

A Bitcoin Framework: An Alternative Payment System for Rural Areas of South Africa using Low-end Mobile Phones

¹Nelisiwe Peaceness Dlamini, ²Mfundo Shakes Scott, ³Kishor Krishnan Nair

¹Computer Science Department, University of Fort Hare P/Bag X1314, Alice 5700, South Africa

²CSIR Modelling and Digital Science, P.O. Box 395, Building 17B, Pretoria, 0001, South Africa

¹201514843@ufh.ac.za ²SScott@ufh.ac.za ³KNair@csir.co.za

Abstract—Bitcoin is a peer-to-peer, decentralized payment system; that can be used as electronic money and as a payment method. Research done on Bitcoin has escalated due to the properties it possesses which are similar to fiat currency. Some of the properties highlighted are that Bitcoin does not require personal information, the transfers made between the Bitcoin users are direct and the intervention of centralized authority when transferring bitcoins is absolved. A number of solutions have been presented to use Bitcoin, to address problems in developing communities, such as rural areas. Such problems include limited access to financial services and technology-deprivation, which is due to the imbalances in the standards of living and costs incurred when a person owns a bank account. In this study, numerous software and hardware components are combined to design a Bitcoin framework. This Bitcoin framework is tested on a low-end mobile phone but also functions on any mobile phone. A Mobile Bitcoin Wallet System is then developed to demonstrate the feasibility of the Bitcoin framework, thereafter use cases are provided to assess the Bitcoin wallet. The observed outcome from this system includes the ability to send bitcoins to another user using a low-end mobile phone and indicates that Bitcoin can be used to supplement the existing payment system. It also provides access to financial services. A few issues, such as the volatility of Bitcoin and the exchange of bitcoins to fiat currency, need to be addressed in future work to enhance such a system.

Keywords—Bitcoin, Blockchain, Bitcoin Wallet, Electronic Money, Financial Inclusion, Low-end Mobile Phones

I. INTRODUCTION

Over the years various electronic payment methods using fiat currency, a currency issued and approved by the government, have been attempted especially in developing countries in their attempt to facilitate financial inclusion to its poorest population. However, the major drawback of such payment methods is that they are all centralized, and regulated either by the government, financial institutions, or Mobile Network Operators (MNOs). Due to this drawback, inventors were motivated to recommend alternative decentralized solutions and it led to the invention of cryptocurrencies [1]. Cryptocurrencies succeeded in eliminating the presence of central authorities primarily through the use of cryptographic techniques [2]. Cryptocurrencies attained huge popularity when Satoshi Nakamoto (a person or a group of people) invented Bitcoin and informed the world by writing a paper. Later on, the Bitcoin client software was released as an open source software. Bitcoin solved the major issues in cryptocurrencies such as double spending, the issue of privacy and trusting central authorities. This was attributed to the fact that Bitcoin was designed as a decentralized, peer-to-peer payment system [2]-[3].

In addition to this, Bitcoin can also be used as electronic money denoted by the unit “bitcoin” or BTC, but it cannot be physically represented as a currency. Bitcoin is facilitated by a technology known as the blockchain. The blockchain is a public ledger that records all transactions taking place in the Bitcoin network chronologically [4]. Furthermore, the blockchain ensures the integrity of all transaction information and ensures that digital coins are not double spent. The possibility of this has always been a conundrum for the cryptography experts. However, Satoshi overcame this problem by combining previous unique contributions from researchers, who had been working towards solving such problems for decades [3].

Satoshi Nakamoto presented a decentralized electronic payment system that has the ability to verify and clear transactions [3]. This was achieved without the need for a financial institution and user’s personal information. However, there is a need for a Bitcoin address, which can be used to transfer bitcoin value from one person to another, from a file known as a Bitcoin wallet [5]. A Bitcoin address is a hashed public key and has a corresponding private key. It is used to sign a transaction that is created by a user when they spend bitcoins. After a transaction is created, the user broadcasts it to the Bitcoin network using the application downloaded and installed on their computer or smartphone device. This application, e.g. the Bitcoin client software, mobile Bitcoin wallet, or online Bitcoin wallet, allows the user to access a Bitcoin wallet, create transactions and be part of the Bitcoin Network [4].

The next step is to wait for a confirmation, to be informed of the transaction’s progress, which is executed by the miners. A miner is also part of the Bitcoin network and their task is to collect the propagated transactions into blocks and mine the block. Mining a block requires the miner to solve a mathematical problem known as proof of work, which utilizes cryptography and requires computing power [3]. After finding the solution the miner broadcasts the solution to other nodes (members of the Bitcoin network). If the other nodes that are connected to the Bitcoin network, agree on the solution, the miner can then add such a block to the blockchain, and collect a reward for solving the problem. The Bitcoin transaction is then confirmed and the bitcoins are delivered to the owner’s Bitcoin wallet [2]-[4].

Since the inception of Bitcoin, there has been tremendous developments using the Bitcoin protocol and many businesses have deployed their in-house systems in which they integrated the blockchain and are coming up with various use cases that employ this technology [6].

In this paper a Bitcoin framework is designed and to verify that it performs as expected, a Bitcoin SMS wallet prototype is developed. The user interacts with the system developed to acquire a Bitcoin wallet.

The rest of this paper is organized as follows; Section II discusses the Related Work, Section III conceptualizes the Bitcoin Framework. Section IV conducts the testing of the Bitcoin Framework. This section also aims to prove the concept of the Bitcoin SMS wallet. Section V, concludes the paper and Section VI discusses the future work.

II. RELATED WORK

The research area of cryptocurrencies continues to emerge worldwide. However, majority of the existing research work that has been done is more inclined towards discussing the security of Bitcoin, the issues around trust and regulation, the advancement of cryptographic methods, and the Bitcoin protocol itself [7]. Few researchers have focused on how the technology-deprived people in developing areas can use or access Bitcoin. Thus, there is a gap that has not been addressed appropriately. In South Africa, people have started examining Bitcoin and the number of people encouraging the use of Bitcoin is growing [8]. Numerous Bitcoin start-ups have developed systems and applications. These applications include:

- BitX, a Bitcoin exchange company in South Africa, offers a mobile Bitcoin wallet application, used to manage and store Bitcoin value [9].
- A crowdfunding platform for African schools which uses the blockchain technology to provide electricity credit by exchanging the donated cryptocurrency to electricity credit [10].
- Ice3x, a Bitcoin exchange company in South Africa allows people to buy, sell and send Bitcoin and Litecoin [11].

The systems and applications put in place for a Bitcoin transaction require a person to have access to the latest technology, e.g. Internet connection, smartphone, and computer and to sign up to use an exchange company bank account details are required.

The blockchain technology which facilitates Bitcoin is now used to create solutions that address various problems and enhance existing solutions. The proposed solutions include solving problems, such as protecting personal data and putting an end to intentional deception [12]. These solutions are as follows:

- The use of smart contract systems has elicited more secure methods and frameworks for using smart contracts. Hawk is one of the models proposed, not only to use smart contracts but to also preserve the users' privacy. It is a smart contract system that is decentralized and conceals the financial transactions between various stakeholders [13].
- A gaming device was also invented, which utilizes Bitcoin as a currency in the form of a reward [14].

The list of the proposed solutions is endless, and while the blockchain continues to be employed to solve problems, Bitcoin is still utilized for other purposes, such as making payments to merchants who accept it. Furthermore, Bitcoin

has been proposed in solving a lot of challenges, such as the chargeback challenge faced by merchants when cardholders successfully reverse payments they made to the merchants [4]. The major challenges are as follows:

- In some economies, the standard of living is very low and people do not have adequate access to basic financial services. This is due to the fact that the financial services are unaffordable and unavailable in remote areas [4].
- In some countries, such as Zimbabwe and Libya, due to the currency devaluation, currencies of other countries are used as alternatives. Bitcoin can then be standardized and used as a unique and an alternative currency in such instances [4].

This paper, therefore, presents a Bitcoin framework that can be used by people in the rural areas of South Africa. Such people are mostly technology-deprived but possess low-end mobile phones. This Bitcoin framework will provide an alternative and easily accessible solution to the problem of not having access to basic financial services and will augment the methods that are used for remittances or money transfer, such as Western Union and Money Gram [4]. The usage of Bitcoin is proposed to be employed to various use cases, for instance, remittances, for micropayments and as donations to the disadvantaged countries. It can be used as an alternative payment method and as a payment system in such areas, which totally absolves centralized authorities, such as, the financial institution [4].

A system that allows people in an undeveloped area, such as, a rural or marginalized area with limited technology to acquire bitcoins would be highly beneficial. Furthermore, it augments the current financial methods used to cater for the people who do not have access to methods of being financed. Such a system would certainly add a lot of value due to the following key reasons:

- A Bitcoin wallet is affordable and does not require a monthly fee.
- The transaction fees are very low if not insignificant. For example, to exchange bitcoins to ZAR on ICE3x Exchange Company, a person is charged a fee of 0.00014356 BTC which is R1.19 based on currency rate on Thursday 11/08/16, 14:38pm.
- The user can keep their Bitcoin wallet forever.
- The user can use the Bitcoin wallet as a method of saving.
- The user can receive bitcoins from a person residing in another country.
- The user does not have to possess a bank account to exchange bitcoin value to the desired money denomination.

In South Africa, Bitcoin is not regulated and the South African Reserve Bank (SARB) alienates itself from the virtual currencies sector and its use. However, SARB has highlighted that developments around this sector will continue to be monitored and a possible change in its position exists [15]. Hence this study focusses on Bitcoin to highlight its relevance as an alternative payment method and intends to achieve value.

III. THE BITCOIN FRAMEWORK

The Figure below illustrates the Architectural Design of the Bitcoin framework for the rural and marginalized areas in developing countries such as South Africa.

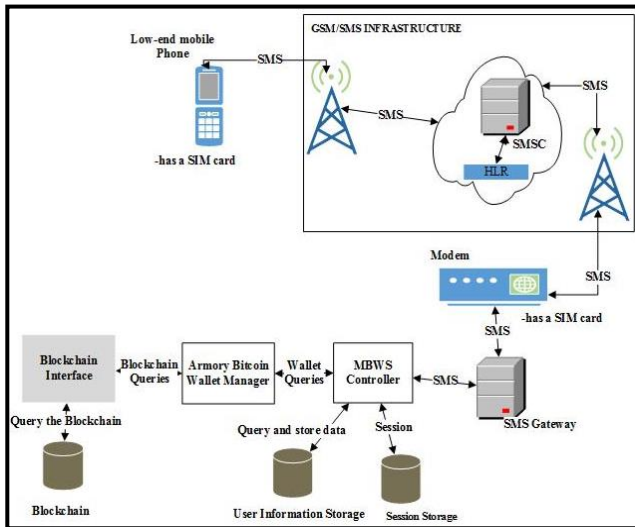


Figure 1: The Architectural Design

Each of the components used to design and construct the Bitcoin Framework are discussed as follows:

- **Low-end mobile phone:** The low-end mobile phone is used by the user, to send SMSs to the GSM modem connected to the computer. Such SMSs are in the form of commands, e.g. *Help*, *Getwallet*, *Bal*, *Addr* and *Send*. The user sends an SMS command and receives a response. The commands used are:
 1. **Help:** To request details on which commands are available to be used and their description.
 2. **Getwallet:** It is used when the user wants to acquire a Bitcoin wallet from the system. The user can then use this wallet to generate a Bitcoin address and receive and send bitcoins.
 3. **Addr:** It is used when the user would like to generate a Bitcoin address from the Bitcoin wallet. This address can be given to another Bitcoin user who wants to send bitcoins. The user gets a new Bitcoin address that is unused every time this command gets issued.
 4. **Bal:** It is used to request the balance, which is the amount of bitcoins available in the Bitcoin wallet.
 5. **Send:** It is used to initiate a transaction. A session is opened for the user on which the system requests the user's Personal Identification Number (PIN), the amount of bitcoins being sent and the destination mobile phone number, which is the recipient's mobile phone number. The user can only send bitcoins to a recipient who has a record in the system. However, the user can receive Bitcoins from a Bitcoin user who does not have a record on

the system as long as they have knowledge of the user's Bitcoin address.

The SMS's sent from the user's mobile phone are charged at the MNO's standard SMS rates. The user can also use the SMS bundles purchased from the MNO.

- **GSM modem:** The GSM modem used in this design uses a CELL C MNO SIM card. This modem is connected to the computer and can communicate with other devices subscribed to the MNO. The SMS responses from the modem are charged at the MNO standard SMS rates.
- **SMS Gateway:** The SMS Gateway is customized to parse the SMSs retrieved from the GSM modem, then converts the string to lowercase and strips the spaces from the beginning and at the end of the string. The message is then processed by the MBWSC, which executes the required function for the command. For the SMS Gateway to respond packages are required, and they are the *Python GSMmodem package*, which controls the modem and the *Pyserial package*, which encapsulates access to the serial port. The serial port is used by the GSM modem to connect to the computer. Fig. 2 demonstrates the interaction between the GSM modem, the SMS Gateway and the MBWSC. When the SMS from the user is delivered to the GSM modem, the SMS is parsed and processed. Processing the SMS includes validating the text input from the user. This ensures that the input is not malformed data and thus prevents text input that does not conform to the expected SMS commands.
- **ABWM:** ABWM is a Bitcoin wallet Manager and it helps the developer to acquire access to the blockchain. This open source application is used to create encrypted Bitcoin wallets which are stored in the computer's data storage, used by the developer.
- **MBWSC:** The MBWSC is the program that controls the steps that are further executed upon receiving the SMS command. It executes the command, e.g. if the SMS sent is *Addr*, the following steps are executed:
 1. Check if the user's record exists in the system. This would mean the user has a Bitcoin wallet allocated to him/her.
 2. If the user's record does not exist in the system, send the user an SMS letting him/her know that he/she does not have a Bitcoin wallet.
 3. If the user's record does exist, then get the next unused Bitcoin address from the user's wallet.
 4. Send the Bitcoin address to the user.
- **Blockchain interface:** The blockchain interface allows the user to interface with the blockchain and the Bitcoin Network. To do this, the Bitcoin Client software, version 0.12.0, was deployed in the testing system.

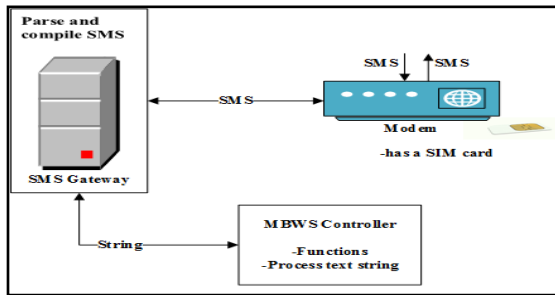


Figure 2: Interaction between Components

- **Database Tables:** Since MBWSC program consists of most of the functionalities, it has to query and store information pertaining to the user in the database tables. The database used is Microsoft SQLite due to its performance, accessibility, and portability [16]. The database contains two tables and are elaborated as follows:

1. **USERS_INFO:** This database table contains the users' records. The table attributes are displayed as in Fig. 3. The attributes in the table are: a **unique_id** that identifies each user; **reg_date**, this is the date when the user acquired the Bitcoin wallet; **cell_num** is the users mobile phone number (a Bitcoin wallet can only be allocated to one mobile phone number); **wallet_filename** is the name of the wallet file; **PIN** is the passphrase used to unlock the Bitcoin wallet; **balance** is the user's bitcoin balance available in the Bitcoin wallet, and **trans_count** is the number of transactions made by the user. This number is incremented every time a user completes a successful transaction.

USERS_INFO	
PK	UNIQUE_ID
	REG_DATE
	CELL_NUM
	WALLET_FILENAME
	PIN
	BALANCE
	TRANS_COUNT

Figure 3: USERS_INFO table

2. **SESSION:** This database table contains the users' session data, which is recorded when the user forwards the *Send SMS* command to send bitcoins. The table attributes are displayed as in Fig. 4. The attributes in the table are: an **id** that identifies the user and is always 1; **trans_date** is the date when the user initiated the transaction; **cell_num** is the user's mobile phone number (who is initiating a transaction). The **last_msg** and the **next_msg** contains the actions executed by the user, e.g. when the user sends the SMS command *Send*, the string 'send' is saved in the row cell where the column name is last_msg. The row cell where the column name is next_msg has the string 'pin' (in small letters), which is the next expected input from the user.

The PIN is verified and if it is correct, the system sends an SMS to the user requesting the amount they want to send. The last msg is updated to 'pin' and the next_msg is updated to 'amount'. When the system receives the SMS containing the amount that the user wants to send to another user (recipient). The system checks if the user sending bitcoins has sufficient bitcoin value remaining in their Bitcoin wallet, to proceed with the transaction. If he/she has enough funds, the system requests the destination mobile phone number. The last msg is updated to 'amount' and the next_msg is updated to 'destination'. When the system receives the SMS with the destination mobile phone number, the destination mobile phone number is verified. If it is correct and if the user exists in the database table USERS_INFO, the transaction is created, signed, and broadcasted by the system. The user subsequently receives an SMS letting him/her know that the bitcoins are sent. The recipient also receives an SMS letting him/her know that bitcoins were received from the sender.

SESSION	
PK	ID
	TRANS_DATE
	CELL_NUM
	LAST_MSG
	NEXT_MSG

Figure 4: SESSION table

The components are integrated into the testing system to assess and evaluate the Mobile Bitcoin Wallet System and demonstrate its feasibility. Each component serves its own purpose, e.g. the modem receives and sends SMSs, but to have a functional system, such components work together by communicating with each other.

IV. TESTING

The objective of this system is to prove the concept that is presented by testing the developed Bitcoin SMS wallet. Three use cases are considered for testing and evaluation and the screenshots depict how such user actions are executed by the system.

A. Use Case Testing

1. Use Case 1

Use Case Name: Get Bitcoin address

Actors:

- Bitcoin User
- Bitcoin Wallet
- Mobile Bitcoin Wallet System

Use Case Description: Bob who has a relative, Mary. Mary resides in London; she wants to send bitcoins to Bob. She calls Bob to ask him for a Bitcoin address. Bob needs to get a Bitcoin wallet first. The mobile phone used is a Nokia 105 with a very small screen. Hence, when Bob receives SMSs, he scrolls down to view the rest of the text.

1.1. Bob sends an SMS, *Help* to find out which commands are available.

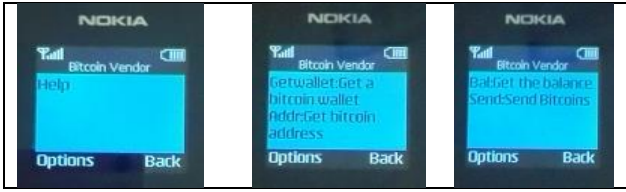


Figure 5: Help Command

1.2. After receiving the message, an SMS is displayed as in Fig. 5 that shows commands available and their description. Now, Bob sends another SMS, *Getwallet*, to acquire a wallet.



Figure 6: Getwallet Command

1.3. Bob now possesses a Bitcoin wallet and the next step is to generate a Bitcoin address. To generate a Bitcoin address, Bob sends an SMS *Addr* and receives the Bitcoin address.

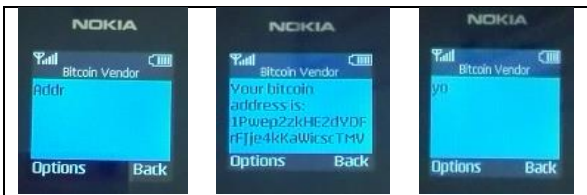


Figure 7: Addr command

When Bob receives the Bitcoin address, he can now contact Mary to give her the Bitcoin address and Mary can send bitcoins to Bob. Mary can use any method available to her to send bitcoins because she now possesses Bob's Bitcoin address. Fig. 8 is a screenshot of the SMS Gateway screen output. It waits to retrieve messages from the user.

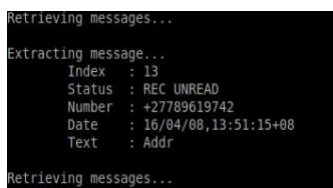


Figure 8: SMS Gateway Screen Output

2. Use Case 2

Use Case Name: Send bitcoins to another Bitcoin user.

Actors:

- Bitcoin User 1 (Jerry)
- Bitcoin Wallet
- Mobile Bitcoin Wallet System
- Bitcoin User 2 (Sarah)

Use Case Description: Jerry, who used the steps utilized by the previous user in use case 1 to acquire a wallet, wants to

send bitcoins to his friend, Sarah. They have already talked about Bitcoin and they know that they should acquire a Bitcoin wallet within the Mobile Bitcoin Wallet System to be able to send bitcoins to each other. Jerry had previously received bitcoins from his cousin, so he does not have to buy bitcoins again. Jerry already has a wallet and tells Sarah to acquire a wallet. Sarah uses the steps used in Use Case 1, thus they both have a Bitcoin wallet.

1.1. Jerry wants to check his balance and he sends an SMS *Bal* and receives an SMS from the system, stating his balance as shown below in Fig. 9.

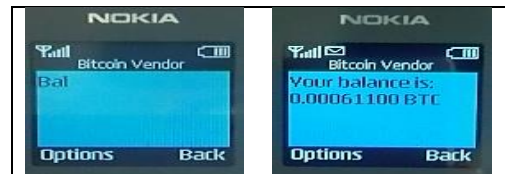


Figure 9: Bal command

1.2. Jerry receives an SMS with the balance and realizes he can still send bitcoins to Sarah. He forwards the *Send* command, the system requests his 'PIN', the amount he wants to send (0.0005BTC), and the recipient's mobile phone number. The bitcoin transactions are as illustrated below in Fig 10.

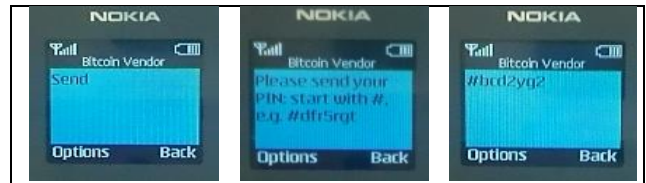


Figure 10: Send command

1.3. Jerry's transaction is successful and Sarah receives an SMS letting her know she has received bitcoins from Jerry. Jerry also receives an SMS letting him know the transaction was successful. The Bitcoin transactions are as illustrated in Fig. 11.

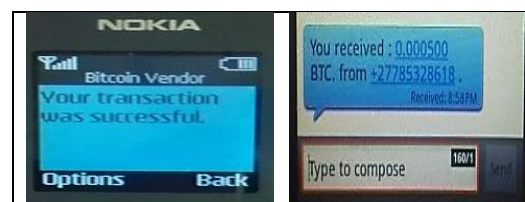


Figure 11: Transaction successful

The user's PIN is encrypted and stored in the database containing the user's details. This also makes it easy to retrieve the PIN for recovery purposes.

3. Use Case 3

Use Case Name: Send to more than one user

Actors:

- Bitcoin User (Agent)
- Bitcoin Wallet
- Mobile Bitcoin Wallet System

Use Case Description: A company that supplies funds to people wants to send bitcoins to the users who are registered for these funds, instead of going to the areas these people reside in or depositing money in their bank accounts. The following screenshots illustrate the steps that the company agent follows after getting a Bitcoin wallet from the Mobile Bitcoin Wallet System.

- 1.1. An agent representing the company has access to a Bitcoin wallet, the system allows the agent to send to more than one user using his/her mobile phone. The agent does this by including the following in the message body, starting with the word *Grant* to show that it is a different transaction, and then included the mobile phone numbers and the amount that should be sent to each Bitcoin user.



Figure 12: SMS from and to agent

- 1.2. The system receives this SMS, processes it by sending the amount of bitcoins to the Bitcoin users as stipulated by the agent in his/her SMS. The Bitcoin user receives an SMS letting him/her know that he/she has received bitcoins and the agent receives an SMS letting him/her know the transaction was successful.

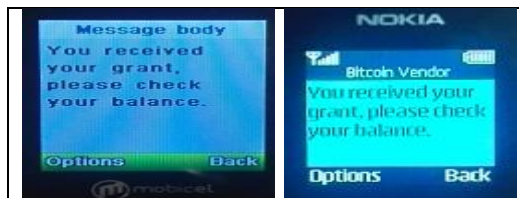


Figure 13: SMS received by the users

The user can then check their balance on their Bitcoin wallet by sending the SMS command *Bal* and can start transacting and purchasing from a vendor who accepts bitcoins. The SMS commands are not case-sensitive; a user can use lowercase, uppercase and include both uppercase and lowercase letters in the text message. Incorrect SMS commands containing typographical errors such as spelling mistakes are handled by validating the text before it is processed. The three use cases discussed in this section were used to prove that the concept of the Bitcoin framework works as expected.

V. CONCLUSION

The mobile Bitcoin wallet merely proves that even a user with a low-end mobile phone can acquire a Bitcoin wallet. For the user in a rural or marginalized area somewhere in South Africa, all they need is to have sufficient airtime in their account and the ability to send SMSs. In proving that this concept works, the developer or person hosting the

Mobile Bitcoin Wallet System in their computer had to be connected to the Internet to access the Bitcoin Network. To deliver the service of acquiring Bitcoin wallets, there needs to be a customized SMS Gateway, which relays messages between the system and the user. The system would be feasible for use in areas deemed as less important because the mobile Bitcoin wallet can be accessed easily. Similar to previous payment methods that have been introduced in the past such as, mobile banking, educating people would also be necessary.

VI. FUTURE WORK

It is anticipated that the mobile Bitcoin wallet can be made better by decreasing SMS response time and offering more options to the user, such as viewing transaction history. Moreover, the user can be presented with easier methods to exchange Bitcoins and vendors offering goods and services in exchange for Bitcoin. The volatility of Bitcoin and the methods that can be used to exchange Bitcoins are not discussed in this paper but methods of managing such would be plausible in future research.

REFERENCES

- [1] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.
- [2] M. D. Sleiman, A. P. Lauf, and R. Yampolskiy, "Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System," *2015 Int. Conf. Cyberworlds*, pp. 332–336, 2015.
- [3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin A Peer-to-Peer Electron. Cash Syst.*, pp. 1–9, 2008.
- [4] B. Y. J. Brito and A. Castillo, "A Primer for Policymakers," *Bitcoin A Prim. Policymakers*, vol. 29, no. 4, pp. 3–42, 2013.
- [5] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," *Cryptol. ePrint Arch. Rep. 2015/464*, vol. PP, no. 99, pp. 1–1, 2015.
- [6] Ripple, "Executive Summary for Financial Institutions," San Francisco, 2015.
- [7] C. (Lancaster U. Sas and I. E. (Universiti T. M. Khairuddin, "Exploring Trust in Bitcoin Technology: A Framework for HCI Research," in *OzCHI '15 Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*, 2015, pp. 338–342.
- [8] A. Nieman, "A Few South African Cents' Worth on Bitcoin," *PER Potchefstroomse Elektron. Regsbl.*, vol. 18, no. 5, pp. 1–33, 2015.
- [9] N. Menezes, "BitX Raises \$4 million FromNaspers Group," *Bitcoinist.net*, 2015. [Online]. Available: bitcoinist.net/bitx-raises-4-million-naspers-group/. [Accessed: 08-Dec-2015].
- [10] T. Jackson, "SA's Bankymoon launches bitcoin crowdfunding platform for African schools," *Disrupt Africa*, 2015. [Online]. Available: <http://disrupt-africa.com/2015/09/sas-bankymoon-launches-bitcoin-crowdfunding-platform-for-african-schools/>. [Accessed: 10-Aug-2016].
- [11] M. Norton, "Ice3X: The African Bitcoin Exchange with a Heart," *Bitcoin Warrior*, 2014. [Online]. Available: bitcoinwarrior.net/2014/08/ice3x-african-bitcoin-exchange-heart/. [Accessed: 08-Dec-2015].
- [12] G. Zyskind, A. S. Pentland, and O. Athan, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *2015 IEEE Secur. Priv. Work.*, pp. 180–184, May 2015.
- [13] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *Cryptol. ePrint Arch. Rep.*, 2015.
- [14] R. E. Michaelson and K. T. LeSourd, "Gaming system, gaming device and method for utilizing bitcoins," U.S. Patent no. 8523657 B2, 2013.
- [15] South African Reserve Bank, "Position Paper on Virtual Currencies," 2014.
- [16] "Benefits of SQLite As A File Format." [Online]. Available: https://www.sqlite.org/aff_short.html. [Accessed: 06-Apr-2016].