RSA-Enhanced Blockchain-Based Multi-Factor Authentication Framework for Secure Financial Transactions

Maha Alwan Alteef, Maytham Mustafa Hammood

Department of Computer Science, College of Computer Science and Mathematics, University of Tikrit, Salah Al Din, Iraq.

Abstract

The given paper introduces a new Multi-Factor Authentication (MFA) framework that is based on blockchain and is combined with RSA encryption to improve the security of decentralized systems during financial transactions. MFA systems in general continue to be susceptible to phishing, SIM-swapping, and session hijacking, particularly within mobile and distributed contexts. The framework proposed integrates Time-based One-Time Passwords (TOTP) and RSA-based cryptographic signatures, making transaction requests authentic and unaltered. It is able to process transactions in a safe and controllable manner by using the logic of smart contracts on Ethereum Level-compatible systems, with the possibility of dynamic transaction cancellation and rejection. It has been shown that the system can provide high security assurances at costs that are tolerable in terms of latency and resources, and this makes the system viable to use in secure financial transactions in decentralized applications.

Keyword: Blockchain Authentication, RSA Encryption, Smart Contracts, Secure Financial Transfers, .TOTP, Decentralized MFA

1. INTRODUCTİON

As digital financial services are increasing, user authentication should be maintained securely and reliably. Although password authentication is used in many systems it falls prone to brute force, phishing, and credential theft methods. Regardless of the standard hashing approaches that are taken, users and companies have begun to adopt Multi-Factor Authentication; of particular use is the Time-based One-Time Passwords (TOTP). However, MFA on phones is subject to phishing, replacing the SIM card of a person, and a session hijack, so that the attackers can make it even with multiple verifications[1,2]. A majority of the MFA systems lack post-authentication security controls. Remarkably, the earlier existing solutions of hybridization between blockchain and MFA lacked substantial strengths in driving transaction management based on reversal, cancellation, and rejection. Therefore, when a user's login is stolen, the victim will hardly block the former. Furthermore, biometric solutions have several issues because they present both privacy and security problems, as well as require dedicated hardware and have their pitfalls that we overcome in the work [3]. The proposed paper presents a block chain-enabled MFA system, which consists of RSA encryption and digital signatures to provide a more secure as well as cryptographically safe authentication protocol. The suggested framework would integrate a TOTP check with the RSA-based signature of transactions to achieve the end-to-end integrity of transactions and avoid well-known attack patterns against decentralized systems. This work has the following contributions: The suggestion is to use a block chain-based MFA framework implemented with RSA digital signatures and developing a logical structure of a smart contract that checks the authenticity of a transaction with the help of public key cryptography. Also Time faulting, cancellation, and rejection of the secure transaction

management process and assessing the effectiveness of the system in aspects of latency, throughput, and crypto resiliency.

2.BACKGROUND AND RELATED WORK

2.1Background

1. **Multi-Factor Authentication (MFA)** is a relatively secure means. Multi-Factor authentication is widely applied since it involves various types of credentials, e.g., passwords, tokens, or biometrics [4]. When biometric authentication is involved, a discriminating evidence of identity is simple to make and they are increasingly being included in the MFA systems. There is no reason to guess that biometrics are impossible to copy since they are individual, and someone can access your biometrics as soon as needed, in case he or she sees your biometric information [5]. MFA helps to avoid such risks as the theft of login passwords and unauthorized use of resources. To illustrate, SIM swappers will not be in a position to access your phone number since they cannot acquire a token that is in your custody. As an example, MFA is present in banking solutions and security entry locks, and identification in mobile IDs in Sweden using Mobilt Bank ID, which recognizes a person and logs where they go and their behavior on the device [6]. Conversely, MFA may also cause some issues, such as being hard to use, as observed by some users, too expensive, requiring certain devices, and compatibility issues with older systems [7]. Besides, cryptography will also need to support massive use, primarily in systems, business, government, and crime investigation, but with sufficient privacy[8].

2. **Blockchain technology** was developed to ensure that transactions are safe, transparent, and cannot be manipulated. By 2008, when Bitcoin was launched, the blockchain technology was established to be used in other fields outside the digital currency[9]. In a blockchain system, only legitimate transactions get entrenched, and the agreement of many nodes ensures this. Instead of the block ledger having a set of random numbers connected with each other, it is instead connected through hash functions [10]. The majority of definitions of blockchain mention that it is decentralized, immutable, and transparent[11], [12].These three primary characteristics of blockchains deal with the security risks of any electronic system. The fact that the design of blockchain cannot be changed allows preventing abuse of authentication records by a user, and distributed authentication also decreases the likelihood of system failure. With blockchain and MFA, identity is confirmed with a log filled with information that cannot be altered and a multitude believes that. Due to this, it becomes possible to avoid or minimize credential reuse, man-in-the-middle attacks, and data breaches [14], [15]. Researchers propose a mechanism of how users would take advantage of such a system creating a pair of public-private keys and linking their credentials with the block chain.

3. **The RSA algorithm** introduced by Rivest, Shamir and Adleman in 1977 is one of the most commonly used asymmetric cryptographic algorithms that is based on the hardness of the mathematical problem of factoring such large prime numbers that when the size of the primes used are relatively large is not considered to be solvable [17]. RSA generates a key pair, a public key encrypts information and a privet key decrypts, and it is giving data confidentiality and realization of data authentication and non-repudiation through digital signature [18]. With multi-factor authentication systems, RSA tokens are used, where dynamic one-time passwords (OTPs) are used, which enhances security by mitigating replay and impersonation attacks [19] , which further improves the scope of security by eliminating replay and impersonation attacks. The RSA processing is intensive, but it is usually applied to encrypt small authentication tokens or session keys[20]. Particularly in blockchain-based MFA systems, where secure tokenization is crucial to financial transactions. User data with unique, non-sensitive identifiers (tokens), and when used in conjunction with RSA encryption, it offers strong protection of identity and access credentials [17, 21].

2.2 Related Work

Various authors have tested the effectiveness of blockchain technology that can be utilized in reinforcing multi-factor authentication in several areas. One of the articles written by Mark E. Geoghegan, named Blockchain-Based Multi-Factor Authentication in Future 6G Cellular Networks, demonstrated that introducing blockchain-MFA in the 6G cellular networks would provide immense enhancement in security by introducing various layers of defense controls [22]. Cloud-enabled IoT saw a package of methods being adopted to ensure that vehicular clouds and other devices become secured (namely, embedded digital signatures, SAML, and single sign-on) [23].

A system was introduced in smart cities that is based on zero-knowledge proofs, smart contracts, and the authentication done via one-time passwords [24]. Still another group investigated privacy, security, and usability of MFA systems based on blockchain and confirmed that it will be beneficial for future digital authentication systems [25]. It has been identified in the literature review that blockchain can enhance the security and simplify MFA installation in various environments, including control systems and IoT [26]. Blockchain was investigated in the setting of healthcare to ensure that sensitive information is secure and to increase accessibility of authentication [27] . The two-factor-authenticated blockchain implementation of the application on the WordPress web pages affirms what decentralized defense systems like MFA can do to avoid hacks [28,29].

In addition to such solutions implemented with the help of blockchain, numerous works and research performed are also devoted directly to RSA-based MFA systems and their role in particular spheres of security. RSA has also been used in the authentication of encryption of access information in the cloud, and this is used when seeking to ensure the confidentiality of data [26] . Biometric verification was combined with RSA in order to enhance accuracy and prevent spoofing attacks in the authentication of IoT [30]. A Web-based authentication framework has also been discovered to be the RSA-generated dynamic tokens and the hashing algorithm (SHA-256) that prevents replay and brute force attacks [31]. These studies and their main technical details are presented in the table below as show in Table.1

Table.1 Studies And Their Main Technical Details RSA-Enhanced Blockchain-Based Multi-Factor

Features	[22]	[23]	[24]	[25]	[26]	Ours
MFA	✓	✓	✓	✓	✓	✓
Blockchain	✓	✓	✓	✓	✓	✓
Smart Contracts	✗	✗	✓	✓	✗	✓
Biometric	✗	✗	✓	✓	✓	✓
Privacy	✓	✗	✓	✓	✗	✓
Adaptive MFA	✗	✗	✗	✗	✗	✓

Although MFA using block chain technology has progressed significantly, existing papers tend to focus on MFA in specific fields rather than its broader application across various systems. Some applications choose to encrypt information using smart contracts for extra privacy. However, many cannot work on a global scale or do not adequately consider users' needs and problems with integration. Furthermore, real-world matters such as resource utilization and adherence to data protection rules have not been thoroughly studied. The next research stage needs to develop frameworks that adapt to users' needs, ensure security, ease of use, and high performance.

3.METHODOLOGY

The research currently follows a design and implementation approach, in which an RSA-based block chain-enhanced Multi-Factor Authentication (MFA) protocol is developed and tested to provide financial transaction security in a decentralized setup. The system is designed with cryptography integrated into its design, smart contracts are developed, and the system is validated.

3.1System Architecture

The system architecture suggested has four main blocks that can cooperate with each other and make the authentication and transactions safe:

1. User Interface: Frontend composed of HTML, CSS, and JavaScript that allows interacting with the block chain wallet through MetaMask, where approvals of transactions are conducted.

2. Backend Server: The backend is implemented with the use of Flask (Python) to carry out the steps of user registration, password hashing, TOTP token generation, creating an RSA key pair, and initial transaction preparation.

3. Blockchain Layer: Transactions, RSA signatures, and tamper-proof storage of transactions are verified using a smart contract on the Ethereum-compatible testnet.

4. Cryptographic Layer: Transactions' hashes are signed with RSA (2048-bit). The on-chain storage of the public keys is intended to be secure, whereas the keys that the user is meant to privately possess are local and stored on their device specifications.

3.2The workflow of Multi-Factor Authentication

The authentication and transaction flow are done through the following steps sequentially:

1. User Authentication: The user will be logging in with username, password, and Time-based One-Time Password (TOTP). This verification will be performed using Google Authenticator. These credentials are checked using a backend server.

2. RSA Key generation: In the event that authentication is successful, the system automatically creates an RSA key pair. The local user storage stores the user secret key, and the secret keys are deployed on the blockchain in the form of a smart contract using the public key.

3. Transaction Preparation: The user is prompted to enter the recipient address, sender wallet address, amount to send, and a valid TOTP token. This transaction information is combined by the system.
4. Hash Generation: To create a unique fingerprint of the transaction, the system stores a SHA-256 hash of the transaction data.

5. Digital Signature RSA: The transaction hash is signed using the user's private RSA key, thus making sure the transaction has authenticity and integrity.

6. Transaction Submission: The approved transaction data, TOTP token, and RSA signature are presented to the blockchain smart contract to be checked.
7. Smart contract Verification: The smart contract has two checks of security:

    - It authenticates the digital signature with RSA using the registered public key.
    - It authenticates the TOTP token to ensure that it is correct and not expired.

8. Execution of a Transaction Decision:

    - In case the RSA signature and TOTP tokens validate correctly, the operation is completed and successfully applied to the blockchain.
    - When either of the two verifications fails, the transaction is automatically rejected.

3.3 Implementation Details

The development and testing technologies of the system are as follows:

1. Frontend: HTML, CSS, JavaScript, MetaMask
2. Backend Python (Flask), RSA cryptography package, PyOTP package - to generate TOTP tokens
3. Blockchain Platform: Ethereum-smart (testnet: Ganache)
4. Smart Contracts: Solidity, which is implemented through Remix IDE

The backend server is responsible for generating RSA key pairs, creating TOTP tokens, and processing transactions. Meanwhile, the smart contract validates these transactions using the stored public keys and dynamic transaction tokens.

3.4Security Consideration

1. The RSA keys are locally generated, so that no transmission of the keys is ever done, and the keys are kept securely on the user apparatus and do not leave.
2. TOTP tokens are bound to time and a device, which minimizes the chance of a token reuse.
3. Verify the Smart contract is developed to reject a bad signature, expired tokens, and replays.
4. The system exploits Web3 wallet signatures and HTTPS to prevent a man-in-the-middle attack.

4. RESULTS AND EVALUATION

4.1Functional Testing

Each of the essential elements was tried in the conditions of common use:

1. Registration of the users, log in, and binding of tokens.
2. RSA signature and key creation.
3. Use of MetaMask to interact with the wallet.
4. Claim/reject and secure transaction flow.

Everything was functioning according to the plan, and both tokens and RSA signatures were appropriately verified by the smart contract[12, 25, 30-34].

4.2 Cryptographic Evaluation

Security is significantly increased by adding cryptographic signing:

1. Key pairs are made locally on a per-session basis by RSA.
2. The smart contract will use the signature of the sender to verify using the same public key.
3. It ensures that messages have origin (authenticity), cannot be altered (immutability), and cannot be replayed or tampered with.

4.3Performance Evaluation

To supplement the low-level benchmarks, the entire system performance was measured on the optimized BFTM framework with the inclusion of RSA encryption and digital signing. This assessment evaluated the actual latency, block confirmation time, throughput, and operational failure rates in secure transactions as shown in table.2 [9, 17. 23].

Table 2:Overall Performance Metrics for the Encrypted System

Metric	Value
Average Latency	193.56 ms
Average Block Confirmation Delay	494.16 ms
Estimated Throughput	309 operations per minute
Failure Rate	6.00%

These values adequately show the possible measurement of a system with regard to performance following the application of RSA encryption and superior levels of validation. Although the latency and block delay get exacerbated by cryptographic overhead and audit log, the throughput is adequate on secure decentralized applications. The observed rate of failure shows rejections that are anticipated by an invalid or expired token, and it demonstrates the appropriate application of access management.

4.3 **Performance Comparison: Original vs. Encrypted System and Security Validation**

Table.3 shows the original (i.e., non-encrypted) system was compared to the enhanced encrypted system to show the trade-offs that were implemented by the particular encryption. In the table.3 below, the most crucial performance indicators of both versions are summarized based on similar tests.

Table 3: Comparison between original and enhanced systems:

Metric	Original System	Encrypted System
Average Latency	101.27 ms	193.56 MS
Block Confirmation Delay	255.71 ms	494.16 MS
Throughput (Estimated)	592 ops/min	309 ops/min
Failure Rate	0.00%	6.00%

On the encrypted system as showed in table 3 and 4. the latency and confirmation delay are significant, and this concerns implementation of cryptographic mechanisms (i.e., RSA key validation and secure session enforcement). As expected, throughput was lowered, but this is a fair trade-off since data security is improved, thereby enhancing the integrity of transactions. Though the failure rate was moderate, the system was relatively stable and resistant to simultaneous use, which means the system had high resilience, and it was quite suitable and practical for real-life financial conditions.[8, 15, 28.30]

The five types of attack scenarios were simulated in Table .4

Table 4: Attack Scenarios and Defense Summary

Attack	Result	Defense
Replay	Rejected	Token hashed; duplicates ignored
MitM	Failed	HTTPS + Web3 wallet signatures prevent replay
Token Injection	Failed	Smart contract accepts only pre-registered hashed tokens
Overwrite	Denied	Only sender (msg.sender) can modify transfer state
DoS	Partially blocked	Invalid entries rejected; frontend slows under high-frequency calls

5. CONCLUSIONS

From the perspective of enhancing such multi-factor authentication methods, the proposed research introduces a modified version of Block chain-Based Multi-Factor Authentication (BFTM) system with the intention of making digital fund transfers safer by enforcing RSA-based cryptographic signatures, TOTP validation, and smart contract logic in the Ethereum community. The offered framework deployed is the combination of the classic authentication techniques (passwords and OTPs) and decentralized trust, as well as digital signature verification, balancing between data integrity and control of transactions on the user side.

6. REFERENCES

1. Jakobsson, M. (2018). Two-factor inauthentication–the rise in SMS phishing attacks. Computers and Fraud Security, 2018(6), 6–8. https://doi.org/10.1016/S1361-3723(18)30053-2
2. Papaspirou, V., Tsoukalas, A., and Fragkoadakis, A. (2022). Security revisited: Honeytokens meet Google Authenticator. In 2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) (pp. 1–8). IEEE. https://doi.org/10.1109/SEEDA-CECNSM57789.2022.9981883
3. Berdik, D., Otoum, S., Schmidt, N., Porter, D., and Jararweh, Y. (2021). A survey on blockchain for information systems management and security. Information Processing and Management, 58(1), Article 102397. https://doi.org/10.1016/j.ipm.2020.102397
4. Grimes, R. A. (2020). Hacking multifactor authentication. John Wiley and Sons. https://doi.org/10.1002/9781119650768
5. Sultan, K., Ruhi, U., and Lakhani, R. (2018). Conceptualizing blockchains: Characteristics and applications. arXiv. https://doi.org/10.48550/arXiv.1806.03693
6. Göransson, A., and Asklund, E. (2020). BankID-based authentication for phone calls [Master's thesis, Lund University]. Lund University Publications Student Papers. https://lup.lub.lu.se/student-papers/search/publication/9017684
7. Jain, A. K., Bolle, R., and Pankanti, S. (Eds.). (2006). Biometrics: Personal identification in networked society (Vol. 479). Springer Science and Business Media. https://doi.org/10.1007/0-306-47006-X
8. Chaurasia, B. K., and Verma, S. (2011). Infrastructure based authentication in Vanets. International Journal of Multimedia and Ubiquitous Engineering, 6(2), 41–54.
9. Acharya, S. A. (2013). Two factor authentication using smartphone generated one time password. IOSR Journal of Computer Engineering, 11(2), 85–90. https://doi.org/10.9790/0661-1128590
10. Fan, K., Ge, N., Gong, Y., Li, H., Su, R., and Yang, Y. (2017). An ultra-lightweight RFID authentication scheme for mobile commerce. Peer-to-Peer Networking and Applications, 10(2), 368–376. https://doi.org/10.1007/s12083-016-0443-6
11. Neha, and Chatterjee, K. (2016). Authentication techniques for e-commerce applications: A review. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 693–698). IEEE. https://doi.org/10.1109/CCAA.2016.7813811
12. Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros and M. Zhegu (Eds.), Research handbook on digital transformations (pp. 225–253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019

13. Atlam, H. F., Alenezi, A., Alassafi, M. O., and Wills, G. B. (2018). Blockchain with Internet of Things: Benefits, challenges, and future directions. International Journal of Intelligent Systems and Applications, 10(6), 40–48. https://doi.org/10.5815/ijisa.2018.06.05
14. Christidis, K., and Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
15. Yue, X., Wang, H., Jin, D., Li, M., and Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10), Article 218. https://doi.org/10.1007/s10916-016-0574-6
16. Atlam, H. F., and Wills, G. B. (2019). Technical aspects of blockchain and IoT. In Advances in Computers (Vol. 115, pp. 1–39). Elsevier. https://doi.org/10.1016/bs.adcom.2018.10.006
17. Al-Badri, K. S. L., & Muhammad, F. Q. (2020). Four band electromagnetic waves absorber using negative refractive index materials (metamaterials). Scientific Journal of King Faisal University Basic and Applied Sciences, 21(1), 1-11, https://doi.org/10.37575/b/sci/2055 .
18. Rivest, R. L., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342
19. Stallings, W. (1995). Network and internetwork security: Principles and practice. Prentice-Hall, Inc. https://dl.acm.org/doi/abs/10.5555/193189
20. Katz, J., and Lindell, Y. (2007). Introduction to modern cryptography: Principles and protocols. Chapman and Hall/CRC. https://doi.org/10.1201/9781420010756
21. Ahmad, M. S., Mohyuddin, W., Choi, H. C., and Kim, K. W. (2018). 4 × 4 MIMO antenna design with folded ground plane for 2.4 GHz WLAN applications. Microwave and Optical Technology Letters, 60(2), 395–399. https://doi.org/10.1002/mop.30969
22. Al-Badri, K., & Ekmekçi, E. (2016). A Numerical Study with Various Intersecting Twin Structures on Tuning the Absorption Spectra in S-Band.
23. Menezes, A. J., van Oorschot, P. C., and Vanstone, S. A. (2018). Handbook of applied cryptography. CRC Press. https://doi.org/10.1201/9780429466335
24. Al-badri, K. S. L. (2020, November). Ultrathin perfect metamaterial absorber based on triquetra shape. In IOP Conference series: Materials science and engineering (Vol. 928, No. 7, p. 072065). IOP Publishing.
25. Asim, J., Khan, A., Al-Khasawneh, A., and Al-Qerem, A. (2022). Blockchain-based multifactor authentication for future 6G cellular networks: A systematic review. Applied Sciences, 12(7), Article 3551. https://doi.org/10.3390/app12073551
26. Kebande, V. R., Awaysheh, F. M., Ikuesan, R. A., Alawadi, S. A., and Alshehri, M. D. (2021). A blockchain-based multi-factor authentication model for a cloud-enabled Internet of Vehicles. Sensors, 21(18), Article 6018. https://doi.org/10.3390/s21186018
27. Ahmad, M. O., Al-Fuqaha, A., and Guizani, M. (2023). BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities. Sensors, 23(5), Article 2757. https://doi.org/10.3390/s23052757
28. Wanisha, I., James, J. B., Witeno, J. S., Bakery, L. H. M., Samuel, M., and Faisal, M. (2024). Multi-factor authentication using blockchain: Enhancing privacy, security and usability. International Journal of Computer, Technology and Science, 1(3), 41–55. https://doi.org/10.62951/ijcts.v1i3.24
29. Fneish, M., El-Hajj, M., and Samrouth, K. (2023). Survey on IoT multi-factor authentication protocols: A systematic literature review. In 2023 11th International

Symposium on Digital Forensics and Security (ISDFS) (pp. 1–7). IEEE. https://doi.org/10.1109/ISDFS58141.2023.10131870

30. Suleski, T., Ahmed, M., Yang, W., and Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health, 9, Article 20552076231177144. https://doi.org/10.1177/20552076231177144
31. Cardoso, J. A. A., Ishizu, F. T., de Lima, J. T., and de Souza Pinto, J. (2019). Blockchain based MFA solution: The use of hydro raindrop MFA for information security on WordPress websites. Brazilian Journal of Operations and Production Management, 16(2), 281–293. https://doi.org/10.14488/BJOPM.2019.v16.n2.a11
32. Eldow, A., Mohamed, A., and Hamid, A. (2021). Information communication technology infrastructure in Sudanese governmental universities. In Recent Advances in Intelligent Systems and Smart Applications (pp. 363–375). Springer. https://doi.org/10.1007/978-3-030-47411-9_21
33. Velásquez, I., Caro, A., and Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. Information and Software Technology, 94, 30–37. https://doi.org/10.1016/j.infsof.2017.09.012
34. Kalpana, P., and Singaraju, S. (2012). Data security in cloud computing using RSA algorithm. International Journal of Research in Computer and Communication Technology, 1(4), 143–146.