International Academic Institute for Science and Technology

International Academic Journal of Economics
Vol. 13, No. 2, 2026, pp. 73-80.

ISSN 2454-2474

International Academic Journal of Economics

www.iaiest.com

Blockchain-Based Financial Regulation for Enhancing Transparency and Economic Security

Pieter De Vries [a], Sophie Van Dijk [b]

[a] *Dutch Institute for Circular Innovation Research, Eindhoven, Netherlands.*
[b] *Dutch Institute for Circular Innovation Research, Eindhoven, Netherlands.*

Abstract

Conventional financial auditing is based on periodic and sample-based audits, which can only identify irregularities after already occurred. This paper suggests a framework based on blockchain for continuous auditing, where both the transaction data, risk scores, and enforcement triggers are recorded on a blockchain that is cryptographically secure. The algorithm for evaluating the risk of each transaction is implemented by a smart contract and raises an alert in the event of an abnormal transaction, liquidity stress, or unauthorized asset transfer automatically as the transaction is recorded. The framework is tested on a simulated ledger with 200,000 transactions with three baselines: periodic manual audit, rule-based monitor, and an off-chain isolation forest. The proposed model achieves a precision of 94.2%, a recall of 91.5%, and an F1 score of 92.8%, with a latency of less than 250ms per transaction at 1,000 transactions per second. The paper concludes with some guidance for risk officers, internal auditors, and compliance units.

Keywords: Blockchain, Continuous Auditing, Financial Regulation, Risk Scoring, Transparency, Economic Security.

DOI: 10.71086/IAJE/V13I2/IAJE1315
Received: 17 March 2026/Revised: 25 April 2026/Accepted: 21 May 2026/Published: 30 June 2026

Introduction

The integrity of the record system of who owns what and who moved what to whom is critical to the financial systems. For decades, this assurance has been provided after the reporting period by sampling a portion of the transactions, testing them, and giving the auditor's opinion. Assurance over these records has been provided for decades with the ex-post approach: that is, an auditor samples a subset of transactions after the reporting period, tests them, and gives an opinion. This type has three disadvantages in construction. In most transactions, sampling is used to look at a subset of transactions. Losses can be compounded over time as there is a delay between the irregularity and the discovery of it. Trust between regulators, firms and the public can be undermined by inconsistent records held in separate institution-controlled databases that can be changed and/or inconsistently reconciled.

There is an alternative kind of assurance on blockchain technology. Tasks are recorded in cryptographically linked blocks in a distributed ledger, which are validated using consensus, meaning that if the blocks are changed in later transactions, this will be visible to all participants. According to Kukman and Gričar, the design not only improves security but enhances the system's efficiency and transparency as well (Kukman & Gričar, 2025). The systematic review by Bhandari et al. on Sustainable Finance shows that blockchain can enhance transparency and accountability in the financial system by providing traceability and tamper resistance of financial information (Bhandari et al., 2025). In financial accounting, Almadadha demonstrates that the use of ledger-based accounting systems enhances security and facilitates more accurate accounting, such as environmental, social, and governance reports (Almadadha, 2024).

Transparency is not enough to make a system secure; it's also necessary to have governance. Mustafa et al., (2025) suggest a legal, technical, ethical, and security-based governance model for e-government, while highlighting the need to have rules in the institution that make it accountable in the presence of technical immutability. Prokopenko et al. report the evolution of financial accounting with blockchain, ranging from its recording to verification, and highlight that blockchain adoption comes with the need for standardization and professionals' readiness (Prokopenko et al., 2024). In the intersection of blockchain and AI, Shi and Wang further explore the most recent trend of leveraging analytics and automation to convert the stored information into decisions (Shi & Wang, 2025).

This limitation forms the basis of how most scholarly works consider the distributed ledger to be an immutable database for verification purposes, separating the transaction recording process from the threat detection function. The traditional systems are limited by having the risk management functionalities separated from the core transactional system; risk analytics is done on the outside and post-committal, hence causing inherent latency in the operations of the banks. What this means is that whereas a tamper-resistant audit trail will be established, any fraud, liquidity bleeding, or transfer of funds will continue unabated in the meantime. It, therefore, becomes imperative to close this architectural gap by integrating intelligent scoring mechanisms within the ledger state transition logic.

This study aims to fill that gap. It aims to create and test a continuous audit system where the record is kept in a blockchain, and the enforcement is carried out through the blockchain. The primary contributions include a conceptual framework of blockchain-anchored continuous auditing, a risk-scoring algorithm, and an automatic triggering system, as well as a comparison of the risks a blockchain-based continuous audit poses to conventional baselines. The rest of this paper is organized as follows. The conceptual model is presented in Section II, the algorithm and experimental set-up in Section III, results in Section IV, managerial implications in Section V, and the conclusions in Section VI.

Conceptual Model of Continuous Auditing

From Periodic Audits to Continuous Assurance

The evidence in the traditional audit cycle is gathered over a period of time, and assurance is a statement that takes a look at a previous time. Assurance is generated during the business process in continuous auditing. All transactions are recorded, verified, and assessed as happen, and the auditor is no longer an evidence collector but a supervisor of a monitoring system. This is where a blockchain fits in, as the record is already time-stamped, ordered, and shared with authorized parties. Zhu et al. review the circulation of blockchain-based digital assets and demonstrate that movement of assets on a blockchain network is both traceable and verifiable, and that distributed ledgers present open challenges on scalability and interoperability (Zhu et al., 2024).

This is the same thing that happens in very different areas. Wei and Zhang demonstrate the process of modeling a digital transaction with a blockchain along an industry chain and the resulting reduction in the effort of reconciliation between industry participants (Wei & Zhang, 2025). Dashkevich et al. suggest blockchain financial statements in which the reporting and liquidity information is generated directly based on the activity on the ledger and not put together later (Dashkevich et al., 2024). Saeedi presents an example of a blockchain-based loyalty program for

providing incentives to households to recycle, where the program's records are transparent and programmable, and can be audited by any program member (Saeedi, 2024). The cases have something in common: that are not only databases but also a location for rules to be executed.

Verification and State Transitions

The basis of the conceptual model depends entirely on the relationship between cryptographic hashing and block validation in order to achieve total data integrity. Through the process of generating a fixed digital fingerprint from every single transaction made, the model creates a sequence of blocks that are connected via embedding the hash value of the previous block in each new one. Any alteration of the records would change its digital fingerprint, resulting in the disruption of the entire cryptographic chain in the process. In addition to that, network validators check every transaction submitted to the system before reaching consensus by validating it as well as verifying user authorization and transaction validity.

From the foundations of secure transactions, the protocol utilizes the concept of the ledger as a state machine that reflects precisely the current balances and obligations. In this paradigm, each transaction corresponds to a particular transition between two valid states, which ensures the consistency of the whole system's accounting. Importantly, compliance with deterministic rules becomes an integral part of the state transition and not an after-the-fact action. Should a particular transaction be inconsistent with the established protocols—e.g., an unauthorized asset transfer and exceeding certain balance limits—it will be stopped by the system before any changes in the state of the ledger take place.

Privacy and Access Control

For compliance with stringent data protection requirements (like GDPR) while at the same time not hindering regulatory supervision, a strict segregation is made between the storage of data and cryptographic validation of the transactions. Personally Identifiable Information (PII), transaction data, and the actual account balances are intentionally stored off the chain on highly secured and encrypted institutional databases or permissioned nodes, whereas only cryptographic hashes, calculated risk scores, and trigger events are stored on the blockchain. In this way, it becomes possible for the internal auditor, automated smart contracts, and external supervisors to check the correctness of every transaction through cryptographically validating the transactions without having access to any of the raw customer data. The approach prevents any kind of single point of failure as far as data leaks are concerned while ensuring full transparency in the auditing procedure.

On the basis of the proposed hybrid architecture, complex cryptographic tools and fine-grained access management techniques may be employed in order to strengthen the protection of confidentiality. As was shown by Kulkarni et al., blockchain-based access control and decentralized KYC systems allow financial institutions to cryptographically validate users' identities and authorization levels without disclosing any private credentials to the rest of the network. In a similar way, implementation of cryptographic techniques including zero knowledge proofs (ZKP) would allow the initiator of a transaction to validate its compliance with certain requirements such as meeting liquidity standards or AML requirements without revealing details of the particular transaction or its recipient. Access to decrypted off-chain layers is tightly controlled via role-based access control (RBAC) lists in permissioned channels in such a way that only authorized compliance officers and regulatory nodes are able to access the protected information if there is an automated trigger or exceptionally high-risk score.

The Audit Cycle

Continuous audit works like a closed system which revolves around a static audit ledger where all the transactions coming in are registered sequentially, then get hashed and verified by the network validators. The verified transactions are then automatically scored through a smart contract and fed to the trigger engine which is programmed to either generate compliance alerts or automatically freeze a transaction if the score meets a certain threshold. The results of this continuous process are then shown on special dashboards for the internal auditors as well as external regulators. The information obtained from such monitoring periods is used to dynamically change risk thresholds for the next operational period.

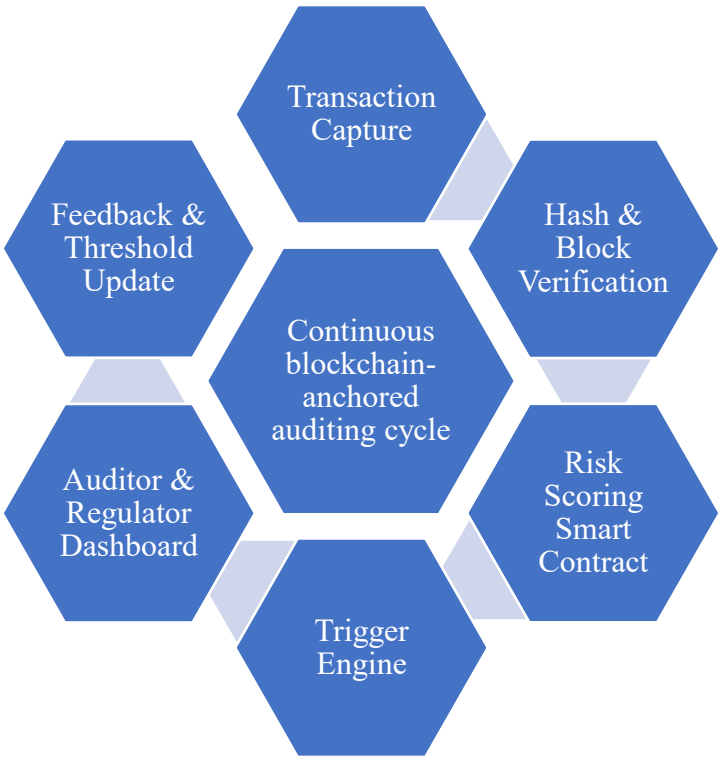


Fig: 1: Conceptual Model of the Continuous Blockchain-Anchored Auditing Cycle

In fig. 1 above, the audit ledger serves as the immutable core and a single source of truth that all other operational stages continuously read and write to. Surrounding the audit ledger are six separate stages that are interlinked using directional arrows, depicting that auditing is not a periodic or retrospective process, but a continuous one. In the course of transactions through this system, hashes are generated, blocks validated, risk scores determined using smart contracts, and automated triggers analyzed for anomaly, liquidity problems or fraudulent transfers. The process ends with a crucial feedback loop in the last stage where new thresholds of risks discovered get fed back to the first stage of profiling and recording of risks. Through such a dynamic feedback process, the system self-calibrates enabling the compliance team and smart contracts to respond in real time to any financial risks.

Algorithmic Framework and Risk Scoring Model

Design of the Risk-Scoring Algorithm

The risk scoring algorithm works in the form of an automated and deterministic smart contract placed directly on the blockchain and executed deterministically for each incoming transaction prior to its state confirmation. At the moment of submission, the smart contract computes the specified list of dynamic feature vectors, namely, the normalized transaction value in relation to the variance of the spending history of the account, short-term burst factor based on the frequency of recent transactions, reputation and flag history of the counterpart prior to the transaction, the temporal anomaly factor based on the hour of the day, and the impact of the transfer on the liquidity buffer of the account. All the features are compared to the dynamically adjusted baseline that represents the expected behavioral pattern of the specific account as well as its peers. The contextual deviation of all the features is computed, aggregated through a weighted vector transformation, and mapped to the continuous risk score ranging from 0 to 1.

To ensure auditability and to avoid any potential post-hoc tampering with the logic, all behavioral profiles, weights, and normalization factors are saved directly on the blockchain. Such design allows to build a completely deterministic environment: each regulator, internal auditor or automated node could re-run the smart contract code based on its history in order to re-calculate and re-verify any produced risk score. Storing risk assessment logic on-chain also protects the system from the adversarial nodes bypassing the risk assessment step since the state changes could not be verified by the consensus nodes without passing the execution of the smart contract code. With such approach, risk assessment is made on-chain instead of off-chain and the auditability trail becomes unchangeable and mathematically verifiable.

Automated Triggers

Trigger engine acts as a central component that provides an operational link between risk scoring process and regulation enforcement in real-time, systematically converting quantitative risk assessment into operational deterministic decisions, which fall under three main operational categories. First, anomaly trigger acts as a persistent monitoring tool: every time when the risk score of a certain transaction exceeds the pre-defined threshold level, the system automatically alerts the compliance department of the particular transaction with its contextual attributes for further manual investigation. At the same time, the liquidity trigger analyzes overall balance sheet stability by assessing whether an incoming asset transfer represents a threat to liquidity levels in the pool and therefore notifies the management about the problem before a liquidity crisis occurs and allows balance sheet adjustments to be made. Unauthorized transfer trigger strictly controls cryptographic access control by verifying the permissions of the initiator of a transaction regarding both asset type and volume.

To facilitate seamless implementation without compromising efficiency, the model utilizes a two-tier calibration system that is determined by the minimum and maximum boundaries. The minimum boundary is calibrated to issue low friction alerts as well as move the flagged transactions to the dashboard of analysts, all while keeping the operational workflow intact. On the other hand, the maximum boundary is calibrated solely for the purpose of dealing with severe breaches and issuing automatic escrow isolation. With punitive measures reserved only for the most certain cases of policy breaches, the two-tiered calibration system prevents any disruption of operations, limits unnecessary interventions, and allows the compliance team to focus on challenging cases.

Experimental Configuration

To create a controlled setting that would facilitate an accurate evaluation of the suggested continuous auditing approach, the experiment was set up in a simulated permissioned blockchain network. In order to counterbalance the obvious lack of fully labeled public data on financial fraud, a starting dataset of 200,000 artificial transactions carried out by 5,000 different users was created. As a result, the researchers had full control over the ground-truth labels needed for proper validation. 2% of transactions (4,000) in the whole dataset represented deliberate anomalies, which were divided into three different types of threat: severe imbalance between balance and value (transactions with unusual values), sudden spikes of transactions (high-frequency submissions), and balance or routing violation (illegal transactions).

For statistical soundness and to avoid data leakage in the testing phase, the 200,000-transaction database was split in the usual 70/30 ratio. The first group of 140,000 transactions served to create behavioral baselines, fine-tune dynamic feature vectors, and calibrate spending parameters per each account. The rest 60,000 transactions were saved only for hold-out testing in order to check real-time execution efficiency. With such an arrangement in a simulated permissioned ledger environment, the test provided an ability to measure the smart contract latency, threshold sensitivity, and transaction execution in controlled synthetic conditions before the comparison with the audit baselines.

Experimental Results and Risk Mitigation Performance

Detection Quality

In analyzing the detection effectiveness of the four models as depicted in figure 2, some differences arise between the two types of processes. For instance, periodic manual audit is characterized with a fair level of precision, which stands at 88.0% due to careful inspection of the transactions that it inspects; however, it exhibits poor recall effectiveness because only few transactions get inspected, and hence, the recall effectiveness stands at 38.5%. On the other hand, the rule-based monitor shows a good level of recall effectiveness, which is 71.2%; however, it depicts poor precision effectiveness because of the large number of transactions that are flagged as legitimate despite being flagged.

Further, the off-chain isolation forest shows good results with better precision effectiveness of 84.1% and better recall effectiveness of 82.6%. Finally, the new on-chain scoring model emerges victorious with better results in all three parameters of analysis with a precision of 94.2%, a recall of 91.5% and an F1-score of 92.8%.

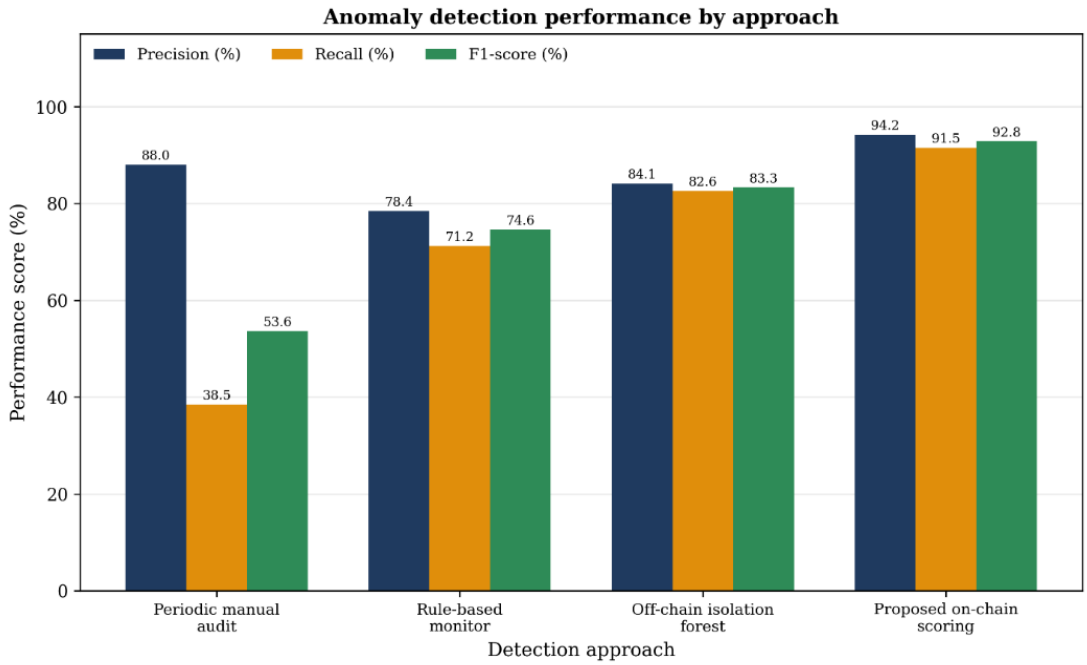


Fig. 2: Anomaly Detection Performance by Approach

Fig. 2 explains that the four detection approaches are listed on the horizontal axis, and the vertical axis is the score (%). There are 3 bars for each approach (precision, recall, and F1-score) that are labeled in the legend. The chart illustrates that the periodic audit has a significant difference between precision and recall, whereas the proposed model maintains high precision and high recall, and these measures are close to each other. This means that it will detect most anomalies and not trigger many false alarms.

The same trend can be seen for the false positive rate. The rate obtained by the rule-based monitor was 9.8%, and that of the isolation forest was 6.4%, whereas the proposed model obtained a rate of 2.1%. The periodic audit was conducted on a small percentage of transactions, with a rate of 1.9%, but only due to the nature of the audit. A low false positive rate is important to compliance teams as lose analyst resources on every false alarm and lose trust in the system when it happens.

Robustness Under Stress

The following stress scenarios were used. In the first, the percentage of transactions that would be considered as anomalies was increased from 2% to 8% to mimic a coordinated attack. Recall for the proposed model dropped by approximately 3 percentage points (from 91.5% to approximately 88.5%), and the recall of the rule-based monitor dropped by over 10 points. The second scenario involved a simulated emergency pull-out of funds to test the liquidity trigger. In repeated tests, the trigger gave the manager an early heads-up and was able to warn before the simulated reserve was depleted, thereby affording the manager an opportunity to act. The results indicate that the framework is slowly degraded instead of having a sudden drop under pressure, but the results are obtained from simulated data and could be verified by testing it with real data.

Managerial and Systemic Implications

The findings have practical implications for corporate risk officers, internal auditors, and financial compliance units. Corporate risk officers should treat the risk score as a dynamic monitoring indicator rather than a static reporting measure. Alert and hold thresholds should be defined carefully and reviewed periodically using investigation outcomes. Because the scoring logic is recorded on the ledger, officers can also provide boards and regulators with transparent justification for risk decisions.

Internal auditors can shift their focus from transaction re-performance toward evaluating monitoring features, threshold settings, and the treatment of flagged cases. The tamper-evident ledger supports broader population-level review and enables auditors to concentrate professional judgment on higher-risk areas. Prior research also indicates

that ledger-based reporting can influence the preparation and examination of accounting and liquidity information (Dashkevich et al., 2024).

Financial compliance units should adopt the system gradually. Initial deployment should emphasize monitoring and comparison with existing controls, followed by automated transaction holds only after false-positive rates become acceptable. Governance responsibilities for threshold changes, transaction approvals, and dispute resolution should be established in advance (Mustafa et al., 2025). Privacy safeguards are also essential so that integrity can be verified without exposing personal data (Rasheed & Louca, 2024; Kulkarni et al., 2025). Wider adoption further depends on ledger interoperability and legal recognition of on-chain evidence (Zhu et al., 2024).

Conclusion

In conclusion, this research proposes a robust and efficient blockchain-based continuous auditing architecture which is intended to address the fundamental weaknesses of the current ex-post sample-based approach through incorporation of the blockchain technology, cryptographic immutability, automatic smart contract risk scoring and trigger execution mechanisms. As validated through extensive simulation on 200,000 transactions, the architecture proved itself to be more efficient with high precision of 94.2%, recall of 91.5% and F1 score of 92.8%. The architecture demonstrated graceful degradation and greater resilience under the conditions of simulation stress and scaled attacks. Nevertheless, there are some challenges in regard to practical implementation of the solution because of the use of synthetic dataset, potential increased computational costs when working in low load environment, requirement to conduct careful feature selection to avoid biasness and complicated regulatory requirements regarding obtaining permissions for automatic transaction hold mechanism.

Future research is going to focus on using institutional ledger data for testing, incorporation of cryptographically secure methods that provide protection of sensitive information of users through, for example, zero-knowledge proofs as well as adaptive models which would allow dynamic setting of thresholds. When coupled with rigorous institutional governance frameworks, these advancements will significantly accelerate the realization of transparent, automated, and secure financial regulation.

References

Kukman, T., & Gričar, S. (2025). Blockchain for quality: Advancing security, efficiency, and transparency in financial systems. *FinTech*, *4*(1), 7. https://doi.org/10.3390/fintech4010007

Bhandari, M., Tiwari, G., & Dhakal, M. (2025). Enhancing transparency and accountability in sustainable finance through blockchain technology: A systematic review of the literature. *Journal of Intelligent Management Decision*, *4*(1), 23-43. https://doi.org/10.56578/jimd040102

Almadadha, R. (2024). Blockchain technology in financial accounting: Enhancing transparency, security, and ESG reporting. *Blockchains*, *2*(3), 312-333. https://doi.org/10.3390/blockchains2030015

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*, *67*(1), 37-55. https://doi.org/10.1108/IJLMA-08-2023-0172

Prokopenko, O., Koldovskiy, A., Khalilova, M., Orazbayeva, A., & Machado, J. (2024). Development of blockchain technology in financial accounting. *Computation*, *12*(12), 250. https://doi.org/10.3390/computation12120250

Shi, J., & Wang, Y. (2025). Academic exploration of blockchain and AI in financial services. *Journal of Electronic Business & Digital Economics*, *4*(2), 270-282. https://doi.org/10.1108/JEBDE-08-2024-0023

Zhu, K., Wu, F., Wang, F., Shen, T., Wu, H., Xue, B., & Liu, Y. (2024). Blockchain-based digital asset circulation: A survey and future challenges. *Symmetry*, *16*(10), 1287. https://doi.org/10.3390/sym16101287

Wei, H., & Zhang, Y. (2025). Research on the digital transaction model of the sports industry chain based on blockchain technology. *Scientific Reports*, *15*(1), 25131. https://doi.org/10.1038/s41598-025-10045-7

Dashkevich, N., Counsell, S., & Destefanis, G. (2024). Blockchain financial statements: innovating financial reporting, accounting, and liquidity management. *Future Internet*, *16*(7), 244. https://doi.org/10.3390/fi16070244

Saeedi, K. (2024). Promoting sustainable household engagement in recycling via blockchain-based loyalty program. *Sustainability*, *16*(21), 9191. https://doi.org/10.3390/su16219191

Rasheed, S., & Louca, S. (2024). Blockchain-based implementation of national census as a supplementary instrument for enhanced transparency, accountability, privacy, and security. *Future Internet*, *16*(1), 24. https://doi.org/10.3390/fi16010024

Kulkarni, A. V., Mondal, T., & Modi, D. (2025). Enhancing privacy in banking systems: a blockchain-based access management and KYC solution. *Cogent Business & Management*, *12*(1), 2570063. https://doi.org/10.1080/23311975.2025.2570063