digital systems were found to be better positioned for blockchain integration.

**2. Internal Organizational Factors** encompassed management support, digital culture, employee expertise, and readiness for innovation. Organizational transparency and cross-departmental collaboration emerged as critical enablers for preventing fraudulent activities.

**3. External Environmental Factors** included regulatory clarity, political stability, technology transfer mechanisms, and economic conditions. The absence of comprehensive legal frameworks was identified as a major barrier to the institutionalization of blockchain in Iran's banking sector.

**4. Financial and Technical Factors** related to budget allocation, maintenance costs, access to funding resources, and the ability to conduct real-time financial audits. Banks with higher financial flexibility showed greater potential to adopt blockchain solutions effectively.

The conceptual model developed in this study follows a four-layered structure, placing technological innovation at its core, followed by internal organizational mechanisms, external environmental conditions, and financial-technical capabilities. Each layer interacts dynamically with the others, reflecting the systemic nature of fraud detection processes in modern digital banking.

### Discussion and Conclusion

The findings of this study reinforce the argument that blockchain can serve as a transformative enabler in modern banking fraud detection systems. By combining decentralization, transparency, and immutability, blockchain disrupts the traditional paradigm of trust that relied heavily on central authorities. The model developed in this research demonstrates that effective implementation of blockchain in banking requires the simultaneous alignment of technical, managerial, regulatory, and financial factors.

From a theoretical standpoint, the integration of blockchain into banking operations confirms its capacity to mitigate fraud through real-time auditing, automated verification, and tamper-proof recordkeeping. Technological variables such as scalability, data encryption, and interoperability play crucial roles in ensuring the resilience of fraud detection systems. Organizational variables, including management commitment and digital literacy, determine how effectively blockchain technologies are adopted and utilized. External and financial dimensions—particularly regulatory frameworks, technology transfer, and financial capability—serve as structural determinants shaping the implementation environment.

This study contributes to the growing literature by providing an indigenous conceptual model tailored to the context of Iran's banking system. The combination of meta-synthesis and expert interviews provided both breadth and depth of analysis, bridging theoretical concepts with practical realities. The results align with global findings that emphasize blockchain's role in promoting financial transparency and reducing systemic vulnerabilities.

Ultimately, blockchain represents more than a technological upgrade; it signifies a paradigm shift in how trust, accountability, and verification are conceptualized within financial ecosystems. Its application in fraud detection strengthens not only operational security but also institutional credibility and customer confidence. As banks move toward digital transformation, adopting blockchain-based fraud detection frameworks can serve as a cornerstone for achieving sustainable, transparent, and efficient financial operations in the modern era.

### Authors' Contributions

Authors equally contributed to this article.

**Acknowledgments**

Authors thank all participants who participate in this study.

**Declaration of Interest**

The authors report no conflict of interest.

**Funding**

According to the authors, this article has no financial support.

**Ethical Considerations**

All procedures performed in this study were under the ethical standards.

## طراحی مدل مفهومی کشف تقلب در پرداخت‌های بانکی با رویکرد بلاکچین



### تاریخچه مقاله

تاریخ دریافت: ۳۱ خرداد ۱۴۰۴

تاریخ بازنگری: ۱ آبان ۱۴۰۴

تاریخ پذیرش: ۷ آبان ۱۴۰۴

تاریخ چاپ اولیه: ۲۱ خرداد ۱۴۰۵

تاریخ چاپ نهایی: ۱ تیر ۱۴۰۵

۱. حمید دهقانی<sup>id</sup>: گروه مدیریت، واحد دهقان، دانشگاه آزاد اسلامی، دهقان، ایران

۲. محمدرضا شریفی قزوینی<sup>id\*</sup>: گروه مهندسی صنایع، واحد دهقان، دانشگاه آزاد اسلامی، اصفهان، ایران. ایمیل: [Mo.sharifi@iau.ac.ir](mailto:Mo.sharifi@iau.ac.ir) (نویسنده مسئول)

۳. سعید آقاسی<sup>id</sup>: گروه مدیریت، واحد دهقان، دانشگاه آزاد اسلامی، دهقان، ایران

### چکیده

هدف این پژوهش طراحی یک مدل مفهومی برای شناسایی و کشف تقلب در پرداخت‌های بانکی با استفاده از فناوری بلاکچین است. این پژوهش از نظر هدف کاربردی-توسعه‌ای، از نظر فلسفه تفسیرگرایانه، از منظر رویکرد استقرایی و از حیث استراتژی کیفی است. داده‌ها از طریق مطالعه کتابخانه‌ای، مصاحبه‌های نیمه‌ساختاریافته با ۱۰ خبره حوزه بانکداری و بلاکچین، و پرسشنامه جمع‌آوری شدند. تحلیل داده‌ها با رویکرد فراترکیب و تحلیل مضمون انجام گرفت. برای سنجش پایایی کدگذاری از روش توافق درونی بین کدگذاران همکار استفاده شد که نتایج قابل قبول (۸۱٪ و ۸۳٪) به دست آمد. نتایج نشان داد که عوامل مؤثر بر کشف تقلب در پرداخت‌های بانکی با رویکرد بلاکچین در چهار دسته اصلی قرار می‌گیرند: عوامل تکنولوژیک، عوامل درون‌سازمانی، عوامل برون‌سازمانی و عوامل فنی-مالی. این مدل نهایی نشان داد که فناوری بلاکچین می‌تواند از طریق حذف واسطه‌ها، افزایش شفافیت، بهبود امنیت داده‌ها و کاهش هزینه‌های تراکنش، کارایی کشف تقلب را در نظام بانکی افزایش دهد. همچنین، انتقال فناوری، زیرساخت‌های اطلاعاتی، ظرفیت‌های مالی و عوامل قانونی از مؤلفه‌های کلیدی در موفقیت این سیستم هستند. مدل ارائه‌شده بیانگر آن است که به‌کارگیری فناوری بلاکچین در نظام بانکی ایران می‌تواند به عنوان ابزاری مؤثر برای کشف و پیشگیری از تقلب مالی عمل کند. این فناوری با فراهم کردن شفافیت، امنیت و قابلیت حسابرسی بالا، زیرساختی نوین برای بهبود اعتماد در تراکنش‌های مالی فراهم می‌آورد.

**کلیدواژه‌گان:** کشف تقلب؛ بانکداری؛ بلاکچین؛ تحلیل مضمون؛ فراترکیب

**شبهه استناددهی:** دهقانی، حمید، شریفی قزوینی، محمدرضا، و آقاسی، سعید. (۱۴۰۵). طراحی مدل مفهومی کشف تقلب در پرداخت‌های بانکی با رویکرد بلاکچین. *حسابداری، امور مالی و هوش محاسباتی*، ۴(۲)، ۱۷-۱.



تحولات شتابان فناوری در دهه‌های اخیر، صنعت بانکداری را وارد مرحله‌ای از بازتعریف ساختارها و فرآیندهای خود کرده است. بانک‌ها به عنوان یکی از نهادهای حساس و راهبردی در نظام مالی کشورها، در معرض تهدیدهای متنوعی از جمله تقلب، حملات سایبری، خطاهای سیستمی و ریسک‌های اعتباری قرار دارند. در این میان، رشد فناوری‌های نوین نظیر هوش مصنوعی، یادگیری ماشین و به‌ویژه فناوری بلاکچین، افق‌های تازه‌ای برای ارتقای شفافیت، امنیت و کارایی در تراکنش‌های مالی گشوده است (Motie & Raahemi, 2024). فناوری بلاکچین با فراهم کردن بستری غیرمتمرکز، شفاف و غیرقابل دستکاری برای ذخیره و تبادل داده‌ها، توانسته است زمینه‌ساز انقلابی در نظام‌های مالی و بانکی شود.

در صنعت بانکداری، یکی از مهم‌ترین چالش‌ها شناسایی و مقابله با تقلب‌های مالی و تراکنش‌های غیرمجاز است. تقلب بانکی نه تنها موجب زیان مالی مستقیم می‌شود، بلکه اعتماد عمومی نسبت به نظام بانکی را نیز تضعیف می‌کند. در پژوهش‌های اخیر، مدل‌های داده‌محور متعددی برای تشخیص تقلب معرفی شده‌اند؛ اما اغلب این مدل‌ها در برابر تهدیدهای امنیتی پیچیده و داده‌های غیرشفاف کارایی محدودی دارند (Hamidi & Karbasian, 2024). فناوری بلاکچین با حذف نیاز به واسطه‌ها و ایجاد زنجیره‌ای از سوابق غیرقابل تغییر، می‌تواند به عنوان یک ابزار مؤثر برای شناسایی تقلب‌های مالی به کار گرفته شود (Salimi, 2023).

بلاکچین در ابتدا به عنوان بستر فنی رمز ارزها معرفی شد، اما کاربردهای آن به سرعت فراتر از حوزه رمزپول‌ها گسترش یافت. بر اساس تعریف ارائه شده در گزارش دانشگاه مانهام، بلاکچین یک فناوری توانمندساز است که با فراهم کردن امکان ثبت و اشتراک داده‌ها میان طرفین مستقل بدون نیاز به اعتماد متقابل، بستری برای نوآوری در حوزه‌های گوناگون ایجاد می‌کند (Johansen, 2017). به تعبیر آمارشکاری و لطیفی، این فناوری می‌تواند فرآیندهای بانکی همچون شناسایی مشتری (KYC) را تسهیل کند و شفافیت داده‌ها را بهبود بخشد (Amirshakari & Latifi, 2017).

مطالعات متعددی به بررسی نقش بلاکچین در صنعت بانکداری و حسابداری پرداخته‌اند. برای مثال، آرنا و همکاران (۲۰۲۴) نشان دادند که فناوری بلاکچین در کنار تحول دیجیتال می‌تواند ساختارهای سازمانی و فرآیندهای مدیریتی را به سمت شفافیت و کارایی سوق دهد (Arenal et al., 2024). اسپایخیگر و همکاران (۲۰۲۳) نیز بیان کردند که ساختارهای غیرمتمرکز مبتنی بر سازمان‌های خودگردان غیرمتمرکز (DAO) می‌توانند امکان مدیریت پروژه‌های پیچیده و چندوجهی را از طریق مکانیزم‌های بلاکچینی فراهم کنند (Spychiger et al., 2023).

در پژوهش دیگری، باتینی دی میراندا و همکاران (۲۰۲۴) به بررسی نقش بلاکچین در همکاری‌های بین‌سازمانی پرداختند و مدلی ارائه کردند که بر حفظ حریم خصوصی و رأی‌گیری شفاف برای تصمیم‌گیری جمعی متمرکز است. یافته‌های آنان نشان می‌دهد که بلاکچین می‌تواند ابزاری کارآمد برای مقابله با فساد و تقلب سازمانی در تصمیم‌گیری‌های مالی باشد (Bettini de Miranda et al., 2024). در همین راستا، کومار و همکاران (۲۰۲۴) مدلی از حاکمیت شرکتی مبتنی بر DAO را معرفی کردند که می‌تواند ساختارهای نظارتی را در سازمان‌های مالی به صورت غیرمتمرکز و شفاف بازتعریف کند (Kumar et al., 2024).

در سطح خردتر، کاربرد بلاکچین در مدیریت ریسک و جلوگیری از تقلب در تراکنش‌های مالی نیز مورد توجه پژوهشگران بوده است. لیو و لی (۲۰۲۲) با ارائه مدل CFLedger نشان دادند که چگونه بلاکچین می‌تواند از بروز تقلب در پرداخت‌های برگشتی جلوگیری کند و سازوکار اعتبارسنجی تراکنش‌ها را بهبود بخشد (Liu & Lee, 2022). همچنین، هوآنگ و همکاران (۲۰۲۳) در پژوهشی با عنوان «بیمه خودرو مبتنی بر بلاکچین با حفظ حریم خصوصی» تأکید کردند که استفاده از بلاکچین می‌تواند علاوه بر جلوگیری از تقلب، موجب افزایش اعتماد و شفافیت در تراکنش‌های بیمه‌ای شود (Huang et al., 2023).

از دیدگاه حسابداری و گزارشگری مالی، بلاکچین نیز ظرفیت بالایی برای کاهش تقلب و ارتقای شفافیت دارد. ماحتانی (۲۰۲۲) با تحلیل نظام‌های حسابداری مبتنی بر بلاکچین، بیان کرد که ساختار غیرمتمرکز و رمزنگاری شده این فناوری می‌تواند بسیاری از خلأهای موجود در سیستم‌های سنتی حسابداری را رفع کند و از دستکاری داده‌ها جلوگیری نماید (Mahtani, 2022). در همین راستا، سالیمی (۲۰۲۳) نیز تأکید کرده است که استفاده از بلاکچین در گزارشگری مالی باعث افزایش شفافیت و کاهش زمینه‌های بروز تقلب می‌شود (Salimi, 2023).

در حوزه تحلیل داده و یادگیری ماشین، استفاده از الگوریتم‌های پیشرفته برای شناسایی الگوهای غیرعادی در تراکنش‌های بانکی از اهمیت ویژه‌ای برخوردار است. بنچاجی و همکاران (۲۰۱۸) با استفاده از الگوریتم ژنتیک برای بهبود طبقه‌بندی داده‌های نامتوازن در تشخیص تقلب‌های کارت اعتباری، نشان دادند که رویکردهای هوش مصنوعی می‌تواند دقت مدل‌های شناسایی تقلب را افزایش دهد (Benchaji et al., 2018). با این حال، حتی مدل‌های یادگیری عمیق نیز در صورتی که داده‌های آموزشی فاقد شفافیت یا دستکاری شده باشند، دچار خطا می‌شوند؛ در چنین شرایطی، فناوری بلاکچین می‌تواند با تضمین اصالت داده‌ها، عملکرد این مدل‌ها را بهبود بخشد (Motie & Raahemi, 2024).

در ایران نیز مطالعاتی در زمینه کاربرد بلاکچین در صنعت بانکداری صورت گرفته است. سپانلو و همکاران (۲۰۱۹) با طراحی سامانه‌ای مبتنی بر بلاکچین برای جلوگیری از تقلب در صدور اعتبارات اسنادی، نشان دادند که این فناوری می‌تواند به‌طور مستقیم در کاهش خطاها و تخلفات مالی نقش‌آفرینی کند (Sepanloo et al., 2019). همچنین، حمیدی و کرباسیان (۲۰۲۴) مدلی برای شناسایی تقلب در نظام بانکی ایران با بهره‌گیری از ابزارهای هوشمند ارائه کردند که بر استفاده از فناوری‌های نوین مانند بلاکچین تأکید دارد (Hamidi & Karbasian, 2024).

از منظر نظری، زامان و همکاران (۲۰۲۵) در پژوهشی پیرامون داریی‌های رمزازی اسلامی، نقش بلاکچین را در توسعه داریی‌های دیجیتال مشروع مورد بررسی قرار دادند و به این نتیجه رسیدند که این فناوری می‌تواند چارچوب‌های مالی اسلامی را با شفافیت بیشتر و ریسک کمتر همراه کند (Zaman et al., 2025). همچنین، ژانگ و همکاران (۲۰۲۵) با طراحی سیستم تصمیم‌یار هوشمند مبتنی بر بلاکچین برای مدیریت ریسک در زنجیره تأمین مالی، نشان دادند که بلاکچین می‌تواند نه تنها در بانکداری بلکه در مدیریت مالی گسترده‌تر نیز نقشی تحول‌آفرین ایفا کند (Zhang et al., 2025).

با وجود تمام مزایای فوق، پیاده‌سازی فناوری بلاکچین در بانکداری با چالش‌هایی روبه‌رو است؛ از جمله الزامات زیرساختی، هزینه‌های انتقال فناوری، و ملاحظات قانونی و حاکمیتی. پژوهش آکین‌بووال و همکاران (۲۰۲۴) نشان داد که در بسیاری از نظام‌های بانکی، عدم هم‌راستایی میان سیاست‌های امنیتی، زیرساخت‌های فناوری اطلاعات و سازوکارهای نظارتی، زمینه‌ساز آسیب‌پذیری در برابر تقلب‌های سایبری است (Akinbowale et al., 2024). این موضوع نشان می‌دهد که برای بهره‌گیری مؤثر از بلاکچین در نظام بانکی، لازم است چارچوبی جامع که شامل ابعاد فنی، مدیریتی، اقتصادی و قانونی است طراحی گردد.

در کنار این موارد، تغییر در الگوی اعتماد از نهادهای متمرکز به سازوکارهای غیرمتمرکز مبتنی بر اثبات رمزنگاری، یکی از عمیق‌ترین دگرگونی‌های مفهومی ناشی از بلاکچین است. آمارشکاری و لطیفی (۲۰۱۷) تأکید کردند که استفاده از بلاکچین در فرآیندهای بانکی به‌ویژه احراز هویت مشتریان، می‌تواند به کاهش هزینه‌های اجرایی و افزایش اعتماد مشتریان منجر شود (Amirshakeri & Latifi, 2017). از سوی دیگر، فیتربانا و همکاران (۲۰۲۴) با تمرکز بر نظریه نمایندگی در بانک‌ها، بیان کردند که فقدان شفافیت در گزارشگری مالی از اصلی‌ترین زمینه‌های بروز تقلب است و فناوری‌هایی مانند بلاکچین می‌توانند این فاصله اطلاعاتی را کاهش دهند (Fitriana et al., 2024).

بررسی‌های انجام‌شده در زمینه ارتباط بلاکچین و شفافیت مالی نشان می‌دهد که این فناوری با ویژگی‌هایی چون غیرقابل تغییر بودن داده‌ها، توزیع‌شدگی و امکان حسابرسی آنی، قابلیت جایگزینی برای ساختارهای متمرکز سنتی فراهم می‌آورد (Arenal et al., 2024). همچنین، در پژوهش‌های جدید مشخص شده که استفاده از سازمان‌های خودگردان غیرمتمرکز (DAO) می‌تواند به توزیع عادلانه قدرت تصمیم‌گیری در نظام‌های مالی کمک کند و مانع از تمرکز قدرت در دست گروه‌های خاص شود (Kumar et al., 2024).

در یک جمع‌بندی کلی می‌توان گفت که فناوری بلاکچین نه تنها ابزاری برای ارتقای امنیت و کاهش تقلب در نظام‌های بانکی است، بلکه بستری برای بازتعریف ساختارهای نظارتی، مدیریتی و اعتمادساز در سطح کلان اقتصادی نیز محسوب می‌شود. مدل‌های نوین مدیریت ریسک، شفافیت در گزارشگری مالی، و اتوماسیون فرآیندهای بانکی از جمله دستاوردهای کلیدی این فناوری هستند. با این حال، اجرای موفقیت‌آمیز آن مستلزم طراحی مدلی جامع و بومی است که بتواند عوامل درونی و بیرونی مؤثر بر پیاده‌سازی فناوری بلاکچین در کشف تقلب‌های بانکی را دربر گیرد. لذا، هدف پژوهش حاضر ارائه یک مدل مفهومی برای کشف تقلب در پرداخت‌های بانکی با رویکرد فناوری بلاکچین است.

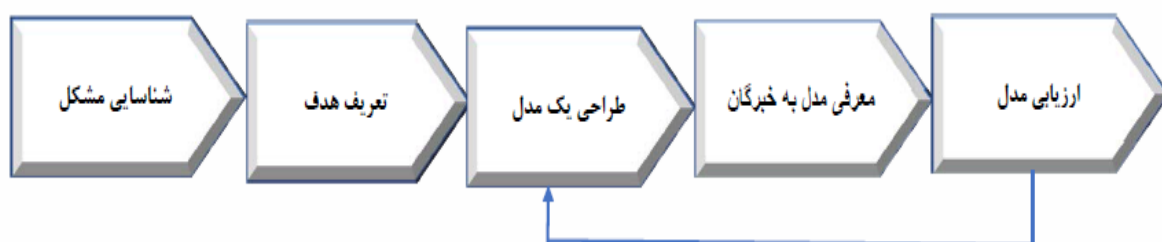
### روش پژوهش و مواد

در بخش اصلی تحقیق، روش گردآوری اطلاعات بصورت کتابخانه‌ای است. در روش کتابخانه‌ای از متن خوانی و سند خوانی استفاده می‌شود. سندهای موجود در این بخش شامل کتاب‌های کتابخانه‌های دانشگاهی، مقالات و مجلات معتبر (Springer، IEEE) سایت‌ها و سیستم‌های اطلاع رسانی اینترنتی و نشریه‌های رسمی دولتی می‌باشد. این پژوهش از نظر هدف کاربردی - توسعه‌ای است چرا که به دنبال ارائه مدلی برای کشف تقلب در پرداخت‌های بانکی بر پایه بلاکچین می‌باشد. از سوی دیگر اکتشافی است زیرا ماهیت این مدل پیش از پژوهش محقق وجود نداشته و محقق بر اساس مصاحبه‌های صورت گرفته، اقدام به طراحی مدل خواهد نمود. مطابق شکل (۱) مدل لایه‌ای پژوهش ساندرز و همکاران (۲۰۱۶) به تبیین لایه‌های پژوهش از فلسفه تا تکنیک مورد استفاده پرداخته است.



شکل ۱. لایه‌های روش تحقیق حاضر بر اساس پیاز پژوهش ساندرز و همکاران (۲۰۱۶)

با توجه به ماهیت پژوهش که از نوع کسب شناخت یک پدیده است و محقق به دنبال فهم مدل کشف تقلب در صنعت بانکداری است، فلسفه پژوهش حاضر تفسیرگرایی است. رهیافت پژوهش حاضر رسیدن به یک شناخت واحد از پدیده کشف تقلب در پرداخت بانکی با استفاده از کسب شناخت‌های متعدد در ذهن مصاحبه شونده‌گان است. بدین ترتیب که از پیش یک مدل و مفهوم واحد پیرامون موضوع پژوهش وجود ندارد و محقق با استفاده از شناخت‌های کسب شده و تجمیع آنها، به یک شناخت واحد می‌رسد. چنین رهیافتی برای کسب شناخت، رهیافت استقرایی است. استراتژی اصلی در این پژوهش کیفی می‌باشد. تکنیک اصلی مورد استفاده در این پژوهش، مصاحبه است. مصاحبه در این پژوهش بر اساس پروتکل تایید شده توسط استاد راهنما و مشاور و با محوریت سؤالات اصلی پژوهش صورت خواهد گرفت. بصورت کلی مراحل مدل‌سازی در این پژوهش مطابق شکل (۲) خواهد بود.



شکل ۲. فلوچارت مراحل تحقیق برای رسیدن به مدل کشف تقلب

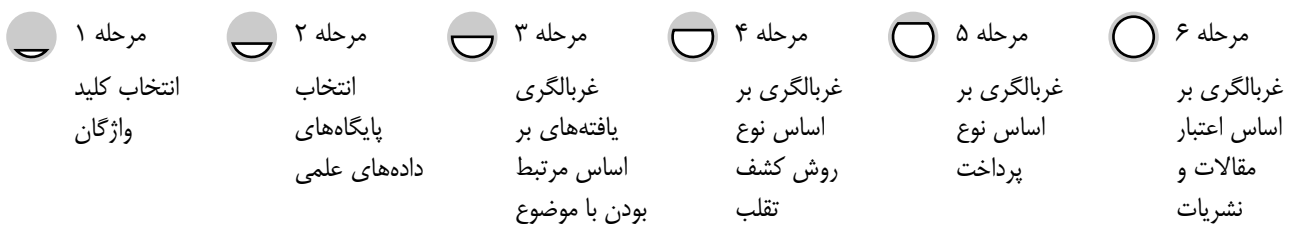
به منظور جمع آوری اطلاعات و داده‌های مورد نیاز از روش کتابخانه‌ای، مصاحبه و پرسشنامه استفاده شده است. ابتدا با استفاده از روش کتابخانه‌ای، چارچوب نظری و اولیه برای تدوین پروتکل مصاحبه استخراج شد. در بخش اول با استفاده از فراترکیب اطلاعات و یافته‌های استخراج شده از مطالعات کیفی دیگر با موضوع مرتبط و مشابه بررسی گردید. فراترکیب، مرور یکپارچه ادبیات کیفی موضوع مورد نظر و تجزیه و تحلیل داده‌های ثانویه و اصلی از مطالعات منتخب نیست، بلکه تحلیل یافته‌های این مطالعات است. به عبارتی، فراترکیب، ترکیب تفسیر تفسیرات داده‌های اصلی مطالعات منتخب است.

روش جمع آوری داده‌های مورد نیاز، مصاحبه‌های نیمه ساختار یافته بود. پروتکل مصاحبه بر اساس مدل طراحی شده در فراترکیب، تدوین گردید. در پایان به منظور بررسی و تایید و رتبه بندی ابعاد و مولفه‌های مدل از پرسشنامه برای جمع آوری داده‌های مورد نیاز استفاده شد.

### یافته‌ها

در این پژوهش به منظور انجام فراترکیب، از الگوی سه مرحله‌ای استفاده می‌شود. نخستین مرحله تنظیم سوال تحقیق در ارتباط با مرور ادبیات است. سوال اصلی پژوهش در این موضوع، تحلیل ابعاد مدل کشف تقلب در حوزه پرداخت با روبکرد بلاکچین است.

در مرحله دوم، مرور سیستماتیک ادبیات است. مدل تحقیق حاضر ابتدا با جمع و ترکیب عوامل موثر بر کشف تقلب در ادبیات شروع می‌شود. برای این منظور ابتدا مرور سیستماتیک ادبیات انجام می‌شود. در شکل (۳) مراحل انجام مرور سیستماتیک ادبیات در این پژوهش نشان داده شده است.



### شکل ۳. فرایند مرور سیستماتیک

بر اساس اهداف و سوالات تحقیق و همچنین مبانی نظری مرتبط با موضوع کشف تقلب، ۶ کلید واژه اصلی انتخاب شد. سپس کلید واژه‌های مدنظر، در ۱۰ پایگاه داده علمی جستجو شد. حاصل این جستجو، پیدا کردن ۳۷۴۲ مقاله مرتبط با کلید واژه‌ها می‌باشد. از آنجا که بسیاری از این مقالات در حوزه‌های نامرتبط بودند، در نهایت ۵۲ مقاله در غربالگری ادبیات پژوهش باقی ماندند. این مقالات بر اساس عوامل موثر در کشف تقلب، سال و نویسنده مورد بررسی قرار گرفتند. بر اساس مطالعه مقالات منتخب، در جدول (۱) عوامل شناسایی شده از منابع به همراه فراوانی ارجاعات گزارش شده است.

### جدول ۱. عوامل شناسایی شده از مقالات و مطالعات پیشین

فراوانی	پارامترهای تاثیرگذار در کشف تقلب	فراوانی	پارامترهای تاثیرگذار در کشف تقلب	فراوانی	پارامترهای تاثیرگذار در کشف تقلب
۱	تهیه اطلاعات کاربردی از فناوری‌های بروز	۳	خلاقیت و دانش مهندسان و نیروی انسانی	۱۱	پارامترهای تاثیرگذار در کشف تقلب فراوانی
۳	مدیریت پژوهش و توسعه	۲	توانمندی کارکنان	۲	پیچیدگی تکنولوژی
۵	مدیریت پیاده سازی فناوری	۲	نوع و کیفیت نیروهای متخصص	۱	سرمایه بر بودن تکنولوژی
۱۲	حساسیت زمانی	۴	آموزش منابع انسانی	۴	میزان اتوماسیون
۶	توسعه اقتصادی	۱	پذیرش فناوری در سازمان	۳	هزینه تکنولوژی
					هزینه و نیازهای نگهداری از تکنولوژی

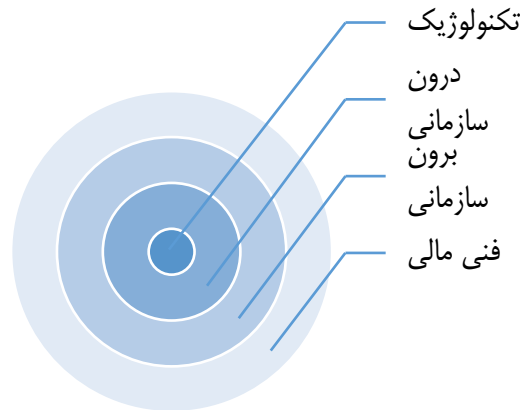
## دهقانی و همکاران

۴	ارزش افزوده تکنولوژی	۱۱	فرهنگ سازمانی	۳	حسابرسی داخلی
۳	موقعیت چرخه عمر تکنولوژی	۱	ظرفیت پیاده سازی	۳	اعلام مراجع قانونی
۳	زمان عرضه تکنولوژی	۱	روش پیاده سازی	۱۲	حسابرسی مستقل
۱	مدت استقرار تکنولوژی	۱	جایگاه فناوری مرتبط در ساختار فنی سازمان	۱	تهدیدهای تصادفی در مقابل تهدیدهای عمدی (برحسب قصد و نیت فرد مرتکب شونده)
۳	عمر تکنولوژی	۱۱	زیرساختها	۲	تهدیدهای انسانی در مقابل تهدیدهای غیرانسانی (برحسب عامل ایجادکننده)
۱	سرعت تحولات تکنولوژی	۳	ظرفیت انتقال دانش فنی	۲	تهدیدهای درون سازمانی
۲	دانش فنی و اطلاعات اسنادی مورد نیاز	۷	زیرساختهای اطلاعاتی و ارتباطاتی	۳	عوامل خطر مرتبط با تهدیدهای امنیتی
۲	تواناییهای مهارتی مورد نیاز	۱	میزان و تعداد فعالیت‌های مشکوک	۳	وضعیت حساب‌های مالی مشتریان
۱	کاربست فناوری و ملزومات آن در محیط پیاده سازی	۱۳	رقابت و تراکم رقبا در داخل و خارج	۱	حجم روزانه مبادلات مالی
۱	مطابقت فناوری با شرایط جغرافیایی	۱	موقعیت استراتژیک سازمان مالی اجرا کننده	۱	حجم میانگین هر تراکنش
۱	اهمیت رعایت استانداردهای حفاظتی و امنیتی	۱۱	تجهیزات و ابزار فنی	۱	تعداد تراکنشها
۲	استقبال از تغییر در میان مدیران	۱	امکانات ارتباطی میان بخش‌های سازمان مالی اجرا کننده	۱	بستر انجام تراکنشها
۱	تمایل به کارآفرینی در میان مدیران	۴	ارتباطات فنی با سایر سازمانها	۱	عوامل خطر مرتبط با ویژگی‌های عملیاتی
۲	به روز بودن مدیران	۱	همسویی با اهداف ملی	۱	عوامل خطر مرتبط با ویژگی‌ها و نفوذ مدیران
۳	دانش و تخصص مدیران	۱	همسویی با اهداف اجتماعی	۱	عوامل خطر مرتبط با شرایط بازار و صنعت
۳	آگاهی مدیران از فناوری‌های نوظهور	۱	همسویی با فرهنگ جامعه	۱	عوامل خطر مرتبط با تبعیت مدیران بانکها از کنترل‌های داخلی و استانداردهای لازم-الاجرا
۱	مراکز تحقیقاتی درون سازمان مالی اجرا کننده	۲	حساسیت عمومی نسبت به موضوع	۱	معافیت‌های مالیاتی
۱	مراکز تحقیقاتی دانشگاهی	۷	تأمین مالی فناوری و تصمیم‌گیری مالی	۲	حذف تعرفه‌های گمرکی و عوارض
۲	شهرک‌های تحقیقاتی و پارک‌های فناوری	۲	میزان دسترسی به منابع مالی (ارزی) موردنیاز	۵	تسهیلات قانونی
۱	همکاری‌های دولت - صنعت- دانشگاه	۱	هزینه‌های فناورانه	۳	الزامات اجباری (مانند رویه‌های صدور گواهی‌نامه‌های امنیتی)
۲	تخصیص بودجه به واردات فناوری	۷	مؤسسات تحقیق و توسعه	۳	اشتراک اطلاعات
۱	معافیت‌های مالیاتی	۲	حذف تعرفه‌های گمرکی و عوارض	۱	پایگاه داده یکپارچه
۱	تدوین، تصویب و نظارت بر اجرای سیاست‌های جامع علوم و فناوری	۱	پیش‌بینی مستمر تحولات فناورانه جهانی	۴	فناوری اطلاعات و ارتباطات
		۱	تعیین ضوابط انتخاب فناوری مناسب توسط سازمان مالی اجرا کننده یا نهادهای سطح بالاتر	۱	رصد فناوری

در گام بعدی فرایند فراترکیب، تجزیه و تحلیل یافته‌های کیفی مدنظر است. در این گام کدهای شناسایی شده از منابع که پیش از این استخراج و فراوانی آن‌ها مورد بررسی قرار گرفت، دسته بندی می‌شوند و در قالب مفاهیم و مقوله‌هایی تجمیع می‌شوند. مبنای دسته بندی کدها، بر حسب میزان تشابه کدها با یکدیگر است. بدین ترتیب که کدهایی

که از ترکیب و تلفیق آن‌ها یک مفهوم انتزاعی مشترک ایجاد می‌شود در یک دسته قرار گرفته و نامگذاری روی آن‌ها صورت گرفت. به همین ترتیب از ترکیب مفاهیمی که نزدیک به یکدیگر بود، مقوله‌هایی شکل گرفت. این دسته بندی بر مبنای درک و شهود پژوهشگر صورت داده است. همچنین نامگذاری مفاهیم و مقوله‌ها نیز بر اساس سلیقه پژوهشگر و بر مبنای مطالعات صورت گرفته روی داد.

مقوله‌های مدل در چهار سطح تکنولوژی به عنوان قلب و مرکز هسته کشف تقلب در حوزه پرداخت با رویکرد بلاکچین قرار می‌گیرد. سپس لایه عوامل درون سازمانی قرار دارد که کشف تقلب را انجام می‌دهند. در لایه بالاتر سطح عوامل برون سازمانی قرار دارد. در بیرونی‌ترین سطح، لایه عوامل فنی مالی مطرح می‌شود. این مدل کلی پژوهش بصورت یک مدل ۴ لایه‌ای در شکل (۴) نشان داده شده است. همچنین این چهار مقوله به همراه مفاهیم استخراج شده در شکل (۵) نمایش داده شده است.



شکل ۴. مدل چهار لایه‌ای استخراج شده از فراترکیب

جامعه خبرگان در مصاحبه‌ها متشکل از خبرگان حوزه پرداخت، رویکرد بلاکچین و بانکداری ایران است. در واقع این افراد توانمندی درک، فهم و ارائه نظر در مورد فرایند کشف تقلب در حوزه پرداخت با رویکرد بلاکچین در بانکداری ایران را داشتند. در این رویکرد با استفاده از معیارهایی که برای تعریف خبره‌ها بیان شد به انتخاب خبره‌ها پرداخته شد. تعداد افرادی که باید مورد مصاحبه قرار گیرند از ابتدا مشخص نبود و مصاحبه‌ها تا رسیدن به اشباع نظری ادامه یافت. در نهایت پس از انجام مصاحبه‌ها، اشباع پذیری تا مصاحبه دهم انجام شد و بدین ترتیب ۱۰ مصاحبه در این پژوهش صورت گرفت.

در گام بعدی طراحی مدل، کدگذاری مصاحبه‌ها انجام می‌شود. بدین ترتیب که مصاحبه‌های صورت گرفته با ۱۰ خبره انجام شده و سپس هر جمله از مصاحبه‌ها مطالعه شده و در ادامه کدهای اولیه استخراج می‌شود. برای محاسبه پایایی مصاحبه در همین مرحله کدگذاری باز، با روش توافق درونی کدگذار همکار، از دو محقق همکار که آشنایی کامل به نظریه داده بنیاد داشتند درخواست شد تا به عنوان همکار پژوهش، در این پژوهش مشارکت نموده و فرایند استخراج مفاهیم و کدهای باز را مجدداً انجام دهند. کدگذاری اول در اختیار محقق همکار اول و کدگذاری مصاحبه هشتم در اختیار محقق همکار دوم قرار داده شد. نتایج به دست آمده از کدگذاری و نتیجه توافق درونی بر اساس فرمول زیر، به شرح جدول می‌باشد:

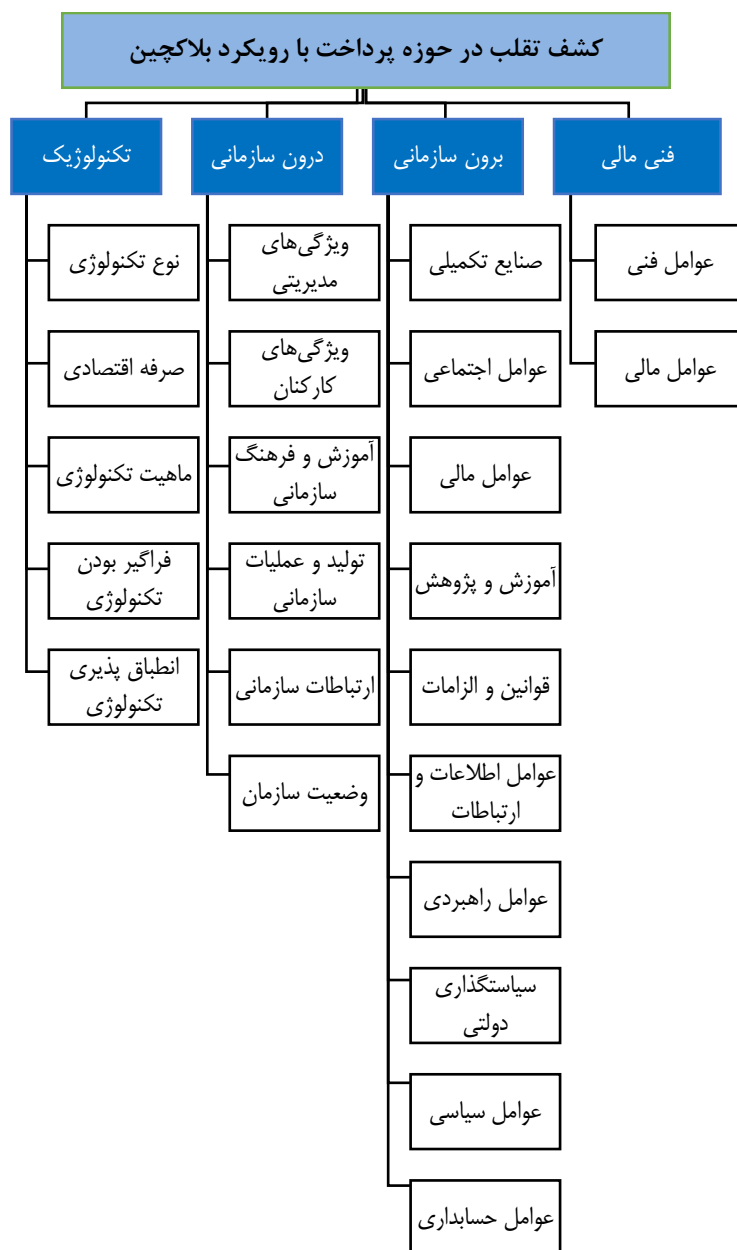
فرمول توافق درونی:

$$100 \times \frac{\text{تعداد توافق}}{\text{تعداد کل کدها}}$$

جدول ۲. نتایج محاسبه پایایی بین کدگذاران همکار

ردیف	کدگذار	شماره مصاحبه	تعداد کل کدها	تعداد توافقات	درصد پایایی توافق درونی
۱	همکار پژوهشی اول	۱	۴۲	۳۵	۸۳٪
۲	همکار پژوهشی دوم	۸	۲۷	۲۲	۸۱٪

همانطور که در جدول فوق مشاهده می‌شود، توافق درونی در کدگذاری اول ۸۳ درصد و در کدگذاری دوم ۸۱ درصد است که با توجه به حد قابل قبول ۶۰ درصد برای پایایی، می‌توان نتیجه گرفت که پایایی کدگذاری قابل قبول می‌باشد.



شکل ۵. مدل ابعاد و مولفه‌های اصلی استخراج شده از فراترکیب

با مشخص شدن مقوله‌های اصلی و مفاهیم از کدهای استخراج شده، جداول نهایی و مدل پژوهش در ادامه ارائه شده است. این مدل بر اساس ابعاد و مولفه‌های شناسایی شده طراحی گردید و روابط بین عوامل نیز بر اساس روابط منطقی طراحی شد.

در مدل برخاسته از ادبیات تحقیق که با رویکرد فراترکیب بوده است، مجموعه عوامل موثر بر کشف تقلب در چهار دسته اصلی عوامل تکنولوژیک، عوامل درون سازمانی و برون سازمانی و عوامل فنی مالی قرار می‌گیرد. این عوامل در شکل ۴-۶ قابل مشاهده می‌باشد. همچنین بر مبنای عوامل مستخرج از نظرات خبرگان عمده عوامل بدست آمده از ادبیات تحقیق، در نظرات خبرگانی که در طی فرآیند پژوهش مورد مصاحبه قرار گرفتند نیز وجود دارد و لذا در مدل طراحی شده قابل مشاهده است، انعکاس یافته است. در شکل (۶) مدل نهایی کشف تقلب در حوزه پرداخت با رویکرد بلاکچین مشاهده می‌شود.



کشف تقلب در چهار دسته اصلی شامل عوامل تکنولوژیک، عوامل درون‌سازمانی، عوامل برون‌سازمانی و عوامل فنی-مالی طبقه‌بندی می‌شوند. این دسته‌بندی هم‌راستا با یافته‌های پژوهش‌های بین‌المللی است که بر نقش چندبعدی فناوری بلاکچین در کاهش تقلب، افزایش شفافیت و بهبود اعتماد تأکید دارند (Motie & Raahemi, 2024).

فناوری بلاکچین، با ایجاد زنجیره‌ای از تراکنش‌های رمزنگاری‌شده و غیرقابل‌تغییر، باعث ارتقای امنیت داده‌ها و حذف نیاز به نهادهای واسطه در فرآیندهای مالی می‌شود (Kumar et al., 2024). یافته‌های حاضر نیز نشان داد که استفاده از بلاکچین می‌تواند احتمال وقوع تقلب‌های رایج در تراکنش‌های بانکی نظیر جعل، پرداخت‌های تکراری و تغییر در سوابق حسابداری را به شکل چشمگیری کاهش دهد. در همین راستا، پژوهش اسپایخیگر و همکاران (۲۰۲۳) با تمرکز بر سازمان‌های خودگردان غیرمتمرکز، بیان داشتند که ساختارهای مبتنی بر بلاکچین قادرند جریان تصمیم‌گیری را شفاف‌تر کرده و از رفتارهای فرصت‌طلبانه در سازمان‌ها جلوگیری کنند (Spychiger et al., 2023).

در حوزه عوامل تکنولوژیک، نتایج مصاحبه‌های کیفی نشان داد که پیچیدگی فناوری، سطح دانش مهندسی و زیرساخت‌های فنی موجود از جمله مهم‌ترین موانع پیاده‌سازی مؤثر بلاکچین در بانک‌هاست. این یافته با نتایج مطالعه لیو و لی (۲۰۲۲) هم‌خوانی دارد که مدل CFLedger را به عنوان راهکاری برای پیشگیری از تقلب در پرداخت‌های برگشتی معرفی کردند و تأکید داشتند که موفقیت این سیستم منوط به توانایی سازمان در یکپارچه‌سازی زیرساخت‌های فنی است (Liu & Lee, 2022). همچنین، بتی‌نی دی میراندا و همکاران (۲۰۲۴) در پژوهش خود به نقش بلاکچین در همکاری‌های بین‌سازمانی اشاره کردند و نتیجه گرفتند که پیاده‌سازی مؤثر آن مستلزم زیرساخت‌های اطلاعاتی قدرتمند و نظام رمزنگاری پیشرفته است (Bettini de Miranda et al., 2024).

در بخش عوامل درون‌سازمانی، تحلیل مضمون نشان داد که فرهنگ سازمانی، مدیریت منابع انسانی و میزان آگاهی مدیران از فناوری‌های نوظهور در پذیرش فناوری بلاکچین نقش تعیین‌کننده دارند. همان‌گونه که فیتریانو و همکاران (۲۰۲۴) اشاره کردند، ضعف در شفافیت داخلی و عدم هم‌راستایی میان کارکنان و مدیران از عوامل اصلی بروز تقلب در بانک‌هاست (Fitriana et al., 2024). بر این اساس، آموزش نیروی انسانی و ارتقای سواد دیجیتال در سطوح مختلف سازمان می‌تواند از بروز خطاهای انسانی و رفتارهای متقلبانانه جلوگیری کند. یافته‌های پژوهش حاضر نیز نشان داد که بانک‌هایی که در مسیر دیجیتالی شدن و آموزش کارکنان گام برداشته‌اند، نرخ کمتری از تخلفات مالی را تجربه می‌کنند.

عوامل برون‌سازمانی شامل سیاست‌های اقتصادی، مقررات نظارتی، انتقال فناوری و شرایط سیاسی نیز از دیگر ابعاد مهم مدل محسوب می‌شوند. نتایج نشان داد که هرگونه تغییر در قوانین و سیاست‌های کلان اقتصادی می‌تواند بر نحوه پیاده‌سازی فناوری بلاکچین اثرگذار باشد. این نتیجه با یافته‌های سپانلو و همکاران (۲۰۱۹) هم‌راستا است که در مدل پیشنهادی خود برای صدور اعتبارات اسنادی، بر ضرورت هماهنگی میان چارچوب‌های قانونی و فناوری‌های جدید تأکید کردند (Sepanloo et al., 2019). به‌طور مشابه، آکین‌بووال و همکاران (۲۰۲۴) در پژوهشی در صنعت بانکداری آفریقای جنوبی نشان دادند که ضعف در هماهنگی میان نهادهای نظارتی و بانک‌ها، زمینه‌ساز گسترش تقلب‌های سایبری و ناکارآمدی در مدیریت ریسک است (Akinbowale et al., 2024).

در بعد فنی و مالی، نتایج نشان داد که عوامل مرتبط با ظرفیت مالی سازمان، هزینه پیاده‌سازی، و توانایی حسابرسی داده‌ها از مؤلفه‌های کلیدی موفقیت در اجرای سیستم‌های مبتنی بر بلاکچین هستند. در همین راستا، ماختانی (۲۰۲۲) به این نتیجه رسید که فناوری بلاکچین می‌تواند فرآیندهای حسابداری را با کاهش نیاز به میانجی‌ها و افزایش قابلیت حسابرسی خودکار دگرگون کند (Mahtani, 2022). یافته‌های مشابهی نیز در پژوهش سالیمی (۲۰۲۳) گزارش شده است که نشان می‌دهد بلاکچین باعث ارتقای شفافیت در گزارشگری مالی و کاهش فرصت‌های تقلب می‌شود (Salimi, 2023).

از منظر مفهومی، نتایج مدل حاضر حاکی از آن است که ترکیب فناوری بلاکچین با رویکردهای تحلیلی نوین نظیر شبکه‌های عصبی گرافی، دقت کشف تقلب را به شکل قابل توجهی افزایش می‌دهد. مطی و راهمی (۲۰۲۴) در مرور نظام‌مند خود بر تشخیص تقلب مالی مبتنی بر شبکه‌های گرافی نشان دادند که ادغام این شبکه‌ها با بلاکچین، موجب افزایش دقت پیش‌بینی و کاهش نرخ خطا در مدل‌های تشخیص تقلب می‌شود (Motie & Raahemi, 2024). بدین ترتیب، هم‌افزایی میان فناوری‌های داده‌محور و ساختارهای غیرمتمرکز بلاکچین می‌تواند تحولی بنیادی در رویکردهای امنیت مالی ایجاد کند.

از سوی دیگر، پژوهش حاضر نشان داد که اعتماد عمومی نسبت به فناوری‌های نوین مالی هنوز در سطح مطلوبی قرار ندارد و یکی از چالش‌های اساسی، مقاومت فرهنگی در برابر تغییر است. یافته‌های آمارشکاری و لطیفی (۲۰۱۷) نشان داد که اجرای فناوری بلاکچین در بانک‌های ایران مستلزم ایجاد فرهنگ اعتماد و آگاهی عمومی در میان کاربران و کارکنان است (Amirshakeri & Latifi, 2017). همچنین، نتایج مصاحبه‌های انجام‌شده در این پژوهش بیانگر آن است که بسیاری از مدیران بانکی با وجود آگاهی از مزایای بلاکچین، به دلیل نبود دستورالعمل‌های قانونی و زیرساختی از پیاده‌سازی آن اجتناب می‌کنند. این یافته با نتایج ژانگ و همکاران (۲۰۲۵) سازگار است که به ضرورت تدوین سیاست‌های حمایتی و چارچوب‌های اجرایی برای گسترش فناوری بلاکچین در زنجیره تأمین مالی اشاره کردند (Zhang et al., 2025).

در بعد بین‌المللی، استفاده از بلاکچین در حوزه دارایی‌های اسلامی و نظام‌های مالی شرعی نیز اهمیت یافته است. زامان و همکاران (۲۰۲۵) در پژوهش خود تأکید کردند که فناوری بلاکچین می‌تواند با فراهم کردن شفافیت و قابلیت پیگیری تراکنش‌ها، به تطابق بیشتر نظام مالی اسلامی با اصول شرعی کمک کند (Zaman et al., 2025). این دیدگاه نشان می‌دهد که کاربردهای بلاکچین نه تنها محدود به کشف تقلب نیست، بلکه می‌تواند نقش کلیدی در بازتعریف شفافیت و مشروعیت در نظام‌های مالی ایفا کند. در سطح خرد، پژوهش بنچاجی و همکاران (۲۰۱۸) نیز نشان داد که ترکیب الگوریتم‌های هوش مصنوعی با بلاکچین، دقت و سرعت تشخیص تقلب را افزایش می‌دهد و موجب کاهش هزینه‌های نظارتی در سیستم‌های بانکی می‌شود (Benchaji et al., 2018). نتایج پژوهش حاضر نیز تأیید می‌کند که استفاده از مدل‌های یادگیری عمیق و بلاکچین به صورت هم‌زمان، یکی از نوآورانه‌ترین مسیرها برای توسعه سامانه‌های هوشمند کشف تقلب در بانکداری دیجیتال است.

در نهایت، مدل نهایی پژوهش حاضر با یافته‌های پژوهش‌های پیشین درباره مزایای بلاکچین هم‌سو است. همان‌گونه که آرنا و همکاران (۲۰۲۴) اشاره کردند، بلاکچین نه تنها ابزار فنی بلکه سازوکار نهادی برای بازآفرینی شفافیت و اعتماد در اکوسیستم‌های مالی است (Arenal et al., 2024). بدین ترتیب، نتایج این پژوهش تأیید می‌کند که فناوری بلاکچین در تعامل با عوامل سازمانی و قانونی، می‌تواند به‌عنوان یک ابزار کلیدی در پیشگیری از تقلب‌های مالی در نظام بانکی ایران ایفای نقش کند.

پژوهش حاضر اگرچه مدلی جامع برای کشف تقلب در پرداخت‌های بانکی ارائه می‌دهد، اما با چند محدودیت همراه است. نخست، به دلیل ماهیت کیفی پژوهش و محدود بودن جامعه خبرگان به ۱۰ نفر، نتایج قابلیت تعمیم آماری ندارند. دوم، در برخی موارد محدودیت دسترسی به داده‌های دقیق بانکی و اطلاعات محرمانه، مانع از تحلیل عمیق‌تر برخی مؤلفه‌ها شد. همچنین، نوظهور بودن فناوری بلاکچین در نظام بانکی ایران باعث گردید برخی خبرگان فاقد تجربه عملی در این زمینه باشند که می‌تواند بر عمق تحلیل‌ها تأثیر گذاشته باشد.

پیشنهاد می‌شود در پژوهش‌های آینده، مدل ارائه‌شده با رویکردهای کمی نظیر مدل‌سازی معادلات ساختاری یا تحلیل مسیر مورد آزمون قرار گیرد تا روابط علی میان متغیرها با دقت بیشتری بررسی شود. همچنین، می‌توان تأثیر عوامل فرهنگی و رفتاری در پذیرش فناوری بلاکچین را در میان مدیران و کارکنان بانکی بررسی کرد. مطالعات تطبیقی میان کشورهای در حال توسعه و توسعه‌یافته نیز می‌تواند به شناخت الگوهای موفق انتقال فناوری در حوزه کشف تقلب کمک کند.

بانک‌ها و نهادهای مالی باید با سرمایه‌گذاری هدفمند در زیرساخت‌های فناوری، آموزش نیروی انسانی و اصلاح فرآیندهای مدیریتی، مقدمات اجرای گسترده بلاکچین را فراهم کنند. ایجاد چارچوب‌های قانونی شفاف، همکاری میان دولت، بخش خصوصی و مراکز پژوهشی، و تدوین سیاست‌های تشویقی برای استفاده از فناوری‌های غیرمتمرکز از دیگر اقدامات ضروری است. افزون بر این، فرهنگ‌سازی در میان مشتریان بانکی برای اعتماد به سامانه‌های مبتنی بر بلاکچین می‌تواند گامی مؤثر در جهت کاهش تقلب و ارتقای شفافیت در نظام بانکی کشور باشد.

## مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

## تشکر و قدردانی

از تمامی کسانی که در طی مراحل این پژوهش به ما یاری رساندند تشکر و قدردانی می‌گردد.

## تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافی وجود ندارد.

## حمایت مالی

این پژوهش حامی مالی نداشته است.

## موازن اخلاقی

در انجام این پژوهش تمامی موازن و اصول اخلاقی رعایت گردیده است.

## References

- Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2024). Analysis of cyberfraud in the South African banking industry: a multiple regression approach. *Journal of Financial Crime*, 31(4), 952-973. <https://doi.org/10.1108/JFC-04-2023-0094>
- Amirshakari, N., & Latifi, Z. (2017). The Role of Blockchain Technology in Facilitating the Know Your Customer (KYC) Process in the Banking Industry. Seventh National Conference on Electronic Banking and Payment Systems, Tehran, Iran.
- Arenal, A., Armuna, C., Ramos, S., Feijoo, C., & Aguado, J. M. (2024). Digital transformation, blockchain, and the music industry: A review from the perspective of performers' collective management organizations. *Telecommunications Policy*, 48(8), 102817. <https://doi.org/10.1016/j.telpol.2024.102817>
- Benchajji, I., Douzi, S., & Ouahidi, B. E. (2018). Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection. International Conference on Advanced Information Technology, Services and Systems, [https://doi.org/10.1007/978-3-030-11914-0\\_24](https://doi.org/10.1007/978-3-030-11914-0_24)
- Bettini de Miranda, L. M., Garcia, R. D., Ramachandran, G. S., Ueyama, J., & Müller Guerrini, F. (2024). Blockchain in inter-organizational collaboration: A privacy-preserving voting system for collective decision-making. *Journal of Information Security and Applications*, 85, 103837. <https://doi.org/10.1016/j.jisa.2024.103837>
- Fitriana, L., Sinarasri, A., & Nurcahyono, N. (2024). Factors Affecting Financial Statement Fraud in Banking Sector: A Agency Perspective. *Maksimum*, 14(1), 102. <https://doi.org/10.26714/mki.14.1.2024.102-113>
- Hamidi, H., & Karbasian, M. (2024). Presenting a model to detect the fraud in banking using smart enabling tools: Case Study One of the State banks of Iran. *International Journal of Engineering*, 37(3), 529-537.
- Huang, C., Wang, W., Liu, D., & Lu, R. (2023). Blockchain-Assisted Personalized Car Insurance With Privacy Preservation and Fraud Resistance. *Ieee Transactions on Vehicular Technology*, 72(3), 3777-3792. <https://doi.org/10.1109/tvt.2022.3215811>
- Johansen, S. (2017). *Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation*. Mannheim University, Department of Information Systems, Copenhagen.
- Kumar, S., Rani, N., & Upadhyay, P. (2024). Towards novel blockchain decentralised autonomous organisation (DAO) led corporate governance framework. *Technological Forecasting and Social Change*, 204. <https://doi.org/10.1016/j.techfore.2024.123417>
- Liu, D., & Lee, J.-H. (2022). CFLedger: Preventing chargeback fraud with blockchain. *Ict Express*, 8(3), 352-356. <https://doi.org/10.1016/j.ict.2021.06.001>
- Mahtani, U. (2022). Fraudulent practices and blockchain accounting systems. *Journal of Accounting, Ethics and Public Policy*, 23(1), 97-148. <https://doi.org/10.60154/jaapp.2022.v23n1p97>
- Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, 240, 122156. <https://doi.org/10.1016/j.eswa.2023.122156>
- Salimi, R. (2023). The Impact of Blockchain on Transparency and Fraud Reduction in Financial Reports. *Quarterly Journal of Accounting and Financial Research*, 9(3), 75-90.
- Sepanloo, H., Esmaeili, V., & Narenji, M. (2019). A blockChain- based approach towards overcoming fraud in issuing letter of credit. Electronic Banking and payment systems conference, Tehran, Iran.
- Spychiger, F., Lustenberger, M., Martignoni, J., Schädler, L., & Lehner, P. (2023). Organizing projects with blockchain through a decentralized autonomous organization. *Project Leadership and Society*, 4, 100102. <https://doi.org/10.1016/j.plas.2023.100102>
- Zaman, A., Tlemsani, I., Matthews, R., & Mohamed Hashim, M. A. (2025). Assessing the potential of blockchain technology for Islamic crypto assets. *Competitiveness Review: An International Business Journal*, 35(2), 229-250. <https://doi.org/10.1108/CR-05-2023-0100>
- Zhang, X., Zhang, Y., Liu, X., & Wang, R. (2025). Blockchain-Based Intelligent Risk Management Decision Support System for Supply Chain Financing. *International Journal of Intelligent Information Technologies (IJIT)*, 21(1), 1-24. <https://doi.org/10.4018/IJIT.369153>