International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 06 | June - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Secure and Flexible Blockchain-BasedOffline Payment Protocol

Mr. Prasanna Kumar M J
Assistant Professor
Computer Science and Engineering
BGS Institute of Technology
Adichunchanagiri University

Poorvika D A
20CSE062
Computer Science and Engineering
BGS Institute of Technology
Adichunchanagiri University

Abstract:
Off-chain transactions aim to tackle the scalability issues of on- chain processes and enable smoother blockchain-based payments over unreliable networks. However, existing solutions often struggle to strike a balance between security and flexibility. Our hypothesis suggests that by leveraging loosely synchronized clocks and channels with known latency bounds, two offline parties can conduct secure and flexible off-chain transactions. To support this hypothesis, we've introduced a new blockchain-based offline payment protocol. Our approach utilizes on-chain smart contracts and offline wallet interactions to ensure resilience against intermittent on-chain connectivity. By employing platform-agnostic Trusted Execution Environments (TEEs) and open transactions, our protocol achieves flexible and trusted computations. Through empirical evaluation, conducted using Intel Software Guard Extensions (SGX), we have demonstrated that our protocol is highly efficient and offers advanced security and flexibility. Additionally, we've tested our construction against various real-world attacks, confirming its security and robustness within a universally composable framework under synchronous settings. This research significantly contributes to the development of safe and user- friendly offline payment solutions for blockchain technology

Keywords-Blockchain, offline payment, smart contract, security, flexible, protocol.

1. INTRODUCTION

In today's global economy, blockchain technology is increasingly recognized for its role in bypassing trusted intermediaries. The initial demonstration of its practicality came through Bitcoin, proposed by the pseudonym Satoshi Nakamoto. Ethereum, the second most valuable cryptocurrency, introduced the concept of smart contracts, enabling a wide range of applications beyond finance. Governments, academics, and professionals are turning to blockchain to solve various real-world challenges in finance, e-health, cloud services, and autonomous vehicle networks. Security, scalability, and decentralization are critical considerations in blockchain research, although achieving all three simultaneously, as per Vitalik's trilemma, remains elusive. While much attention has been given to synchronous networks, there's a growing interest in enhancing blockchain solutions for adversarial networks with intermittent connectivity.

Offline payments have emerged to facilitate transactions conducted offline and reconciled later with network connectivity. Off-chain transactions are pivotal in enabling offline payments within blockchain frameworks. Payment channels have been instrumental in addressing scalability concerns at the layer-2 level but face criticism for their reliance on pre- established channels and the locking of funds, hindering flexibility and introducing security vulnerabilities. Addressing these issues could enhance the adoption of blockchain technology in real-world offline-first applications.

We have developed a comprehensive threat model that considers the multitude of security challenges present in blockchain-based offline payment systems. Our aim is to demonstrate the resilience of our approach through

universal composability (UC) under synchronous conditions.

Additionally, we have established a methodology for provisioning source code and evaluating its performance. By analyzing the lexical characteristics of our protocol's source code, we ensure its integrity and assess its efficiency using metrics relevant to real-world applications.

II. RELATED WORK

This section revisits the existing literature on offline blockchain- based payments. Presently, research in this area has predominantly emphasized either security or flexibility, with few constructions managing to address both requirements effectively.

Neither of the aforementioned solutions provides instant settlement for the payee's offline account. In cases of poor on-chain connectivity, these approaches struggle to verify transaction status promptly and update offline account balances in a timely manner. Maintaining accurate balance information is crucial for ensuring the coherence of future transactions.

Igboanusi et al. introduced the PureWallet (PW) framework, employing Ethereum smart contracts. However, their system lacks a mechanism to detect token forgery, making it unsuitable for real- world applications where basic security requirements are essential. Additionally, tokens in their framework cannot be redistributed, requiring on-chain network availability to update account states, limiting flexibility in offline transactions.

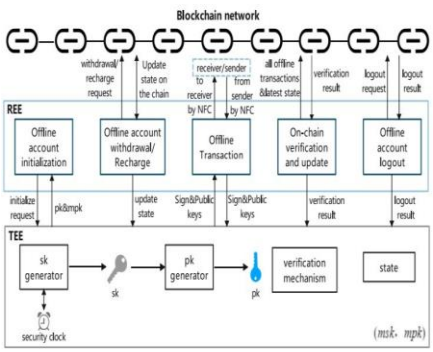
Wang et al. proposed the MOBT wallet model, which generates key pairs for offline wallets using the master public key property of hierarchical deterministic (HD) wallets.

In their research, Wang et al. proposed a method where wallets only need to store and back up the master private keys, rather than individual private keys generated for each offline transaction. This approach addresses scalability concerns related to storage, as the size of offline wallets does not increase with the number of transactions performed. Additionally, they implemented an interactive signature protocol to prevent Kleptographic attacks on offline wallets.

Despite recent advancements in offline payment solutions supporting open transactions and enhancing flexibility, they often compromise on basic security requirements. The balance between flexibility and security in these solutions tends to favor flexibility, with security thresholds remaining relatively low.

To our knowledge, existing approaches have not effectively achieved a high level of both security and flexibility simultaneously. Our proposed blockchain-based offline payment protocol aims to address this limitation for the first time in the literature.

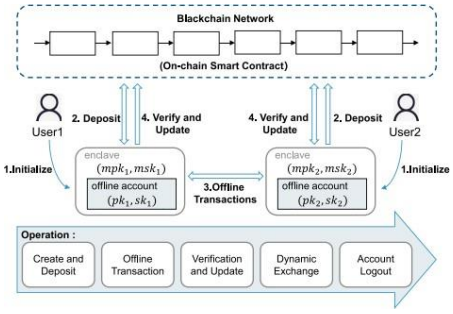
III. The System's Architecture



1. Our objective is to develop a secure blockchain-based offlinepayment protocol that demonstrates the following characteristics: Coins and data unforgeability: Our protocol must prevent maliciousactors from executing coin forgery attacks, and users should beunable to forge transaction data in their offline wallets. Consistency: Unconfirmed on-chain transaction states should not be considered valid in offline scenarios. Offline payees should have thecapability to independently verify the legitimacy of an offline transaction on-site. Resistance to double-spend, double-deposit, and man-in-the-middle attacks: Our scheme should effectively prevent double-spending and attempts to deposit multiple times from the same offline transaction. Additionally, it should mitigate offline identity spoofing and deter man-in-the-middle attacks.

2. Our goal is to develop a flexible blockchain-based offline payment protocol with the following features: Open transactions: Our protocol supports open transactions, allowing users to engage in off-chain transactions without prior commitment to an on-chain multi-signature account. Coin redistribution: We aim to enable coin redistribution using divisible cryptocurrency, allowing users to transact divisible units without the need for a change address, unlike the Bitcoin system. Instant settlement and platform-agnostic design: Offline payeesshould update their account balances promptly, and our protocolshould be deployable across various Trusted ExecutionEnvironment (TEE) platforms. Offline Transaction Atomicity: Offline commits should accurately update user offline accounts with non-repudiation, while offline aborts should revert the user's offline state to its previous values with coherence. Optimistic Responsiveness: To maximize flexibility, our protocol leverages weaker on-chain synchrony and performs optimally during on-chain asynchrony.

IV. IMPLEMENTATION



V. EXPERIMENTS

This protocol implements functions within a blockchain-based offline payment scenario and assesses them against existing offline payment solutions in the blockchain realm. It evaluates against basic security needs like preventing coin forgery, offline transactiondata forgery, double-spending, double-deposit, and man-in-the- middle attacks. Additionally, it addresses practical flexibility requirements, such as open transactions, offline coin redistribution, and instant settlement for offline payments, to meet user demands inreal-world application scenarios.

VI. CONCLUSIONS

This study aimed to investigate the feasibility of conducting blockchain-based offline payments between two parties while ensuring both security and flexibility. To address this objective, wedeveloped an innovative offline payment protocol suitable for situations of partial network asynchronism. Our methodology involves the utilization of on-chain smart contracts when the on- chain connectivity is strong, and the execution of secure off-chain transactions utilizing compatible Trusted Execution Environments(TEEs) during periods of poor on-chain network performance. We established a threat model specifically tailored for blockchain-based offline payments across an asynchronous network. Our analysis demonstrated that our framework satisfies essential security prerequisites in real-world offline payment settings, effectively safeguarding against coin forgery attacks, offline transaction forgery, double-spend and double-deposit attacks, as well as man-in-the-middle attacks. Additionally, our protocol demonstrates versatility through the implementation of open transactions, facilitating coin redistribution and instant settlement.We conducted an evaluation of our protocol using Intel SGX and conducted an empirical performance analysis on the Ethereum blockchain. Furthermore, we offered a theoretical comparison between our approach and existing constructions. Our results indicate that our protocol strikes a balance between security and flexibility when juxtaposed with current solutions. These findingshold significance for various stakeholders including businesses, governmental entities, academics, and industry practitioners.
However, a notable limitation of our scheme is its lack of support for fully asynchronous mode, representing an area ripe for future research. Our study underscores the necessity for secure and adaptable offline payment solutions to enhance user experience andfoster broader adoption of blockchain technology.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Decentralized Bus. Rev., 2008, Art. no. 21260.

[2] V. Buterin et al., “A next-generation smart contract and decentralized application platform,” White Paper, vol. 3, no. 37, pp.2–1, 2014.

[3] “Biggest cryptocurrency in the world - Both coins and tokens - Based on market capitalization on November 11, 2022.” Statista. Accessed: Nov. 2022. [Onlline]. Available: https://www.statista.com/statistics/ 1269013/biggest-crypto-per- category-worldwide/ [4] B. Sriman and S. G. Kumar, “Decentralized finance (DEFI): The future of finance and defi application for Ethereum blockchain based finance market,” in Proc. Int. Conf. Adv. Comput., Commun. Appl. Informat. (ACCAI),2022, pp. 1–9.

[5] P. Kar, K. Chen, and J. Shi, “DMACN: A dynamic multi- attribute caching mechanism for NDN-based remote health

monitoring system,” IEEE Trans. Comput., vol. 72, no. 5, pp. 1301–1313, May 2023.

[6] M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo, and J. Yu, “Cloudchain: A cloud blockchain using shared memory consensus and RDMA,” IEEE Trans. Comput., vol. 71, no. 12, pp. 3242–3253, Dec. 2022. [7] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng, and F. Dressler, “BLOWN: A blockchain protocol for single-hop wireless networks under adversarial SINR,” IEEE Trans. Mobile Comput., vol. 22, no. 8, pp. 4530–4547, Aug. 2023.

[8] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu, and X. Cheng, “wChain: A fast fault-tolerant blockchain protocol for multihop wireless networks,” IEEE Trans. Wireless Commun., vol. 20, no. 10, pp. 6915–6926, Oct. 2021.

[9] V. Buterin. “Ethereum. On sharding blockchains.” GitHub. Accessed: Nov. 19, 2019. [Online]. Avalable: https://github.com/ethereum/wiki/

[10] J. S. Bellagarda, “The potential effect off-chain instant payments will have on cryptocurrency scalability issues-the lightning network,” in Proc. Int. Conf. Inf. Resour. Manage. (CONFIRM), 2019, vol. 2, pp. 1–14.

[11] N. Ying and T. W. Wu, “xlumi: Payment channel protocol and off-chain payment in blockchain contract

systems," 2021, arXiv:2101.10621.

[12] L. Zhong, Q. Wu, J. Xie, J. Li, and B. Qin, "A secure versatile light payment system based on blockchain," Future Gener. Comput.Syst., vol. 93, pp. 327–337, Apr. 2019.

[13] E. Rohrer, J. Malliaris, and F. Tschorsch, "Discharged payment channels: Quantifying the lightning network's resilience to topologybased attacks," in Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW), 2019, pp. 347–356.

[14] A. Mizrahi and A. Zohar, "Congestion attacks in payment channel networks," in Financial Cryptography and Data Security, N.Borisov and C. Diaz, Eds., Berlin, Heidelberg: Springer BerlinHeidelberg, 2021, pp. 170–188.

[15] J. Poon and T. Dryja, "The bitcoin lightning network: Scalableoff-chain instant payments," 2016