




A Secure and Reliable Model for Financial Documents Using Digital Signature and Blockchain Technology

Fatemeh Mohammad Saeidia¹, Mohammad Hadi Zahedi^{2*}, Elham Farahani³

¹ Department of Information Technology, Faculty of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran

² Assistant Professor, Department of Information Technology, Faculty of Industrial Engineering, K. N. Toosi University of Technology, Tehran, Iran

³ Assistant Professor, Faculty of Computer Engineering, Iranian eUniversity, Tehran, Iran

* Corresponding author email address: zahedi@kntu.ac.ir

Article Info

Article type:

Review Article

How to cite this article:

Mohammad Saeidia, F., Zahedi, M. H., & Farahani, E. (2025). A Secure and Reliable Model for Financial Documents Using Digital Signature and Blockchain Technology. *AI and Tech in Behavioral and Social Sciences*, 3(1), 23-33.

<https://doi.org/10.61838/kman.aitech.3.1.3>



© 2025 the authors. Published by KMAN Publication Inc. (KMANPUB), Ontario, Canada. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

ABSTRACT

Today, financial documents are no longer recorded and stored as paper documents but as digital documents based on the Internet platform. For this reason, the misuse of financial data has increased, leading to extensive research on the secure storage, sharing, and exchange of data. One of the methodologies used in this field is blockchain. To effectively combat these risks, businesses are turning to innovative solutions such as blockchain technology and digital signatures. These advanced technologies provide strong transaction authentication and provide enhanced defense. Digital signatures and blockchain technology work together to increase the security and reliability of digital transactions. Blockchain provides essential elements such as transparency, immutability, and consensus, while digital signatures work to verify authenticity and integrity. Combining these two powerful tools creates a robust solution that creates secure and reliable digital interactions that minimize the risk of fraud and foster trust in the digital ecosystem. This paper explores digital signatures and blockchain technology and explore how they can help improve security. In this study, we have designed a model based on blockchain and digital signature to improve data security by examining existing system models and data exchange security methods. Finally, this research has improved blockchain security for the transfer of financial documents.

Keywords: Financial Documents, Blockchain, Digital Signature, Security

1. Introduction

In the current technological era, numerous emerging technologies are transforming various sectors of the global economy. Among these, blockchain technology has gained prominence, particularly in financial institutions. Blockchain technology plays a pivotal role in securing transactions within financial institutions, often functioning as a decentralized third-party intermediary. This technology offers one of the most secure and neutral financial systems, allowing for the creation and reading of records while preventing any subsequent alterations. This immutability protects both customers and financial institutions from fraudulent activities (León & Tuffaha, 2022).

Despite its advantages, blockchain technology faces several challenges, including issues related to reputation, energy consumption, and environmental impact due to its association with digital currencies. Furthermore, blockchain technology is still in its developmental stages, characterized by a lack of interoperability, complexity, and limited scalability. Additional challenges include poor user experience, insufficient training, security and privacy concerns, and the absence of comprehensive regulations governing blockchain across various sectors, such as banking, healthcare, education, and finance (Hasselgren et al., 2020; Mettler, 2016).

Given the critical importance of financial documents, which are frequently targeted by hackers, it is essential to develop a model that enhances the security and reliability

of these documents using blockchain technology and digital signatures. This study aims to create a secure channel for exchanging financial documents, mitigating the risks posed by malicious actors.

The specific objectives of this study are as follows:

- To examine the role of blockchain technology in the financial system.
- To enhance the security and reliability of financial documents through the application of blockchain technology and digital signatures.
- To propose policy recommendations for the financial sector to improve financial transactions.

2. Literature Review

Blockchain technology has evolved beyond its initial association with digital currencies, such as Bitcoin. Today, it is recognized as a critical technology for applications requiring immutable, traceable data, encrypted and distributed ledgers, and secure transactions. This section reviews the existing literature on blockchain technology, focusing on its importance, its role in the financial system, and its application in financial transactions.

2.1. The Importance of Blockchain Technology

The concept of blockchain was introduced by Satoshi Nakamoto in 2008 (Nakamoto, 2008). Ahmad et al. (2018) acknowledged that Bitcoin, a decentralized digital currency, represents one of the most prominent applications of blockchain technology (Ahmad et al., 2018). DeVries (2016) suggests that blockchain is among the most significant emerging technologies, widely adopted not only by central banks but also by commercial banks to safeguard their daily transactions (DeVries, 2016).

A typical blockchain operates as a peer-to-peer network controlled by decentralized computers that maintain a record of financial transactions (Tasatanattakool & Techapanupreeda, 2018). Once a transaction is recorded, it cannot be altered, ensuring the security of financial exchanges between parties. Blockchain technology extends beyond the financial sector and is applicable in various industries, including agriculture, manufacturing, and services (Collomb & Sok, 2016). In essence, blockchain is valuable in any context where there is a risk of fraud and where third-party intermediaries may misuse confidential information.

Buitenhek (2016) argues that blockchain is ideally suited for any situation involving third-party intermediaries, a fact

that has driven its widespread adoption by companies and the rapid growth of blockchain developers. While blockchain provides secure and efficient online transactions, its advantages are sometimes misunderstood. Some individuals and organizations conflate blockchain technology with digital currencies like Bitcoin, despite their distinct applications and functionalities (Buitenhek, 2016).

The primary purpose of blockchain technology is to securely record transactions in a ledger. These records are maintained in a peer-to-peer network, eliminating the need for intermediaries to validate transactions. Consequently, financial transactions, international trade agreements, commercial contracts, voting processes, and other activities can be conducted directly between parties without intermediaries (Milani et al., 2016).

Security is the foremost concern in blockchain technology, particularly for online transactions. The decentralized nature of blockchain provides a high level of security, protecting information from unauthorized access and theft (Karame, 2016). Felin and Zenger (2018) highlight the transparency of blockchain, noting that all participants in the network can view the transaction history from start to finish (Felin & Lakhani, 2018). De Filippi et al. (2018) further emphasize that blockchain reduces the likelihood of disputes due to its open and accessible nature (De Filippi & Hassan, 2018).

Bashir (2016) examines the widespread adoption of blockchain in the financial sector, noting that it is a cost-effective alternative to traditional models. Many companies are now adopting blockchain technology to save resources and time while enhancing the security of sensitive information (Bashir, 2017). Tapscott and Tapscott (2017) argue that blockchain is particularly well-suited for the banking and finance industries (Tapscott & Tapscott, 2017). Moreover, Niranjnamurthy et al. (2019) observe that blockchain transactions are significantly faster than traditional systems, allowing parties to send or receive financial documents within minutes. Blockchain technology is considered one of the most secure and reliable systems, resistant to hacking and delays (Niranjnamurthy et al., 2019).

As previously mentioned, blockchain eliminates the need for intermediaries in financial transactions, thereby reducing third-party costs (Treleaven et al., 2017). It also enhances transparency between parties by enabling direct transactions. Through blockchain, banks and financial institutions can significantly improve their economic efficiency (Tapscott & Tapscott, 2016).

2.2. *The Role of Blockchain Technology in the Financial System*

Ali et al. (2020) investigate the adoption of advanced technologies by the financial system, emphasizing that these technologies enhance transparency, reduce costs and time, and improve safety levels. Leon and Tuffaha (2022) support these findings, asserting that blockchain technology acts as a catalyst in the financial system by facilitating financial transactions, which in turn encourages the adoption of blockchain technology within the financial sector. Their study further indicates that blockchain has the potential to nearly eliminate manual processes within financial systems (León & Tuffaha, 2022).

Grover et al. (2018) examine the impact of blockchain technology on trust and the security of financial transactions. They report that the transition to advanced digital payment systems initially raised concerns about trust and reliability. However, their findings suggest that blockchain technology has significantly enhanced the security of financial transactions and has transformed the financial industry (Grover et al., 2018).

Queiroz et al. (2020) discuss the features of blockchain that are particularly beneficial to the financial sector. Their study highlights that each network participant receives a copy of every new transaction, ensuring transparency and security. They also emphasize that the decentralized nature of blockchain prevents any single entity from controlling the network, making it secure and auditable (Queiroz et al., 2019).

Frizzo-Barker et al. (2020) build on the findings of Queiroz et al. (2019), further exploring the security features of blockchain. They note that once financial transaction records are shared among network members, it becomes nearly impossible to alter or illegally add new transactions. The study also reports that blockchain technology maintains a chronological history of financial transactions, and any attempt to modify or delete a transaction would require compromising thousands of records, a task beyond the capability of a single individual or group (Frizzo-Barker et al., 2020).

Ahram et al. (2017) explore the use of blockchain technology for international money transfers, noting that it offers a cost-effective and secure alternative to traditional methods. Their study reports that several banks have adopted blockchain technology to address issues related to the cost and time associated with cross-border transactions. Additionally, customers can access blockchain technology

via digital devices, such as laptops or mobile phones (Ahram et al., 2017).

Nguyen (2016) investigates the individual use of blockchain, suggesting that it offers a fast, low-risk solution that protects users from online fraud. The study also predicts that blockchain technology will reduce the need for cash payments, wire transfers, and post-dated checks, which are prone to being untraceable, time-consuming, or susceptible to forgery (Nguyen, 2016).

Cocco et al. (2017) examine the impact of blockchain on financial institutions, particularly within the banking sector. They find that blockchain allows for the traceability of ownership and financial transactions, creating opportunities for automation. The study also reports that blockchain reduces human error and enables financial institutions to operate continuously (Cocco et al., 2017).

Min (2019) discusses the evolution of blockchain from its initial use in cryptocurrency transactions to its current applications across various sectors. Min argues that blockchain's decentralization, security, transparency, and resistance to alteration make it a valuable innovation for addressing critical issues in the financial sector. The study concludes that blockchain technology has the potential to reform the financial industry by transforming the management of various financial services (Min, 2019).

Guo and Liang (2016) examine the monopoly of the banking sector and suggest that customers seek alternatives due to restrictions such as minimum balance limits and banking fees. Blockchain technology emerges as a competitor, offering full financial inclusion without these constraints. The study highlights that customers can perform all necessary transactions using blockchain technology on mobile devices (Guo & Liang, 2016).

Leon and Tuffaha (2022) assert that blockchain technology reduces the risk of fraud by maintaining an immutable record of financial transactions (León & Tuffaha, 2022). Yaga et al. (2019) note that blockchain innovation is being adopted by significant financial markets, including NASDAQ and the London Stock Exchange, to issue and monitor private endorsements. The study indicates that other stock exchanges, such as those in Tokyo, South Korea, and India, are also exploring the potential benefits of blockchain technology (Yaga et al., 2019).

Treleaven (2017) explores how blockchain could democratize stock exchanges by reducing the role of intermediaries and lowering transaction costs. The study suggests that this decentralization could make stock trading

more accessible and transparent, thereby decreasing the need for traditional market intermediaries (Treleaven et al., 2017).

Mettler (2016) argues that the evolving global financial landscape necessitates innovations like blockchain to increase efficiency and reduce costs. The study predicts that by 2020, blockchain will have a significant impact on the financial sector worldwide, driving organizations to invest in this technology to remain competitive (Mettler, 2016).

While distributed ledger technology (DLT) presents significant potential, Beck and Müller-Bloch (2017) note that several challenges must be addressed before successful blockchain-based solutions can be implemented. They argue that blockchain is a radical innovation that may require significant organizational changes and introduce uncertainties related to technology, market conditions, and resources (Beck & Müller-Bloch, 2017).

The establishment of standards is crucial for the evolution of blockchain technology. Grant (2021) defines a standard as a format, interface, or system that ensures interoperability. Deshpande et al. (2017) emphasize the importance of developing standards for blockchain technology to facilitate its adoption across various industries (Deshpande et al., 2017). Meiklejohn (2018) proposes side chains as a potential solution to the interoperability challenges between different blockchain networks (Meiklejohn, 2018).

The complexity of blockchain technology necessitates overcoming several obstacles to its successful application across different use cases. Grant (2002, 2019) and White (1986) argue that as the complexity of a product increases, a differentiation strategy becomes more valuable. Blockchain's ability to connect multiple participants and store various attributes offers significant potential for enhancing financial products in the banking sector (Grant, 2002, 2019; White, 1986).

2.3. *The Role of Blockchain Technology in Financial Transactions*

As highlighted in previous studies, Ahram (2017) argues that blockchain technology is among the top emerging technologies in the financial system and plays a crucial role in securing financial transactions. The study also notes that blockchain acts as a third-party intermediary, reducing the likelihood of fraud and minimizing the cost of financial transactions (Ahram et al., 2017). Leon and Tuffaha (2022) define a financial transaction as an event or activity in the

financial system that alters the value of assets, liabilities, or equity (León & Tuffaha, 2022). Financial transactions always involve money and are typically recorded in journals as the first step in financial statement preparation (Ozili, 2018).

Tasca and Tessone (2017) categorize financial transactions into those performed manually and those conducted electronically, noting that manual transaction methods have largely been supplanted by automated systems (Tasca & Tessone, 2017). Pande (2019) emphasizes that financial transactions are critical to the global economy, with trillions of transactions processed daily, many of which are still conducted manually. Examples of financial transactions include money receipts, purchase orders, and expense reports, each of which requires accurate documentation (Pande, 2019).

Batubara (2018) outlines the stages of blockchain-based financial transactions, beginning with the customer's intent to buy or sell financial assets. In the second stage, the customer verifies these assets within the blockchain network. Finally, the transaction is recorded in the blockchain, creating an immutable block of information (Batubara et al., 2018).

Hasselgren (2020) suggests that transaction fees in blockchain systems consist of various layers of charges imposed by financial institutions. While traditional financial intermediaries require substantial time and resources to process transactions, blockchain technology accelerates the transfer process, making it both faster and cheaper. The study also notes that blockchain could potentially disrupt traditional financial institutions (Hasselgren et al., 2020).

Nam (2021) examines the positive impact of blockchain technology on financial transactions, highlighting insights from industry experts and empirical data (Nam et al., 2021). Pan (2020) concurs, reporting that over 50% of board members agree that blockchain technology has had a significant impact on financial transactions over the past three years. The study also explores the use of blockchain for asset management, record-keeping, cryptocurrencies, and the development of smart contracts for trading platforms (Pan et al., 2020).

Golosova and Romanovs (2018) investigate the relationship between liquidity and blockchain-based financial transactions. They argue that blockchain technology enhances liquidity, reduces capital costs, increases transparency for stakeholders, and facilitates

national and international payment transfers (Golosova & Romanovs, 2018).

Swan (2017) outlines the benefits of blockchain technology in capital markets, where it streamlines processes, reduces settlement times, and lowers transaction costs. The study also reports that blockchain reduces the risk of fraud and error, digitizes financial assets, and simplifies trading and management within the financial system (Swan, 2017).

3. Proposed Model

As previously discussed, digital signatures offer a secure and decentralized method for verifying the integrity and origin of documents. This section presents a model that incorporates digital signatures into blockchain-based financial documents and outlines the various components of the proposed model.

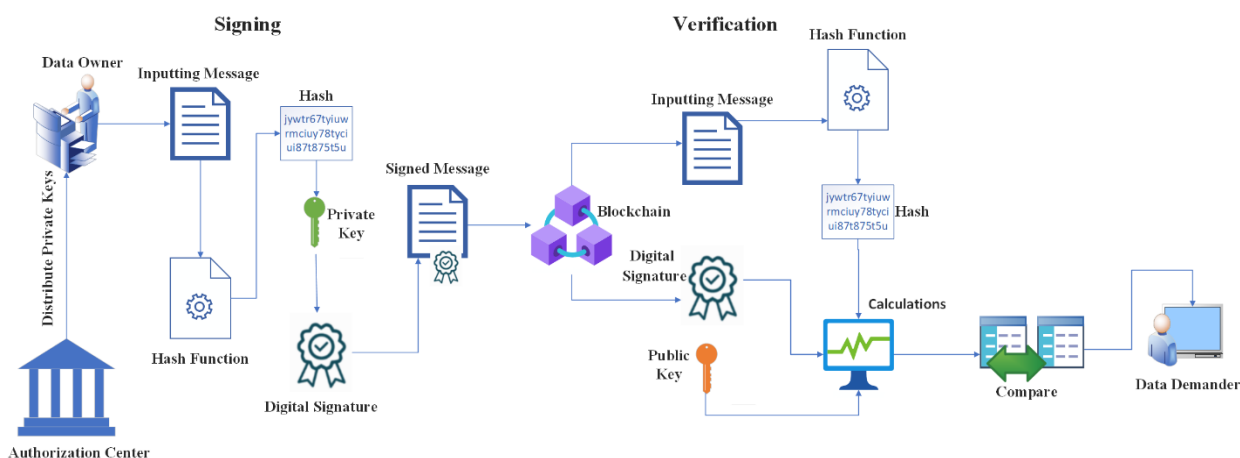
Figure 1 provides a graphical representation of the digital signature model for blockchain-based financial documents. This model leverages the security, integrity,

and validity provided by digital signatures, thereby enhancing trust among participants within the blockchain network. The proposed model facilitates a secure and decentralized process for digitally signing financial documents using blockchain technology. In this process, public and private keys are generated for each user or entity within the network. The document's content is first converted into a unique string using a cryptographic hash function. The private key is then used to create a digital signature for the hashed content. The recipient of the document verifies this digital signature using the public key of the signer. Finally, the signed document is stored on the blockchain along with metadata, ensuring both the immutability and authentication of the document.

Beyond the fundamental signing and verification steps, this model also includes mechanisms for revoking compromised private keys, secure key management to safeguard keys, and compliance with legal standards and regulations related to digital signatures and financial documents.

Figure 1

The Proposed Model



The stages of this model are interconnected in a sequential chain. The generation of Public Key Infrastructure (PKI) keys forms the foundation for digital signatures. Hashing the document links the signature to the document's actual content. The signing and verification process confirms both the identity of the signer and the authenticity of the document. Blockchain integration ensures the document's immutability and public accessibility. The revocation mechanism preserves security by invalidating compromised keys. Secure key

management practices protect private keys from unauthorized access. Lastly, regulatory compliance ensures the model's legal validity.

Each step in this model is crucial for the effective operation of the entire system, collectively providing a comprehensive framework for digitally signing financial documents using blockchain technology.

3.1. *Setting up Public Key Infrastructure (PKI)*

The proposed model employs a PKI system to manage digital signature keys. This involves generating public and private key pairs for each user or entity within the blockchain network. The public key is openly shared, while the private key remains confidential.

3.2. *Hashing the Document*

Before the document is signed, its content is hashed using a cryptographic hash function, such as SHA-256. This process generates a unique, fixed-size string of characters representing the document's content.

3.3. *Signature Process*

In the signature process, the private key is used to sign the financial document. Specifically:

- When a user or entity wishes to sign a financial document, they use their private key to create a digital signature for the hashed content, ensuring that the signature is unique to both the document and the signer.
- The digital signature algorithm generates a signature that is then attached to the document.

3.4. *Verification Process*

The verification process involves the following steps:

- The recipient hashes the content of the received document using the same cryptographic hash function.
- The recipient then decrypts the digital signature using the signer's public key to obtain the hash value.
- The recipient compares the calculated hash value with the decrypted hash value. A match confirms that the document has not been altered and was indeed signed by the purported signer.

3.5. *Blockchain Integration*

During blockchain integration, the following steps are undertaken:

- The signed document is stored on the blockchain along with metadata, such as the signer's identity, timestamp, and relevant transaction details.
- Blockchain's immutability ensures that once a document is recorded, it cannot be altered or

deleted without the consensus of network participants.

3.6. *Cancellation Mechanism*

The proposed model includes a cancellation mechanism to invalidate compromised or invalid keys. This ensures that once a private key is compromised, it can no longer be used to sign documents.

3.7. *Secure Key Management*

The proposed model suggests the following steps for secure key management:

- Implementing robust key management practices to protect private keys from unauthorized access.
- Considering the use of hardware security modules (HSM) or secure key vaults for enhanced protection.

3.8. *Compliance with Regulations*

This step ensures that the model complies with regulations and standards related to digital signatures and financial documents, such as the eIDAS regulation in the European Union or the UETA and ESIGN laws in the United States.

3.9. *Discussion and Evaluation*

The case study examined in this section compares the proposed model of this study with the model proposed by Wang and Guan (2023). In their study, Wang and Guan propose a traceable and secure data-sharing scheme based on blockchain technology. Their solution includes an encryption-based data protection method to enable fine-grained access control for shared data. Their proposed scheme is evaluated for performance and security, demonstrating higher throughput, enhanced data security, and reduced encryption and decryption overhead (Wang & Guan, 2023).

3.10. *Comparison of Data Security*

In this section, the proposed model of this study is compared with Wang and Guan's model concerning on-chain data security, data integrity, trustworthiness, authorization, authentication, reliability, validation, scalability, privacy, and regulatory compliance. The results are summarized in Table 1. Below, we refer to the first

model as the proposed design of this study and the second model as the design proposed by Wang and Guan.

3.10.1. On-chain Data Security

First model: This model typically employs encryption or digital signatures to protect on-chain data, ensuring high security.

Second model: This model uses the ECC encryption algorithm to store the data hash as ciphertext on the blockchain. Both models offer comparable security for on-chain data.

Performance: Both models demonstrate similar performance in this regard.

3.10.2. Data Integrity

First model: This model uses blockchain to store data hashes, benefiting from the blockchain's immutability, which ensures high data integrity.

Second model: This model similarly stores data hashes on the blockchain to ensure data integrity.

Performance: Both models perform similarly in this regard.

3.10.3. Trustworthiness

First model: This model employs a central authority to validate data, potentially enhancing system trust.

Second model: This model verifies data authenticity through data hashing, which offers high security but may lack the reliability associated with a trusted central authority.

Performance: The first model performs better in this regard.

3.10.4. Authorization

First model: This model uses a central authority to manage permissions, simplifying access control.

Second model: This model employs attribute-based encryption, allowing data owners greater control over access, thus providing more flexibility.

Performance: The second model excels in precise access control, while the first model is superior in management simplicity.

3.10.5. Authentication

First model: As previously mentioned, this model uses a central authority for user authentication, simplifying the process.

Second model: This model authenticates users before granting access to the system.

Performance: The first model performs better in this regard.

3.10.6. Reliability

First model: This model stores data hashes on the blockchain and encrypts the data off-chain, such as financial documents. Even if off-chain data is lost or corrupted, it can be recovered using the blockchain-stored hash.

Second model: This model stores only data hashes on the blockchain, with the data itself encrypted and stored in the InterPlanetary File System (IPFS). Data loss or corruption in IPFS would render it irrecoverable without a backup.

Performance: The first model has superior reliability.

3.10.7. Validation

First model: This model uses the blockchain to verify data authenticity, ensuring that only authorized users can access unmanipulated data.

Second model: This model also uses data hashing to verify authenticity, similar to the first model, and offers high security.

Performance: Both models exhibit similar performance in this regard.

3.10.8. Scalability

First model: This model is generally more scalable due to its distributed blockchain, capable of handling large amounts of data and users without performance degradation.

Second model: The second model may face scalability challenges due to its more centralized nature, particularly if many users access the system simultaneously.

Performance: The first model outperforms in scalability.

3.10.9. Privacy

Second model: Although the second model employs encryption to protect data, privacy concerns persist due to

the distribution of private keys. If these keys are compromised, unauthorized data access is possible.

First model: The proposed model in this study includes a cancellation mechanism to mitigate such risks.

Performance: The first model offers better privacy protection.

3.10.10. Regulatory Compliance

Second model: The second model lacks a clear regulatory framework, posing risks for organizations required to comply with specific regulations.

First model: The first model adheres to clear regulatory frameworks, ensuring compliance with relevant regulations.

Performance: The first model is superior in regulatory compliance.

3.11. Final Review of the Proposed Model and Comparative Analysis

As outlined in the previous section, the proposed model of this study can be compared with Wang and Guan's model, as summarized in Table 1.

Table 1

Comparison of the Performance of the Proposed Model of This Study with Wang and Guan's Model

No.	Feature	First Model	Second Model	Better Performance
1	On-chain Data Security	Encryption or digital signatures	ECC encryption	Both models are similar
2	Data Integrity	Blockchain	Blockchain and data hashing	Both models are similar
3	Trustworthiness	Central authority	Hash data	First model
4	Authorization	Central authority	Feature-based encryption	Second model for precise access control; First model for simplicity of management
5	Authentication	Central authority	System authentication	First model
6	Reliability	Blockchain and off-chain encryption	Blockchain and IPFS	First model
7	Validation	Hash data and blockchain	Hash data	Both models are similar
8	Scalability	High	Middle	First model
9	Privacy	High	Middle	First model
10	Regulatory Compliance	High	Down	First model

Based on the comparative analysis, the proposed model in this study, which utilizes blockchain technology for secure and immutable data storage and transfer, offers several distinct advantages:

- **Security:** The proposed model employs encryption and other security measures to protect data from unauthorized access and manipulation. Blockchain ensures an immutable record of data, making it resistant to tampering or deletion.
- **Trust:** The model relies on a centralized approach to manage the signature and verification process, which fosters confidence in the identity of data owners and the authenticity of the data. The Licensing Center acts as a trusted authority, ensuring the reliability of data verification.
- **Efficiency:** The proposed model is capable of processing transactions quickly and efficiently. Blockchain's distributed nature eliminates single points of failure, allowing the system to operate efficiently even under increased loads.

- **Adaptability:** The model is flexible and can be configured to meet various compliance requirements, making it suitable for storing sensitive data such as medical records or financial documents.
- **Programmability:** The model supports a wide range of applications, including identity management, supply chain management, electronic voting, and more.

Conversely, the second model, despite its advantages, also presents several drawbacks:

- **Complexity:** The second model is inherently complex and challenging to understand and implement, which may deter some organizations from adopting it.
- **Scalability:** The second model may struggle with handling large volumes of data, as blockchain's distributed database can experience slowdowns as data volume increases.

- **Privacy:** While the second model uses encryption to protect data, there are privacy concerns. Private keys are distributed for data access, and if these keys are compromised, unauthorized data access is possible. The cancellation mechanism in the proposed model of this study mitigates this risk.
- **Regulation:** The second model lacks a clear regulatory framework, which poses a risk for organizations that must adhere to specific compliance requirements.

4. Conclusion

In the current landscape, many businesses are adopting blockchain technology to enhance the security of their financial documents. The integration of blockchain with digital signatures represents a significant advancement in document security and reliability.

The proposed model in this study offers a comprehensive process for signing, hashing, verifying, and storing documents within a blockchain network. Signed documents are permanently stored on the blockchain, ensuring their immutability and integrity. This model is particularly advantageous in fields such as financial document management, where blockchain provides an immutable and transparent platform that prevents forgery or manipulation. Additionally, digital signatures verify the identity of signers and prevent repudiation.

Ultimately, this system simplifies and streamlines the document-signing process by eliminating intermediaries and reducing the need for paperwork.

The adoption of blockchain and digital signatures for securing financial documents is a transformative development. This system offers significant benefits to businesses across various industries by providing enhanced security, reliability, efficiency, and transparency. Moreover, researchers can build on existing studies to further develop blockchain technology and address security challenges.

The integration of blockchain and digital signatures is poised to revolutionize the management of financial documents, enhancing security, efficiency, and transparency. Continued research and development are necessary to advance digital signature algorithms, optimize document storage on the blockchain, and establish security and control models based on identity and permissions. Furthermore, careful consideration of legal and regulatory issues is essential. With ongoing innovation and research,

individuals and organizations can realize substantial benefits, including increased security, transparency, efficiency, and cost savings. This will benefit various stakeholders, secure financial document processes, and drive transformation in this domain.

Authors' Contributions

F. M. S., M. H. Z., and E. F. collaboratively conceptualized the research focus and objectives. F. M. S. led the design and development of the proposed model, integrating blockchain and digital signature technologies. M. H. Z. contributed primarily to the literature review, focusing on existing security methodologies and the integration of blockchain technology. E. F. specialized in the technical aspects, particularly the implementation and testing phases of the digital signature application within the model. All authors participated in the analysis and interpretation of the results and collaborated on writing and revising the manuscript to ensure the discussion and conclusions were robust and clearly articulated. They all approved the final manuscript for submission, ensuring the integrity and accuracy of the work presented.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethics Considerations

Not applicable.

References

Ahmad, F. A., Kumar, P., Shrivastava, G., & Bouhleb, M. S. (2018). Bitcoin: Digital decentralized cryptocurrency. In *Handbook of research on network forensics and analysis techniques* (pp. 395-415). IGI Global. <https://doi.org/10.4018/978-1-5225-4100-4.ch021>

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. 2017 IEEE technology & engineering management conference (TEMSCON),

Bashir, I. (2017). *Mastering blockchain*. Packt Publishing Ltd. <https://books.google.com/books?hl=en&lr=&id=urkrDwAAQBAJ&oi=fnd&pg=PP1&dq=%5B1%5D%09Bashir+I.+Mastering+blockchain:+Packt+Publishing+Ltd.%3B+2017.+&ots=Ixak0f7t0Q&sig=XmDF-R2xqq88Tvq85OaKzeG7BFc>

Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. Proceedings of the 19th annual international conference on digital government research: governance in the data age,

Beck, R., & Müller-Bloch, C. (2017). Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization.

Buitenhok, M. (2016). Understanding and applying blockchain technology in banking: Evolution or revolution? *Journal of Digital Banking*, 1(2), 111-119. <https://doi.org/10.69554/TXYN8464>

Cocco, L., Pinna, A., & Marchesi, M. (2017). Banking on blockchain: Costs savings thanks to the blockchain technology. *Future Internet*, 9(3), 25. <https://doi.org/10.3390/fi9030025>

Collomb, A., & Sok, K. (2016). Blockchain/distributed ledger technology (DLT): What impact on the financial sector? *Digiworld Economic Journal*(103). https://www.academia.edu/download/50652048/DWEJ_103_COLLOMB_SOK.pdf

De Filippi, P., & Hassan, S. (2018). Blockchain technology as a regulatory technology: From code is law to law is code. In

Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards*.

DeVries, P. D. (2016). Kripto para birimi, bitcoin ve geleceğin analizi. *International Journal of Business Management and Commerce*, 1(2), 1-9. <https://ijbmcnet.com/images/Vol1No2/1.pdf>

Felin, T., & Lakhani, K. (2018). What problems will you solve with blockchain? *MIT Sloan management review*. https://www.researchgate.net/profile/Teppo-Felin/publication/328598250_What_problems_will_you_solve_with_blockchain/links/5d1d26e1a6fdcc2462bdb287/What-problems-will-you-solve-with-blockchain.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail&_rtd=e30%3D

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51, 102029. <https://doi.org/10.1016/j.ijinfomgt.2019.10.014>

Golosova, J., & Romanovs, A. (2018). The advantages and disadvantages of the blockchain technology. 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE),

Grant, R. M. (2002). *Contemporary Strategy Analysis* (Vol. 4). Blackwell. <https://www.academia.edu/download/43126581/Granrtaaa.pdf>

Grant, R. M. (2019). *Contemporary Strategy Analysis: Text and cases*. John Wiley & Sons Ltd. <https://books.google.com/books?hl=en&lr=&id=TadJEAAAQBAJ&oi=fnd&pg=PR5&dq=%5B1%5D%09Grant+RM.+Contemporary+Strategy+Analysis:+Text+and+cases.+Chichester:+John+Wiley+%26+Sons+Ltd%3B+2019.+&ots=oSU7TLglO7&sig=AopYpTqDQToZ47M65lb3NviXWXY>

Grover, P., Kar, A. K., & Ilavarasan, P. V. (2018). Blockchain for businesses: A systematic literature review. Conference on e-Business, e-Services and e-Society,

Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, 2, 1-12. <https://doi.org/10.1186/s40854-016-0034-9>

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences-A scoping review. *International Journal of Medical Informatics*, 134, 104040. <https://doi.org/10.1016/j.ijmedinf.2019.104040>

Karame, G. (2016). On the security and scalability of bitcoin's blockchain. Proceedings of the 2016 ACM SIGSAC conference on computer and communications security,

León, L. M. C., & Tuffaha, A. (2022). Application of blockchain technology in the financial services industry. the big four. *Information Management*, 54, 102199. <https://lup.lub.lu.se/student-papers/record/9086140/file/9086162.pdf>

Meiklejohn, S. (2018). Top ten obstacles along distributed ledgers path to adoption. *IEEE Security & Privacy*, 16(4), 13-19. <https://doi.org/10.1109/MSP.2018.3111235>

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom),

Milani, F., García-Bañuelos, L., & Dumas, M. (2016). Blockchain and business process improvement. In

Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 62(1), 35-45. <https://doi.org/10.1016/j.bushor.2018.08.012>

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. In

Nam, K., Dutt, C. S., Chathoth, P., & Khan, M. S. (2021). Blockchain technology for smart city and smart tourism: latest trends and challenges. *Asia Pacific Journal of Tourism Research*, 26(4), 454-468. <https://doi.org/10.1080/10941665.2019.1585376>

Nguyen, Q. K. (2016). Blockchain-a financial technology for future sustainable development. 2016 3rd International conference on green technology and sustainable development (GTSD),

Niranjnamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, 22, 14743-14757. <https://doi.org/10.1007/s10586-018-2387-5>

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, 18(4), 329-340. <https://doi.org/10.1016/j.bir.2017.12.003>

Pan, X., Pan, X., Song, M., Ai, B., & Ming, Y. (2020). Blockchain technology and enterprise operational capabilities: An empirical test. *International Journal of Information Management*, 52, 101946. <https://doi.org/10.1016/j.ijinfomgt.2019.05.002>

- Pande, J. (2019). Cashless Transaction-Mobile Transaction. Proceedings of 10th International Conference on Digital Strategies for Organizational Success,
- Queiroz, M. M., Telles, R., & Bonilla, S. H. (2019). Blockchain and supply chain management integration: A systematic review of the literature. *Supply Chain Management: An International Journal*. <https://doi.org/10.1108/SCM-03-2018-0143>
- Swan, M. (2017). Anticipating the economic benefits of blockchain. *Technology Innovation Management Review*, 7(10), 6-13. <https://doi.org/10.22215/timreview/1109>
- Tapscott, A., & Tapscott, D. (2017). How blockchain is changing finance. *Harvard business review*, 1(9), 2-5. https://capital.report/Resources/Whitepapers/40fc8a6a-cdbd-47e6-83f6-74e2a9d36ccc_finance_topic2_source2.pdf
- Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin. <https://cir.nii.ac.jp/crid/1130282272788309120>
- Tasatanattakool, P., & Techapanupreeda, C. (2018). Blockchain: Challenges and applications. 2018 International Conference on Information Networking (ICOIN),
- Tasca, P., & Tessone, C. J. (2017). Taxonomy of blockchain technologies. Principles of identification and classification. In.
- Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer*, 50(9), 14-17. <https://doi.org/10.1109/MC.2017.3571047>
- Wang, Z., & Guan, S. (2023). A blockchain-based traceable and secure data-sharing scheme. *Peerj Computer Science*, 9, e1337. <https://doi.org/10.7717/peerj-cs.1337>
- White, R. E. (1986). Generic business strategies, organizational context and performance: An empirical investigation. *Strategic management journal*, 7(3), 217-231. <https://doi.org/10.1002/smj.4250070304>
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. In.