IST-Africa 2017 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2017
ISBN: 978-1-905824-56-4

Development of an SMS System Used to Access Bitcoin Wallets

Nelisiwe Peaceness DLAMINI[1], Mfundo Shakes SCOTT[2], Kishor Krishnan NAIR[3]
CSIR, P.O. Box 395, Building 17B, Pretoria, 0001, South Africa
Department of Computer Science, University of Fort Hare,
P/Bag X1314, Alice, 5700, South Africa
Tel: +27 (0) 40 602 2745, Fax: + 27 (0) 86 248 9404,
Email: [1] 201514843@ufh.ac.za, [2] SScott@ufh.ac.za, [3] KNair@csir.co.za

Abstract: The popularity of Crypto currencies has not gone unnoticed, Bitcoin which is an electronic payment system and Internet money, is a leading crypto currency and continues to grow from being popular amongst the people who have knowledge about this technology, i.e. the developers, investors and tech-savvy enthusiasts and those that don't. If a person wants to use Bitcoin they need to have a Bitcoin wallet which stores the public and private keys used when sending and receiving bitcoins. Most of these Bitcoin wallets were developed for people who have access to technologies such as smart phones, computers and an Internet connection. This paper presents a simplified Short Message Service (SMS) system that can be used by people who do not have access to these technologies. The system was developed as a prototype and tested on a low-end mobile phone to demonstrate its capabilities. It still needs to be enhanced further to enable anyone to use it, e.g. increase the speed of transactions and SMS responses and the use of better security methods.

Keywords: Crypto currency, Bitcoin, Bitcoin wallet, low-end mobile phone

1. Introduction

The topic of finding solutions by using various technologies to allow developing communities to have access to affordable financial services; such as saving, transferring and receiving funds, has been a never-ending one. Developing communities are well known for experiencing challenges when it comes to accessing various financial services due to costs of managing a bank account, lack of important documentation, fulfilling bank balance requirements, the distance between the bank branches and the people's homes and the irregularities in received income [1]. These services include Bank branches, mobile branches, Automated Teller Machines (ATMs), Agency banking, online banking and mobile banking, which are most popularly used by people who possess bank accounts [2]. In Kenya M-Pesa, which was introduced by a Mobile Network Operator (MNO) partnered with a bank, is always referred to as a successful solution. M-Pesa is a "mobile phone-based money transfer service" [2], that allows a person to send and receive electronic money at low transaction costs and store this value on a mobile phone account. People can use the stored value as a form of payment or convert it to fiat money (cash).

Providing access to financial services results in financial institutions accumulating high costs especially if it is to the poor underdeveloped communities hence these solutions are not only offered by financial institutions but by non-bank financial institutions, such as MNOs. Apart from financial products offered by third parties who increase transaction costs due to intermediation, the advancement in technology now allows a faster and cheaper way of accessing financial services using crypto currency [3]. Crypto currency is a term

that is used to describe a system that utilises cryptography to securely exchange and transfer digital value or currency in a manner that is decentralised [4].

Crypto currencies are a form of payment technology that is decentralised and can be accessed anywhere and anytime but require devices such as computers, smart phones and an Internet technology which might be challenging to an average person residing in a marginalized area, hinder the simplification of the use of crypto currencies and the production of solutions allowing these to be used as a payment method by disadvantaged people. This restricts the participation of these users if they do not have access to these devices and technology, therefore this paper proposes an SMS system that allows the user to access a Bitcoin wallet by sending an SMS from a feature or low-end mobile phone, which is a mobile phone with limited capability, e.g. no Internet or Bluetooth connection, but allows the user to send and receive SMSs and make voice calls.

2. Overview

There is a variety of crypto currencies, also known as "electronic cash" [5], to select from, e.g. Ripple, Ethereum, Litecoin and Dogecoin, nevertheless Bitcoin remains prominent.

1.1 The Crypto currency - Bitcoin

Despite the popularity Bitcoin has gained, its adoption is still amongst the software developers, tech-savvy people and is not yet popular amongst the novice users. Bitcoin is a decentralised electronic payment system that was deployed in 2009, and is also used as electronic cash. It is an open source software which has allowed other software developers to use the software's source code to branch out and create their own alternative currencies, such as Litecoin. It was developed to abolish the reliance of financial institutions and the government with the aim to decrease the transaction costs accumulated and allow people to manage their own funds. This was achieved by using the blockchain to facilitate Bitcoin instead of relying on a third party to approve transactions [5].

1.2 Blockchain and Transactions

The blockchain is a distributed database where all the Bitcoin transactions are chronologically recorded, after the miners solve a cryptographic puzzle. Miners are the users that collect all new transactions that are created by Bitcoin users into a block and maintain the blockchain, by solving a mathematical problem. When the mathematical problem is solved the miners confirm and add the blocks containing transactions into the blockchain, thus generating new bitcoins. Solving the mathematical problem requires massive computational power and electricity which is why some miners work in groups to pool the resources they possess [6]. The process of finding the solution to the mathematical problem takes approximately 10 minutes and the block which contains all the new transactions made by Bitcoin users is added to the blockchain and confirmed. The miner who presents a valid solution first, is rewarded 12.5 Bitcoins (BTC) which is an amount that is halved after every 4 years with the intention to control the aggregate of Bitcoins that will ever exist [7].

1.3 Bitcoin Wallets

A Bitcoin address is associated to a Bitcoin wallet, to be part of the Bitcoin Network a Bitcoin user requires a Bitcoin wallet, which can be considered as a way of enrolling on the Bitcoin Network. Bitcoin allows two willing parties to directly transact with each other, but both parties require a Bitcoin address, which is how a person is identified on the Bitcoin Network. It also identifies the destination of the Bitcoins in the blockchain and is used by a Bitcoin user to send or receive Bitcoins. A Bitcoin address is a public key that is hashed using the cryptographic hash algorithms Secure Hash Algorithm (SHA-256) and RACE

Integrity Primitives Evaluation Message Digest (RIPEMD-160) and it has a corresponding private key [6]. These keys are stored and generated from the Bitcoin wallet file. The private key is used to digitally sign the created transaction before it is broadcasted and processed by the miners [8]. The information that is contained in the blockchain consists of the Bitcoin addresses and the associated bitcoin balance.

There are many types of Bitcoin wallets that can be used; these include the Bitcoin reference client which is in a form of an installable software, it is open source and is known as Bitcoin Core. This software was released after the Bitcoin paper was published [8]. The Bitcoin Core software is installed by the user on their personal computer and requires the user to have access to the Internet. Access to the Internet is required to download and update the blockchain and connects the user to other users known as peers in the network.

When this software is installed the Bitcoin user gets access to a Bitcoin wallet which is a wallet file type *.dat*, and is used to generate as many Bitcoin addresses needed to receive bitcoins. This software manages the private keys used to sign transactions and the public keys which are needed to spend bitcoins, therefore the user needs to secure the computer used to restrict unauthorised access. Armory Bitcoin Wallet Management (ABWM) application is also an open source software that when installed by the user on their computer, allows the user to create multiple Bitcoin wallets instead of limiting the user to one wallet. This application depends entirely on the Bitcoin Core software to update the blockchain and access the latest transactions in this ledger [9].

The ABWM allows online and offline storage of the Bitcoin wallet. In online storage, the Bitcoin wallet is stored locally on the user's computer which is connected to the Internet. In offline storage, the Bitcoin wallet is stored and managed in a device that is not connected to the Internet, such as external storage. In offline storage the user can create the transaction offline but to execute or broadcast the transaction the user needs to be online and connect to the Internet [7].

A user does not need to download and install the Bitcoin software they can register or enrol on websites hosting online Bitcoin wallets. The Bitcoin wallets are hosted by a third party that manages the user's private keys which removes the burden of security from the users and places it on the third parties [10]. Another option is to download a Bitcoin wallet application, if the user possesses a smart phone. Numerous applications exist such as; Blockchain Bitcoin wallet, Android Bitcoin wallet, Bitcoin Smart wallet and Coinbase Bitcoin Wallet. These wallets are developed to encourage the adoption of Bitcoin beyond the Bitcoin enthusiasts, investors and developers to improve the availability and accessibility of Bitcoin to people [7].

3. Objectives

The aim of this paper is:

1. To develop a prototype and portray use-cases of the mobile Bitcoin wallet system that allows a person using a feature or low-end mobile phone to access a Bitcoin wallet by sending an SMS.
2. To explain how this mobile Bitcoin wallet can assist people by allowing the non-restricted access to financial services.

4. Methodology

This mobile Bitcoin wallet system (MBWS) required many entities to be combined hence the prototyping method was used, this method assisted in clarifying the requirements of the MBWS and determining what the functionalities were. Prototyping can either produce a product that be thrown away after demonstration or a product that can evolve into a better system, but in both options it is still beneficial [11]. This method was used to portray the

possibility of combining different entities to implement the proposed MBWS model. In Figure 1, the prototyping model used to develop the MBWS is demonstrated. The following steps are conveyed on the prototyping model to define the deliverables; establish prototype objectives produces a prototyping plan, define prototype functionality produces an outline definition, develop prototype produces an executable prototype and evaluate prototype produces an evaluation report. These steps were applied in the following manner:

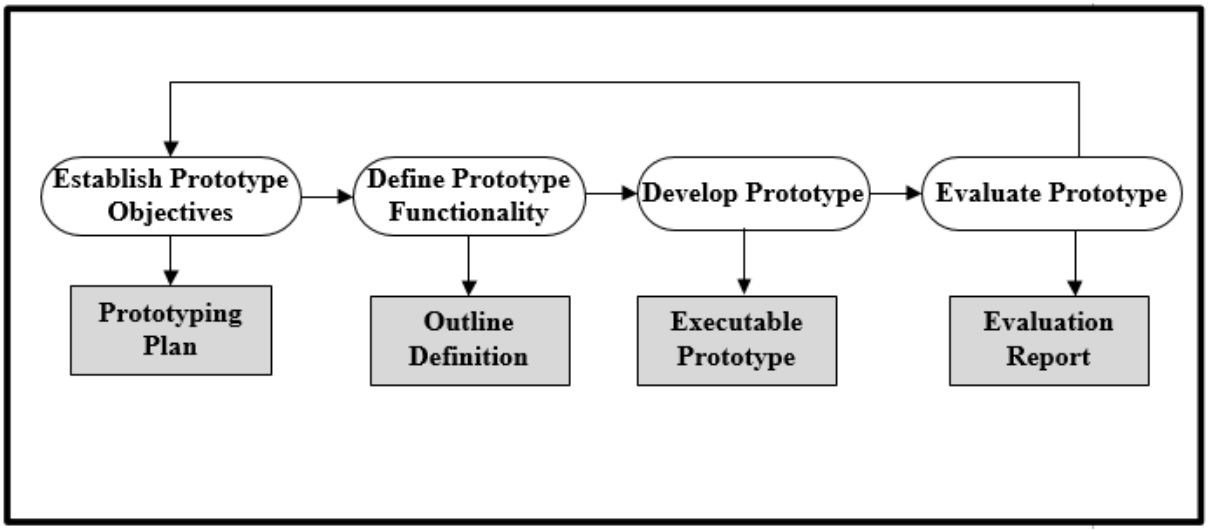

Figure 1: Prototyping Model [12]

4.1 *Establish Prototype Objectives*

To determine the objectives of the prototype to be developed, it had to be considered that the developed prototype should be accessible and simplified for the people. A Bitcoin wallet access model was the result after establishing the prototype objectives. To find the objectives, the design of the prototype was established to help define the non-functional and functional requirements of the system. This design included listing all the entities to be used which included; the Bitcoin client software, the ABWM dependencies required for installation, hardware components such as a computer, Global System for Mobile Communications (GSM) modem, Subscriber Identity Module (SIM) cards and a low-end mobile phone. The objectives of the prototype are:

- To develop a system that is interoperable with all MNOs in South Africa
- To allow the user to have access to the Bitcoin wallet information from a low-end mobile phone
- To secure the stored Bitcoin users' information
- To simplify the Bitcoin wallet for the user

4.2 *Define Prototype Functionality*

Before the actual development, the functionality of the prototype was defined, the functionality of the system is a detailed list of how the system functions, which is defined as follows:

- The developed prototype should allow the user to access the Bitcoin wallet
- The person should use their low-end mobile phone to enrol on the system
- The developed prototype should allow the user to send bitcoins
- The prototype should allow the user to receive bitcoins from other users
- The prototype should allow the user to generate more than one Bitcoin address
- The prototype should allow the user to request the balance of bitcoins remaining
- The prototype should alert the user when they receive bitcoins
- The prototype should allow the user to change the password allocated when enrolled

4.3 *Develop Prototype*

Defining the prototype functionality resulted to an outlined definition of the system which led to the development of the prototype. The functionality was implemented and tested to reduce the bugs in the source code, improve the design of the prototype and to produce a prototype that works correctly. To test if the developed prototype was the desired output, SMSs were sent from the low-end mobile phone, using the designated SMS commands such as; help, address, getwallet, changepassword, send and balance. These SMSs are sent to the GSM modem connected to the computer and are processed by the system.

4.4 *Evaluate Prototype*

Evaluation of the prototype was a step that followed after the prototype was developed to check if it met the objectives. This included checking if it produces the desired result (e.g. if a user sends an SMS command to generate a Bitcoin address, the user should receive an SMS containing a Bitcoin address from their allocated Bitcoin wallet). The prototype was also compared to a mobile banking service system to identify similarities. The developed prototype was refined and fixed by repeating all the steps listed by the prototyping model.

5. Technology Description

Different technologies were used to develop the MBWS, the list of these technologies and the description for each technology is as follows:

- Python Programming Language: Most of the software products were developed using Python, therefore to allow seamless integration between these applications and the MBWS, Python was used as a programming language. A few Python packages were installed on the computer used, these include; Anaconda 2.7 Interpreter for Python, pySerial 2.7 and Python-gsmmodem0.9 to communicate with the GSM modem
- GSM modem: The GSM modem uses a SIM card to send and receive SMSs, a SIM card must be registered with an MNO to allow the ability to communicate with other devices with SIM cards. In this system the GSM modem uses a Cell C SIM card. The downside of using a GSM modem is that the SMS's received require constant deletion depending on the SIM card memory allocation, therefore not allowing space to save SMS's received.
- Feature/low-end mobile phone: The term low-end or feature mobile phone implies that the phone has basic features, such as making voice calls, sending and receiving text messages. It does not have features such as Internet and Bluetooth connectivity. A Nokia 105 is an example of a feature mobile phone which was used as one of the technologies; an MTN SIM card was inserted in the mobile phone.
- Microsoft SQLite database: The database was used to store the Bitcoin users information this includes the users mobile phone number, the balance, transactions created, wallet file names and the date when the user enrolled on the system.
- Armory Bitcoin Wallet Management Application: This is the integrated application which assists in creating multiple encrypted Bitcoin wallet files. These wallets are deterministic Bitcoin wallets, which allows the generation of the private key from one seed and requires a once-off back up. This application also aids to connect to and get information from the blockchain which is a record of all the transactions taking place in Bitcoin. This application provided flexibility, allowing the creation of one to many Bitcoin wallets unlike the Bitcoin Core software which only allows one Bitcoin wallet to be generated and managed.

6. Developments

The development phase of this MBWS required various technologies to be setup before the actual implementation of the system.

6.1 *Setting Up the ABWM*

To set up the ABWM it was compiled from its source code which required dependencies to be installed in the computer. The required dependencies are listed in the Table 1:

Table 1: Software Dependencies

GNU Compile Collection Linux: Install package g++
Crypto++ Linux: Install package libcrypto++-dev
SWIG Linux: Install package swig
Python2.6/2.7 Linux: Install package python-dev
Python Twisted – asynchronous networking Linux: Install package python-twisted
PyQt 4(for Python 2.X) Linux: Install package libqtcore4,libqt4-dev,python-qt4, and pyqt4-dev-tool
Qt4reactor.py: combined eventloop for PyQt and Twisted
Bitcoin Core daemon (Bitcoind): The Bitcoind program allows access to the Bitcoin Network

6.2 *Setting Up the GSM Modem for Communication*

The GSM modem was plugged into the computer and the processing of the text messages was made possible by installing two packages, pySerial 2.7 and Python-gsmmodem 0.9. These packages enable the developer to control the GSM modem attached to the system to retrieve the SMSs received by the SIM card and respond to these SMSs by sending an SMS back to the sender.

6.3 *Access to the MBWS*

To access the MBWS, seven SMS command functions were implemented to allow the processing of the SMS commands sent by the user. These commands are sent by the user to access different functionalities of the system and are as follows:

- Help command, used to request the description of all the commands used
- Address command, used to generate a Bitcoin address from the Bitcoin wallet
- Balance command, used to request the balance of bitcoins available from the Bitcoin wallet
- Send command, used to send bitcoins to a Bitcoin user who is enrolled (using their mobile phone number) or a Bitcoin user who is not enrolled. When sending to a user that is not enrolled on the system the user should send to the Bitcoin address.
- ChangePassword command, used to change the password
- Getwallet command, used to enrol on the system
- Grant command, used to send bitcoins to many Bitcoin users

The greatest challenges in implementing this system were encountered especially when the Bitcoin client and the SMS application were integrated.

- The use of the ABWM was complex due to the various programming languages that are used and the numerous lines of source code, which contained a lot of bugs that had to be solved.
- To view the updated transaction, the full blockchain database had to be scanned for every new transaction. This resulted in the blockchain taking 3 times its allocated size. The size of the blockchain was approximately 70GB and disk space on the computer is 226GB. This caused a major challenge because the blockchain would grow and the computer disk space would be insufficient and it was RAM intensive,

which slowed down the entire system. This particular problem was fixed and a new version of the ABWM software was shared on GitHub for other software developers.

- Requesting the Bitcoin balance after generating a Bitcoin address resulted in the blockchain taking more than 30 minutes to complete rescan because it had to register the new Bitcoin address first which can be a shortfall to the system because it consumes time when requesting a balance.

For the third party hosting this system, a lot would have to be considered, due to the complexity of the Bitcoin system. Securing the Bitcoin wallet files and preventing unauthorised access is the main concern, since hosting these wallets requires the third-party to ensure that the user's private keys are safe. If the third party's system is compromised, bitcoins can be stolen and cannot be reclaimed or reversed. If an open source Bitcoin wallet management software is used, having to deal with the complex Bitcoin system is mitigated but if the company desiring to host the Bitcoin wallet chooses to implement a Bitcoin wallet management software then the complexity of the Bitcoin system has to be taken into consideration.

6. Results

In this section, four screenshots demonstrate four SMS commands that can be used. Figure 2 shows the Getwallet command, to enrol on the MBWS the user sends this command and is enrolled on the system and he receives a password that he can use to access his Bitcoin wallet.

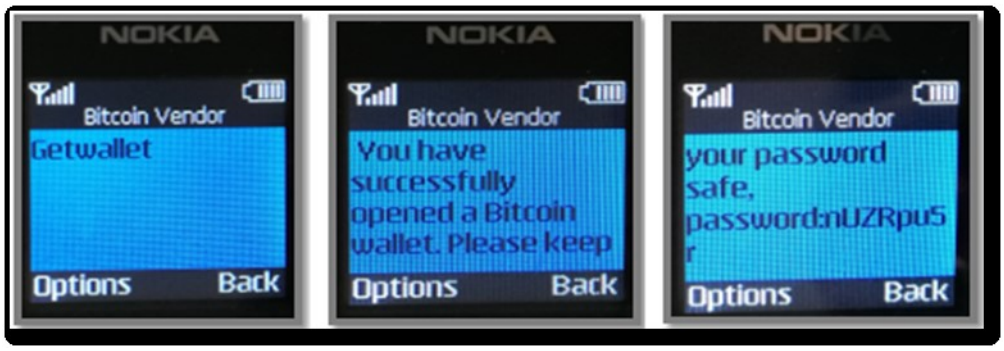

Figure 2: Getwallet Command

Figure 3, demonstrates the Address command, this command is sent by the user when he wants a Bitcoin address, he can use it to receive bitcoins from other users.

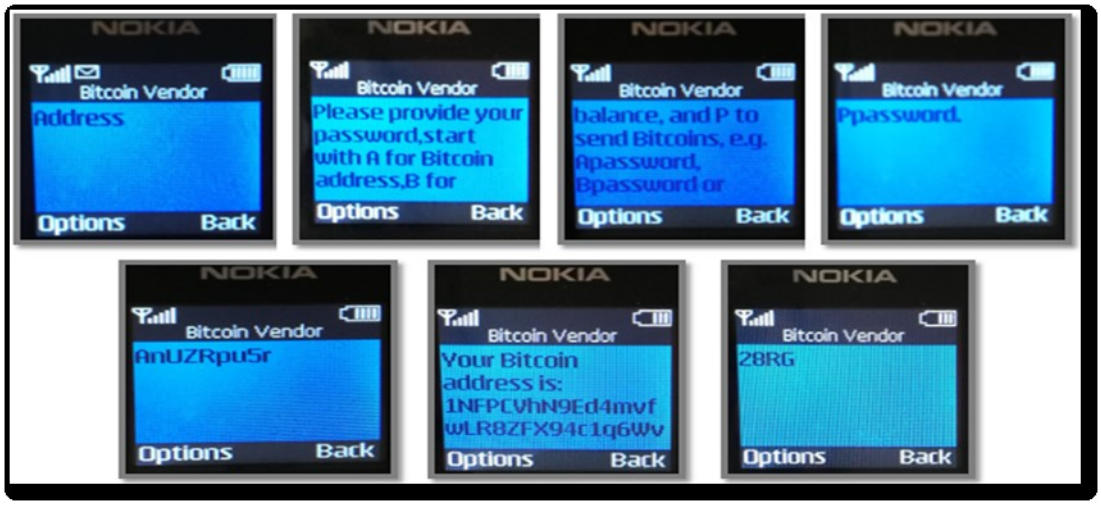

Figure 3: Address command

Figure 4 demonstrates the Balance command, this command is sent by the user when he wants to check the balance of bitcoins in his Bitcoin wallet. Currently this user has a balance of 0 BTC (BTC is used to denote Bitcoin value).

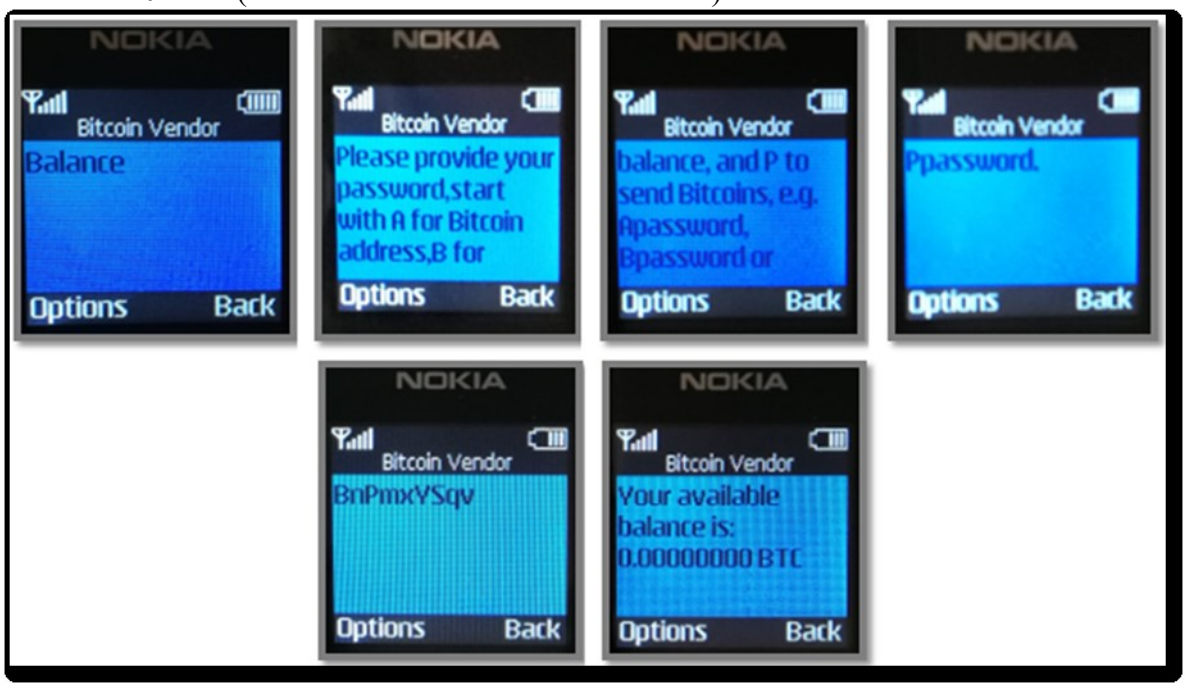

Figure 4: Balance Command

Figure 5 demonstrates the Changepassword command, which is used when the user wants to change the password.

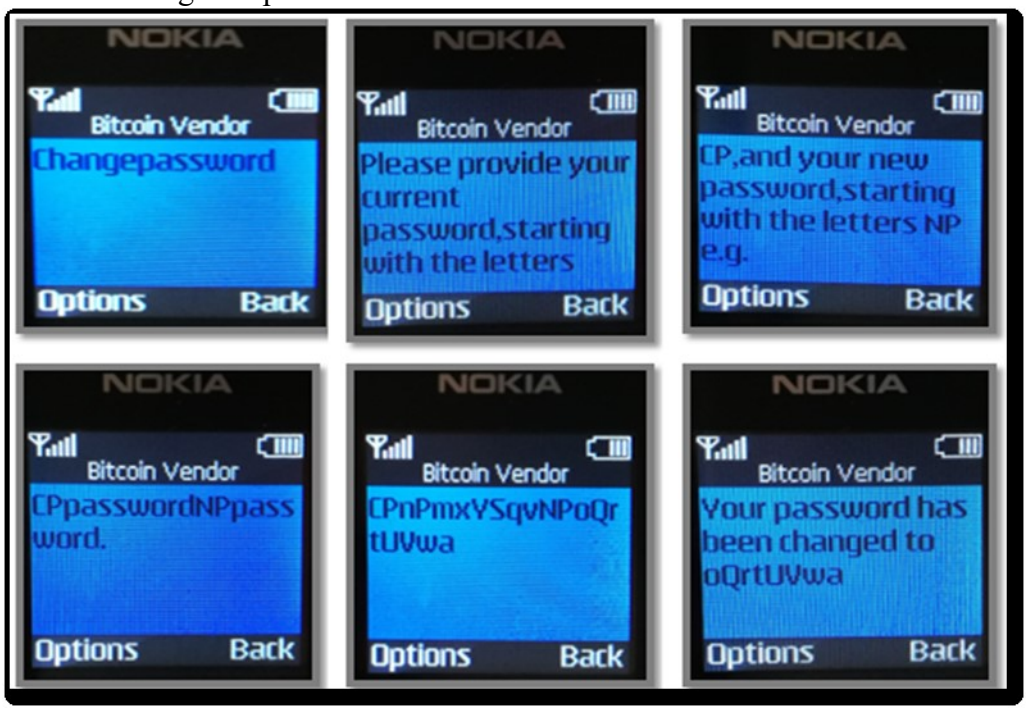

Figure 5: Changepassword Command

The user's password is not stored in the system, therefore if the user forgets the password the Bitcoin wallet will not be recoverable by sending an SMS to the MBWS. The SMSs sent are not free the user needs airtime to use this system. These Screenshots were captured when the system was tested if it meets the objectives outlined.

7. Business Benefits

The use of Bitcoin continues to grow, despite the regulation uncertainties shared across many countries permitting its use. To increase the adoption of Bitcoin, pragmatic companies continue to deliver applications that are useful to the people, e.g. companies like Dell, Microsoft, Overstock, Expedia which allow Bitcoin users to purchase online and pay using bitcoins. In Kenya, BitPesa which is a payments platform allowing people to make payments to and from sub-Saharan countries and also exchanges Bitcoin for fiat currency is quiet a success [13][14]. Bitmari is a remittance start up in Zimbabwe which allows farmers to use Bitcoin as an alternative currency, in South Africa, Bitcoin exchange companies such as, Ice3Cubed and Luno allow people to buy or sell bitcoins. The list of existing start up companies is increasing but a gap still exists in the adoption and prominence of Bitcoin as an alternative currency [15][16][17].

A system that only requires what the people possess, e.g. a feature phone and airtime will help increase the user base gradually and expose people to this technology. Using a system that requires a user to send an SMS from a mobile phone also alleviates the process of learning how Bitcoin works and figuring out the core functionality, because people are more accustomed to the use of mobile phones and leaves them with the task of acquiring knowledge on how to exchange Bitcoin for goods, services or fiat currency. The system developed also allows users who have online Bitcoin wallets or Bitcoin wallet applications installed e.g. Blockchain Bitcoin wallet, Coinbase Bitcoin wallet, Bitx Smart Bitcoin wallet, etc., to transfer bitcoin value to Bitcoin users who are enrolled on the system. It also allows the transfer of bitcoins from one Bitcoin address to the next within the same Bitcoin wallet.

The results derived from the developed system show that Bitcoin can be used by a company that wants to transfer money to many people at a low cost, it can also be used by people who do not have a bank account but seek to have access to funds using their mobile phone. While this system is used to access a Bitcoin wallet and it is not linked to a bank account like cell-phone and mobile banking services. If enough methods of exchange are offered i.e. vendors exchanging bitcoins for other currencies for instance ZAR and other vendors accept bitcoins for purchases of goods and services, then a Bitcoin wallet service can be useful as an alternative payment method due to the similar requirements and functionality to the cell-phone banking service, existing payment methods and can even be used for remittances.

8. Conclusions

A few use-cases have been suggested for Bitcoin as electronic money such as remittances, cross border transactions, payment method, and many companies are developing applications and systems to execute these use-cases. This paper has presented a method to acquire a Bitcoin wallet and access it using a low-end mobile phone, just by sending an SMS. This system was developed as a proof of concept and to demonstrate its feasibility, but it still requires other functionalities for it to be a fully functional system that can be made available to people.

These functionalities include the ability to check the previous transactions that took place, to convert bitcoins to ZAR instantly to avoid volatility and enable it to respond to a large amount of SMSs and to translate the language used. The system also needs to be enhanced and optimized in terms of scalability and speed of transactions and SMS responses and security. The use of Bitcoin also presents an opportunity for new use–cases, such as local stores accepting Bitcoin for goods and services and exchanging Bitcoin for ZAR, which would contribute to the convenience of payments for those people who do not have access to a bank account. Although Bitcoin presents opportunities, for it to be exploited and adopted, people still need to be educated about Bitcoin.

References

[1] R. J. Gordon, “Finance and Development: Africa Growth Up’s and Downs,” 2016.

[2] O. N. Montfort Mlachila, Dennis Dykes, Sabina Zajc, Paul-Harry Aithnard, Thorsten Beck, Mthuli Ncube, “Banking in Sub-Saharan Africa: Challenges and Opportunities,” 2013.

[3] M. Yang, “Cryptocurrency in China : Light-Touch Regulation in Demand,” 2016.

[4] E. Dourado and J. Brito, “Cryptocurrency,” *The New Palgrave Dictionary of Economics*. Palgrave Macmillan, pp. 1–10, 2014.

[5] S. Nakamoto, “Bitcoin : A Peer-to-Peer Electronic Cash System,” *Bitcoin A Peer-to-Peer Electron. Cash Syst.*, pp. 1–9, 2008.

[6] K. Okupski, “Bitcoin Developer Reference,” Eindhoven, 2014.

[7] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A First Look at the Usability of Bitcoin Key Management,” in *Workshop on Usable Security (USEC). 2015.*, 2015.

[8] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. a. Kroll, and E. W. Felten, “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” *2015 IEEE Symp. Secur. Priv.*, pp. 104–121, May 2015.

[9] R. Grinberg, “Bitcoin : An Innovative Alternative Digital Currency,” *Hast. Sci. Technol. Law J.*, vol. 4, no. 1, pp. 160–180.

[10] S. Barber, X. Boyen, E. Shi, and E. Uzun, “Bitter to Better — How to Make Bitcoin a Better Currency,” *Financ. Cryptogr. Data Secur.*, vol. 7397, pp. 399–414, 2012.

[11] W. Mackay and M. Beaudouin-Lafon, “Prototyping tools and techniques.,” in *The human-computer interaction handbook*, A. Sears and J. A. Jacko, Eds. Hillsdale, NJ, USA: L. Erlbaum Associates Inc., 2002, pp. 1006–1031.

[12] J. Greensmith, “Software Prototyping (Lecture 10).” The University of Nottingham, Nottingham, pp. 1–29, 2012.

[13] L. Shin, “Elizabeth Rossiello Describes How BitPesa Slashes International Payment Fees,” 2016. [Online]. Available: https://www.forbes.com/sites/laurashin/2016/06/15/elizabeth-rossiello-describes-how-bitpesa-slashes-international-payment-fees/#445ebdfd2a6d. [Accessed: 01-Mar-2017].

[14] M. Sparkes, “Britons can now buy Dell computers with Bitcoin - Telegraph,” *The Telegragh*, 2015. [Online]. Available: http://www.telegraph.co.uk/technology/news/11425250/Britons-can-now-buy-Dell-computers-with-Bitcoin.html. [Accessed: 01-Mar-2017].

[15] N. Gambanga, “Bitcoin startup Bitmari introduces farmers in rural Zimbabwe to cryptocurrency as a cash alternative - Techzim,” *TECHZim*, 2016. [Online]. Available: http://www.techzim.co.zw/2016/10/bitcoin-startup-bitmari-introducing-rural-zimbabwe-cryptocurrency-cash-alternative/. [Accessed: 01-Mar-2017].

[16] J. Southurst, “ICE3x Launches Nigeria’s First Bitcoin Exchange,” *Coindesk.com*, 2015. [Online]. Available: http://www.coindesk.com/ice3x-launches-nigerias-first-bitcoin-exchange/. [Accessed: 01-Mar-2017].

[17] P. Rizzo, “BitX Rebrands as Luno, Reveals Bitcoin Sandbox Project - CoinDesk,” *Coindesk*, 2017. [Online]. Available: http://www.coindesk.com/bitx-rebrands-luno-reveals-bitcoin-sandbox-project/. [Accessed: 01-Mar-2017].