3 Міжнародна науково-практична конференція
Modern Perspectives on Science and Economic Progress
Секція 11. Інформаційні технології та кібербезпека

Nataliia Dolhova
PhD in Technical Sciences, Associate Professor
Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics
natalya.dolgova@hneu.net
Olena Shapovalova
PhD in Technical Sciences, Associate Professor
Department of Cybersecurity and Information Technologies
Simon Kuznets Kharkiv National University of Economics
olena.shapovalova@hneu.net

Use of Blockchain Technology in Secure Document Management Systems

In the context of ongoing digital transformation affecting both corporate information systems and critical infrastructure facilities, the issue of ensuring integrity, authenticity, and traceability of the electronic document lifecycle becomes increasingly important. Traditional electronic document management systems based on centralized storage and logging models demonstrate limited resistance to retrospective tampering, as trust in the history of changes relies on the assumption of the integrity of the administrator or the owning organization. Under such conditions, there is a need to transition to models where trust is ensured not by organizational mechanisms but by cryptographic guarantees.

In this context distributed ledger technologies particularly blockchain open new opportunities for building highly reliable document management systems. The use of blockchain enables the creation of an environment where each document modification is recorded as an immutable entry verified by network consensus. At the same time direct storage of documents on the blockchain is impractical due to throughput limitations and confidentiality requirements, which necessitates the use of hybrid architectures.

Within this study a Secure Document Management System (SDMS) architecture is proposed based on the separation of content and evidence layers. Document content is stored off-chain in encrypted form while the distributed ledger stores only cryptographic hashes, metadata, digital signatures, and timestamps. This approach ensures a balance between performance and trust as blockchain acts as an independent integrity verification mechanism.

In the proposed architecture blockchain is not considered a universal data storage medium but rather a specialized infrastructure component that functions as a trust anchor for the entire document lifecycle. This approach differs fundamentally from

traditional blockchain usage models where it serves as a storage or transaction log and helps avoid limitations related to scalability and data volume.

Within SDMS blockchain is used as a mechanism for cryptographic anchoring of key document states, ensuring immutability of evidentiary attributes regardless of the system's content layer. This means that even in the event of compromise at the application or infrastructure level, the integrity of the document history can be restored and verified using data recorded in the distributed ledger.

Thus blockchain serves as an independent verification infrastructure enabling external audit without the need to trust a specific organization or system administrator. This is particularly important in inter-organizational environments and critical infrastructure systems where no single trusted authority exists.

Unlike approaches where blockchain is integrated at the data storage level, the proposed model implements it as an evidence layer that interacts with the document state chain and ensures cryptographically guaranteed consistency across all document versions. As a result a multi-layer trust system is formed where blockchain acts as an immutable source of truth and the Document State Chain serves as a local integrity verification mechanism.

A key element of the system is the document state chain which forms a cryptographically linked history of changes. Any modification of previous states leads to a violation of the integrity of the entire chain, ensuring guaranteed detectability of tampering. The evidence layer is implemented using Hyperledger Besu [1] enabling a permissioned model with the QBFT[2], consensus algorithm and controlled network access.

To better understand the advantages of the proposed approach it is useful to compare it with traditional centralized systems[3] (Tabl.1).

Table 1. Comparison of Document Management Approaches

Criterion	Metric	Centralized System	SDMS with Blockchain
Trust Model	Type of trust	Organizational	Cryptographic
Data Integrity	Detection rate	≈ 0.2	1.0
Protection against retrospective changes	Hidden modification	Yes	No
Audit	Type	Internal	Independent
Transparency	Access to history	Limited	Full (through DLT)
Verification	Trust required	Yes	No
Scalability	Verification time	Undefined	O(K), linear
Fault tolerance	Single point of failure	Present	Absent
Legal validity	Evidentiary strength	Limited	Enhanced (tamper-evidence)

The implementation of the evidence layer is based on a permissioned blockchain using Hyperledger Besu which allows compliance with enterprise requirements and restricts network access to authorized participants. The QBFT consensus algorithm ensures agreement among nodes even in the presence of partially malicious participants, which is critical for regulated and mission-critical environments.

The effectiveness of the proposed approach was confirmed through experimental studies including analysis of the system's ability to detect retrospective changes, scalability assessment, and verification mechanism validation.

The experimental evaluation focused on testing the ability of the SDMS with blockchain integration to detect retrospective modifications, evaluate verification scalability, and confirm correctness without false positives. A test infrastructure based on a permissioned blockchain using Hyperledger Besu was deployed.

In the first set of experiments various tampering scenarios were simulated including modifications of content, metadata, digital signatures, and timestamps. The results showed that all attempts of retrospective modification were successfully detected due to the cryptographic linkage of document states. In contrast in centralized systems without blockchain some modifications remained undetected.

The second experiment evaluated the dependency of verification time on the length of the document state chain. It was found that verification time increases linearly, indicating predictable scalability without performance degradation.

The third experiment verified correctness in the absence of attacks. Results showed zero false positives, meaning all valid document chains were correctly recognized (Tabl.2).

Table 2. Experimental Results

Hypothesis	Conditions	Metric	SDMS Result	Centralized Model
H1	Data modification (metadata, signatures, time)	Detection rate	1.0 (100%)	≈ 0.2
H2	K = 5–150 states of paper	Verification time (ms)	Linear growth ($R^2 \approx 0.96$)	Unstable
H3	No attacks	False positive rate	0	> 0

The comparative analysis demonstrates that the integration of blockchain into document management systems significantly enhances the levels of data integrity, transparency, and trust. Of particular importance is the capability for independent auditing which does not depend on a specific organization and can be performed by any participant with access to the distributed ledger. This opens up new opportunities for inter-organizational interaction in environments where no single trusted authority exists.

At the same time the implementation of blockchain technologies is accompanied by a number of challenges related to performance limitations, integration complexity, and the need to consider regulatory and legal aspects. However, the proposed approach, based on using blockchain exclusively as an evidence layer, makes it possible to minimize these limitations and ensure the effective application of the technology in practical scenarios.

In conclusion, it can be stated that the use of blockchain in secure document management systems enables a transition from a model of organizational trust to a model of cryptographically guaranteed reliability. The proposed SDMS ensures full

traceability of the document lifecycle, protection against retrospective tampering, and the possibility of independent verification, making it a promising solution for application in domains with increased requirements for security and auditing.

Further research may be aimed at improving system performance, extending access control mechanisms as well as integrating with intelligent document analysis systems which opens new opportunities for the development of modern information technologies in the field of cybersecurity.

References

[1] Ilechukwu, C., Hong, S.-C., & Nag, B. (2026). Financial Document Authentication and Verification Using Hierarchical Tokenization on Permissioned Blockchains. *Journal of Risk and Financial Management*, *19*(4), 239. https://doi.org/10.3390/jrfm19040239

[2] Delladetsimas, A. P., Papangelou, S., Iosif, E., & Giaglis, G. (2025). Leadership Uniformity in Timeout-Based Quorum Byzantine Fault Tolerance (QBFT) Consensus. *Big Data and Cognitive Computing*, *9*(8), 196. https://doi.org/10.3390/bdcc9080196

[3] Yatnalli, V., Bhusare, S. S., Dhulavvagol, P. M., Konnurmath, G., & Shetty, R. (2025). DABFT: A Novel Adaptive Byzantine Fault Tolerance Framework for High-Performance Blockchain Consensus. *Engineering, Technology & Applied Science Research*, *15*(4), 25313–25317. https://doi.org/10.48084/etasr.11970