Vol 8. No. 3 Issue 2 – October, 2015
African Journal of Computing & ICT

www.ajocict.net

A Review of the Bitcoin Digital Payment System with Emphasis on its Security

C. O. Ugochi
Network and Information Security Department
Kingston University
London, United Kingdom
guchiopara@gmail.com

ABSTRACT

Bitcoin is a fast growing cryptographic currency payment system. Although all transactions carried out using this service are publicly available, Bitcoin offers privacy and anonymity to users behind these transactions. This system has faced a lot of criticisms owing to uncertainties regarding the true value of a Bitcoin, and also with regards to the security and privacy provisions of the Bitcoin system. This paper reviews the functionalities of Bitcoin, and discusses the effectiveness of the measures put in place to ensure the security of the overall network. It also highlights the issue of user privacy and anonymity in Bitcoin, and possible ways to address them.

Keywords - Bitcoin; transaction; security; privacy; anonymity

African Journal of Computing & ICT Reference Format:
C. Opara (2015): A Review of the Bitcoin Digital Payment System with Emphasis on its Security. Afri J Comp & ICTs Vol 8, No.3 Issue 2 Pp 21-24.

1. INTRODUCTION

Bitcoin is a pseudonym for the world's first decentralized online crypto-currency payment system. It is decentralized, meaning its operation does not depend on any trusted entity, thus all transactions are carried out over the internet in a peer to peer manner. It was first introduced in 2008 by Satoshi Nakamoto [1] in a report that contained details of the Bitcoin design. The Bitcoin technology is open source and relies heavily on cryptographic primitives such as the use of hash functions and digital signatures to validate ownership.

Since the introduction of Bitcoin, it has gained a lot of attention from the media and the general public. The idea of having an online currency which could be traded alongside hard currencies seemed remarkable and implausible, thus Bitcoin faced many criticisms and opposition from the general public and several government bodies [2]. The lack of acceptance arose mostly from the uncertainties regarding the true value of a Bitcoin, and also the security and privacy of the Bitcoin system. Though still a novel invention, some researchers have analysed the Bitcoin system and have published their findings regarding the feasibility and security of the Bitcoin. Furthermore, there have been other proposed online currencies which are not exactly novel, but are simply modifications of the original invention [3, 4]. However, according to recent reports [5], Bitcoin remains the most popular and most valuable crypto-currency available despite the introduction of newer crypto-currencies.

A. Background on Bitcoin

According to a document on the history of digital payment systems, the concept of a cryptographic currency was first proposed by Wei Dei in 1990's and he called it B-money [4]. A similar concept called Bitgold was also proposed by Nick Szabo. These early digital currencies relied on centralized entities that made anonymous payments impossible [7]. Bitcoin is said to have based its idea on these initial proposals and was proposed in October 2008 by Satoshi Nakamoto, a name which has been speculated to be a pseudonym representing more than one person [8]. In January 2009, the Bitcoin network was officially launched with the release of the genesis block which was the first block in the Bitcoin chain.

The security of the Bitcoin system revolves around trust by computation, that is, network users are required to exhibit proof of work (POW) by completing a computationally hard problem[6]. The collective computing power accumulated by participants over a period of time ensures that no participant or group of participants is allowed to cheat, as they lack the computation strength necessary to dominate the trust system. The more the POW accumulates, the harder it is to dispute.

In this paper, a review of the Bitcoin system will be carried out and the security and user privacy issues relating to Bitcoin will also be discussed. This paper is organized as follows; Section 1presents background information on the Bitcoin system. Section two explains the major operations that make up the Bitcoin system. Section three discusses the security aspects of this system with respect to privacy and anonymity. Section four provides a brief analysis and discussion and section five concludes the report.

According to [9], the first unofficial Bitcoin transaction was made in 2009 between Satoshi and a developer called Hal Finney. Soon after, a significant transaction was made when 10, 000BTCs was used to purchase two pizzas. Later that year, an exchange rate was established for the Bitcoin and this marked a significant breakthrough for the crypto-currency. The Bitcoin is very volatile with unstable exchange rates over time; it has seen a high point of 1110USD per Bitcoin and rates as low as 5USD in 2011. As of the time of writing this report, the value of a Bitcoin is 533USD, falling from a 947USD within one week. This high volatility is a reason why many have condemned the crypto-currency despite its growing popularity and successes. Governments of different countries have also raised concerns about how the untraceability feature of the Bitcoin may lead to tax evasions, money laundering and other illegal transactions. Bitcoin transactions were soon after banned in china [2].

Bitcoin services operate a peer to peer network scheme, hence no central authority or bank is required to make regulations or control the currency, and this attracts both legitimate and illegitimate users who do not want government involvement in their transactions. Bitcoin also assures privacy for its users by allocating pseudonyms called Bitcoin addresses to the users whenever they wish to participate in a transaction [10]. Despite the supposed reliance on pseudonyms for privacy provision, each transaction consists of a chain of digital signatures. This creates serious concerns because since transaction details are publicly available, they can be tracked and linked to a specific user. Androulaki et al [10] in their work evaluated user privacy in Bitcoin when used to conduct daily transactions in a university, according to their results, the measures put in place are not sufficient to provide privacy for most of its users. These privacy and security issues will be discussed in more detail in section three.

2. THE BITCOIN SYSTEM

This section concisely describes how the Bitcoin system works. As mentioned in the previous section, Bitcoin is a peer to peer online payment system that relies on proof of work and public key encryption. Bitcoins (BTCs) are transferred between users by generating transactions [1]. The users take part in these transactions by adopting pseudonyms, commonly referred to as *Bitcoin addresses.* These Bitcoin addresses are the means by which bitcoins are received, quite similar to how email addresses are used to receive and send emails. Each user also has a digital wallet that stores and manages hundreds of Bitcoin addresses belonging to the user. These addresses are individually mapped to separate public/private key pairs using a transformation function [10]. The transfer of ownership of Bitcoins amongst addresses is only possible with the correct keys.

In the Bitcoin system, transactions are broadcast by each user to other peers in the network. The following sections briefly explain the concepts and activities that make up the Bitcoin system.

A. Transactions

As mentioned above, BTCs are transferred between peers by generating a transaction. A transaction is created by digitally signing the hash of the last transaction the Bitcoin was used for and the public key of the intended user, and integrating the signature in the coin [10]. Simply put, a transaction typically has input and output values; the input represents the output of the previous transaction and the output of the current transaction becomes the input for the next transaction. Over time, a chain of signatures is formed, and this can be used to verify the authenticity of a BTC. These digital signatures are a means to avoid double spending attacks by users. The process through which transactions are verified is called *mining* [1].

B. Mining Bitcoins

According to Hobson [11], Bitcoin mining can also be referred to as the process of adding transactions to the block chain so that there can be a general consensus from the users on the same set of transactions, and also so that double spending of Bitcoins is avoided. This process revolves around the proof of work (POW) computations. To start the mining process, the user must run a mining software which carries out the following steps repeatedly;

- All unconfirmed transactions are collected into a block. This also includes the hash of the last block added to the block chain, and in addition a *nonce*, which could be any random number.
- Following step 1, a hash of the newly created block is done, and the hash value is examined. A predefined number known as the 'difficulty' is set and the important factor here is the number of leading zeros. If the number of leading zeros is smaller than the predefined number, then a repeat of step 1 is carried out with an increment to the nonce, while ensuring that a different hash value is reached each time [11]. If the leading zeros are more than the predefined number, then the next step can be taken
- After successfully completing the previous steps, the user is said to have mined a block successfully and the block is added to the block chain. The user can then broadcast the hash (including the transactions) along with the nonce, to other network users. Newly created bitcoins are then awarded to the user in a special coin base transaction [11] and this marks the initial production of bitcoins.

Other network users receive the block and examine its contents to ensure that there are no invalid transactions and that they produce the correct results when hashed. If all values correspond, then this new block will serve as input to a new mining process by another user. And the whole steps are performed again, thus increasing the chain. This is the process of validating transactions. The mining process is not performed by all network participants; instead a few 'special' users carry out the important task of block creation and transaction validation on behalf of the network.

The POW 'difficulty' feature in the mining process is used to control the rate at which blocks are mined, and this has a direct effect on the number of Bitcoins in circulation. The POW difficulty tries to maintain a block mining rate of one block every 10minutes. According to[11], a reward of 25BTC is given to a user after completing a block, and after four years the reward is halved. This encourages miners to work continuously and provide support for the Bitcoin network. The Bitcoin mining process has been taken as a lucrative business up by some users and requires a lot of computational power, which can be very expensive. If invalid blocks are created, network peers will reject them, and the miners will be invalidated.

C. Bitcoin Wallets

A Bitcoin wallet contains all the Bitcoin addresses belonging to a user. These addresses all have individual public keys and the corresponding private keys are stored on the users wallet file locally [11] It is advisable for users to have as many addresses as possible and it is their sole responsibility to keep the wallet file safe. The loss of a wallet file means the loss of associated Bitcoins since they can only be spent with knowledge of the private keys. These Bitcoins remain on the Bitcoin network but are not spendable without the required private keys.

D. Spending Bitcoins

To spend Bitcoins, a user must join the Bitcoin P2P network via a Bitcoin client. A user possesses coins based on previous transactions that named its address as a recipient or as a reward for completing a block [8]. Suppose a user Alice wishes to transfer 2 Bitcoins to another user Bob, first Alice starts a new transaction that endorses coins received from previous transactions which have not been spent by Alice yet. For example, she endorses 5 bitcoins received from Charlie using a digital signature, and takes this as the input to her new transaction. As the output, she indicates that she wants to remit 2 Bitcoins to Bob, leaving her with 3 Bitcoins. The network users collectively agree on the validity of the transaction by adding it to the public history of previously validated transactions which is at the end of the longest block chain [12].

3. SECURITY IN THE BITCOIN SYSTEM

The security of this system is partly based on assumption that it is impossible for dishonest players to gain computation power high enough to compromise the system. That is, as long as there are more valid blocks, it is extremely difficult to outnumber the honest computations. Blocks are added to the longest chain in the network as it is considered as the correct one [11]. Therefore if an attacker wants to modify a block, it will need to compute the POW of the block and all the blocks along the chain. This is an extremely challenging and expensive task. And because more honest users keep validating blocks, the attacker can barely meet up.

This is one of the security advantages of the decentralized Bitcoin system. However, there is also the issue of privacy, anonymity, and possible attacks against network users.

A. Privacy

The Bitcoin system is such that all Bitcoin transactions are publicly available; this is to ensure that the transactions can be validated to curb double spending [13]. The public announcement of these transactions seem like an apparent flaw in the system with regards to privacy, however, privacy can still be achieved by keeping the public keys anonymous. It is visible to the public when someone transfers an amount to another person but no one knows who the sender or recipient is. The use of new key pairs for each transaction is an added measure to provide unlinkability [1]. However, this cannot be avoided with multiple input transactions which could inadvertently disclose that the inputs were from the same owner. Furthermore, it is possible for users to link other users to a wallet address. A user Charlie may broadcast his wallet address on a social networking site requesting for anonymous donations. By observing the block chain, users can deduce the addresses Charlie has been transferring bitcoins to.

B. Theft and Loss of Bitcoins

As with any network and computing system, especially one that promises anonymity and user privacy, the Bitcoin network is an attraction for hackers and Malware creators. The network is susceptible to attacks which can result in the theft of private keys. As reported in [13], a Denial of service attack was launched at a Denmark-based Bitcoin payment service provider and the attackers emptied the wallets of many Bitcoin users. Malware writers according to the same report have been developing malware to steal wallets stored on infected machines. The perpetrators of the DDOS were traced back to Russia, but were never found. This goes to question the reliability of the entire system.

Barber et al [8] proposed the use of threshold cryptography so that private keys can be split into shares and distributed in multiple locations. Thus, instead of having the private keys stored on one device, e.g. laptop, a user can also have it stored on a mobile and a service provider. Therefore the user can only spend Bitcoins when a threshold these storage locations is activated.

4. ANALYSIS AND DISCUSSION

The security provision in terms of anonymity and user privacy in the Bitcoin system can be seen as a strength and also a weakness. The system offers anonymity enough for money laundering and other illegal activities to be paid for without being traceable to any individual. Some of these illegal transactions are made using anonymous web clients such as the Tor network, which makes it even harder for criminals to be caught. The network is purely decentralized, thus there's no central authority to act as an arbitrator in case issues arise.

On a positive note, some honest users just desire a fast and secure payment service without encountering unnecessary charges and restrictions placed by any entity. Anonymous whistle blowing sites also see it as a means to raise funds, while keeping the identities of the contributors private. The novelty of the Bitcoin system makes it difficult to be understood properly. It takes a lot of time to research and grasp the concepts behind generating bitcoins and maintaining wallets. Users who simply read about Bitcoins on the internet and opt to join the network without fully understanding the implications or are not be aware of the security measures needed to guard the Bitcoin wallet, are likely to lose their bitcoins. To protect Bitcoin wallets from theft, threshold cryptography as proposed in [8] may be one way to go about it by splitting the private key into shares and storing in different locations. Though a good idea, it makes spending Bitcoins a hassle, as the user will need to activate the threshold number of devices each time a transaction is to be made. However, it may be a small price to pay as against loosing huge investments.

The publicly available history of transactions could pose a possible risk to Bitcoin. Researchers [12, 14] have downloaded the entire history of Bitcoins to analyse and possibly identify patterns which may threaten the anonymity feature of the Bitcoin system. In their study, they came to the conclusion that it is possible, using appropriate tools and some external identifying information, to associate public keys with each other. Also, they claim that wallet and exchange service providers are capable of tracking user activity to a certain level.

5. CONCLUSION

Bitcoin as a first generation crypto-currency is still yet to reach its maturity. Its volatile nature makes it even less attractive to many who are not confident enough to take risks; however, a fairly large population has joined the Bitcoin network. The flexibility and anonymity provisions, however appealing, come at a security cost. The availability of transactions publicly has a cost of being analysed by external parties to extract information, Bitcoin wallets can easily get lost or stolen, the Bitcoin exchanges could crash, and so on. Though technical affiliates of the Bitcoin network may argue that strong anonymity is not the primary goal of Bitcoin, It is imperative that users are aware of the security implications of Bitcoin before joining the network.

REFERENCES

[1] [1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.

[2] ().

[3] S. C. Glaeser, "Economic Analysis of Cryptographic Currencies on the Basis of Bitcoin," 2014.

[4] S. Sprankel, Technical Basis of Digital Currencies, 2013.

[5] E. Molchanova and Y. Solodkovskyy, "Global service nature of contemporary crypto-currencies," International Economic Policy, pp. 55-72, 2014.

[6] ().

[7] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer and R. Böhme, "Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency," in The Economics of Information Security and PrivacyAnonymous Springer, 2013, pp. 135-156.

[8] S. Barber, X. Boyen, E. Shi and E. Uzun, "Bitter to better—how to make bitcoin a better currency," in Financial Cryptography and Data SecurityAnonymous Springer, 2012, pp. 399-414.

[9] (). History of Bitcoin.

[10] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating user privacy in bitcoin," in Financial Cryptography and Data SecurityAnonymous Springer, 2013, pp. 34-51.

[11] D. Hobson, "What is bitcoin?" XRDS: Crossroads, the ACM Magazine for Students, vol. 20, pp. 40-44, 2013.

[12] F. Reid and M. Harrigan, An Analysis of Anonymity in the Bitcoin System. Springer, 2013.

[13] (). Bitcoin TheftsSurge,DDoS Hackers TakeMillions.InformationWeek. [Online]. .

[14] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in Financial Cryptography and Data SecurityAnonymous Springer, 2013, pp. 6-24.

Author's Biography

Chidimma Opara Ugochi (guchiopara@gmail.com) is a PhD candidate at the University of Nigeria Nsukka. She recently graduated with distinction in Network and Information Security from Kingston University London. Her research interests include network and distributed system security, wireless networking and mobile computing.