An Opportunistic Mesh Network for P2P Cryptocurrency Transactions based on a resilient Blockchain Infrastructure

January 15, 2024

1 Introduction

In an increasingly digital world, where internet connectivity is often taken for granted, there exists a pressing need to develop innovative solutions that transcend the limitations posed by unreliable or absent network access. Nowhere is this challenge more acute than in regions where sporadic or poor internet connectivity is a recurring reality. The thesis project at hand embarks on a pioneering journey at the crossroads of two cutting-edge technologies, opportunistic mesh networks and blockchain. Its overarching goal is to create a resilient and robust foundation for peer-to-peer (P2P) cryptocurrency transactions in such challenging connectivity environments.

The project recognizes that these regions, including many in Africa, where access to traditional financial infrastructure is often lacking or inconsistent, require alternative and dependable means of conducting economic and financial activities. By integrating opportunistic mesh networks with blockchain technology, this initiative aspires to deliver a reliable framework for recording transactions, even in cases of limited connectivity.

Moreover, it acknowledges the scientific and technological challenges inherent in both opportunistic wireless networks and blockchain technology, addressing issues related to wireless communication and consensus protocols, respectively. In this context, the project is not just an exploration of theoretical possibilities but a practical and impactful endeavor aimed at fostering cooperation, decision-making, and economic empowerment among individuals and communities facing the challenges of poor internet access.

This thesis outlines the project's objectives, the methodology to be employed, and its significance in addressing pressing connectivity and financial inclusion issues, with a particular focus on the African use case as a real-world proving ground for the technology's effectiveness. By doing so, this research project aspires to contribute to a more inclusive and resilient digital future, especially for regions where traditional infrastructure falls short.

2 Context

The context for this thesis project lies in the intersection of two cutting-edge technologies: opportunistic mesh networks and blockchain. The project unfolds in a backdrop characterized by the following key elements:

1. **Opportunistic Mesh Networks**: Opportunistic mesh networks are a paradigm for communication that thrives on sporadic or unreliable network connectivity. They are particularly relevant in scenarios where traditional internet access is inconsistent or unavailable. These networks rely on the opportunistic use of local wireless connections, enabling devices to communicate with each other when they are in proximity.

2. **Blockchain Technology**: Blockchain is a decentralized and immutable ledger technology that has gained prominence, primarily through cryptocurrencies like Bitcoin. However, its potential goes beyond digital currencies. It offers secure and transparent transaction recording, making it an attractive technology for various applications beyond finance.

3. **Addressing Technological Barriers**: The project acknowledges that, while promising, both opportunistic mesh networks and blockchain technology have their respective scientific and technological challenges. These include issues related to wireless communication, node cooperation, and, in the case of blockchain, consensus protocols. Addressing these barriers is a crucial aspect of the research.

4. **Suitability for Limited Connectivity**: One of the project's central premises is that this technology can be particularly suitable for regions with poor internet connectivity. By creating a reliable foundation for P2P cryptocurrency transactions in such environments, it aims to facilitate economic and financial activities where traditional banking infrastructure is lacking or unreliable.

5. **African Use Case**: As part of the project's practical application, it will be tested in African countries where sporadic or poor internet access is a real-world challenge. This use case will serve as a valuable testbed for evaluating the system's performance and adaptability in a region where the need for alternative communication and transaction methods is acute.

3 Objective

This thesis project aims to create an opportunistic mesh network as the basis for peer-to-peer (P2P) cryptocurrency transactions using blockchain technology, with a focus on ensuring system robustness and resilience. In addition to addressing scientific challenges in opportunistic wireless networks, the project also confronts technological obstacles associated with blockchain, including the consensus protocol.

The main goal is to establish a secure and reliable network that enables users to conduct decentralized P2P transactions regardless of their location, even in cases of unreliable or absent internet access. By integrating blockchains and opportunistic networks, the project endeavors to provide a dependable framework for recording transactions, even in situations of limited connectivity.

The central objective is to promote collaboration and decision-making among nodes within an opportunistic mesh network to optimize P2P cryptocurrency transactions. Leveraging Federated Reinforcement Learning (FRL), the project seeks to model and improve individual node strategies while considering the overall network's performance.

4 Design and Mathematical Formulation : Collaborative Game-Based Mechanism using Federated Reinforcement Learning

4.1 Components

- **Node Representation**
  Each node is represented as an agent n_i in the Federated Reinforcement Learning setting.

- **Local Model Training**
  At each time step t, node n_i trains a local reinforcement learning model M_i^t using its own data and experiences. This model learns optimal strategies for the specific node's role in cryptocurrency transactions.

- **Collaborative Strategy Sharing**
  Periodically, at each time step t, nodes share their locally trained models M_i^t with a central coordinator or amongst themselves to create a global model M_{global}^t representing the collective knowledge of the network.

- **Global Model Aggregation**
  The global model M_{global}^t is aggregated using a federated averaging approach:
  $$M_{\text{global}}^t = \frac{1}{N} \sum_{i=1}^{N} w_i^t \cdot M_i^t$$
  where N is the total number of nodes, and w_i^t is the weight assigned to node i at time t based on its performance or contribution.

- **Model Update and Distribution**
  The updated global model M_{global}^t is then redistributed to all nodes for further fine-tuning and improvement of their individual strategies.

- **Collaborative Decision-making**
  Nodes utilize the global model M_{global}^t along with their local knowledge to

make collaborative decisions, optimizing actions for P2P cryptocurrency transactions.

- **Reward System**
  The reward for each node n_i at time t is a function of successful transactions, efficient resource utilization, and collaborative actions contributing to the network's overall performance, denoted as R_i^t.

4.2 Reinforcement Learning Basics

Reinforcement Learning (RL) involves an agent learning to make decisions by interacting with an environment. The agent receives feedback in the form of rewards or penalties based on its actions. The objective is to learn a policy that maximizes the cumulative reward over time.

The agent's behavior is formalized using a Markov Decision Process (MDP), defined by a tuple $\langle S, A, P, R \rangle$:

S: set of states

A: set of actions

P: state transition probabilities

R: reward function

The agent's policy, denoted as π, defines the probability distribution over actions given a state: $\pi(a|s) = P(A_t = a|S_t = s)$.

The goal is to find the optimal policy, denoted as π^*, that maximizes the expected cumulative reward, typically defined as the discounted sum of rewards: $G_t = \sum_{k=0}^{\infty} \gamma^k R_{t+k+1}$, where $0 \leq \gamma \leq 1$ is the discount factor.

The agent's objective is to maximize the expected return G_t by selecting appropriate actions at each state.

4.3 Integration with Blockchain

In our collaborative mechanism, we utilize the blockchain to maintain the global federated model. The blockchain provides an immutable and decentralized ledger, ensuring the integrity and security of the global model.

Each transaction on the blockchain involves updating the global model based on contributions from nodes. Smart contracts can govern these transactions, ensuring the agreed-upon federated learning rules are followed.

By integrating with the blockchain, we enhance transparency, security, and trust in the collaborative learning process.

5 Opportunistic Networks and Blockchains

Opportunistic networks (OppNets) are a type of computer network that enables communication in challenging or intermittent connectivity environments. Unlike

traditional networks that rely on continuous connectivity (like IEEE 802.3 for cabled transmission or IEEE 802.11 for wireless), opportunistic networks take advantage of intermittent connections and use store-and-forward techniques to deliver messages. Due to this behavior, they are often classified as Delay Tolerant Networks (DTN) [1, 2].

In opportunistic networks, devices communicate with each other whenever they come into proximity or establish temporary connections, such as through Bluetooth, Wi-Fi, or other wireless technologies, even unlicensed bands [3]. Messages are stored on devices and forwarded to other devices when opportunities for connectivity arise. This can occur when devices are within range or during overlapping network coverage.

These networks are particularly useful in situations where traditional infrastructure-based networks are unavailable, unreliable, or prohibitively expensive. Examples include remote areas, disaster-stricken regions, or mobile scenarios where devices are frequently moving.

Although opportunistic networks provide a flexible and adaptable communication infrastructure, enabling communication in challenging or dynamic environments where traditional networks may not be feasible, it has several challenges to be addressed [4]:

- Connectivity: Opportunistic networks rely on intermittent connections, which can be sporadic and unpredictable. The lack of continuous connectivity makes it challenging to establish timely communication between nodes. As a result, message delivery delays and disruptions can occur.

- Network Partitioning: The intermittent nature of opportunistic networks often leads to network partitioning, where groups of nodes become isolated from each other. When partitions occur, communication between nodes in different partitions becomes impossible unless they come into proximity again. This can hinder the overall efficiency and effectiveness of the network.

- Limited Storage and Resources: Devices in opportunistic networks typically have limited storage capacity, processing power, and battery life. Storing and forwarding messages requires the allocation of these limited resources, and if not managed properly, it can lead to resource exhaustion, degradation of performance, and increased energy consumption.

- Security and Privacy: Opportunistic networks are vulnerable to security threats, such as unauthorized access, tampering, and data interception. Moreover, due to the nature of opportunistic networks, where messages are relayed through multiple nodes, ensuring data privacy becomes a challenge. Protecting the network and maintaining data integrity and confidentiality are significant concerns [5].

- Routing and Message Delivery: Routing in opportunistic networks is complex due to the lack of global network knowledge, dynamic topology, and

intermittent connectivity. Finding efficient and reliable routing paths in such environments is challenging. Additionally, ensuring timely and successful message delivery is difficult, especially when the destination node is not immediately reachable.

- Scalability: As the number of nodes in an opportunistic network increases, scalability becomes a concern. Routing and message delivery algorithms must scale well to handle a growing number of nodes and messages without significantly impacting performance.

- Protocol Heterogeneity: Opportunistic networks often involve devices with different communication technologies, protocols, and capabilities. Integrating and interoperating between heterogeneous devices can be complex and requires the development of suitable protocols and mechanisms to ensure seamless communication.

Concerning the security aspect of OppNets, one particular problem arises from the lack of knowledge of neighbors' identities, caused by mobility and variety of nodes. Therefore, trust is a main issue among nodes and attackers can use vulnerabilities as insecure interfaces, and unencrypted communications for malicious behaviors, like private data collection [6].

The issues on security of OppNets have their roots in poor system design or inefficient implementation of cryptography. Inadequate system design may be characterized by an inability to handle encryption techniques or the presence of unencrypted and insecure transactions. Cryptography can be compromised if essential components or functions are removed to reduce the processing burden on the hardware platform [6]. Network designers could use traditional cryptography algorithms, such as RSA, but they are not adapted for low capacity devices, as, for instance, in sensor networks [7].

Therefore, one particular solution is the use of blockchains. Such structures operate on a decentralized network, where multiple nodes participate in the validation and verification of transactions. This decentralized nature provides inherent security benefits, as there is no single point of failure or control. In contrast, RSA relies on a centralized authority for key management, which can be vulnerable to attacks or compromise [8].

Another key aspect of opportunistic networks is the hardware usage of neighbor nodes. This implies that nodes are actively sending, receiving and forwarding messages, even though they were not initially foreseen as the backbone infrastructure. Although in theory, this solves the problem of connectivity in crowded areas or uncovered zones, in practice a cost is associated to the owner of the forwarding node (in terms of battery, data consumption or general hardware performance). Therefore, a compensation mechanism should be investigated to reward the nodes (and owners) as a function of their participation on the overall communication [9].

6 Contribution of Tincnet

6.1 Research Expertise

Tincnet is a research team within the Networks and Telecommunications (N&T) Department of Paris-Est Créteil University (UPEC). The team contributes significantly to the CIFRE thesis on "Opportunistic Mesh Network for P2P Cryptocurrency Transactions based on a Resilient Blockchain Infrastructure," under the guidance of Dr. Sami Souihi.

Tincnet specializes in adaptive mechanisms in large-scale dynamic systems, focusing on three main axes:

- **Next-generation and large-scale distributed architectures**: Proposing configurable and disaggregated systems based on paradigms such as Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). These architectures aim to be resilient and trustworthy, incorporating blockchain technology.
- **Configurable and autonomous systems**: Developing mechanisms that rely on context-enhanced knowledge and Machine Learning (ML) to provide approaches requiring minimal human intervention. These systems can be easily configured using natural language.
- **Use Cases and Applications**: Applying research approaches to practical and realistic use cases, ensuring the relevance and applicability of their findings.

6.2 Support and Infrastructure

Tincnet provides a conducive research environment for the CIFRE thesis, under the direction of Sami Souihi with co-supervision by Thiago Abreu.

The support includes:

- **Research Supervision**: Dr. Sami Souihi, an accomplished researcher with expertise in the field, supervises the thesis, offering valuable guidance and direction. Thiago Abreu, an associate professor at UPEC, also contributes to the research, particularly focusing on performance evaluation and system modeling in the area of sensor wireless networks and machine learning.
- **Technical Expertise**: Tincnet offers technical expertise in network architectures, blockchain integration, and AI applications, enriching the research and implementation phases of the thesis.
- **Collaborative Environment**: Being part of an academic research team allows for collaboration with peers, sharing ideas, and gaining insights from a diverse group of researchers.

- **Platform for AI Experimentation and Model Training :** That will offer the possibility to develop, optimize, and evaluate AI models aimed at enhancing transaction speed, security, and resource allocation.

7 Contribution of Ejara

7.1 Industry Expertise

Ejara is an industry partner specializing in blockchain technology and cryptocurrency solutions. Their contribution to the CIFRE thesis significantly enhances the practical application and industrial relevance of the research.

- **Blockchain Solutions**: Developing innovative blockchain solutions for various applications, including secure transactions and data integrity.
- **Cryptocurrency Expertise**: Providing in-depth knowledge and experience in the field of cryptocurrencies, ensuring a comprehensive understanding of the subject matter.
- **Technical Guidance**: Offering technical guidance and insights into blockchain infrastructure and its integration with P2P cryptocurrency transactions.

7.2 Support and Resources

Ejara offers valuable support and resources to facilitate the successful completion of the CIFRE thesis:

- **Workspace and Technical Environment**: Providing a dedicated workspace for the doctoral candidate, equipped with the necessary tools and technologies for research and development related to blockchain and cryptocurrency.
- **Access to Data and Transactions**: Granting access to a comprehensive database of transactions, enabling the analysis and study of real-world cryptocurrency transactions for the thesis.
- **Platform for Experimentation**: Offering access to a platform for experimentation, allowing the doctoral candidate to validate research findings and implement practical solutions in a controlled environment.
- **Technical Mentorship**: Assigning technical mentors from Ejara to guide the doctoral candidate, ensuring a clear understanding of blockchain technology and its applications in the cryptocurrency domain.

References

[1] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Communications*, vol. 4, pp. 1787–1791(4), October 2010.

[2] S. Huang, X. Liu, and Z. Ding, "Opportunistic spectrum access in cognitive radio networks," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pp. 1427–1435, IEEE, 2008.

[3] H. A. B. Salameh and M. Krunz, "Channel access protocols for multihop opportunistic networks: challenges and recent developments," *IEEE network*, vol. 23, no. 4, pp. 14–19, 2009.

[4] S. Trifunovic, S. T. Kouyoumdjieva, B. Distl, L. Pajevic, G. Karlsson, and B. Plattner, "A decade of research in opportunistic networks: challenges, relevance, and future directions," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 168–173, 2017.

[5] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: a survey," *Security and Communication Networks*, vol. 8, no. 9, pp. 1812–1827, 2015.

[6] W. Yang, Y. Wan, and Q. Wang, "Enhanced secure time synchronisation protocol for ieee802. 15.4 e-based industrial internet of things," *IET Information Security*, vol. 11, no. 6, pp. 369–376, 2017.

[7] S. K. Dhurandher, J. Singh, P. Nicopolitidis, R. Kumar, and G. Gupta, "A blockchain-based secure routing protocol for opportunistic networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–13, 2022.

[8] C. Lepore, M. Ceria, A. Visconti, U. P. Rao, K. A. Shah, and L. Zanolini, "A survey on blockchain consensus with a performance comparison of pow, pos and pure pos," *Mathematics*, vol. 8, no. 10, p. 1782, 2020.

[9] M. Zichichi, L. Serena, S. Ferretti, and G. D'angelo, "Indamul: Incentivized data mules for opportunistic networking through smart contracts and decentralized systems," *Distributed Ledger Technologies: Research and Practice*, vol. 2, no. 2, pp. 1–28, 2023.