Advancing Mobile Money Payments Through Blockchain and Interoperability Protocols

Edem Kodjo Agbezoutsi[1], Pascal Urien[1(✉)], and Toundé Mesmin Dandjinou[2]

[1] 19 Place Marguerite Perey, 91120 Palaiseau, France
{kodjo.agbezoutsi,pascal.urien}@telecom-paris.fr
[2] Université Nazi BONI, 01 BP 1091 Bobo-Dioulasso, Burkina Faso

Abstract. Currently, mobile network operators (MNOs) manage their own Mobile Money (MM) transaction solutions, making them responsible for managing transaction databases and their interaction with customers. The goal of integrating Mobile Money transactions onto the Blockchain is to improve trust in the Mobile Money system. In this paper, we propose a Mobile Money payment protocol based on Blockchain technology, called "Mobile Money Using Blockchain (2MUB)". This protocol aims to improve the security, speed, interoperability and trust of financial transactions by using the advantages of Blockchain technology while offering an intuitive user experience. We discuss various aspects of this protocol, including advantages for users, potential challenges, and opportunities for its large-scale adoption, particularly in developing countries where Mobile Money is a real economical fact. Account management of users using approved BIP (Bitcoin Improvement Proposal) standards allows for revealing only the minimal transaction data necessary for traceability in an enhanced version of this protocol. However, this may increase the size of transaction data on the Blockchain to some extent. In addition to improving trust in the MM ecosystem, it also addresses the problem of interoperability by federating Mobile Money solutions in the ecosystem. Finally, we present the results of a case study to demonstrate the effectiveness of our protocol in a real-world environment, such as Burkina Faso.

Keywords: Security · Blockchain · Payments · Mobile Money · USSD · traceability · trust · protocol

1 Introduction

The Internet is now accessible in most parts of the world, with an estimated 60% of the population being connected in 2021 [1], totaling 4.5 billion people online. However, there is an unequal distribution of network coverage across continents. The disparity in Internet access, known as the digital divide, is a significant challenge, particularly in developing countries. This divide is particularly prominent in rural areas where Internet coverage remains limited.

The USSD technology using the 2G channel of GSM is advantageous for the development of Mobile Money. Mobile Money does not require Internet connection (3G and

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 274–287, 2025.
https://doi.org/10.1007/978-3-031-81570-6_18

higher channels) for its implementation and operation, but instead uses the USSD/GSM channel, which constitutes an advantage for countries whose GSM coverage is much higher than mobile internet.

Mobile Money plays an important role in monetary transactions in developing countries. It allows access to financial services even in remote rural areas. However, it has shortcomings such as the presence of multiple operators, a lack of federation and interoperability between Mobile Money solutions, a lack of trust in operators, and an uniqueness of the database at the Mobile Money operator.

In an increasingly digital world, the use of mobile payment systems is on the rise, particularly in developing countries. However, interoperability between different mobile payment systems remains a significant challenge. That's why we propose a Mobile Money payment protocol based on blockchain technology, called "Mobile Money Using Blockchain (2MUB)". This protocol aims at improving the security, speed and interoperability of financial transactions by using the advantages of blockchain technology while providing an intuitive user experience. We will discuss various aspects of this protocol, including the benefits for users, potential challenges, and opportunities for its large-scale adoption, particularly in developing countries where Mobile Money is an economic reality. Here we will present the results of a case study to demonstrate the effectiveness of our protocol in a real-world environment, such as Burkina Faso.

To address the limitations of current Mobile Money solutions, we proposed in our previous work [2, 3] the use of blockchain to enhance trust within the Mobile Money ecosystem. In our earlier research, we explored the traceability and federation of mobile payment solutions using blockchain technology. We described how blockchain services can be leveraged to improve transparency and security in Mobile Money transactions, presenting a concrete example of implementing blockchain for the federation of Mobile Money providers in Africa. We also examined the advantages of this federation, such as interoperability, accessibility, competition and innovation, along with the challenges involved in establishing an efficient Mobile Money federation. The objective of this study is to provide a detailed definition of the protocol enabling Mobile Money payments supported by blockchain services.

A major challenge in blockchain transactions is the transaction per second (TPS) limit. TPS is closely tied to the consensus algorithm for validating transactions and mining blocks. Initially, Ethereum and Bitcoin had TPS of 15 and 7 respectively [4], both using proof of work (POW) consensus. Currently, Ethereum has adopted proof of stake (POS) consensus, which allows for faster block mining and improved ecological sustainability. This has enabled Ethereum to reach a TPS of 160,000 [5]. To compare, Visa and MasterCard can process around 1700 TPS and PayPal 200 TPS. In 2019, Orange Money Burkina recorded 15 million transactions per day, equivalent to 174 TPS. In 2020, this increased by 23% to 18.45 million transactions, or 214 TPS. With a requirement of about 600 TPS for federation of three Mobile Money platforms in a country like Burkina Faso, Ethereum can handle the TPS load. Hence, using the Ethereum blockchain to improve the Mobile Money ecosystem is a crucial aspect of our contribution.

This paper is organized in five sections. Section 2 (related works) describes, in practice and research, how interoperability is conceived and deployed. Section 3 discusses the contribution blockchain could bring to the Mobile Money ecosystem. The Mobile

Money payment protocol on the blockchain is described in Sect. 4 and illustrated by transactions recorded on Ethereum test blockchain. Section 5 presents management of user accounts and the overall architecture.

2 Related Works

Interoperability has become a concern with the rise of Mobile Money in developing countries due to the diversity of solutions offered by different providers. in [6] interoperability in Mobile Money refers to the ability for customers to transfer money between accounts at different Mobile Money Operators (MMOs) as well as between accounts at Mobile Money schemes and bank accounts. Leading countries in Mobile Money such as India, Kenya, Tanzania and Rwanda have each adopted a solution that suits their economic environment and laws.

In 2008, the Reserve Bank of India issued guidelines for interoperability among prepaid payment instrument providers [6]. These guidelines aimed to facilitate money transfers between different digital wallets through the regulator-provided Unified Payments Interface (UPI) [7]. However, this central model may lead to integration complexities and only bank-backed mobile wallets with valid customer information are eligible to participate. The study in [8] proposes three options for customer detail lookup during processing, including a central database, a peer-to-peer query, and a hierarchical lookup. The peer-to-peer option is initially considered the most suitable for the Indian market, but this may change as the system size increases. Other options in the Indian landscape include the Mobile Payment Foundation of India model for interoperability in a highly regulated financial environment.

In Kenya, the Mobile Money market is well established in the African region and provides person-to-person money transfer services to low-end unbanked customers. Interoperability is not mandatory in Kenya's National Payments System regulations. However, payment service providers are allowed to make their own interoperable arrangements. The Central Bank of Kenya has left it to the market to decide how providers interoperate but has proposed a framework for easier interoperability [9]. So far, interoperability in Kenya has happened through bilateral agreements between Mobile Money providers rather than a common central system [10, 11]. A common central system, however, could improve coordination, customer experience and faster implementation of interoperability compared to private switches or bilateral agreements. This is also the case in Burkina Faso.

In Tanzania, there are 4 mobile network operators offering Mobile Money services to subscribers. It's one of the world's most successful Mobile Money markets with 25% of the population being active users, transacting 2 billion dollars per month in 2014 [12]. According to a study, Tanzania launched Account to Account (A2A) interoperability in 2014 and the regulatory environment allowed providers to freely choose the best technical model for their interests, resulting in providers opting for bilateral point to point integrations for interoperability [3].

Rwanda has a mature and competitive Mobile Money market with various providers offering similar services such as balance maintenance, deposits, withdrawals, and fund transfers. However, there is currently no central clearing and settlement system for

Mobile Money providers to offer interoperability. A study in [13] reviewed the regulation of Mobile Money in Rwanda and suggested a light-handed regulatory approach. New regulations in Rwanda require interoperability before integration can occur, but it is currently limited to transactions through agents. Interoperability between the banking system and Mobile Money is also available, but it requires a physical visit to a bank branch. The next step would allow for remote payment from one provider's account to another.

The study in [14] suggested using blockchain technology to create a prototype system for Mobile Money interoperability that is based on a decentralized shared ledger. This would ensure non-repudiation, protect data privacy, and authenticate the origin of the data. But these authors don't propose a protocol doing so.

In [6] authors develop the ideas which create the interoperability between Mobile Money providers. "As we have demonstrated in our contributions [2], they take into account the MMOs and banking institutions that are integral parts of the ecosystem and perform Mobile Money transaction operations between them." These proposals are supported by the laws and regulations in place within the economic area. The proposals' schemes are as follows:

- bilateral agreements between schemes and banks;
- neutral processor between schemes, and between schemes and banks;
- commercial processor between schemes, and between schemes and banks;
- using a bank and a national Automated Clearing House (ACH) to interface with other banks;
- direct connectivity to national ACH for all schemes and banks;
- commercial processor for bank interface, bilateral between schemes.

Overall, interoperability in Mobile Money is a complex issue that varies across countries. Different solutions and models are being explored to enhance interoperability, improve coordination, and provide seamless money transfer services for customers.

3 Mobile Money and Blockchain: A Better Future

3.1 Mobile Money

The trend of mobile payment, known as Mobile Money, is rapidly growing in developing countries. It involves transactions made by using a mobile device, and can be credited to a bank card, the operator's bill, or an electronic wallet. The electronic wallet can be funded through cash deposits from an agent, merchant, or bank transfer, and is tied to the customer's SIM card number, which is managed by the Mobile Network Operator (MNO). Mobile Money is implemented using Unstructured Supplementary Service Data (USSD) technology, which enables the sending of short commands from a mobile device to the Global System for Mobile Communications (GSM) network via the signaling channel. Unlike SMS, USSD operates on a session-oriented connection rather than a store-and-forward architecture and has a maximum text message length of 160 bytes [15]. This ease of deployment and use, even for non-literate populations, makes USSD [14] a key factor in the growth of Mobile Money.

USSD command uses numeric codes with the prefix '*' and the suffix '#'. Specifically, a user enters command like "*xxx#" and accesses to a pop-up menu which can be navigated through the phone keys. A Mobile Money transfer usually consists of 4 steps; registration, encashment, transfer and withdrawal [2].

3.2 Blockchain's Contribution

Blockchain can be used in different sectors and can meet different needs. Blockchain is applied to almost every field we can think of, such as banking [7] [8, 17], finance [8, 9], electoral voting [16, 17], education [18, 21], insurance [20] [21], agriculture [24], health [22], to name a few. The areas of application remain very broad and are not limited to what has been mentioned above. The technology's key features and uses focus on security, fraud prevention, traceability, and trusted third-party concerns. Our solution tackles the challenges of Mobile Money by integrating two primary elements: *tracing transactions and federating Mobile Money solutions through the use of blockchain technology*. Our proposal is a blockchain-based Mobile Money payment protocol that provides increased security by eliminating a central point of failure and reducing the risk of corruption or hacking. Furthermore, the decentralized system offers greater user flexibility by enabling transactions anytime, anywhere, without relying on a centralized infrastructure.

4 Enhancing Mobile Money Transactions with Ethereum Blockchain

4.1 Mobile Money Protocol for Blockchain

We introduced in [2] a *Mobile Money Protocol for Blockchain*, described by Fig. 1.

Actors involved in a transaction using this version of the protocol are as follows:

- **Customer A:** the initiator of the transaction, transferring an amount to Customer B.
- **Customer B:** the recipient of the transaction initiated by Customer A.
- **MNOA (Mobile Network Operator A):** it plays a central role in the transaction system as the custodian of the accounts for Customer A and Customer B.
- **The controller:** it plays a crucial role in monitoring communication exchanges and transactions within the economic space. Its primary responsibility is to store all data related to each transaction to enhance trust between customers and the MNO.
- **Central Bank:** it is responsible for ensuring the stability of the currency in the economic context.
- **Blockchain:** a technology used to record and secure transactions in a decentralized manner.

1. The transaction session is initiated by Customer A through his mobile device interface by entering the command **999*2#*.
2. The MNO receives the command from Customer A interpreted as a request for a money transfer from account A to account B to be recorded in the blockchain.

3. Exchanges occur between the customer making the payment and the MNO in order to gather information that will be stored in an *InfoRx.json* file (as seen in the left part of Fig. 2. The MNO generates a random number (*RandomNum)* with 256 bits of entropy.
4. The MNO generates an Ethereum RequestTx transaction specifically for Customer A. This transaction is assigned the identifier IdReqTx. The data field of this transaction comprises the concatenation of the SHA256 hash of the content of the InfoRx.json file with the random number. In other words, it is represented as hash(InfoRx.json || RandomNumber).
5. The MNO then posts RequestTx on the blockchain, using its Ethereum address as the destination account.
6. The MNO initiates an SMS notification to Customer A, seeking validation or rejection of the transaction request. Simultaneously, a copy of the transaction data is dispatched to a legacy controller or regulator for further processing and oversight.
7. The MNO verifies the information contained in InfoRx, including Customer A's identification and authentication, the necessary balance for transferring the specified value of X, and Customer B's identifying information.
8. The MNO transfers the amount X from account A to account B by creating the Ethereum transaction TransfTx (identified as IdTransfTx). The data field of this transaction is the hash value of the InfoTx.json file, which contains information such as IdReqTx, RandomNum, and the status of the transaction (Yes/No), as shown in the right part of Fig. 2
9. The MNO posts the TransfTx transaction to the blockchain, using its Ethereum address as the destination account.
10. The MNO finally provides complete information to the legacy controller/regulator. It sends SMS confirmations to both the receiver and sender, including the transaction identifier (IdTransfTx), the status of the transaction (Yes/No), and the RandomNumber. This enables them to retrieve and verify the transaction on the blockchain.

For each transaction, the MNO creates a mapping table between the information IdReqTx and IdTransfTx, and shares it with the legacy regulator/controller. This entity guarantees to customers the authenticity of every blockchain transaction performed by the MNO. It verifies the information provided by the MNO and stored in the blockchain, and sends a warning if there is an issue.

The current version of our protocol involves transactions between accounts of the same operator, and records data on the blockchain in hashed form [25].

In order to improve this protocol and to add interoperability between accounts while also providing non-compromising information to users and allowing authorized actors to track transactions, we introduce a user account management system based on BIP standards. This mapping of Mobile Money accounts to BIP 32 addresses will al low for improved tracking and management of the transactions.

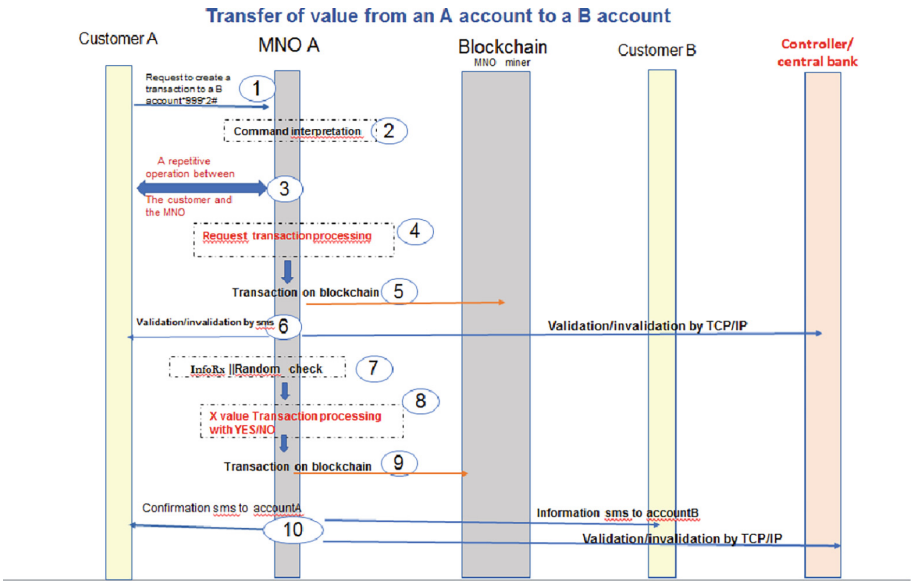

Fig. 1. Sequence diagram of Mobile Money transaction


```
"InfoRx":{
 "Op Code": "2",
 "Source number": "76 17 82 65",
 "Destination number": "74 43 38 19",
 "Transfer amount": "50000 CFA",
 "MNO id": "0011"
}
```

```
"InfoTx":{ "IdReqTx":
"0xe75def95df7aee86fef20fb0bbb9ec1ebc23be4ceea9017
0fe9455abd22f4f7f"},

"RandomNum":{ "Random Number":
"C4483BACC2DE4BA1852387A96D7FC"},

"StatusTx": { "transaction valid":"Yes" }
```


Fig. 2. InfoRx.json Request Transaction Information (left part), InfoTx.json Transaction Information (right part)

5 User Account Management and Expert Architecture

The ownership of tokens, cryptocurrencies, and other assets on the blockchain is managed using cryptographic keys, addresses, and digital signatures. These keys are not stored in the blockchain network, but instead are generated and stored by users in a wallet (either physical or logical) which operates in a similar manner to a traditional customer account. Next section explains how customer accounts are managed by sponsoring entities such as MNOs and banks.

5.1 Organization of Users' Account

In our contribution, the blockchain is at the center of transaction operations, so user accounts are managed either by the MNO (this is the classic case, as these are basically Mobile Money accounts) or by a partner bank or by an institution capable of financially

guaranteeing the franchises with the regulating central bank. This management for end-users is possible thanks to their infrastructures participating in the blockchain. A Mobile Money account is under the control of a sponsoring actor, because all accounts are associated with SIM identifiers managed by MNO.

During registration operation, a customer account is created and associated with the use of blockchain services. A wallet that operates on the blockchain does not contain funds, an account or wallet in the blockchain system manages key pairs that enable transactions to be created (unlocking funds assigned to it, or locking funds to another account).

A sponsoring actor performs the process by generating the keys associated with the customer's Mobile Money wallet. At the current stage of research and recommended best practices, the management of a customer's wallet will be carried out according to the BIP32 [26] standards. Thus, the operator generates a daughter key pair for the customer from its master key, which will constitute the root for the generation of several other key pairs and addresses associated with future customer transactions. From the customer root, two key branches A and B are initially generated. The A branch is used, when the client uses his mobile phone for transactions with USSD commands, and the B branch when the client goes through a TCP/IP application. The BIP32 standards are used to avoid escalation attacks. The procedures of BIP32 are briefly described in the section dedicated to the Hierarchical Deterministic (HD) Wallet.

From a seed, the sponsoring actor derives key branches that will correspond to the accounts of the customers; a second possibility consists in generating a seed for the account of each customer. This will allow the sponsoring actor to have control over the accounts of the clients under his sponsorship in order to solve any problems that may arise (i.e. when the sender has the wrong recipient and the operator has to cancel the transaction operation).

At the end of this procedure, the sponsoring actor responds to the customer by means of an "account status sms" (successful creation; failed creation with reasons: authentication problem, server unavailability). A wallet is created for the customer, who can access it through an application using the TCP/IP channel on the network (Branch A) and also through the classic USSD Mobile Money application (Branch B). To carry out a transaction via a TCP/IP application, the customer receives an ID and password by SMS, allowing him to access his account. The management of his account is dynamic and data (ID and password) change every access request from the customer to his online account, to increase security.

5.2 Architecture of the Mobile Money Ecosystem Using the Blockchain

We plan three deployment scenarios in order to test our contribution, which we can be illustrated by Fig. 3:

- **Scenario 1** corresponds to use the current MNO Mobile Money architecture and a gateway to access Blockchain. This is the actual situation in Mobile Money ecosystems. Thus, the customer-MNO segment set-up remains unchanged, except that instead of having a MNO database, it is rather a blockchain infrastructure that validates Mobile Money transactions and federates the Mobile Money solutions of the same ecosystem. The channel is of course USSD.

- **Scenario 2** is associated to the use of the open-source tools of the [27] project on segment 1: Customerr-MNO. This is the case in a laboratory test environment where we replace the MNO with elements from the OSMOCOM project. Thus, the MNO will no longer be a black box. The channel is of course the USSD as in scenario 1.
- **Scenario 3** is related to the use of an application that could directly access the blockchain through the TCP/IP channel to perform transactions in the blockchain. The use of the TCP/IP channel will guarantee a high level of transparency. This channel allows each actor to create, verify all Mobile Money transactions made via USSD on the blockchain. This TCP/IP channel offers greater security than the USSD channel.

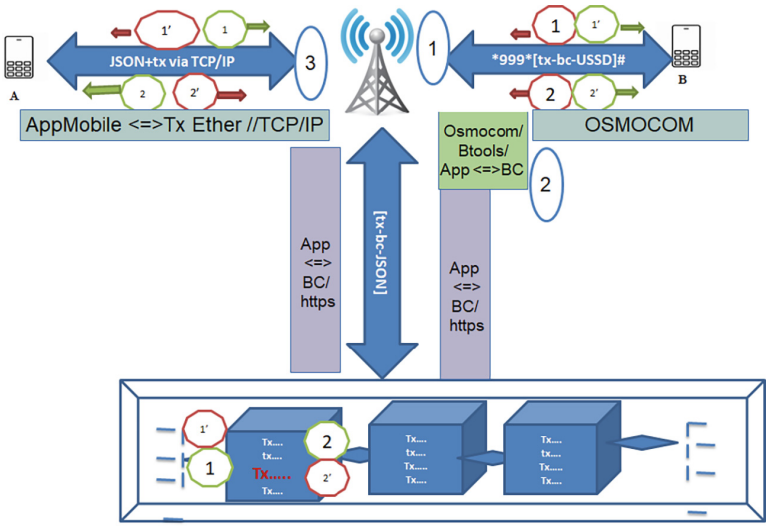

Fig. 3. Three scenarios for experimental architecture

6 Mobile Money Interoperability by 2MUB

6.1 Interoperability DAP

Interoperability requires a compensation system. Many thoughts have been proposed with different architectures. Our contribution is based on a Decentralized Autonomous Platform (DAP) that manages compensation rules in compliance with regulations in the economic space.

The components of our Decentralized Autonomous Platform are as follows:

1. **Smart Contracts:** self-executing agreements between parties with terms of the agreement directly written into code.
2. Blockchain technology: a secure, decentralized, and tamper-proof ledger for storing data.

3. **Cryptocurrency or tokens:** a digital asset used to incentivize and reward users for participating in the platform. This point will be further developed in future work.
4. **User interface:** a way for users to interact with the platform and access its services. Here, we always retain the USSD Mobile Money interface which is a key factor for the adoption of Mobile Money, even by non-literate individuals.
5. **Backend infrastructure:** servers, databases, and other technology that support the platform's functionality. And decentralized governance system: a mechanism for making decisions and managing the platform in a democratic and transparent manner.

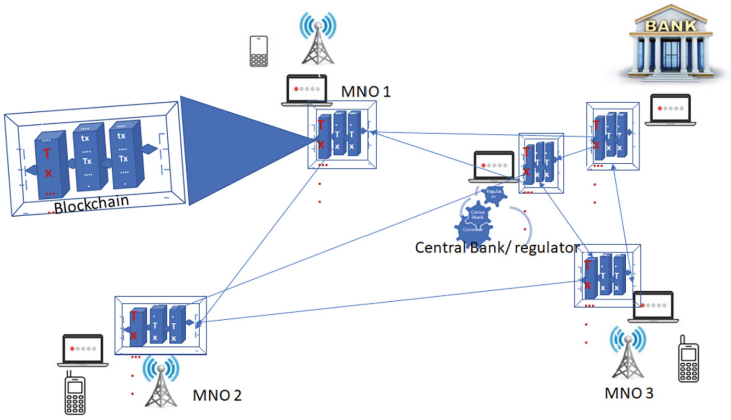

Fig. 4. The Mobile Money ecosystem in blockchain context

Figure 4 provides an insight into the involvement of actors in the Mobile Money ecosystem in the deployment, by showcasing the blockchain nodes (previously introduced in [2]).

6.2 Compensation-Based Interoperability in Smart Contracts

For a transaction between account A of MNO 1 and account B of MNO 2, the operators first have each a credited account in the compensation chamber with a guarantee to secure the transactions for a given period. This operation is transparent to the users. Then, the compensation between the operators takes place as in a banking system.

We achieve interoperability between user accounts and the federation of Mobile Money Operators (MMOs) through a smart contract.

The compensation operations between the MMOs, as outlined in Fig. 5 corresponding to the code of the smart contract, occur through the following steps:

- **Operation identification:** Mobile Money operators identify financial operations they want to compensate, based on criteria such as date, amount, beneficiary, etc.
- **Compliance verification:** Mobile Money operators verify the compliance of the operations to be compensated with internal policies and rules.

- **Fund transfer:** Mobile Money operators perform fund transfers to compensate the operations. This transfer can be made by wire transfer, check or other means of payment.
- **Compensation confirmation**: Mobile Money operators confirm compensation by exchanging confirmation messages.

```
pragma solidity >=0.7.0 <0.9.0;

contract MobileMoneyCompensation {
    address public operator1;
    address public operator2;
    // structure pour stocker les opérations à compenser
    struct Operation {
        uint256 amount;
        address beneficiary;
        uint256 date;
        bool verified;
        bool compensated;
    }
    // tableau pour stocker les opérations
    Operation[] public operations;

    constructor(address _operator1, address _operator2) public {
        operator1 = _operator1;
        operator2 = _operator2;
    }
    // ajouter une opération à compenser
    function addOperation(uint256 _amount, address _beneficiary, uint256 _date) public {
        operations.push(Operation({
            amount: _amount,
            beneficiary: _beneficiary,
            date: _date,
            verified: false,
            compensated: false
        }));
    }

    // vérifier la conformité de l'opération
    function verifyOperation(uint256 _operationId) public {
        Operation storage operation = operations[_operationId];
        require(!operation.verified, "Lopération a déjà été vérifiee.");
        require(msg.sender == operator1 || msg.sender == operator2,
        "Seul l'opérateur peut vérifier l'opération.");
        operation.verified = true;
    }

    // effectuer le transfert de fonds pour compenser l'opération
    function compensateOperation(uint256 _operationId) public {
        Operation storage operation = operations[_operationId];
        require(operation.verified, "L'opération n'a pas été vérifiée.");
        require(!operation.compensated, "L'opération a déjà été compensée.");
        require(msg.sender == operator1 || msg.sender == operator2,
         "Seul l'opérateur peut compenser l'opération.");
        operation.compensated = true;
        operation.beneficiary.transfer(operation.amount);
    }

    // enregistrer les détails de la compensation
    function recordCompensation(uint256 _operationId) public {
        Operation storage operation = operations[_operationId];
        require(operation.compensated, "L'opération n'a pas été compensée.");
        require(msg.sender == operator1 || msg.sender == operator2,
        "Seul l'opérateur peut enregistrer la compensation.");
    }
}
```

Fig. 5. Mobile Money Compensation Smart Contract Code

- **Recording:** Mobile Money operators record compensation details in their respective systems.
- **Liquidation:** Liquidation is the final step of compensation, where funds are transferred to the appropriate beneficiary accounts.

This code defines a smart contract called MobileMoneyCompensation (see Fig. 5) which allows adding operations to be compensated, verifying them, compensating them, and recording the compensation details. Mobile Money operators are identified using their Ethereum addresses.

7 Conclusion

In this paper, we proposed an improvement to the Mobile Money payment protocol using blockchain technology. This upgrade takes into account the presence of multiple mobile network operators (MNOs) and the involvement of banks as Mobile Money providers. The main challenge associated with this multiplicity of actors is the interoperability between customers of different providers. To solve this problem, we proposed the use of a decentralized application (DAP) through the design of smart contracts to define rules and protocols. We also examined the use cases of this approach in Mobile Money ecosystems such as India, Tanzania, etc. 2MUB allows an improvement of transactions traceability and increases trust in the Mobile Money ecosystem.

In perspective, our next works will involve developing the ability to support our Mobile Money transactions on a cryptocurrency that is not a standard cryptocurrency (such as bitcoin, Ethereum, or altcoin), but rather a digital form of the currency in the zone. Thus, for each monetary zone where Mobile Money is deployed on the blockchain, there will be two forms of the same currency: digital in the form of cryptocurrency and physical. Later, it will be a matter of showing in detail how we use the BIP32/39/44 standards to manage Mobile Money user accounts on the blockchain.

References

1. '60% of the World's Population Is Now Online — DataReportal – Global Digital Insights'. Accessed 12 Oct 2022. https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet#:~:text=As%20we%20revealed%20in%20our,total%20population%20is%20now%20online.&text=More%20than%20330%20million%20people,the%20start%20of%20April%202021
2. Agbezoutsi, K.E., Uriene, P., Dandjinou, T.M.: Towards blockchain services for mobile money traceability and federation. In: 2019 3rd Cyber Security in Networking Conference (CSNet), pp. 14–20 (2019). https://doi.org/10.1109/CSNet47905.2019.9108970
3. Agbezoutsi, K.E., Urien, P., Dandjinou, T.M.: Mobile money traceability and federation using blockchain services. Ann. Telecommun. **76**(3), 223–233 (2021). https://doi.org/10.1007/s12243-021-00840-4
4. Zhang, S., Lee, J.-H.: Analysis of the main consensus protocols of blockchain. ICT Express **6**(2), 93–97 (2020). https://doi.org/10.1016/j.icte.2019.08.001
5. '160 000 transactions par seconde (TPS) - Ethereum (ETH) et ChainLink (LINK) pourraient faire mieux que VISA', CryptoActu. Accessed 14 Jul 2021. https://cryptoactu.com/160000-transactions-par-seconde-tps-ethereum-eth-chainlink-link-visa/

6. Dick, C.: A2A InteroperAbIlIty Making Mobile Money Schemes Interoperate. Consult Hyperion Gunnar Camner, GSMA. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/03/A2A-interoperability_Online.pdf
7. Lakshmi, K.K., Gupta, H., Ranjan, J.: UPI based mobile banking applications – security analysis and enhancements. In: 2019 Amity International Conference on Artificial Intelligence (AICAI), pp. 1–6 (2019). https://doi.org/10.1109/AICAI.2019.8701396
8. Kumar, S.B.R., Rabara, S.A., Martin, J.R.: A system model and protocol for mobile payment consortia system. In: 2009 International Conference on Test and Measurement, pp. 438–442 (2009). https://doi.org/10.1109/ICTM.2009.5413011
9. Interoperability in Branchless Banking and Mobile Money | Blog | CGAP. Accessed 02 Feb 2023. https://www.cgap.org/blog/interoperability-in-branchless-banking-and-mobile-money
10. Writer, S.: Kenya's Central Bank gives mobile money interoperability thumbs up. ITWeb Africa. Accessed 02 Feb 2023. https://itweb.africa/content/6GxRKMYJBl1qb3Wj
11. Why is mobile money interoperability important for Kenya?. Financial Sector Deepening Kenya. Accessed 02 Feb 2023. https://www.fsdkenya.org/blogs-publications/blog/why-is-mobile-money-interoperability-important-for-kenya/
12. The impact of mobile money interoperability in Tanzania · 2020. 3. 16. · interoperability in Tanzania that is the focus of this publication. After more than a decade of mobile - [PDF Document]', vdocuments.mx. Accessed 05 Jan 2023. https://vdocuments.mx/the-impact-of-mobile-money-interoperability-in-2020-3-16-interoperability-in.html
13. Argent, J., Hanson, J.A., Gomez, M.P.: The Regulation of Mobile Money in Rwanda. https://www.theigc.org/sites/default/files/2013/08/Argent-Et-Al-2013-Working-Paper.pdf
14. Mvula, F., Phiri, J., Tembo, S.: A Blockchain based Mobile Money Interoperability Scheme. IJACSA **11**(1) (2020). https://doi.org/10.14569/IJACSA.2020.0110117
15. Al-juaifari, M.K.R.: Secure SMS mobile transaction with peer to peer authentication design for mobile government. Am. J. Eng. Res., 7 (2015)
16. Gupta, P.: End to end USSD system. TATA Tele Service Limited, INDIA, July, vol. 7, p. 2010 (2010)
17. Popova, N.A., Butakova, N.G.: Research of a possibility of using blockchain technology without tokens to protect banking transactions. In: 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1764–1768 (2019). https://doi.org/10.1109/EIConRus.2019.8657279
18. Hanifatunnisa, R., Rahardjo, B.: Blockchain based e-voting recording system design. In: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–6 (2017). https://doi.org/10.1109/TSSA.2017.8272896
19. Thuy, L.V.-C., Cao-Minh, K., Dang-Le-Bao, C., Nguyen, T.A.: Votereum: an Ethereum-Based E-Voting system. In: 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF), Danang, pp. 1–6. IEEE, Vietnam (2019). https://doi.org/10.1109/RIVF.2019.8713661
20. Nguyen, Q.K.: Blockchain - a financial technology for future sustainable development. In: 2016 3rd International Conference on Green Technology and Sustainable Development (GTSD), pp. 51–54 (2016). https://doi.org/10.1109/GTSD.2016.22
21. Liu, Q., Guan, Q., Yang, X., Zhu, H., Green, G., Yin, S.: Education-industry cooperative system based on blockchain. In: 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pp. 207–211. IEEE, Shenzhen (2018). https://doi.org/10.1109/HOTICN.2018.8606036
22. He, X., Alqahtani, S., Gamble, R.: Toward privacy-assured health insurance claims. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1634–1641. IEEE, Halifax, NS, Canada (2018). https://doi.org/10.1109/Cybermatics_2018.2018.00273

23. Nath, I.: Data exchange platform to fight insurance fraud on blockchain. In: 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), pp. 821–825. IEEE, Barcelona, Spain (2016). https://doi.org/10.1109/ICDMW.2016.0121
24. Wu, H.-T., Tsai, C.-W.: An intelligent agriculture network security system based on private blockchains. J. Commun. Netw. **21**(5), 503–508 (2019). https://doi.org/10.1109/JCN.2019.000043
25. Mutambaie, M.K.: Blockchain Technology – The Next Computing Paradigm Shift, South Africa, p. 7 (2024)
26. bitcoin/bips32. Bitcoin (2022). Accessed 29 Mar 2022. https://github.com/bitcoin/bips/blob/274fa400d630ba757bec0c03b35ebe2345197108/bip-0032.mediawiki
27. 'Overview - OsmocomBB - Open Source Mobile Communications'. Accessed: Jul 2022. https://osmocom.org/projects/baseband