Digital Currency: The Emergence of Bitcoins

Thabiso Peter Mpofu1, Budwell Masaiti2, Macdonald Mukosera3

1M.Tech. Student, Department of Computer Science, School of IT, Jawaharlal Nehru Technological University Hyderabad, India
2Jawaharlal Nehru Technological University Hyderabad, College of Engineering, Kukatpally, Hyderabad 500085, India
3Jawaharlal Nehru Technological University Hyderabad, School of Information Technology, Kukatpally, Hyderabad 500085, India

Abstract: Bitcoins are a crypto currency whose concept was developed in 2009 by Satoshi Nakamoto. Bitcoins are digital currencies which operate on a peer to peer system. The system is decentralized as there is no central regulatory authority as with fiat currency. For an individual to transact you need a bitcoin wallet which has one or more private and public keys associated with it. Unlike fiat currency and electronic payment methods such as Visa and MasterCard which are based on trust, Bitcoin usage is based on cryptographic proof. Bitcoin usage has been on the increase and they can be converted into fiat currency through bitcoin exchanges.

Keywords: Bitcoins, decentralized, peer to peer, crypto currency, fiat currency, cryptographic proof, bitcoin exchange, bitcoin wallet

1. Introduction

Bitcoins are a digital currency based on a whitepaper published by Satoshi Nakamoto in 2009[1]. The current money system is a centralized system as all transactions have to pass through a middleman which are banks.[16] Banks impose relatively higher transaction charges on the transactions done thus costing the person to transact. Nakamoto proposed a peer to peer system for the exchange of the digital currency now termed as bitcoins. However, there was a problem of double spending as an individual could spend the same bitcoin multiple number of times. This problem was solved by the implementation of time stamping to provide computational proof of chronological order of transactions. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work [1]. This is achieved through miners who form nodes in the network and are responsible for providing the proof of work. The miners are rewarded through newly minted coins and through transactions costs. In the peer to peer system, you create a bitcoin wallet for you to be able to buy and transact in bitcoins [16]. A bitcoin wallet has a private and public key associated with it. The private key should be known by the owner of the bitcoin wallet only [3][12][13]. The private key is like the Automated Teller Machine (ATM) pin code where holder of the card is the only one who is supposed to know as the pin. The bit coin wallet contains details of the number of coins contained.

2. How it Works

Bitcoin is based on a peer-to-peer network of users. For a person to join the network they require a bitcoin wallet. A bit coin wallet has one or more private and their corresponding public keys. The public key identifies a client to the rest of the network. The private key remains anonymous and only the account holder should know the private key [3][12][13]. The private key is like the Automated Teller Machine (ATM) pin code where holder of the card is the only one who is supposed to know as the pin. The bit coin wallet contains details of the number of coins contained.

To send bit coins to someone else, the structure of the transactions is shown in figure 1 above. The sender signs a transaction request with her private key. The transaction is broadcast to the entire network and anyone can verify using the sender’s public key if it was the sender who indeed sent the transaction request.

Participants with a lot of processing power form the peer-to-peer network and they verify transactions by bundling transactions into transaction blocks. Together they form a collective consensus regarding the validity of this transaction by appending it to the public history of previously agreed-upon transactions (the longest block-chain). This process is known as mining. The miners’ computers calculate a hash function by applying a SHA256 hashing operation towards certain targeted hashes with a specific number of zeros.
The mining computers calculate new hash values based on a combination of the previous hash value as shown in figure 2, the new transaction block, and a nonce. Miners have no way of telling which nonce will produce the required hash, many hashes with different nonces are therefore produced until an appropriate hash is produced leading to transaction verification. The whole procedure requires a lot of processing power and it is rewarded awarding newly minted bitcoins and/or transaction fees for each block they add to the block chain. The transaction is then verified and the recipient receives their bitcoins in their wallet.

3. Benefits

3.1 Anonymity

Details such as name and date of birth are not required to transact with bitcoins. A private and public key are the ones that are only required [2]. However anonymity has been known to be compromised in certain instances [2]. Even though various deanonymization techniques have been proposed [11], the peer to peer bitcoin network remains relatively anonymous compared to payment via Visa or MasterCard where you fill in your personal details before usage of the service. Others have proposed to increase the level of anonymity by augmenting the current bitcoin peer to peers protocol to allow for fully anonymous currency transactions [6].

3.2 Decentralised

The bitcoin network relies on a peer to peer system. There is no centralized control. Members of the peer to peer network self regulate themselves from transfers of bitcoins to the minting of new bitcoins

3.3 Liquidate to hard currency

The bitcoins can be liquidated to hard currency through bitcoin exchanges such as www.igot.com available in countries such as India. On 7 June 2014 a bit coin was trading at an average price of 650 American dollars [17].

3.4 Block reward

For each block miners add to the block chain, they get rewarded with newly minted bitcoins which started out at 50 bitcoins (BTC) and is halved every 210,000 blocks, about every four years. 99% of all BTC will be issued by 2032.

3.5 Transaction fees

Transaction fees create an incentive for the miner to use their bandwidth in the verification procedure. The miner has the option of excluding or including transactions in the block. Lower transaction fees also benefit the users of the peer to peer network as it means less expense for them.

3.6 Low fees

The transaction fees are relatively low in the peer to peer system compared to the centralized system where all transactions have to pass through the bank.

4. Security Issues

Bitcoins have become targets for hackers as they are able to be traded for hard currency. With traditional currency, if your currency disappears in your account, the bank has to answer for that and reimburse you. Unlike with traditional currency, if your bitcoins disappear, there will be no one to reimburse you. Attacks on bitcoins have been on an increase as they have proved to be very attractive due to their non traceability and anonymity. Various attacks such as attacks using botnets in the bitcoin peer to peer network [4] to various hacker attacks have been reported [5]. The bitcoin network relies on a public ledger which is implemented using transaction blocks. The use of blocks has been shown to be a vulnerability. The reliance on blocks not only delays the clearing of transactions, but it also poses a threat to the network itself. Large blocks are propagated slowly in the network, giving an attacker an advantage. Changes to the current protocols are proposed though the measures are for the short term [10]. Users should be alert and be proactive in the protection of their assets. Nearly 850,000 bitcoins were stolen by hackers from now bankrupt former bitcoin exchange MtGox. The following security measures were proposed in an article published online in the Forbes magazine [15].

i. Evaluate the type of wallet you want to use

Wallets can be operated either on a computer, mobile device or offline. Maintaining your account offline is the most preferred and only go online when you need to transact.

ii. Use file and folder encryption to protect your wallet

The bitcoin wallet can be encrypted to provide an extra layer of protection

iii. Update your bitcoin wallet software

Just like any other software, regularly update your bitcoin wallet and get the latest bug fixes and security updates

iv. Use a secure password, or two factor authentication

Use a long password which is not easy to guess. A combination of letters and numbers is encouraged. Adding another dimension to the authentication process such as token or USB key to make a more secure double factor authentication

v. Keep your Bitcoins backed up off system
v. Practice general computer security best practice
Similar to the bank multiple signatory system. Multiple users are required to for authentication to take place. Authentication is carried out through cryptography. It makes it more difficult for an attacker to gain access as they have to break cryptographic keys for multiple users.

vi. Consider using the multi-signature feature
Keeping your general security such as antivirus and firewalls in place is highly encouraged. Keeping measures in place decreases the likelihood of an attacker targeting you as you are less vulnerable. The reliance on blocks not only delays the clearing of transactions, but it also poses a threat to the network itself. Large blocks are propagated slowly in the network, giving advantage to an attacker. Changes to the current protocols are proposed through the measures are for the short term [10]

vii. Practice general computer security best practice
Keeping your general security such as antivirus and firewalls in place is highly encouraged. Keeping measures in place decreases the likelihood of an attacker targeting you as you are less vulnerable. The reliance on blocks not only delays the clearing of transactions, but it also poses a threat to the network itself. Large blocks are propagated slowly in the network, giving advantage to an attacker. Changes to the current protocols are proposed through the measures are for the short term [10]

5. Future Work
Transactions involving bitcoins are on the increase. In India btcjam is loaning bitcoins to entrepreneurs to finance their business as is done with normal currency [14]

6. Conclusion
Bitcoins are the only digital currency that has had a widespread usage across the globe and it appears it is here to stay. Various security issues are however proving to be the major deterrent to the adoption of bitcoins in the mainstream.

Various governments have been skeptical over bitcoin usage as they have no control over it. Only time will tell on whether more and more people adopt bitcoins as a currency or not.

References
23+India+Borrowers+Business+Newsfeed+CPC


Author Profile

Thabiso Peter Mpofu received B. Tech degree in Computer Science at Harare Institute of Technology (HIT), Zimbabwe in 2010. He is currently pursuing M. Tech Computer Science at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of Data Mining, Network Security and Mobile Computing.

Budwell T Masaiti received the B.Tech Hons degree in Computer Science from Harare Institute of Technology (Zimbabwe) and Daejeon University (South Korea) in 2011. During 2011-2012, he worked as a Teaching assistant at Harare Institute of Technology in the Computer Science Department. He is currently pursuing M Tech Computer Science at Jawaharlal Technological University Hyderabad College of Engineering. (India)

Macdonald Mukosera received the B.Tech Hons degree in Computer Science from Harare Institute of Technology in 2010. During 2011-2012, he worked as a Teaching assistant at Harare Institute of Technology in the Software Engineering Department. He is now studying M Tech Computer Science at Jawaharlal Technological University Hyderabad in School of Information Technology.