Secure, Transparent and Uniform Mobile Money for Internet-Underserved Areas Using Sporadically-Synchronized Blockchain

Sankalp Ghatpande[1], Hadja Ouattara[2], Daouda Ahmat[3], Zakaria Sawadogo[2], and Tegawendé F. Bissyandé[1,2(✉)]

[1] SnT, University of Luxembourg, Luxembourg City, Luxembourg
sankalp.ghatpande@uni.lu
[2] Université Ouaga I Pr. Joseph Ki-Zerbo, Ouagadougou, Burkina Faso
hadja.ouattara@gmail.com, zakaria.sawado@gmail.com, bissyande@fasolabs.org
[3] Université Virtuelle du Tchad, N'Djamena, Tchad
daoudique@gmail.com

Abstract. This position paper presents the design and outline of the implementation of a mobile money scheme that adapts to the realities of Internet-underserved Areas while exploiting the benefits of Internet protocols. In particular, we implement security and transparency in mobile money transactions using a lightweight permissioned Blockchain infrastructure. Nevertheless, due to network latency and potential connectivity issues, the design of the platform accepts semi-offline transactions: it leverages USSD, a 2nd Generation mobile protocol, only as a back-up channel to force writing of offline transactions to the permissioned ledger and ensure smooth synchronization of the blockchain.

Keywords: Mobile money · Blockchain · ICT4D · Internet-underserved areas

1 Introduction

Electronic payments have experienced a rapid development in the last decade with hundreds of customers worldwide [7]. Mobile banking services, in particular, are now widely adopted within developing countries where they enabled far remote population (e.g., in rural areas) to reach financial services which were not available due to the absence of infrastructure from the traditional banking institutions.

Electronic cash has been a hotbed for investigation in academia as well as industry since the early 90s with the seminal paper by Chaum [6]. Cryptographic techniques were heavily used to provide security for such electronic cash,

G. Mendy et al. (Eds.): AFRICOMM 2018, LNICST 275, pp. 120–130, 2019.
https://doi.org/10.1007/978-3-030-16042-5_12

including protecting against forgery and addressing the double-spending problem. However, in general, the solutions that were being introduced required a trusted third-party such as banks to generate, distribute and validate the digital cash. Bitcoin [12] is a pioneer electronic cash system that neither relies on banks (or any other form of central authority) for the issuance of the coins, neither for their distribution, nor for validating the transactions. There are now over thousands of merchants worldwide that accept bitcoins as currency [4] and has an increasingly large support from payment processors.

In recent years, Bitcoin has been thoroughly studied by researchers and industry practitioners for its use, going from a rigorous analysis in terms of security [9] to analysis of its economic impact [11]. Moreover, a number of alternative cryptocurrencies (altcoins) have been proposed that made considerable changes to the initial design and goals of the Bitcoin. For example, ZCash[1], CryptoNote[2] have been designed with the goal of providing more privacy. Litecoin[3] makes use of different mining mechanisms while others like Ethereum[4] extend the Bitcoin transaction capabilities to enable more flexible approach towards novel transactions scenarios such as Smart contracts.

The challenging aspects of digital currency security, including forgery and double-spending, are addressed in Bitcoin using asymmetric cryptography and a distributed time-stamping mechanisms that is based on Proof-of-Work. As a result a transaction cannot be considered to be confirmed as soon as they are received on the blockchain because it takes some time for the network to verify and integrate them in an atomic state that is hard to change. Consequently, the recipient of any blockchain-based transaction requires an online connection with its underlying blockchain network in order to confirm the validity of the transaction, which takes a certain amount of time[5]. **This makes offline payments with cryptocurrencies extremely challenging** despite offline payment being highly desirable in real world (e.g., in internet-underserved areas). Additionally, Bitcoin payments are increasingly used at many Point-of-Sale (PoS) terminals for immediate payments, where purchased assets are released within a few minutes after the payment and before the transaction confirmation have been generated by the network, although it was already shown that such deployments are vulnerable to double-spending attacks [10]. This has led for the introduction and wide-spread use of permissioned-ledgers, i.e., blockchains that make use of assets *other* than fully-decentralized Bitcoins and where nodes are vetted before they can participate in the blockchain, reducing the requirement for majority consensus before a transaction is validated.

[1] https://z.cash/.
[2] https://cryptonote.org/.
[3] https://litecoin.com.
[4] https://ethereum.org/.
[5] Currently the validation delay takes on average 10 min.

This Paper. In this paper, we present the design of a new protocol that will enable secure payments with electronic cash, based on blockchain, in semi-offline settings and in scenarios where payments/transactions needs to be immediately validated. In particular, our contribution is proposing a *solution for semi-offline payments* that is possible on permissioned ledger. To the best of our knowledge, this is the first solution that does not require both the payer and the payee to be online (either over internet or any another form of communication). The solution relies on an offline wallet (device) of the payee that uses cryptographic signatures to provide the assurance of a valid transaction between two parties even when they are not connected at transaction-time to the underlying blockchain.

2 Background

In this section, we provide a brief overview of the basics of blockchain, as well as the current state of the SIGMMA project for blockchain-based mobile money.

2.1 Blockchain Basics

The Bitcoin ecosystem consists of two types of users: Normal users and miners. A normal user utilizes the Bitcoin network for exchanging bitcoins with another user by means of transaction, either being the sender or recipient in such a transaction. These users are identified using their unique addresses which are associated with asymmetric key pairs. In practice, a single transaction may consists in transferring funds between several accounts at once, i.e. it can involve several senders and receivers. Nevertheless, for reasons of simplicity we will assume throughout the paper that a transaction has one sender and one recipient only.

The miners in the Bitcoin ecosystem are the actual backbone of the network. These miners work on validating the transactions and including them into the public history of all the successful transactions into a *blockchain*. These miners have no special account but rather normal user account where they receive rewards for their efforts in verifying transactions. In the case of permissioned ledgers, the role of miners is effectively taken by validators who work similarly as the miners but *without receiving any rewards for their efforts*. The validators have the authority to encode new transactions into a permissioned-blockchain.

The blockchain is simply a logical sequence of blocks that are chained to each other which is extended by appending new valid blocks at its end. Each block within the chain references the previous valid block, which defines the unique order of blocks within the chain. Appending a new block requires the miners to solve a cryptographic puzzle, which itself requires a significant computational effort depending on the consensus protocol which is used. Such a puzzle is then different for the different altcoins: for instance, the Bitcoin requires finding an input towards a hash function of a random nonce which results in a hash value less than a specific target value. This requires the miners to usually have a large computational capabilities where they have to compute a number of hashes until a solution is found. The target value for the puzzle is a security parameter which

regulates the difficult of the puzzle, which is adjusted by the network based on the computational power within the network. For more comparative details, we refer the reader to our comparative enumeration of consensus protocols [13].

Once a block has been created and appended to the blockchain, all the transaction included within this block are considered to be confirmed by the network. Subsequent blocks will be appended to the current block making it harder to tamper with the past transaction as ti would require recomputing all the subsequent blocks within the chain. There are different ways to verify the transaction. The miners and validators can perform a full verification (i.e., check for all the blocks within the chain), mobile clients that are incapable of large computation performs a lightweight processing known as simple payment verification (SPV). As opposed to full verification, SPV users verify only the transaction and its confirmed issued by the network i.e. it checks for headers of the blocks for validation without checking all the transaction included within such block, which is considered to be sufficient to ensure that the blocks are part of the blockchain and were generated correctly.

2.2 Mobile Money and the SIGMMA Project

Digitization of payments, transfers, and remittances is key to transparent and inclusive economic growth in low income countries, as it will increase customer convenience, reduce transaction costs substantially, and minimize the need for unaffordable physical infrastructure (e.g., local bank branches). Various stakeholders across the financial and IT ecosystems are expected to be impacted by the penetration of Mobile money. For example: (1) a vast portion of the economy involving person-to-person (P2P) payments in networks of families and friends will benefit from the security and efficacy of remote transactions; (2) the enormous amount of businesses in the informal sector who are trading today but who do not have access to the formal payment infrastructure will be served; (3) governments will gain in reduced payment costs and increased transparency; (4) banks and financial institutions will finally be able to tap into the economic potential of unbanked populations; (5) finally, broad acceptance of digital-payment platforms should benefit stakeholders beyond the payment industry, as it will incite innovation and spur growth.

Over the last decade, the continent has been positioning itself as a leader in Mobile money–cashless electronic payment that use mobile telephones as the main payment mechanism, rather than using a smartphone only as a conduit to a user's bank or credit card account. The GSM Association (GSMA) Mobile Money programme, based on data collected from its network of 850 operators around the world, has recently stated that: *Mobile money has done more to extend the reach of financial services in the last decade than traditional "bricks and mortar" banking has in the last century.* [3]: While, by 2015, mobile money was available in 93 countries, more than half the mobile money companies are operating in Africa. The biggest success story in Africa is Kenya-based M-Pesa, a service launched by UK-based Vodafone for SafariCom in 2007. Within two years, about 38% of Kenya's adult population was using M-Pesa. By 2015,

M-Pesa had 13.9 million active users – with an estimated 40% of Kenya's GDP flowing through its network [1].

M-Pesa's growth however is based on special circumstances, as reported by The Economist Intelligence Unit: "M-Pesa was started by a mobile phone operator that already had a very high market share [of 70%]. Financial regulations around these types of services in Kenya were very loose at the time. The government was very supportive, as it was keen to use mobile financial services to make government payments throughout the country" [15]. In a piece for the BBC's Matter of Life & Tech, Burkman even argues that M-Pesa, "the poster child of mobile money in Africa", paints a false picture of the continent since the reality is that "mobile money has only really taken off in one country out of 55 on the continent" [2]. In other countries, the quest to replicate Kenyan M-Pesa success remains a difficult struggle. Even attempts to launch M-Pesa in neighbouring countries like Tanzania and South Africa have faced a range of obstacles [2]. Throughout the region (i.e., sub-Saharan Africa), several mobile money systems initiated by telecom operators and banks, and often based on SMS/USSD technologies as in M-Pesa, are beginning to pay off (although at a lesser scale than M-Pesa). We enumerate four limiting factors that currently prevent a full-blown adoption of mobile money in sub-Saharan Africa:

1. Mobile money payments are currently made using interfaces that target feature phones. Yet, smartphone penetration in Africa has rapidly evolved [8], and user-friendly apps can now help to improve adoption.
2. SMS/USSD messages are easily hacked by malware on smartphones which have become common among users. Besides, in case of fraud, it is impossible to track money flows beyond cash-out desks/agents [5].
3. Client and service provider accounts are tightly associated to network operators or banks. This situation challenges the possibility of transactions across operators while hindering innovation: service creation is not open to the large public [16].
4. There is little participation of low income country consumers to the global financial market; E.g., limitations on cross-border transactions challenges the access to online resources such as MOOC courses.

In 2017, the SnT Interdisciplinary centre at the University of Luxembourg has initiated, together with partners from Universities in Senegal, Burkina Faso, Cote d'Ivoire and Netherlands, a project for Secure, Interoperable Mobile Money in sub-Saharan Africa (SIGMMA) based on the blockchain technology. The SIGMMA platform is a digital vehicle to fiat currencies produced by the central bank. Thus, it is not a bitcoin-like platform where cryptocurrencies are mined (i.e., generated based on the computing power put forth to resolve complex algorithmic problems). Instead, our similarity with bitcoin is only related to the use of the underlying technology of blockchain to validate transactions and store them in a distributed ledger for transparency. Currencies get in and out of the system through cash-in/cash-out points where exchange operations are performed

Table 1. Bitcoin vs e-Money (©CGAP report [14])

	Bitcoin	e-Money
Accessibility	Largely limited to internet connection	Access to electronic devices such as mobile phones, and an agent network
Value	Determined by supply and demand, and trust in the system	Equal to amount of fiat currency exchanged into electronic form
Customer ID	Anonymous	Financial Action Task Force standards (especially KYC rules) apply for customer identification (though such standards permit simplified measures for lower risk financial products)
Production	Mathematically generated, "mined" by peer network	Digitally issued against receipt of equal value of fiat currency of central authority
Issuer	Community of developers, called "miners"	Legally established e-money issuer
Regulator	None	Regulated by central authority, typically central bank

by traditional financial service providers. We now describe differentiating points between different models in digital currencies, in order to better position the SIGMMA platform as cryptocurrency-based e-Money platform. The following table is an excerpt of the CGAP report on "Bitcoin vs Electronic money" [14] (Table 1).

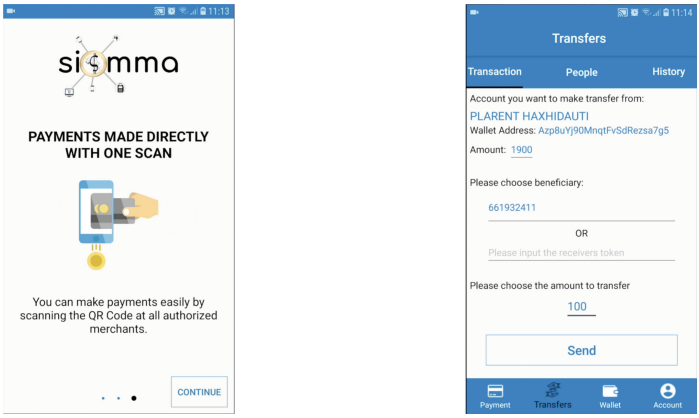
SIGMMA is implementing an e-money platform on top of the blockchain technology: the cryptocurrencies transacted should then be considered as digital fiat currencies. Indeed, these are typical e-Money currencies (whose value is equal to the amount of exchanged fiat currency), but which are circulating in a blockchain network allowing to guarantee transparency, security and interoperability across systems.

Figure 1 illustrates screenshots from the current app of the SIGMMA prototype. The core technology for validating transactions is based on the Exonum[6] framework. Although promising, the current prototype did not support offline payments which are necessary for internet-underserved areas where connectivity is unstable. This paper presents our idea for moving SIGMMA for supporting semi-offline payments with a sporadically-synchronized blockchain.

[6] https://exonum.com/.

2.3 Challenges Towards Offline Payments

1. The first challenge towards offline mobile money payments that are based on blockchain relates to the use of *constrained devices*. As an order of comparison, for full bitcoin wallets it can take days to download and validate the whole blockchain even on modern desktop personal computers. Wallets on mobile devices may not even be able to perform Simple Payment Verification as they may not have enough resources to store the block headers. This itself makes it challenging to ensure that the device is capable of validating the transaction in some manner.
2. The second challenge relates to the need to guarantee the synchronization of the blockchain whenever the disconnected party goes online. Malicious parties may explore the possible to roll back some transactions while offline so as to repudiate any block that will be associated with the client.



(a) Support of payment with QR code (b) Support for Person-to-person payments

Fig. 1. Screenshots from the SIGMMA app

3 Semi-offline Blockchain-Based Mobile Money

The SIGMMA platform already ensures interoperability by allowing legacy mobile money operators to plug in, enabling cross-operators transactions. Transparency and Security are assured by the underlying transparent ledger of the blockchain, while uniformity (i.e., the possibility to undertake any financial operations) is provided through an Application Programming Interface (API) on top of which new services can be built (e.g., person-to-person payments, Point-of-sale payment, online banking services, etc.). Unfortunately, currently the SIGMMA app does not fully account for instability in internet connection with the fragile infrastructure available in sub-Saharan Africa.

3.1 Model of the System

The system used can be represented in the traditional four-layer model which can be developed within the Exonum framework:

- *Network*: This layer tracks the adresses and connection routes to the different computing nodes that participate in maintaining the blockchain.
- *Protocol*: This layer defines the basic rules that define the behaviour of participants within the network. It formalizes the features such as immutability, byzantine fault tolerance and scalability of transactions.
- *Data*: This layer implements the blockchain storage. The blockchain itself will include the identities, transactions, account balances, contracts and its states that users of the network has stored.
- *Application*: This layer defines how services can be implemented by offering APIs.

Concretely, our system consists of a permissionned blockchain infrastructure which includes a blockchain **B** and validators **V**. These validators are similar in as miners in the traditional bitcoin-based blockchain. Validators, contrary to miners, are not rewarded since they are part of the system with the function to ensure integrity of the chain while finalizing the different transactions as state within the chain. We have multiple users (Alice and Bob here) where Alice wants to send an offline transaction τ to Bob. Both users have their handheld devices which are registered on the blockchain with a unique identity: typically, this is seamlessly done via the installation of the SIGMMA app. The unique identity is a public key used to identify the user on the network. Each of the device is also capable of performing a computational operation that can generate a unique secret key for each user and can apply signature on a piece of data.

Additionally, the handheld devices are connected to validators (which are operated by the service provider) either via normal 3G cellular network or using Wi-Fi capabilities. Furthermore, each of the device has a certificate that presents legitimacy of the validator to which the user is subscribed to.

3.2 Proposed Protocol Design

We present protocol design for each phase of our solution: committing-coins, offline transaction confirmation and pushing to the underlying blockchain.

Notations. We denote an operation as $A(in) \longrightarrow out$, where A is the name of operation, in is the input requires and out the output of the operation, which may be a boolean value. We have $sig(sk; d) \longrightarrow \sigma$ to denote signature on the data d using the signature key sk which can be verified using the operation $verify(pk, d, \sigma) \longrightarrow false, true$. Figure 2 shows the overall flow of offline and online validations.

In the committing-coins phase of the protocol, the payer Alice first indicates the amount b that she would like to load in her sub-wallet W_s. Next the wallet creates a transaction τ_1 that transfers b coins to this sub wallet and pushes this towards the underlying blockchain.

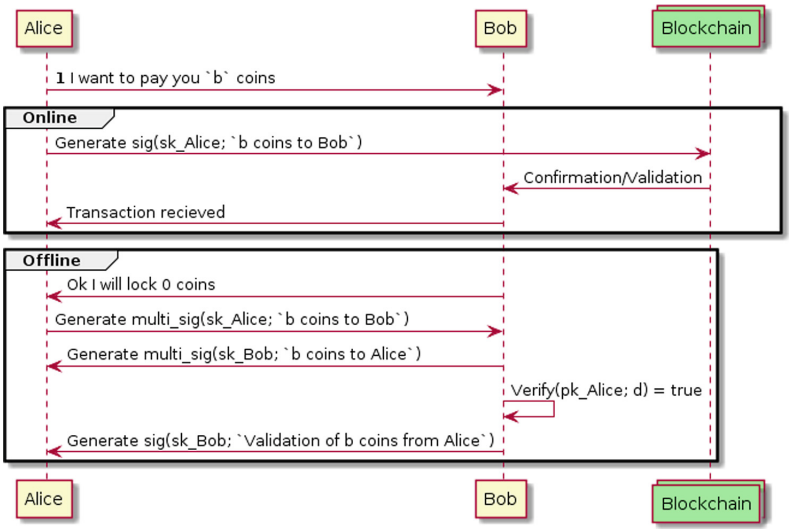


Fig. 2. Online vs offline protocols with the blockchain

As both Alice and Bob may not have any online connection during the payment, the offline transaction τ is sent using local interfaces that are commonly available in majority of the handheld devices (such as Bluetooth and NFC) for peer-to-peer connectivity recognized by the SIGMMA app available in both devices. Nevertheless, if both are online (in any form) then the transaction would be directly pushed towards the blockchain like normal blockchain transactions. However, both parties are bound to occasionally online, e.g., Alice goes online to receive a transaction to her account, and Bob to redeem the offline transaction that he received after payment. Finally, to prevent any roll-back of transactions made offline (which would lead to inconsistencies), once a transaction is made offline, a USSD message is committed by the SIGMMA app towards a telecom operator gateway. Since USSD message are always successful (in the sense that they get queued and cannot be canceled by the user, and will be sent out once cellular network connectivity appears), no offline transaction can be removed from the ledger. We further put a threshold on the number of transactions that a single user can make offlines before it must synchronize against the blockchain, so as to avoid latency in complex merging of blocks.

4 Concluding Remarks

There is a huge effort within the academia and industry towards democratizing the use of Blockchain on the one hand, and improving mobile money on the other hand.

Mobile money business has helped drive a large improvement towards achievement in providing the access towards financial services to those who are

generally unreachable. Services through informal, yet technically sound systems, such as the micro-credit association or community driven savings club which are often refereed as powerful means to drive low-income people towards the traditional financial institutions. These alternative ways do not require the mandatory identification requirements and in many cases relay on mobile technologies that allow conducting transactions without the need of being physically present at the bank or other financial entity. Currently, mobile operator services are generally not interoperable with other operators, which means that transactions are limited *only* within the operator's system. Furthermore, the operators tend to charge transaction fees to establish monopoly within the economy of a particular region.

Blockchain projects have been known for its ability to store and transmit values across national and trans-national borders at large scale at relatively low cost but would require a logical approach and understanding of its underlying technology including access to stable Internet access and a relatively modern smartphone. In developing countries, people tend to live on daily wages that are approx 10$ per month where the requirement of 100$ smartphone along with Internet charges make it out of scope for majority of the population.

The SIGMMA project is working towards a sustainable solution to the security, interoperability, transparency and cross-border issues of Mobile money in sub-Saharan Africa. We plan to roll out a test prototype of the proposed solution for sporadically-synchronized blockchain which accounts for the realities of constraints of internet-underserved areas.

References

1. Telecoms in Kenya: A new East Africa campaign. https://goo.gl/H3cFyR
2. Making mobile money pay in Africa (2017). https://goo.gl/vl1WDi
3. GSM Association: State of the industry report on mobile money (2015). https://goo.gl/xdJj79
4. Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better — how to make bitcoin a better currency. In: Keromytis, A.D. (ed.) FC 2012. LNCS, vol. 7397, pp. 399–414. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32946-3_29
5. Central Bank of Kenya: Launching of the financial geospatial mapping survey (2015). https://goo.gl/MF9rUU
6. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology, pp. 199–203. Springer, Boston (1983). https://doi.org/10.1007/978-1-4757-0602-4_18
7. Dunn, E.: Advanced payments report (2017). http://edgardunn.com/wp-content/uploads/2017/06/EDC_AdvancedPaymentA4_2017.pdf
8. Ericsson: Ericsson report: Mobile internet use doubling year-on-year in sub-Sahara Africa. https://goo.gl/0iITaZ
9. Eyal, I., Sirer, E.G.: Majority is not enough: bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 436–454. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45472-5_28
10. Karame, G.O., Androulaki, E., Capkun, S.: Double-spending fast payments in bitcoin. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 906–917. ACM (2012)

11. Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of bitcoin mining, or bitcoin in the presence of adversaries. In: Proceedings of WEIS, vol. 2013, p. 11 (2013)
12. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
13. Ouattara, H.F., Ahmat, D., Ouedraogo, F.T., Bissyande, T.F., Sie, O.: Blockchain consensus protocols - towards a review of practical constraints for implementation in developing countries. In: EAI International Conference on e-Infrastructures and e-Services for Developing Countries (AFRICOMM) (2017)
14. Parker, S.R.: Bitcoin vs electronic money, CGAP report (2014). https://goo.gl/po06th
15. The Economist Intelligence Unit: Mobile money in Africa: Promise and perils. https://goo.gl/DUI47i
16. World Bank Development Research Group, the Better Than Cash Alliance, and the Bill & Melinda Gates Foundation: The opportunities of digitizing payments (2014). https://goo.gl/wTlECK