Resilient Offline Payment Networks: Self-Healing Mesh Architecture for Infrastructure-Free Commerce

Quang Huy Do
LISSI-TincNET Research Team, University of Paris-Est Creteil, France

Thiago Abreu
LISSI-TincNET Research Team, University of Paris-Est Creteil, France

Sami Souihi
Universite Paris-Saclay, CEA, List, F-91120, Palaiseau, France
LISSI-TincNET Research Team, University of Paris-Est Creteil, France

ABSTRACT

In recent years, mobile payment plays a vital role in enabling users to get access to numerous mobile applications such as money transfer, mobile banking, digital wallet, etc. However, mobile-payment platforms depend on continuous Internet connectivity, a resource that is still limited and unreliable in many regions. In this paper, we propose a method for offline payment with wireless mesh networks that enables secure, offline, real-time settlement. Our approach implemented with Mininet-Wifi demonstrates that it can achieves 97.28% transfer success rates with 250+ nodes, sub-1500ms transaction latency, and automatic recovery from 33% node failures.

1 INTRODUCTION

According to [12], the global mobile payment market projected to reach 7.58 trillion USD by 2027, at a CAGR of 29.0% during the forecast period. This remarkable expansion is particularly significant in developing countries, where mobile wallets have become the dominant payment method. The study [3], found that transactions via mobile wallets and phones were the equivalent of 87% of GDP in Kenya and 82% in Ghana.

However, internet infrastructure is one the main reasons that challenges mobile payment for wide adoption. The internet infrastructure deployment in developing countries—particularly across Africa—remains severely constrained. Less than a third(27%) of adults in Africa can have access mobile Internet services [10]. In bustling open-air markets, traders and shoppers often have internet capable phones in their pockets yet still pay with cash because the network is down or too slow to authorize transactions in real time. Compounding these challenges, internet shutdowns happened 21 times in 2024 in African countries, the highest number in a single year [4]. During shutdowns, mobile money agents and end users lose access to their wallets, resulting in the suspension of peer-to-peer transfers and merchant transactions.

Traditional mobile money systems further worsens these limitations, as they depend on centralized banking infrastructure for transaction settlement. These systems become inaccessible during network disruptions, with studies showing that internet shutdowns could have an estimated GDP impact of approximately $3 million per day of disruption, amounting to 0.4% of daily GDP [11]. Additionally, the complex security validation processes require extensive Know Your Customer (KYC) procedures that systematically exclude populations, particularly affecting the 850 million adults globally who do not have a form of ID, while mobile money providers typically charge significant fees ranging from 4.64% to 4.80% for cross border remittances [8]. In contrast, a blockchain based settlement layer enables peer-to-peer value transfer without relying on any single institution. It remains available even during network disruptions, reduces transaction costs by removing intermediaries, and provides a transparent, tamper resistant ledger that can serve users outside the conventional financial system [9].

Thus, in this paper, we propose a method that leverages wireless mesh networking and blockchain technology, enabling devices to form decentralized, peer-to-peer communication networks. In this architecture, mobile devices communicate directly with each other, relaying payment information across multiple hops until reaching the destination node. To address the challenges of trust and transaction validation in such a decentralized environment, we introduce a decentralized weighted voting mechanism. In this system, authority nodes (such as mobile money agents, merchants, or trusted community members) are assigned voting weights proportional to their historical transaction volumes or reputational metrics. When a payment is initiated, a quorum of these weighted authorities collectively validates and signs the transaction, providing robust consensus and reducing the risk of fraud or double spending.

Contributions. We make the following contributions:

- Propose a novel, infrastructure independent mobile payment architecture that uses wireless mesh networking to enable resilient, peer-to-peer transactions in environments with unreliable or limited internet connectivity.
- Introduce a decentralized weighted voting to ensure secure, transaction validation within decentralized networks, mitigating risks of fraud and double spending.
- Provide an evaluation of the proposed system under realistic connectivity constraints and user mobility.

Outline. The remainder of this paper is structured as follows. Section 2 provides background and related work. Section 3 details the proposed offline payment methodology. Section 4 presents the experimental results and analysis. Finally, Section 5 concludes the paper with a discussion of key findings and future research directions.

2 RELATED WORK

LIO-Pay [14] currently represents the state of the art in offline payment research. The protocol tackles the offline payment trilemma by

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

combining blockchain anchoring with cryptographically secure tokens executed inside trusted execution environments (TEEs). While this hardware design prevents double spending and facilitates loss recovery without continuous connectivity, it imposes three practical barriers to large scale deployment in low resource contexts such as rural Africa: (i) it relies on specialized secure elements or TEEs that are absent from most entry level smartphones, (ii) it introduces a centralized trust dependency on hardware vendors and authorities, and (iii) the cost of having millions of devices with certified TEEs is economically limited.

It is also worth to mention Fastpay [2], that inspires our design. FastPay employs a committee of authorities that pre-sign account certificates; clients obtain a quorum of signatures in a single network round, delivering sub-100 ms settlement latency and >80 k TPS. We extend FastPay by replacing its static weighted quorum with a dynamic, decentralized weighted voting scheme inspried by Cabinet[15]. Specifically, authority nodes are selected through a hybrid admission process that combines stake commitment with performance-based evaluation: candidate nodes must lock a minimum stake to get admitted into the authority set. Once admitted, each authority's voting power is updated according to an audit score that reflects both performance (recent transaction throughput, uptime) and trust metrics (peer reputation, history of misconduct). Moreover, we remove infrastructure dependencies, we embed this enhanced FastPay atop a mesh network formed directly among mobile nodes. By employing decentralized weighted voting with a mesh overlay, our system sustains secure payments across multi hop paths during prolonged internet or cellular outages, overcoming the deployment barriers faced by prior offline payment solutions.

In fact, there are already several solutions that reuses commodity WiFi and Bluetooth radios to enable a peer-to-peer mesh networking. Among existing mesh based solutions, LNMesh [7] demonstrates that Bitcoin Lightning Network channels can be relayed over WiFi/BLE mesh network, achieving sub-second confirmations and onchain interoperability. While the work looks promising, it requires conditions that may limit its practical deployment in real world scenarios. For instance, LNMesh requires an active internet connection to establish and settle Lightning channels before and after a payment session. This requirement cannot be promised in environments prone to sudden or prolonged internet outages, where users may not have the opportunity to open a channel in advance and close them after transfer is done. In contrast, the protocol proposed in our work requires only a one time token deposit prior to offline usage, eliminates the need for an active internet connection during the transaction process.

3 METHODOLOGY

3.1 Overview

We consider our system as a side chain. Our protocol keeps a local ledger, a copy of Users' balances, taken from the main blockchain; so they can keep making payments even if the internet goes out. Before going offline, Users lock some of their money on the main blockchain—this ledger is a smart contract blockchain such as Ethereum [1]. Inside the mesh, our Authorities move these prefunded balances quickly between Users, while the main blockchain stays untouched. When connectivity returns, the mesh sends one batched update back to the main blockchain so its balances and the mesh balances line up again.

3.2 System Architecture

Figure 1 shows the architecture of our offline-payment protocol. Our system involves two types of participants:

- Users: nodes that create and receive payment requests.
- Authorities: nodes that contribute weighted signatures to achieve local consensus and prevent double spending while offline.

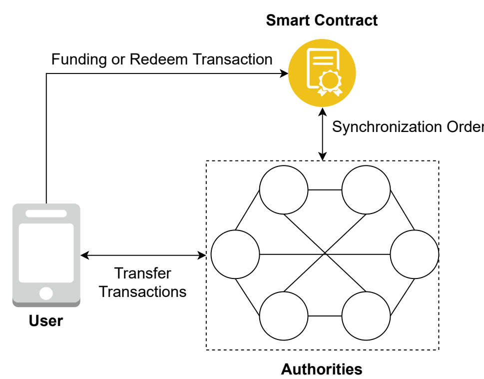

Figure 1: System Architecture

A detailed description of the protocol is deferred to two subsequent sections: the funding phase in sub-section 3.3.1 and the transfer and settlement phase in sub-section 3.3.2.

3.3 Offline Payment Protocol

3.3.1 Depositing Funds. As illustrated in Figure 2, an user initiates a deposit by invoking the on chain smart contract on the main blockchain. The contract locks the specified amount and returns a signed deposit receipt that binds the value to the user's public key and the current mesh-committee epoch. The user forwards this receipt to a nearby authority, which verifies the on chain signature and records the corresponding balance in the local mesh ledger. Once at least a quorum of Authorities attest to the receipt, the funds become immediately spendable inside the offline mesh, guaranteeing that every token circulating off chain is fully collateralized on the main chain ledger.

3.3.2 Transferring Funds And Settlement. Figure 3 depicts an offline payment between two Users. The Sender creates a transfer order and broadcasts it to the Authorities. Each Authority independently checks the Sender's balance and, if valid, adds its weighted signature to the order and send back a signed transfer order. After collecting enough signed signatures from a quorum, the Sender can form a transfer certificate and forward it to the Receiver as proof of payment. To conclude the order, the Sender or Recipient broadcast the transfer certificate (called confirmation order) to all authorities. With the certificate, Authorities update respective balances of Seller and Recipient and then the transaction is considered final.

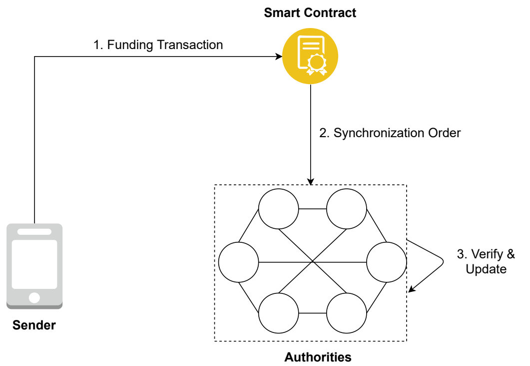

Figure 2: Transfer of funds from Blockchain to Protocol

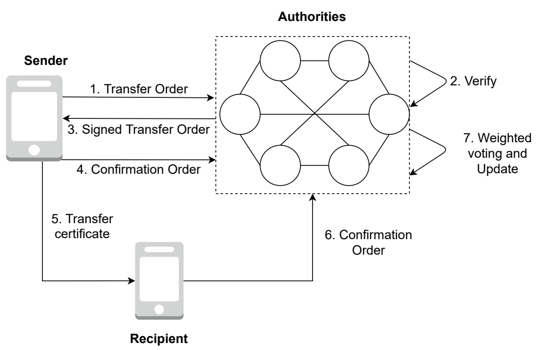

Figure 3: Transfer of funds between Users

4 EVALUATION

4.1 Experimental Setup

We perform the emulations with **Mininet-WiFi** [5] over an area of 1000×1000 m^2. All the emulations are averaged over 10 runs with each emulation running for 3000 s. Emulations are performed with 200 User and 50 Authorities. Each User sends one transfer order at 10 s interval time. Propagation loss model `logDistance` is used to limit the transmission ranges of the nodes. The transmission range of the nodes is set as 5m for evaluation. The mobility model used is Random Way Point [6] to mimic the movement of mobile user in real world. The detail of all emulation parameters is shown on GitHub. [1]

4.2 Results

Table 1: Transaction performance with 50 Authorities and 200 Users.

Metric	Median	95th pct.	Success Rate
End-to-End Latency	1200 ms	1500 ms	97.28%

Table 1 shows that our protocol confirms payments in a median of 1200 ms and stays below 1500 ms at the 95th percentile, marginally exceeding the one-second target for retail transactions. Overall, 97.28% of transfers finish within the 1500 ms. Detail simulation result can be seen on Github 1.

[1] https://github.com/HuyPHD2024-2027/smart-pay

5 CONCLUSION

Our early results show that an offline payment protocol over a mesh network can clear retail payments in around 1.5 second even when internet connectivity is unavailable. These results, however, reflect best-case laboratory conditions: traffic is evenly distributed across nodes and authority load is still modest. Future work will therefore (i) validate the protocol on real mobile devices, (ii) integrate privacy primitives such as Coconut [13] credentials and confidential balances, and (iii) design a fee model that discourages abuse while incentivizing honest authorities. Addressing these challenges will transform the current protocol into a deployable, privacy-preserving and economically sustainable offline payment system.

REFERENCES

[1] Henri Arslanian. 2022. Ethereum. In *The book of crypto: The complete guide to understanding bitcoin, cryptocurrencies and digital assets*. Springer, 91–98.

[2] Mathieu Baudet, George Danezis, and Alberto Sonnino. 2020. Fastpay: High-performance byzantine fault tolerant settlement. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 163–177.

[3] Tijsbert Creemers, Thiruneeran Murugavel, Frédéric Boutet, Ositiana Omary, and Takeshi Oikawa. 2020. Five strategies for mobile-payment banking in Africa. (2020).

[4] digWatch. 2025. Internet shutdowns surge in Africa despite human rights concerns. (2025).

[5] Ramon R Fontes, Samira Afzal, Samuel HB Brito, Mateus AS Santos, and Christian Esteve Rothenberg. 2015. Mininet-WiFi: Emulating software-defined wireless networks. In *2015 11th International conference on network and service management (CNSM)*. IEEE, 384–389.

[6] Esa Hyytiä and Jorma Virtamo. 2007. Random waypoint mobility model in cellular networks. *Wireless Networks* 13, 2 (2007), 177–188.

[7] Ahmet Kurt, Abdulhadi Sahin, Ricardo Harrilal-Parchment, and Kemal Akkaya. 2023. LNMesh: Who said you need internet to send Bitcoin? Offline lightning network payments using community wireless mesh networks. In *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 261–270.

[8] Christopher Lowe. 2024. The Commercial Sustainability of Mobile Money Providers in Interoperability Initiatives. (2024). Accessed: 2024-02.

[9] Fernanda da Silva Momo and Ariel Behr. 2021. Blockchain: Effects in transactions costs from information governance. *BAR-Brazilian Administration Review* 18, spe (2021), e200047.

[10] Onkokame Mothobi and Kago Kebotsamang. 2024. The impact of network coverage on adoption of Fintech and financial inclusion in sub-Saharan Africa. *Journal of Economic Structures* 13, 1 (2024), 5.

[11] Manasa Patnam and Weija Yao. 2020. The real effects of mobile money: Evidence from a large-scale fintech expansion. (2020).

[12] Mohamed Khalil Regragui. 2022. The african mobile wallets: an empirical analysis of the services and the anticipated trends. (2022).

[13] A Sonnino, M Al-Bassam, S Bano, S Meiklejohn, and G Danezis. 2018. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. arXiv 2018. *arXiv preprint arXiv:1802.07344* (2018).

[14] SS Sravan, Susmita Mandal, and PJA Alphonse. 2024. LIO-PAY: Sustainable low-cost offline payment solution. *Electronic Commerce Research and Applications* 67 (2024), 101440.

[15] Gengrui Zhang, Shiquan Zhang, Michail Bachras, Yuqiu Zhang, and Hans-Arno Jacobsen. 2025. Cabinet: Dynamically Weighted Consensus Made Fast. *arXiv preprint arXiv:2503.08914* (2025).