A Blockchain based Mobile Money Interoperability Scheme

Fickson Mvula[1], Simon Tembo[3]
Department of Electronics and Electrical Engineering
School of Engineering, UNZA
Lusaka, Zambia

Jackson Phiri[2]
Department of Computer Science
School of Natural Sciences, UNZA
Lusaka, Zambia

***Abstract*—Developing Countries in Africa in general and Zambia in particular, have seen a rapid rise in use of mobile payment platforms. This has not only revolutionized access to finance for the poor but also allowed them access to other financial products such as savings or insurance. With a growing number of mobile money providers in Zambia, there is need for a solution that would enable integration of the mobile money provider's systems using a central clearinghouse for purposes of clearing and settlement to achieve mobile money interoperability. In this study, we first reviewed the technical landscape and features of mobile payment systems in Zambia and then assessed the feasibility of using blockchain technology in proposing a settlement and clearing system that would facilitate mobile money interoperability. A prototype system was then designed in which amounts being interchanged between providers are managed as assets on a permissioned blockchain. The system runs a distributed shared ledger, which provides non-repudiation, data privacy and data origin authentication, by leveraging the consistency features of blockchain technology.**

Keywords*—Blockchain; mobile money interoperability; clearing and settlement; blockchain security

I. Introduction

There is a growing number of mobile money wallet services providers in Zambia which has led to the creation different autonomous financial ecosystems with little to no interoperability between them. We define interoperability as an ability of one mobile money subscriber on one network, to transfer value to another on a different network [1]. Attempts have been made to close this gap through provision of bilateral arrangements between mobile money providers which has proved problematic as there are delays in settlement due to ledger trust issues.

Currently, there is currently no live implemented system that allows interoperability between the different mobile financial services wallet providers in Zambia. The proposed Zambia National Switch project [4] being undertaken by the Zambia Electronic Clearing House Limited (ZECHL) will among others enable participants in the mobile financial ecosystem to interchange money by providing a clearing and settlement platform. The system implementation will be phased and the first phase expected to cater for interoperability of commercial banks and expected to be launched at the end of 2019. The second phase will cater for integration of other financial services such as mobile money and telegraphic money transfers [5].

The National Financial Switch system however, being a traditional database based central system will have a number of shortfalls in as far of effective provision of the desired features identified for clearing and settlement of account to account (A2A) interoperability transactions. Firstly, there will be integration complexity as every participant will be required to connect to a central node. This central node of processing will hinder efficiencies in end-to-end processing speed and thus availability of funds may be hampered. Further, there will be no network resilience offered by distributed data management system such as one provided by a distributed ledger system. And furthermore, there may be operational and financial risks as a result of a single central node rather than a distributed one.

Integration of wallet provider's systems through a central clearing house for purposes of clearing and settlements [2] is necessary to achieve interoperability. Blockchain technology presents a perfect opportunity as a potential technology to disrupt payment, clearing and settlement because of its ability to introduce a set of synchronized ledgers managed by one or more entities rather than individual non communicating ledgers [3]. This would lead to a reduction in the reliance on traditional central ledger managed by a trusted entity for holding and transferring funds.

In this paper, we present a study that proposes the design of a secure and trusted blockchain based clearing and settlement architecture that will allow seamless interoperability for mobile financial services in Zambia. The paper is divided into five sections. Section 2 gives a background to Blockchain technology and shows how it could be used to support the use case in the study while Section 3 gives the literature review and describes similar approaches that others have used to solve the interoperability problem. Section 4 presents the research methodology while Section 5 covers the results of the research.

II. Clearing and Settlement on a Blockchain

A. Blockchain Defined

A blockchain can be defined as an immutable ledger for recording transactions, maintained within a distributed network of mutually untrusting peers. Every peer maintains a copy of the ledger. The peers execute a consensus protocol to validate transactions, group them into blocks, and build a hash chain over the blocks. This process forms the ledger by ordering the transactions, as is necessary for consistency. Blockchains have emerged with Bitcoin and are widely regarded as a promising technology to run trusted exchanges in the digital world [6].

The two main categories of blockchains are public and private blockchains. In a public or permission-less blockchain, anyone can participate without a specific identity. Public blockchains typically involve a native cryptocurrency and often use consensus based on proof of work (PoW) and economic incentives. Permissioned blockchains, on the other hand, run a blockchain among a set of known, identified participants. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which do not fully trust each other, such as businesses that exchange funds, goods, or information.

By relying on the identities of the peers, a permissioned blockchain can use traditional Byzantine-fault tolerant (BFT) consensus instead of incentives based consensus mechanisms.

B. Blockchain in Funds Clearing and Settlement

The proposed solution is directed primarily at arrangements that involve restricted ledgers (access to which is for approved users only) or permissioned blockchains, reflecting the main types of arrangement currently being developed in the financial sector, such as one required for a mobile money account to account interoperability among a number of disparate network providers.

Clearing and settlement of a financial transaction, regardless of the asset type, requires a network of participants, an asset or set of assets that are transferred among those participants, and a transfer process that defines the procedures and obligations associated with the transaction. Typically, the set of direct participants are financial institutions such as banks or brokers and indeed mobile wallet providers in the case of mobile financial services. Indirect participants include end users such as subscribers in this case. An asset can be any financial instrument, such as a monetary instrument, security, commodity, or a derivative.

In a mobile financial services ecosystem, the asset type of interest is virtual money (or e-money) being transferred from one wallet to another across the network of participants. Communications among the participants in a network involve sending electronic messages, acknowledgements, statements, and other information between computer systems typically maintained by a network operator and its participants.

It is worth noting at this stage that the current implementation of such networks is such that each participant maintains and is responsible for their own financial ledger which acts as their single source of truth on the status of their data. To achieve interoperability, a common central authority may be necessary which would be entrusted by their participants with updating and preserving the integrity of a central ledger and, in some cases, managing certain risks on behalf of participants.

The case for Distributed ledger technology (DLT) as a potential technology to disrupt payment, clearing and settlement implementations is because of the technology's ability to introduce a set of synchronized ledgers managed by one or more entities rather than individual non communicating ledgers. This would lead to a reduction in the reliance on traditional central ledger managed by a trusted entity for holding and transferring funds and other financial assets.

DLT may radically change how assets are maintained and stored, obligations are discharged, contracts are enforced, and risks are managed. Proponents of the technology highlight its ability to transform financial services and markets by [7]:

- Reducing complexity.
- Improving end-to-end processing speed and thus availability of assets and funds.
- Decreasing the need for reconciliation across multiple record-keeping infrastructures.
- Increasing transparency and immutability in transaction record keeping.
- Improving network resilience through distributed data management.
- Reducing operational and financial risks.

III. Literature Review

In their basic sense Mobile payments platforms allow their users to pay and transfer funds in mobile money, but also offer access to other financial products, such as savings and bill payments. A study in [8], reviewed the economic features of mobile payment systems in developing countries, and studied the cooperation models that can emerge between the different firms potentially involved in a mobile payment transaction. Focus was drawn on the main competition concerns that public authorities should be concerned about, and which regulatory tools could be considered as a remedy. Key among some of the key challenges in mobile money schemes was the issue of interoperability. Different concepts of interoperability are relevant and need to be distinguished according to their implications for regulation and business models differ.

Different approaches have been undertaken by different countries in an attempt to implement interoperability for their mobile money financial systems. This section reviews a number of such proposed architectures for mobile payments that support interoperability. These have been drawn from well-developed mobile money markets and they include India, Kenya, Rwanda, and Tanzania. Next, a number of blockchain based use cases were reviewed and presented to support the case for use of blockchain in a system model proposed.

A. Interoperability Schemes in other Similar Markets

In 2008, the Reserve Bank of India (RBI) provided an interoperability platform called UPI [9]. This is however, a central integrating node which suffers integration complexities.

Alternative architecture approaches proposed [10] with hierarchical lookup. Kumar et al. also proposed architectural choices [11]. However, their model is specific to highly regulated financial environment in India, where every transaction is processed by a bank.

Other options in the Indian landscape include, the Mobile Payment Foundation of India [11] which is also developing a model for interoperability. Further, Kumar et al. have proposed architectural choices for interoperability [11]. However, their model is specific to highly regulated financial environment in India, where every transaction is processed by a bank.

Interoperability is not mandated under the Kenyan National Payments System (NPS) regulations but instead payment service use bilateral arrangements [12], [13], [14] rather than through a common central switch system. But as has been observed by [15] a common switch, with its own set of rules for participation, technical and operational issues, improves coordination and customer experience, and allows for a much faster implementation of interoperability, as compared to private switches or bilateral agreements.

Like Kenya and the other East African countries, Rwanda has an equally mature and highly competitive mobile money landscape [16]. Again similar product offerings are on offer by the different mobile money providers and these include balance maintenance, deposits, withdrawals and transfer of funds with convenience that is not currently being met by the commercial banks to the poor unbanked.

Despite mobile money services having been operational for a long time now, Rwanda equally does not have a formalized central clearing and settlement system that offers interoperability for the mobile money providers. This study [16] reviewed the regulation of mobile money aspects in Rwanda and considered among others, interoperability for the country with the aim of fostering a conducive financially inclusive society. The study proposes a light handed regulatory approach owing to the highly technical and capital intensive nature of the mobile money industry.

While countries like Kenya have bilateral based interoperability models in place of a central integrator mode, Rwanda has yet been to establish one. New regulation in Rwanda requires interoperability of all payment systems before integration could be realized. What has rather been observed in this market however, is the fact that subscribers transacting across networks through the use of agents. For example, an MTN user can always send money to a Tigo user, but the receiver will have to visit an MTN agent to withdraw the cash and the charges are slightly higher. In addition, if the subscriber then wants to use that cash on the Tigo system, he will have to visit a Tigo agent to make the deposit – so getting cash from a deposit in one system to a deposit in another requires visiting two agents.

Interoperability between the Rwanda banking system and mobile money services is similarly available in a weak form – it requires a physical visit to a bank branch. The next step in interoperability would allow the remote payment from an account on one provider directly into the account of another via a command from a mobile phone or bank branch.

There are four different mobile network operators all providing mobile money services to their subscribers in Tanzania [17]. Tanzania is one of the most successful mobile money markets in the world with more than 25% of the population being active mobile money users (with almost 11 million in December 2013) and transacting an estimated USD 2 billion in transactions per month in 2014 [17].

According to a study [18] by the GSMA on account to account (A2A) interoperability models in Tanzania and Pakistan, A2A interoperability was launched in Tanzania in 2014, and in Pakistan in 2015. The study found that in both Pakistan and Tanzania, the regulatory environments were enabling for A2A interoperability and that providers freely choose the technical model that best suited their commercial interests rather than being restricted to a pre-determined or preferred model defined by regulation. This has led to Tanzanian mobile money providers opting for bilateral point to point integrations as a preferred model for interoperability.

As been pointed out [1], bilateral models may seem easy to deploy where there are limited parties involved but later suffer several disadvantages including the increase in complexity with number of parties, duplication of efforts and an increase in complexity of maintenance over time.

Literature studied showed a number of different approaches to interoperability employed in different countries. One such an approach is the use of a Central Bank led national switching system for clearing and settlement.

Mobile money services in Zambia are regulated by the Central bank and therefore, this makes the use of a central switch an ideal and suitable enough approach to interoperability. So far, the technological setup used in such an approach has been with a central database system.

A number of problems with this approach have pointed out including, complexity of integration, introduction of a single point of failure and lack of trust. This paper therefore proposed a blockchain based solution approach to address these shortfalls.

A number of blockchain use cases are presented in the following section to highlight some of the properties of blockchain that make it a suitable technology to address these problems.

B. Blockchain use Cases

The A number of blockchain based solutions have been proposed by various researchers across different industries over the last few years that the technology has matured. This section highlights some of these solutions.

Firstly, [19] examined the use of Distributed Ledger Technologies (DLT) in the area of payments, clearing and settlement and identified both a number of opportunities and challenges facing its long-term implementation and adoption. Further calls for tamper-resistant data stores solutions are made in [20] by proposing the use of a write once and read multiple times data storage solution.

Similar calls are echoed in an attempt to solve problems in the management of clinical records [21]. It is argued that a blockchain technology has the potential to solve the records management problems by providing a single, secure, decentralized storehouse of clinical data for all patients.

A solution for parking slot management in a trust less network is proposed here [22] which seek to provide a platform capable of being used without a third trusted party.

In [23], a decentralized traceability system based on Internet of Things (IoT) and blockchain is proposed for the food industry. While [24] proposes a hybrid architecture for supply chain management based on a set of private distributed ledgers for storing sensitive customer information and a public

ledger where a hash of each private event is stored along with the monitoring events.

Like many such similar use cases proposed, the goal to implement a secure and trusted system that takes advantage of the blockchain properties of transparency, immutability and shared consensus [25].

IV. Research Process

This study was guided by three (3) main objectives. Firstly, a targeted survey and interviews were conducted to establish how mobile financial services are currently implemented in Zambia. Further, literature and documentation on mobile money system and service implementation was consulted to understand how they are setup. The goal was to try to establish and highlight short falls and inefficiencies in implementation that prevent interoperability and thereby identify opportunities for improvements.

Secondly, an analysis as to whether a conceptual model for inter operator mobile financial transactions payments, clearing and settlement in a secure, transparent and trusted manner could be proposed and designed. The goal was to establish if blockchain technology would be an ideal technology to achieve the proposed design.

Finally, we carried out an implementation of a prototype that demonstrates Blockchain security services in a permissioned and regulated environment. The designed system was a prototype system in which amounts being interchanged between mobile money providers are managed as assets on a permissioned blockchain. The system runs a distributed shared ledger which prevents amount theft as well as fraud such as transferring invalid amounts, or transferring multiple copies of an amount, by leveraging the consistency features of the blockchain.

A. Survey Design

A list of interview questions were designed into a survey and administered to a target audience of respondents, deliberately selected according to set criteria. Further, walk in interviews were conducted with subject matter experts to validate and verify researched literature and documentation on mobile money systems and service implementation. The goal was to try to establish and highlight short falls and inefficiencies in implementation that prevent interoperability and thereby identify opportunities for improvements in the solution design.

B. Survey Participant Target Group

The research participants were purposively selected basing on their expertise, experience and skills relating to the subject under study in order to get rich and relevant information. Survey participation was drawn from employees of Zambia's mobile money operators and employees from Zambia's mobile money regulatory and supervisory authority, the Bank of Zambia. The operators included the major Mobile Network Operators (MNOs), Airtel (Airtel Money), MTN (MTN Mobile Money) and Zamtel (Zamtel Kwacha).

Participation was further extended to non-MNO providers who have been running money transfer services on mobile and have since extended their product offerings to include the mobile wallet feature on their services, which allows customers to hold value and transact off those accounts. These included Zoona (who run the Zoona Plus wallet), Broadpay (who run the Broadpay wallet) and cGrate (who run the Konse Konse wallet).

C. Survey Sampling Rationale

Due to the specialized nature of the data that the research required, survey respondents had to be conveniently sampled. The Bank of Zambia, for example, is the regulatory authority that supervises and regulatory financial services providers in Zambia. They do this through among others registration and designation of payment systems and institution as well as oversight of both systemic and non-systemic payment systems.

The central bank is also responsible for the clearing and settlement infrastructure and processes in the country. It was felt strongly therefore, that they would be well positioned to provide information on payment system interoperability from regulatory and standards perspectives. Participation therefore, was also drawn from a number of Bank of Zambia staff with varying specializations. These included Payments Systems specialists, Financial Institutions Supervision specialists, Information Systems specialists and Information Systems Security specialists.

D. Blockchain Decision Model

For the second part of the study, we looked at whether and how a blockchain based solution would be ideal for this use case. This was necessary because unlike in Bitcoin's permission-less blockchain, where any writer and reader can join at any time, permissioned blockchains have restricted read and write access thus share close similarities with a centralized database systems. This thus naturally brings up the question whether a blockchain is better suited than a centralized database.

A flow chart based decision model was therefore, adopted and used to determine the suitability of the technology to be adopted as proposed by Wüst and Gervais [26]. The model used here is shown in Fig. 1. Other such similar models have been proposed [27], [28]. This model was found more suitable as it provides a detailed description of the decisions leaving less room for misinterpretation. The model consists of a decision tree based on the following scenario properties:

1) Storing state: Refers to the need of storing data that may change both in volume and in content over time.

2) Existence of multiples writers: These are the writers that have a common interest in agreeing on the validity of the stored state.

3) Need for trusted third party: A Trusted Third Party (TTP) is a centralized entity that could manage changes and updates the state. A TTP, if present, may also control who can read the state stored.

4) Are all writers known: This refers to knowing the identity of all writers.

5) Are all writers trusted: When writers are trusted, they are expected not to behave maliciously. When writers are not trusted, they may behave maliciously.

6) Public verifiability of sate: This property determines who may read the state stored on the blockchain, and verify the integrity of the ledger.

Based on these six properties, the model determines one of four possible solutions as the best solution for the scenario:

- Permissionless blockchain: Anyone may join the network and read from the state stored, and write to the blockchain.
- Public permissioned blockchain: A limited set of participants may write to the blockchain. Anyone may join the network and read the state.
- Private permissioned blockchain: A limited set of participants may join the network, and write a new state. Only this set can read the state.
- Don't use blockchain: This end state is reached when one of the properties (1), (2), (3), or (5) above is not met.

E. Proposed Solution Design

A formal software development methodology was followed in the design and implementation of the solution prototype proposed. Object Oriented Analysis and Design methodology using the Object Modeling Techniques (OMT) phases to model the different aspects of the prototype was used. The proposed framework consists of a common replicated ledger in which transferred amounts are managed as assets on a permissioned blockchain based on Hyperledger Fabric [29] as summarized in Fig. 2.

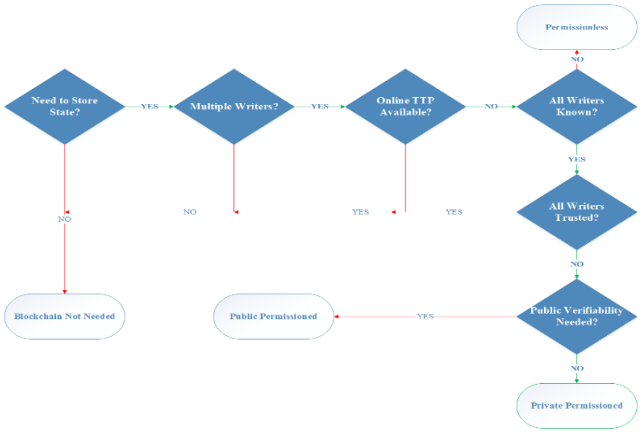

Fig. 1. Decision Model Adopted on Blockchain use Case (Source: wüst and Gervais [26]).

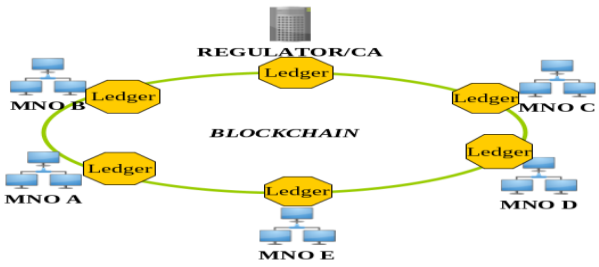

Fig. 2. Proposed Highlevel Network Architecture.

Hyperledger Fabric is an open source permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts [30]. It is designed for business use cases where the blockchain is operated by a set of known, identified, and often vetted participants. This capability is known as a permissioned blockchain. A permissioned blockchain provides a way to secure the interactions among a group of entities that know each other, have common business interests, and want to manage a decentralized network (rather than turning management of their ledgers over to a single party) [31].

By relying on the identities of the peers, a permissioned blockchain can use traditional crash fault tolerant (CFT) or Byzantine fault tolerant (BFT) consensus protocols that are used by many other distributed programs [32]. Hyperledger Fabric offers high levels of performance, protection, and transaction privacy.

Fabric was chosen because of its highly modular and configurable architecture that makes it adaptable to a number of use cases. Fabric also supports the use of general purpose programming languages such as Java in the development of smart contracts and therefore, was an ideal choice for this prototype.

Blockchain approach was used to provide key security requirements of confidentiality, origin authentication, non-repudiation and availability.

1) Blockchain network architecture: The network layout is depicted in Fig. 2 as a shared, replicated, permissioned distributed ledger where all participants have a copy of the ledger alongside their data. The blockchain architecture gives participants the ability to share a ledger that is updated every time a transaction occurs through peer-to-peer replication.

The Fabric network consists of the following basic components [33]:

1) Ledger: A ledger which consists of the world state and the blockchain. The world state contains the status of all assets that are tracked on the ledger (who owns a particular asset, for example), while the blockchain contains a history of all state changes. Ledgers are replicated across a channel and stored on peers.

2) Peers: These are the transaction endpoints for organizations and make up much of the physical structure of a network. They are maintained by members (organizations) whose identities are known by the blockchain network. Peers can maintain multiple ledgers (they have one for every channel they are a member of) and endorse transactions.

3) A channel: This contains a subset of network members who want to communicate and transact privately. Ledgers are channel specific (that is, every channel has a separate ledger). Only the peers on a channel can see the assets and transactions for its ledger. As a result, channels ensure privacy for participants within the network.

4) Chaincode: Hyperledger Fabric smart contracts are implemented in chaincode. When an application needs to interact with the ledger, it invokes these contracts by sending

transactions into the Fabric network. This is the case because chaincode predominately interacts only with the database component of the ledger and not the historical transaction log.

5) Orderer: The Ordering Service, usually composed of multiple orderers, provides consensus and ordering of transaction. It does so by bundling transactions into blocks, which are then added to the blockchain.

6) The Certificate Authority (CA): This identifies all entities in the network: Peers, the ordering service, and the participants who are submitting transactions and accessing the ledger. These identities are provided and secured by using a public key infrastructure (PKI). Peers use the CA to cryptographically sign transactions and contracts, whereas participants use the CA to prove that they have a right to access the network.

7) SDK: The Hyperledger Fabric Client SDKs enable interaction between your client application and your blockchain network. With support for multiple languages, the SDK contains APIs that allow an app to connect to and to access the smart contracts and the ledger for the channel the peer is on.

Fig. 3 shows the main nodes and components that make the proposed solution. Each participants (labelled as MNO in Fig. 2) maintains their own mobile money systems. As part of the Fabric network, each participant also runs peers which allows them to connect to the rest of the blockchain network. These peers receive transaction requests from participant systems though an Application Programming Interface (API) provided by the Software Development Kit (SDK).

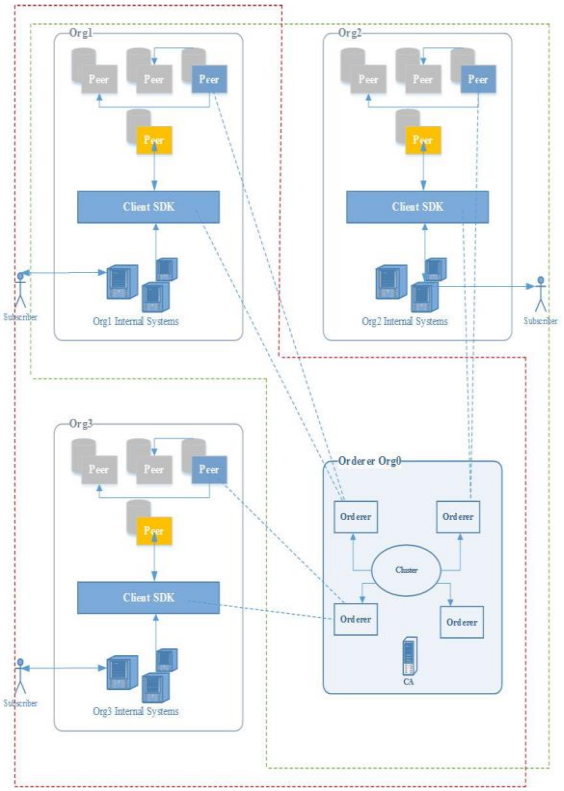

Fig. 3. Blockchain Solution Architecture.

Each pair of participants (Org1 and Org2 B for example) connect through a separate channel interface that allows them to maintain data privacy between the two. The Orderer node is responsible for ordering and writing transaction requests to the ledger before replication.

2) Use Case Model: The main asset that is transacted on the proposed network is a transfer and this represents a request made by one subscriber through a participant to transfer an amount to another subscriber on a different participant's network. Fig. 4 shows the main use cases in the system while Fig. 6 shows the states through which the transfer transitions.

Two main classes of actors are identified in the ecosystem and these are the direct participants and non-direct participants. The direct participants are the mobile money providers that directly take part on the blockchain and the clearing house which is a special institution (the "settler") responsible for netting and settlement. The non-direct actor is the subscriber who participates through the Operator and represents the mobile money subscribers.

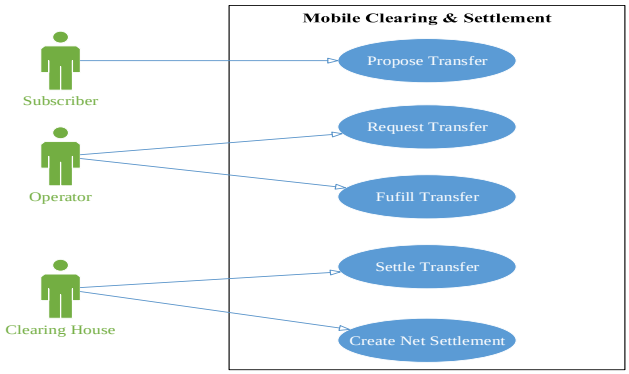

Fig. 4. Solution use Case Diagram.

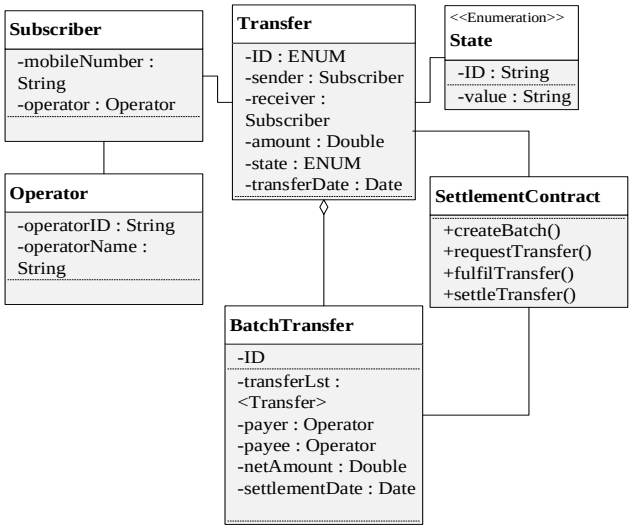

Fig. 5. Solution Class Diagram.

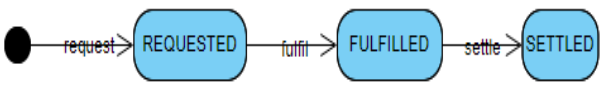

Fig. 6. State Transition Diagram for the Transfer Asset.

A special program called a smart contract was implemented that models this transaction logic that transitions the transfer between their different states. Smart contracts allowed us to define the key business processes and data that are shared across the different organizations collaborating in the network. Fig. 5 shows the class model that captures the smart contract and depicts the main objects that make up the smart contract.

V. Results and Analysis

In this section we present the results of the study. Key findings of the baseline are presented and their subsequent application to the study. Highlights of the prototype system designed are also given in terms of code artefacts as well as screenshots of the experimental Fabric network that was setup.

A. Baseline Study Results

Participation was drawn from providers with varied subscriber bases (Fig. 7) and each using different platforms and reported facing integration challenges (Fig. 8) Overall, on inter operator integration, the general feeling was that it was manageable and could be eased with the use of a central integrator rather than having every operator to integrate individually with every other provider.

B. Decision Model Analysis

A Decision model was adopted and used to assess blockchain suitability to this use case [26]. Key findings from the baseline study were used in the flow chart decision tree as prescribed in this model and it was established that for this particular use case, we could make use of a permissioned blockchain as a technology. Table I summarizes these findings.

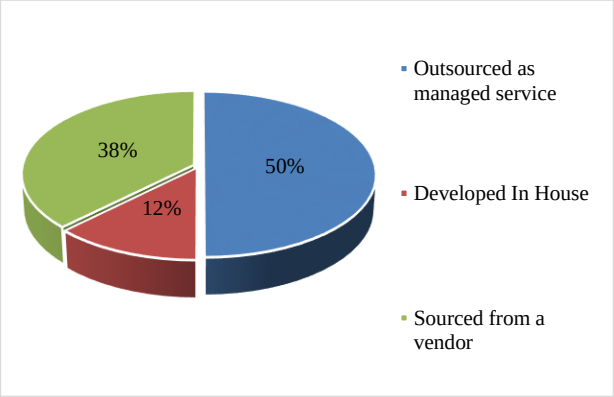

Fig. 7. Mobile Money Operator's Platform Sources.

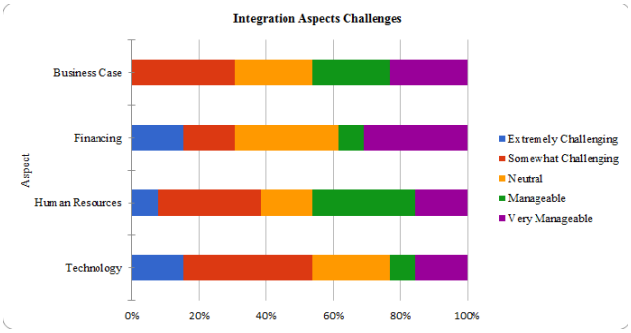

Fig. 8. State Transition Diagram for the Transfer Asset.

TABLE. I. Key Survey Findings

Decision Model Analysis		
Decision State	***Finding Description***	***Result***
Storing state	Existence of different independent mobile money operators	YES
Existence of writers	Existence of technological platforms or systems on which these operators run their services	YES
Trusted Online Third Party	Controlled access to the network with permissioning.	NO
Are all writers known	The need for integration among these systems to provide interoperability	YES
Are all writers trusted	Security and privacy of transactions	NO
Public verifiability of state	Security and privacy of transactions	NO

[a] Decision tree based on [26]

A number of important aspects such as the need to store state, existence of multiple writers were used to arrive at the decision of the solution. Other aspects like the need for central management and the relatively low number of writers were also considered to arrive at the decision.

C. Chaincode Implementation

This section highlights the main implementation aspects of the prototype system as proposed. Presented are the code snippets of the major parts of the chaincode that drives the smart contract on the fabric network.

1) The contract class: The main smart contract classes is the SettlementContract class and this contains the transaction definitions for the system. These are the request, fulfil, settle and batch transactions that have been defined and which move the assets through the application life cycle (Fig. 6).

The SettlementContract class implements the ContractInterface and so the Settlement contract uses built-in features of these classes, such as automatic method invocation, a per-transaction context, transaction handlers, and class-shared state. Fig. 9 shows code snippet of this implementation detail.

This class contains implementation of a number of methods that control application lifecycle. Firstly, the requestTransfer (Fig. 10) method creates a new transfer context object between two participants (sender and receiver) which is saved on the ledger as an asset.

The fulfilTransfer (Fig. 11) method is another transaction method and it transitions a transfer object in REQUESTED state and sets it to the FULFILLED state (after the receiver has fulfilled the transaction as confirmation that funds have been moved that participant's account).

The settleTransfer (Fig. 12) method is also another transaction method and it transitions a transfer object in FULFILLED state and sets it to the SETTLED state. This method is called by the createBatch method during the net settlement process at the end of business day.

Finally, the createBatch method is a settlement process method that is called to collate all transfers between any pair of participants and create a BatchTransfer asset which is stored on the ledger.

This class and methods make up the transaction logic part of the system and represent the control flow logic of processing. Next we highlight the object implementation which represents the main assets.

```
@Contract(name = "org.momo-switch.transfer", info = @Info(title = "Momo Contract", description = "",
@Default
public class SettlementContract implements ContractInterface {
```

Fig. 9. Settlement Contract Class Definition.

```
    @Transaction
    public Transfer fulfilTransfer(TransferContext ctx, String receiver, String transferNumber) {

        // Retrieve the current transfer using key fields provided
        String transferKey = State.makeKey(new String[] { transferNumber });
        Transfer transferToBeFulfilled = ctx.transferList.getTransfer(transferKey);

        // Check transfer is indeed in REQUESTED state
        if (transferToBeFulfilled.isRequested()) {
            transferToBeFulfilled.setFulfilled();
        } else {
            throw new RuntimeException(
                    "Transfer " + transferNumber + " already fulfilled or is not requested");
        }

        // Update the transfer state on the ledger
        ctx.transferList.updateTransfer(transferToBeFulfilled);
        return transferToBeFulfilled;
    }
```

Fig. 10. Request Transfer Method.

```
    @Transaction
    public Transfer requestTransfer(TransferContext ctx, String sender, String receiver, String transferID, String transferDateTime,
            String settlementDateTime, int amount) {

        // create an instance of the transfer
        Transfer transfer = Transfer.createInstance(sender, receiver, transferID, transferDateTime, settlementDateTime,
                amount,"");

        // Smart contract, rather than transfer, moves transfer into REQUESTED state
        transfer.setRequested();

        // Add the transfer to the list of all transfers in the ledger
        ctx.transferList.addTransfer(transfer);

        // Return created transfer to caller of smart contract
        return transfer;
    }
```

Fig. 11. Fulfil Transfer Method.

```
    @Transaction
    public Transfer settleTransfer(TransferContext ctx, String issuer, String transferNumber) {

        String transferKey = Transfer.makeKey(new String[] { transferNumber });

        Transfer transferToBeSettled = ctx.transferList.getTransfer(transferKey);

        // Check transfer is not already SETTLED
        if (transferToBeSettled.isFulfilled()) {
            transferToBeSettled.setSettled();
        } else {
            throw new RuntimeException(
                    "Transfer " + transferNumber + " is not ready for settlement");
        }

        // Update the transfer
        ctx.transferList.updateTransfer(transferToBeSettled);
        return transferToBeSettled;
    }
```

Fig. 12. Settle Transfer Method.

2) The main object classes: The main object classes that represent assets on the ledger are the Transfer and the BatchTransfer classes. These classes have member valuables that represent the properties of the assets and have respective createInstance methods which are used to initialize their respective objects so as ensure instantiation of these objects is through a transaction rather than through the classes.

These classes also extend the State class which is used to control lifecycle states of the assets and represents the ledger level Fabric state database. Fig. 13 shows the main parts of these classes.

The other object classes include the Operator and the Subscriber and these used to represent logical member variables for the respective objects for easier management. Code snippets showing implementation are presented in the appendix for those.

```
@DataType()
public class Transfer {

    //Transfer State values
    public static final String REQUESTED = "REQUESTED";
    public static final String FULFILLED = "FULFILLED";
    public static final String SETTLED = "SETTLED";
    public static final String REJECTED = "REJECTED";

    @Property()
    private Subscriber sender;
    @Property()
    private Subscriber receiver;
    @Property()
    private Double amount;
    @Property()
    private String transferDate;
    @Property()
    private String transferID;
    @Property()
    private String state = "";
```

```
@DataType()
public class BatchTransfer {
    private String ID;
    private ArrayList<Transfer> transferList;
    private Operator payer;
    private Operator payee;
    private Double netAmount;
    private String settlementDate;

}
```

Fig. 13. Asset Class Definitions.

VI. CONCLUSION

The study proposed the use of blockchain technology to solve the problem of mobile money interoperability in Zambia. A structured approach was used to confirm the gap and then decide a technological solution through the use of a structured decision model for careful determination. We further designed a prototype system on the Hyperledger Fabric network which could develop in an Object Oriented language such as Java for deployment.

We can thus conclude that mobile money interoperability settlement is a valid use case for a permissioned blockchain technology and would be an ideal solution approach rather than the traditional central processing database systems.

VII. LIMITATIONS AND FUTURE WORKS

This study focused on a gap verification of the interoperability problem as well as a technical implementation of a prototype solution. The prototype also only considered the funds transfer between participating entities and their subsequent settlement and did not look at other technical aspects such as the regulatory aspects and the financial and business sides of the ecosystem. The prototype was only experimental and could only be deployed on a development network and not in a live network with integration with mobile network operators for a more real world demonstration.

ACKNOWLEDGMENT

Acknowledgment of special thank you goes to the University of Zambia (UNZA) Department Of Computer Science and Department of Electronics and Electrical Engineering for the support and guidance during the study.

REFERENCES

[1] D. Clark and G. Camner, "A2A Interoperability: Making mobile money schemes interoperate," no. February, 2014.

[2] M. Tompkins, A. Olivares, and M. Tompkins, "Clearing and Settlement Systems from Around the World : A Qualitative Analysis Clearing and Settlement Systems from Around the World : A Qualitative Analysis by," 2016.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, no. June, pp. 557–564, 2017.

[4] Bank of Zambia, "Payment Systems Vision and Strategy 2018-2022," Bank of Zambia, Lusaka.

[5] T. TEMBO, "National financial switch to start this year," Daily Mail, 2017. [Online]. Available: http://www.daily-mail.co.zm/national-financial-switch-to-start-this-year/. [Accessed: 21-Jan-2018].

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," pp. 1–9, 2013.

[7] D. C. Mills et al., "Distributed Ledger Technology in Payments, Clearing, and Settlement," 2016.

[8] M. Bourreau and T. Valletti, "Competition and Interoperability in Mobile Money Platform Markets: What Works and What Doesn't? (*)," Commun. Strateg., 2015.

[9] R. B. of I. Department of Payment and Settlement Systems, "Prepaid Payment Instruments (PPIs) – Operational Guidelines for Interoperability," no. 808. Mumbai, India, pp. 2–4, 2018.

[10] D. Kumar, T. A. Gonsalves, A. Jhunjhunwala, and G. Raina, "Mobile payment architectures for India," Proc. 16th Natl. Conf. Commun. NCC 2010, no. 1, pp. 4–8, 2010.

[11] K. Kumar and M. Tarazi, "Interoperability in Branchless Banking and Mobile Money. Consultative Group to Assist the Poor (CGAP).," CGAP, 2012. [Online]. Available: http://www.cgap.org/blog/interoperability-branchless-banking-and-mobile-money-0.

[12] M. Mamabolo, "Kenya's Central Bank gives mobile money interoperability thumbs up," IT WebAfrica, 2018. [Online]. Available: http://www.itwebafrica.com/fintech/842-kenya/243988-kenyas-central-bank-gives-mobile-money-interoperability-thumbs-up. [Accessed: 20-Dec-2018].

[13] Central Bank of Kenya, "Mobile Money Interoperability," no. January, p. 2018, 2018.

[14] M. Mamabolo, "Kenya pilots mobile money interoperability," IT WebAfrica, 2018. [Online]. Available: http://www.itwebafrica.com/mobilex/309-kenya/242443-kenya-launches-mobile-money-interoperability-pilot-today. [Accessed: 20-Dec-2018].

[15] M. Bourreau and S. Hoernig, "Interoperability of Mobile Money: International Experience and Recommendations for Mozambique," no. December, 2016.

[16] J. Argent and J. A. Hanson, "The Regulation of Mobile Money in Rwanda," J. ICT, 2013.

[17] Bank of Tanzania, "National Payment System Directorate Statistics:" [Online]. Available: http://www.bot-tz.org/PaymentSystem/statistics.asp. [Accessed: 18-Dec-2018].

[18] GSMA, "Choosing a Technical Model for A2A Interoperability: Lessons from Tanzania and Pakistan," no. December, 2015.

[19] D. C. Mills et al., "Distributed Ledger Technology in Payments, Clearing, and Settlement," Ssrn, 2016.

[20] B. Smith and K. Christidis, "IBM Blockchain: An Enterprise Deployment of a Distributed Consensus-based Transaction Log," Proc. Fourth Int. IBM Cloud Acad. Conf., pp. 1–4, 2016.

[21] D. Ivan, "Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records," 2016.

[22] R. J. Reisman, "Air Traffic Management Blockchain Infrastructure for Security , Authentication , and Privacy," pp. 1–14, 2019.

[23] F. Tian, "A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things," 14th Int. Conf. Serv. Syst. Serv. Manag., vol. 323, no. 2, pp. 511–519, 2015.

[24] H. Wu, Z. Li, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, "A distributed ledger for supply chain physical distribution visibility," Inf., vol. 8, no. 4, pp. 1–18, 2017.

[25] A. Baliga, "The Blockchain Landscape Office of the CTO," Persistent Syst. Ltd, p. 21, 2016.

[26] K. Wüst and A. Gervais, "Do you need a Blockchain?," IACR Cryptol. ePrint Arch., no. i, p. 375, 2017.

[27] M. Peck, "Do You Need a Blockchain?," IEEE Spectrum, 2018. [Online]. Available: https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain. [Accessed: 12-Dec-2018].

[28] T. Koens and E. Poll, "What Blockchain Alternative Do You Need ?".

[29] E. Androulaki et al., "Hyperledger fabric," pp. 1–15, 2018.

[30] Varun Raj, "Hyperledger Fabric Architecture: Explained in detail," 2018.

[31] J. Garzik, "Public versus Private Blockchains. Part 1: Permissioned Blockchains," 2015.

[32] M. Sethumadhavan, "On Blockchain Applications: Hyperledger Fabric And Ethereum," Int. J. Pure Appl. Math., vol. 118, no. 18, pp. 2965–2970, 2018.

[33] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," Work. Distrib. Cryptocurrencies Consens. Ledgers (DCCL 2016), 2016.