Enhancing Node Reliability in Opportunistic Networks through Blockchain Integration

Quang Huy Do[†‡], , Thiago Abreu[†], Baah Kusi[‡], Nelly Chatue Diop[‡], Sami Souihi[†]
[†]LISSI-TincNET Research Team, University of Paris-Est Creteil, France
[‡] Ejara lab, France
Email: huy.dq184271@sis.hust.edu.vn, thiago.abreu@u-pec.fr, baah.kusi@ejara.africa, nelly@ejara.io, sami.souihi@u-pec.fr

***Abstract*—In challenging environments or low network resource areas, peer-to-peer payments face significant hurdles due to unreliable connectivity and limited infrastructure. Leveraging the integration of opportunistic networks and blockchain, this paper presents a novel approach to enhance node reliability and ensure transparency in transaction processing even in areas with limited network conditions. This method aims to ensure the resilience and efficiency of opportunistic network by integrating a sharding-based blockchain technology. Our approach securely stores essential network information and transaction data on the blockchain to foster a trustworthy and transparent transactional environment. We also apply sharding-based blockchain to increase network throughput and manageability. Integration of blockchain and opportunistic networks addresses the challenges of peer-to-peer payments, establishes tamper-proof data, enhances node reliability, and provides transparency in collaborative decision-making within the network.**

***Index Terms*—Opportunistic Networks, Blockchain, Smart Contract, Reliability, Security, Transparency.**

I. Introduction

In the bustling markets across various regions of Africa, where daily transactions are an important part of daily life, there is a noticeable shift away from using physical cash. This shift is highlighted by the significant adoption of mobile payments among internet users, with 84 percent in Kenya and 60 percent in Nigeria opting for digital transactions in 2021 [1]. Additionally, several African governments actively encourage the use of mobile payments, especially considering the challenges posed by the COVID-19 pandemic [2]. This reflects a growing reliance on digital financial solutions. Beyond just offering convenience, these mobile payments also play a crucial role in promoting financial inclusion. This is particularly important in areas where a significant part of the population doesn't have access to traditional banking services.

Despite the progress made in digital transactions, the need for a stable internet connection poses a significant challenge, particularly in areas like traditional marketplaces with limited or sporadic network access [3]. To tackle this challenge, opportunistic networking [4] offers a promising solution. It relies on direct device-to-device (D2D) communication to enable secure and efficient transactions on mobile phones, even when there is no reliable internet connection available. This approach is especially beneficial in regions where network conditions are unpredictable, meeting the growing demand for mobile payments in such areas.

Another challenge in current digital payment is that it relies on third-party payment systems, which often involve extra fees and complex validation processes. To tackle the challenges linked with third-party payment systems, using blockchain [5] technology emerges as a game-changing solution. Unlike centralized systems, blockchain operates in a decentralized manner, providing built-in security without the need for extensive protective measures. This paper focuses on using blockchain specifically to store essential network information, boosting the reliability of nodes when handling peer-to-peer transactions. The decentralized and unchangeable nature of blockchain ensures secure storage of vital data, creating a foundation for peer-to-peer transactions. By employing blockchain to store network information, the system becomes more resilient and transparent, effectively overcoming issues associated with challenging environments and traditional payment methods.

In this paper, we present an integrated opportunistic network with sharding-based blockchain [6]. Our proposed system leverages using smart contracts [7] to store essential network information to increase performance when finding optimal routes for package transferring hence enhancing overall system performance.

- The first contribution is to propose the use of blockchain in an opportunistic network environment, enhancing transparency, security, and reliability in transaction processing and network operation.
- We propose a sharding-based blockchain designed to enhance throughput by distributing the workload across multiple shards. This approach also simplifies management, making it easier to handle and enhance the throughput of the blockchain system.

The rest of this paper is organized as follows. Section II provides background work on blockchain, sharding, smart contracts, and opportunistic networks. Section III provides an overview of our proposed system and states the problem. The performance analysis for sharding-based blockchain with opportunistic networks is presented in Sec. IV. Finally, Section V concludes the paper and highlights our future work.

II. BACKGROUND

A. Blockchain

Blockchain [5] is a decentralized digital ledger technology that was originally developed to support the cryptocurrency Bitcoin. The core idea of blockchain is decentralization, which means that it does not store any of its databases in a central location. Instead, the blockchain is copied and spread across a network of participants (i.e. computers). Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change. This decentralized architecture ensures robust and secure operations on the blockchain with the advantages of tamper resistance and no single-point failure vulnerabilities, which improves efficiency in domains requiring a high level of transparency and data privacy like the 5G network.

B. Sharding

Sharding, according to related work, [8] [6], is one of the most promising solutions for the scalability problem. Originally, sharding [9] is a type of database partitioning technique that separates a huge database into much smaller, faster, more easily managed parts called data shards. The key idea of sharding in the blockchain is to split the network into smaller committees. Each can independently process a disjoint set of transactions (or a "shard"). With sharding, nodes only have to communicate with nodes within its shard and only store the transactions happening in its shard.

C. Smart Contract

Smart contracts, operating on blockchain technology, enhance transparency and security for opportunistic networks by automating agreements and ensuring trust among parties. These contracts, visible to authorized users on blockchains, offer transparency through their immutable and visible source code [7]. By transferring digital trust inherent in blockchain transactions to complex agreements, smart contracts enable secure interactions even in unstable network conditions where paths may change rapidly. Additionally, the automation and enforcement capabilities of smart contracts contribute to improved efficiency, traceability, and security within opportunistic networks, aligning with the need for reliable communication in unpredictable environments

D. Opportunistic Network

Opportunistic networks, characterized by their dynamic and self-organizing nature, operate on temporary connections rather than fixed routes [4], enabling data exchange in challenging conditions like sparse infrastructure or variable topologies. These networks leverage intermittent connectivity among nodes, allowing communication even without direct pathways through the assistance of intermediate nodes. By utilizing idle bandwidth and epidemic routing algorithms, opportunistic networks offer benefits such as cost reduction, support for low-latency applications, and improved resource utilization. Additionally, these networks address the need for communication in highly unpredictable environments by adapting to the unstable topology and intermittent connections present in such scenarios.

III. Smart Contract Integration With Opportunistic Network

A. System Overview

1) System Model: In our innovative approach to Smart Contract Integration with Opportunistic Networks, we introduce a dynamic system model aimed at enhancing efficiency and transparency within the network, as illustrated in Fig. 1. The opportunistic network environment is structured into two key layers: the controller layer and the infrastructure layer.

The infrastructure layer comprises network nodes that are strategically organized into groups, creating more manageable subsets known as shards. This partitioning strategy is implemented to significantly boost network throughput, allowing for parallelized processing and improved scalability. By dividing the network into shards, we enhance the efficiency of data processing and resource utilization.

On top of the infrastructure layer, we introduce the controller layer, which consists of several distributed controllers. Each controller is responsible for managing and processing network information within its assigned shard. Essential network information includes distances between nodes, position, range, and status of each node, etc. This decentralized approach ensures that controllers operate independently, acquiring and updating network data autonomously.

Our system model uses smart contracts to store essential network information. This integration enhances both node reliability and transparency. Each controller monitors and securely records pertinent network data through smart contracts, ensuring that critical information is immutably stored on the blockchain. This proactive approach fortifies the reliability of nodes in handling various transactions and introduces a layer of transparency to the network's operations.

To address the issue of unreliable connectivity, our system leverages the opportunistic network's inherent capability to utilize direct D2D communication. In scenarios where nodes experience intermittent connectivity, the system relies on intermediate nodes to relay transaction data to controllers. The controllers, having relatively better connectivity and resources, manage the communication with the blockchain network. This method ensures that even in challenging environments, transaction data can eventually be synchronized with the blockchain once a stable connection is available.

2) Sharding-based Blockchain: The blockchain architecture is implemented using a sharding approach to address the scalability challenges commonly associated with blockchain technology. In our sharding-based blockchain system, the infrastructure layer is divided into multiple shards, each corresponding to a small region within the Opportunistic Network, as shown in Fig. **??**. Each shard is managed by a distinct controller within the controller layer. This partitioning strategy significantly enhances network throughput, allowing for parallelized processing and improved scalability. The decentralized nature of sharding-based blockchain ensures robust and secure operations with the advantages of tamper resistance and no single-point failure vulnerabilities. The integration of sharding-based blockchain with Opportunistic Networks leverages the advantages of both technologies. By aligning each shard with a specific region in the Opportunistic Network, the system becomes easier to manage and monitor. Each controller in the controller layer is responsible for managing and securely recording pertinent network data through smart contracts, ensuring that critical information is immutably stored on the blockchain. This proactive approach fortifies the reliability of

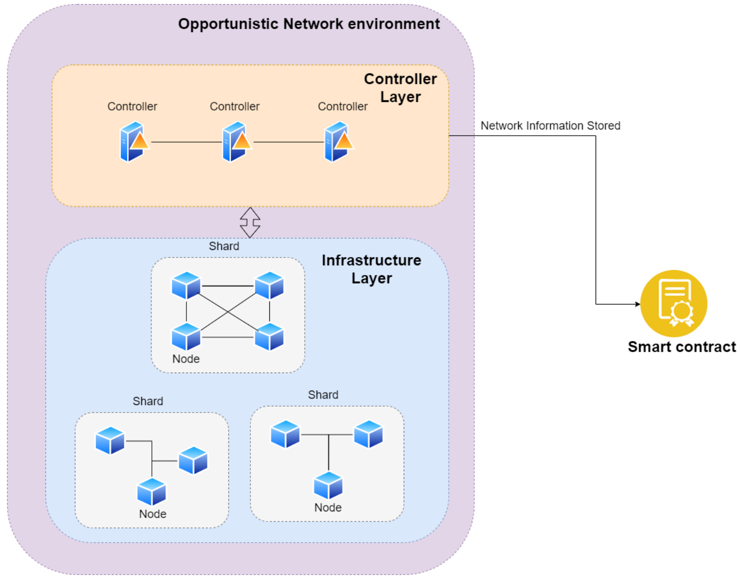

Fig. 1: Proposal design

nodes in handling various transactions and introduces a layer of transparency to the network's operations.

B. Problem statement

1) Performance:

- **Optimal Routing Efficiency:** Utilize smart contracts to optimize the routing path within opportunistic network, enabling nodes to dynamically identify and adapt to the most efficient routing paths despite intermittent connectivity, thus minimizing delays and ensuring timely message delivery.
- **Resource management:** Efficient resource allocation within opportunistic network requires addressing the limited storage, processing power, and battery life of individual nodes. The problem statement involves optimizing strategies that effectively utilize these constrained resources while maintaining network performance.
- **Efficient Transaction Handling:** Utilize opportunistic network to handle peer-to-peer transactions in challenging environments by integrating blockchain technology. The decentralized nature of blockchain ensures secure and efficient transaction processing, fostering a reliable environment for peer-to-peer transactions.

2) Security and Transparency:

- **Increased Security and Availability in Challenging Environments:** Utilize blockchain technology to enhance the security and availability of nodes in opportunistic network, particularly in dynamic and unpredictable connectivity scenarios. Strategies should be devised to mitigate disruptions, enhance node availability, and maintain network functionality in challenging environments.
- **Transparency and Trust:** Implement mechanisms that leverage blockchain technology with smart contracts to guarantee transparent communication and decision-making processes among nodes in opportunistic network. Strategies should be devised to foster a secure and transparent environment, establishing trust in data transactions.

IV. Performance Evaluation

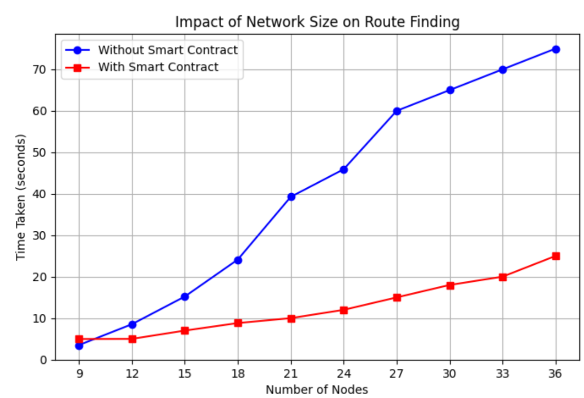

Fig. 2: Impact or Network Size in Route Finding

A. Experiment setup

In this section, we analyze the performance of our proposed system using smart contracts and compare the metrics of our proposed platform with the system without using smart contracts in two scenarios: ideal environment and real-world environment with the inconsistent model. In ideal environment, all nodes are online and function normally all the time. Whereas inconsistent model for real-world environment refers to cases in real-world scenarios where not all nodes in an opportunistic network are consistently available due to various factors like power constraints, hardware failures, and node mobility. We define the nodes that are unstable as inconsistent nodes. To simulate this inconsistency, we introduced a model where a certain percentage of nodes in the network are

Parameter	Value
The number of blockchain shards	3
The initial number of nodes	9
The maximum number of nodes	36
The initial number of inconsistent nodes	1
The maximum number of inconsistent nodes	10
Propagation Model	logDistance, exp=4.5
Network Type	adhoc
Mobility Model	Random Direction

TABLE I: Simulation Parameters

offline at a certain time interval. This model allows us to evaluate the robustness of our system in a more realistic and challenging environment. We used Mininet-Wifi [10] to deploy an opportunistic network and Tezos-k8s [11] to deploy Tezos blockchain infrastructure on a Kubernetes [12] cluster for testing. Besides, we use PyTezos [13] to handle contract interaction with Python 3.11 and Ubuntu 20.04. The parameters setting used in the simulations is summarized in Table I.

B. Results and Analysis

1) Performance: In our experiment, we set up to calculate the time it takes for a node to find the optimal route from itself to the destination node in two scenarios: ideal environment and real-world environment with inconsistent model.

a) Performance in Ideal Environment: Fig. 2 shows the superior performance of our proposed scheme using smart contracts compared to that when not using ones. In a system not using smart contracts, the process of finding the optimal route from the source to the destination node involves nodes repeatedly searching for the shortest neighbor node and checking if that node is the destination node. In this process, each node has to ping and check the distance between itself and the neighbor, as well as its coverage area. However, with the integration of smart contracts, we have a controller responsible for pushing all the necessary information, such as distance and coverage area, to the smart contract. As a result, when finding the optimal route, nodes no longer need to ping each other, significantly reducing the computational overhead and enhancing the efficiency of the route-finding process. Specifically, when the number of nodes in our platform reaches 36, the performance enhancement due to the smart contract integration becomes particularly evident. At this scale, the time to find a route when using smart contracts improves by approximately 300% compared to the system without smart contracts. However, with a smaller number of nodes, specifically 9, the performance of the system not using smart contracts is slightly better. This is because, with a smaller node count, fetching information from the smart contract takes longer than the traditional ping method, leading to a slight delay in route determination.

b) Performance in Inconsistent Environment: Fig. 3 illustrates the impact of node inconsistency on the optimal route-finding process. As shown, even in an environment with inconsistent nodes, the use of smart contracts still outperforms the traditional method in terms of route-finding efficiency. Each shard's controller pushes the status of each node in real-time to smart contracts so that when determining the optimal route from source to destination, nodes don't have to check if neighbor nodes are up or not. As a result, the performance gain when using smart contracts compared to not using them becomes increasingly significant as the number of nodes in the network increases. Specifically, when there are 36 nodes, the performance improvement with smart contracts reaches up to 250% compared to the traditional method.

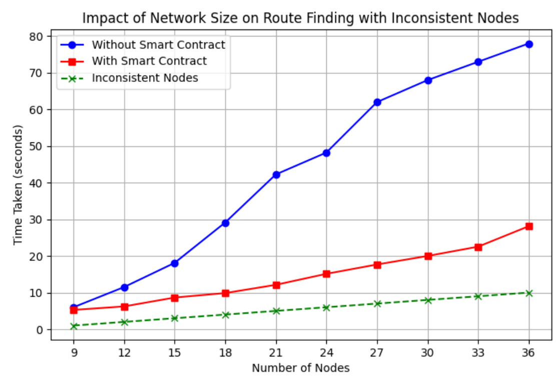

Fig. 3: Impact or Network Size in Route Finding in Inconsistent Environment

2) Security:

a) Transparency and Trust: One of the key advantages of integrating smart contracts with opportunistic networks is the enhanced transparency and trust in data transactions. In traditional systems, nodes often rely on centralized mechanisms to verify the correctness of stored data. However, with the introduction of smart contracts on the blockchain, each node can independently verify the integrity and correctness of the data stored on the blockchain. This decentralized verification process eliminates the need for third-party validation and ensures that the data is tamper-proof and immutable. This enhances the overall trustworthiness of the system and provides a transparent mechanism for data verification. In scenarios where the network consists of nodes with inconsistent status or where the network size is large, this feature becomes particularly beneficial. It allows the network to maintain a high level of data integrity and reliability, even in challenging environments.

b) Increased Security and Availability in Challenging Environments: Fig. 4 illustrates the impact of node inconsistency on the node-status checking in an environment where nodes frequently switch between online and offline states. As demonstrated, even in a network with inconsistent node statuses, the utilization of smart contracts enhances the efficiency of the node status-checking process.

When the network comprises a small number of nodes, the traditional method, where nodes have to ping each other to check if a node is offline or online, performs better than the smart contract approach. However, as the number of nodes in the network grows, the performance advantage of using smart contracts becomes increasingly significant. In detail, when there are 36 nodes, the performance improvement with smart contracts reaches up to 175% compared to the method without smart contracts.

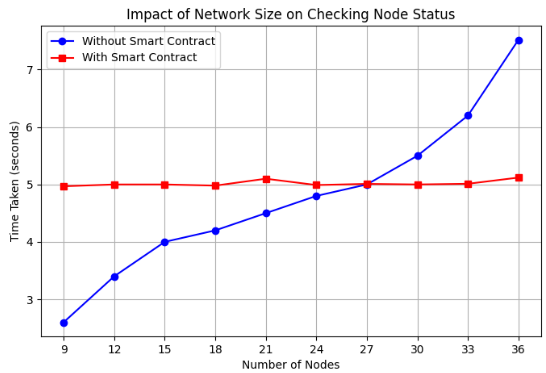

Fig. 4: Impact or Network Size in Checking Node Status In Inconsistent Environment

C. Challenges and Limitations

While our proposed sharding-based blockchain in an opportunistic network environment offers significant advantages in terms of transparency, security, and reliability, it also presents several challenges and limitations. As the number of transactions and nodes in the network increases, managing and maintaining the blockchain can become more complex. Although sharding helps to distribute the workload, it may also introduce challenges related to cross-shard transactions and synchronization. Additionally, while blockchain technology inherently provides security through its decentralized and tamper-resistant nature, the integration with opportunistic networks may introduce vulnerabilities. Ensuring the security of the network against various attacks remains a challenge. Furthermore, utilizing opportunistic networks with limited resource devices can be challenging, especially in meeting the real-time requirements for peer-to-peer payments.

V. Conclusion

In this paper, we introduced a novel approach to enhance transparency, security, and reliability for nodes in opportunistic network environments by integrating a sharding-based blockchain system. Our proposed system leverages the benefits of blockchain technology to store essential network information, thereby improving the overall performance of the network.

The main contributions of this paper include:

- The proposal to use blockchain in an opportunistic network environment to enhance transparency, security, and reliability in transaction processing and network operation.
- The introduction of a sharding-based blockchain designed to enhance throughput by distributing the workload across multiple shards, making the system easier to manage.

While our approach shows promising results, there are still challenges and limitations to address, such as scalability issues, security concerns, and adaptability to dynamic environments. Future work will focus on addressing these challenges and further optimizing the proposed system to meet the evolving requirements of opportunistic networks in the 5G era.

References

[1] M. . Company, "The future of payments in africa," 2022. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/the-future-of-payments-in-africa

[2] G. F. Magazine. (2023) Africa: Digital payments progress. Global Finance Magazine. [Online]. Available: https://gfmag.com/features/africa-digital-payments-progress

[3] M. Singh, P. Verma, and A. Verma, "Security in opportunistic networks," in *Opportunistic networks*. CRC Press, 2021, pp. 299–312.

[4] A.- Manole, R.-I. Ciobanu, C. Dobre, and R. Purnichescu-Purtan, "Opportunistic network algorithms for internet traffic offloading in music festival scenarios," *Sensors*, vol. 21, no. 10, p. 3315, 2021.

[5] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, "Blockchain-based secure distributed control for software defined optical networking," *China Communications*, vol. 16, no. 6, pp. 42–54, 2019.

[6] H. Nam Nguyen, H. Anh Tran, S. Fowler, and S. Souihi, "A survey of blockchain technologies applied to software-defined networking: Research challenges and solutions," *IET Wireless Sensor Systems*, vol. 11, no. 6, pp. 233–247, 2021.

[7] P. Bottoni, N. Gessa, G. Massa, R. Pareschi, H. Selim, and E. Arcuri, "Intelligent smart contracts for innovative supply chain management," *Frontiers in Blockchain*, vol. 3, p. 52, 2020.

[8] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125 244–125 262, 2020.

[9] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "Sok: Sharding on blockchain," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 41–61.

[10] R. R. Fontes, S. Afzal, S. H. Brito, M. A. Santos, and C. E. Rothenberg, "Mininet-wifi: Emulating software-defined wireless networks," in *2015 11th International Conference on Network and Service Management (CNSM)*. IEEE, 2015, pp. 384–389.

[11] O. Alpha. Tezos-k8s. Oxhead Alpha, Inc. [Online]. Available: https://tezos-k8s.io/

[12] T. Kubernetes, "Kubernetes," *Kubernetes. Retrieved May*, vol. 24, p. 2019, 2019.

[13] B. Bad. Pytezos. Baking Bad. [Online]. Available: https://pytezos.org/