KMANPUB AI and Tech in Behavioral and Social Sciences Vol. 3 No. 1 (2025)

Article history:
Received 01 July 2024
Revised 02 September 2024
Accepted 06 September 2024
Published online 01 January 2025

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

Fatemeh Mohammad Saeidia[1], Mohammad Hadi Zahedi[2*], Elham Farahani[3]

[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

Editor	Reviewers
Luis Felipe Reynoso-Sánchez Department of Social Sciences and Humanities, Autonomous University of Occident, Los Mochis, Sinaloa, Mexico felipe.reynoso@uadeo.mx	Reviewer 1: Masoud Mirmoezi Department of Physical Education and Sport Sciences, Islamic Azad University, Central Tehran Branch, Tehran, Iran. Email: massoudmirmoezi@live.com Reviewer 2: Kamdin Parsakia Department of Psychology and Counseling, KMAN Research Institute, Richmond Hill, Ontario, Canada. Email: kamdinparsakia@kmanresce.ca

1. Round 1

1.1 Reviewer 1

Reviewer:

"Blockchain technology plays a pivotal role in securing transactions within financial institutions, often functioning as a decentralized third-party intermediary." - This sentence could be expanded to explain more clearly how blockchain functions as a decentralized third-party intermediary and the implications of this role within financial institutions.

"To enhance the security and reliability of financial documents through the application of blockchain technology and digital signatures." - It would be beneficial to specify which aspects of security and reliability are being addressed. Are you focusing on data integrity, confidentiality, or authentication? A clear distinction is necessary.

"Today it is recognized as a critical technology for applications requiring immutable traceable data, encrypted and distributed ledgers, and secure transactions." - Consider providing specific examples of non-financial sectors where blockchain has been effectively applied to enhance the relevance of the review.

"This immutability protects both customers and financial institutions from fraudulent activities." - This statement should be backed by specific case studies or examples where blockchain immutability has successfully prevented fraud in financial institutions.

"A match confirms that the document has not been altered and was indeed signed by the purported signer." - Clarify what would happen if there is no match. Is there a protocol within the proposed model to handle such discrepancies?

"The signed document is stored on the blockchain along with metadata such as the signer's identity, timestamp, and relevant transaction details." - Consider discussing the potential storage limitations or scalability concerns associated with storing documents and metadata on the blockchain.

"In their study, Wang and Guan propose a traceable and secure data-sharing scheme based on blockchain technology." - A more detailed comparison of the proposed model with Wang and Guan's scheme would be beneficial. For instance, how do the two models differ in terms of encryption methods, and what are the specific advantages of your model over theirs?

"Both models are similar" - The term "similar" is vague. Consider quantifying the similarity in terms of performance metrics, such as processing time, security breaches, or throughput.

"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." - It would be helpful to provide a concrete example or case study where this model could be applied, highlighting the specific benefits realized.

Author revised the manuscript and uploaded the updated document.

1.2 Reviewer 2

Reviewer:

The diagram representing the proposed model lacks a detailed legend or explanation of each step within the figure. Including a more descriptive caption or a breakdown of the model components in the text would enhance clarity.

"The public key is openly shared while the private key remains confidential." - This section would benefit from a brief explanation of how PKI works within the context of the proposed model, particularly how it integrates with blockchain to enhance security.

"This process generates a unique fixed-size string of characters representing the document's content." - It would be useful to include a brief discussion on the choice of cryptographic hash function (e.g., SHA-256) and why it is suitable for this application, considering potential risks such as collision resistance.

"A typical blockchain operates as a peer-to-peer network controlled by decentralized computers that maintain a record of financial transactions." - This statement would benefit from a brief discussion of how different consensus mechanisms (e.g., Proof of Work vs. Proof of Stake) impact the security and efficiency of blockchain networks.

"This step ensures that the model complies with regulations and standards related to digital signatures and financial documents..." - The discussion on regulatory compliance is somewhat limited. Consider elaborating on specific regulations (e.g., GDPR, eIDAS) and how the model aligns with these requirements.

"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." - The introduction could be strengthened by including statistics or data on the frequency and impact of such cyber-attacks, emphasizing the urgency of the proposed research.

"Considering the use of hardware security modules (HSM) or secure key vaults for enhanced protection." - This suggestion is sound but lacks detail. A brief explanation of how HSMs and secure key vaults operate, along with their advantages in the context of the proposed model, would be beneficial.

Author revised the manuscript and uploaded the updated document.

2. Revised

Editor’s decision after revisions: Accepted.

Editor in Chief’s decision: Accepted.