www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 5 May 2016, Page No. 16514-16517

Bitcoin: First Decentralized Payment System

Richa Kaushal[1]

[1]Atma Ram Sanatan Dharma College,
University Of Delhi
Richakaushal1990@gmail.com

Abstract: Bitcoin is the latest addition to the online payment transaction systems. It is a digital currency also known as cryptocurrency. Bitcoin system is the first transaction payment system that deviated from the conventional approach of processing and clearing transactions though the trusted third parties and allowed direct transactions between parties. Thus making the whole system decentralized. It is a pure peer to peer network system which facilitates every party on the network to keep track of all the transactions that are taking place on the network. It uses Cryptography for its implementation and to deal with the internet security threats. This papers aims to explore the need of the decentralized system, technology used for its implementation and also the key features of bitcoin system that makes it so unique as compared to the conventional currency. It also throws the light on the benefits of bitcoin system and its shortcomings.

Keywords: Cryptography, Decentralized, Digital signatures, Hash Function, Blockchain**.**

1. Introduction

Bitcoin is a payment system that facilitates the transfer of value between the parties. It is the first digital and decentralized currency invented by Satoshi in 2008. This system has its own metric for value called as bitcoin or BTC. Bitcoin as the name suggests is digital form of currency and exist only in the internet domain. They are bit like money and bit like a financial bubble as they do not have any physical existences. Bitcoin share many similarities with conventional currency yet are different from each other in the way they are being controlled and distributed. Bitcoins are decentralized form of currency and is not linked to any central banking system or issuing authority as in the case of conventional currency. Bitcoin system provides us the electronic payment system based on cryptography and it uses peer to peer network. Bitcoin transactions are completely non reversible and do not have any threat of fraud to merchants. These transactions are near instantaneous and non refundable and it supports global transactions at the same processing speed as the local transaction. All these features of bitcoin have lead to its rapid growth both in its value and in number of transactions over internet domain. Bitcoins is also known as cryptocurrency as its value is derived from the computational solving of cryptographic problems. In essence we can say that a bitcoin is electronic token that has its own metric for value and does not have any reference to foreign currency and hence is not accountable in any accounts balance sheets.

2. Need for Bitcoin SYSTEM

The major aim that leads to the invention of bitcoin is the need for a system that can process transactions on a network without the intervention of central trusted third parties. In a conventional electronic payment system used over the internet, parties rely on the financial institutions serving as third parties to process electronic payment. This Payment system works on the trust based model and its success depends upon the honesty of the third parties and also on the trust that the participating entities have on the third party. This system works fine for most of the transactions but it has an inherent weakness of trust. There was also the need for non reversible transactions for non reversible services. The non reversible transactions are not supported due to the mediating disputes which also increases the transaction cost. There was also no scope for small size casual transactions as the transaction cost was too high. Therefore there was a need for an electronic payment system that was decentralized and is based on cryptography rather than on trust based model. A system that allows parties to directly transact with each other thereby lowering transaction cost. It should also support non reversible transactions in order to safeguard merchants from fraud.

3. BITCOIN SYSTEM OVERVIEW

Bitcoin system uses peer to peer network to establish a decentralized payment transaction system among a group of nodes that are willing to participate in the payment transactions. This network implements currency life cycle that starts with the creations of bitcoins and supports direct transaction between parties without the need of trusted third party. The network assumes that the majority of the nodes on the network are honest they keep track of all the transactions. Bitcoin system does not have intermediary party to process the transactions therefore few of the participating nodes process the transaction. Theses nodes are responsible to record each transaction in a chronological order in a public ledger called blockchain. The nodes that are involved in processing the transaction are known as miner and the process is known as mining. A reward is given for recording each transaction in the blockchain. Miner competes for making the record and a well defined process chooses the winning miner to update blockchain. Each participant keeps the copy of the updated ledger thus making the whole system decentralized.

4. UNDERLYING CRYPTOGRAPHIC CONCEPTS

The bitcoin system uses cryptography scheme for its implementation and hence it's also known as Cryptocurrency. Cryptography is the study of secure communication between two parties in the presence of other parties in such a way that the message or data can be read and processed only by the intended receiver. The cryptography deals with mainly four aspects of information security. These are confidentiality that ensures the information is accessed only by its legitimate user and no one else. Integrity makes sure that the information is not altered or stored and then transferred between the parties without the alteration being detected. Non Repudiation ensures that the sender of the message cannot deny that they have sent a message. An authentication revolves around verifying the sender and receiver who are involved in a communication are the genuine parties or not. Bitcoin relies on digital signature and cryptographic hash, the two cryptography schemes in order to process and perform valid transaction over the network. Bitcoin system uses digital signatures any cryptographic hash.

4.1. CRYPTOGRAPHIC HASH

Cryptographic hash is used to enforce a serialized way in recording the transaction records in the public ledger. Cryptographic hash function is one way mathematical function that converts input value to another compressed value. The input to the hash function is of arbitrary length but the output is always of a predefined fixed length. Hash functions are pre image resistance which means that it is computationally hard to reverse the hash function and get the input value from its hash value. These functions are also second pre image resistance and even if the attacker knows the input and its hash value it's impossible to find another hash value for the same input. Collision resistance property of hash function makes it impossible to find two input of any length that result in same hash

4.2. DIGITAL SIGNATURES

Digital signatures are used to validate the authenticity and integrity of the message that is transferred between the two parties and is also used to authenticate the parties involved in the transaction. Digital signatures are based on public key cryptography also know as asymmetric cryptograph and it uses public and private key pair. A public key is the value provided by a designated authority and is known to everyone in the network. Private keys on the other hand are derived from the public key and are known only to its owner. To create a digital signature hash function is applied on the message to be signed to generate a message digest. The private key is then used to encrypt the digest to generate the digital signature. The digital signature is appended with the message to be send to the receiver .The receiver receives the message and verify the sender by decrypting the received digital signature using the sender's public key. The decrypting algorithm when applied on the digital signature gives us the message digest which is then compared to the message digest of the received message generated by the receiver. The matching of the message digest indicates that the message has been sent by the sender whose public key has been used by the receiver. It also shows that the message is authentic and has not been altered or tempered.

4.2.1 Necessity of Digital Signatures

Digital signatures are a powerful tool to achieve information security. The receiver of the message verifies the digital signature of a sender and assures that the message could have been created only by the sender as he only posses the private key thereby providing message authentication. The verification process will fail at the receiver end if the message has been altered by the attacker as the message digest of the altered message will be different from the received message digest and hence it provides data integrity. The sender cannot deny from the sending of the message as the message can only by signed by his private key which is only known to him therefore ensuring non repudiation. Therefore digital signatures are the necessity to make a system that is robust against security threats.

5. WORKING OF BITCOIN SYTEM

The working of Bitcoin payment transaction system is divided into two phases. The first phase involves the transaction and the second is updating of the blockchain with the newly processed transaction.

5.1 TRANSACTION

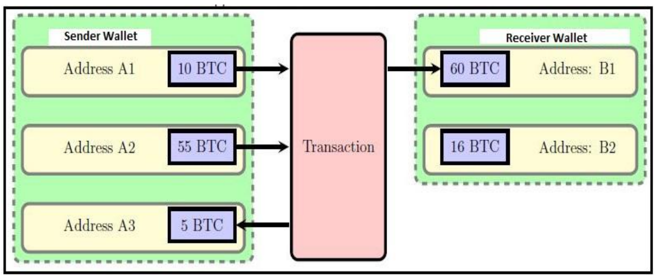

FIGURE 1: Bitcoin Transaction

In a bitcoin transaction system bitcoins reside in a bitcoin address and have a value associated with it. This value specifies the worth of the bitcoins that a particular address have and this information is publically available to every node. The ownership of these bitcoin addresses is controlled through digital signatures i.e. public and private key pair. Every bitcoin has a public key associated with it which is a unique public identity through which these bitcoins are indexed. The private key associated with the bitcoin address provides its ownership and full control. Therefore in order to claim and own bitcoins party must hold the private key of the claimed bitcoins. Every node on the network has a collection of bitcoin address with varied value known as wallet. A transaction in a bitcoin system is defined as the transfer of bitcoins from one or more source address to one or more destination address. To initiate the transfer of bitcoin first a transaction is created which have senders address as the source address and the receiver address as the destination along with the bitcoin balance. The bitcoin balance is the sum of all the values associated with the source address and is necessary to include in transaction as each transaction has multiple source and destinations. After the transaction is created it is signed using sender's private key and is broadcasted over the network. Every node on the network can verify the sender by using sender's public key. The digital signatures used ensure that the sender of the transaction can have only signed the transaction using its private key as it is assumed that the private key is known only to him.

5.2 UPDATING BLOCKCHAIN

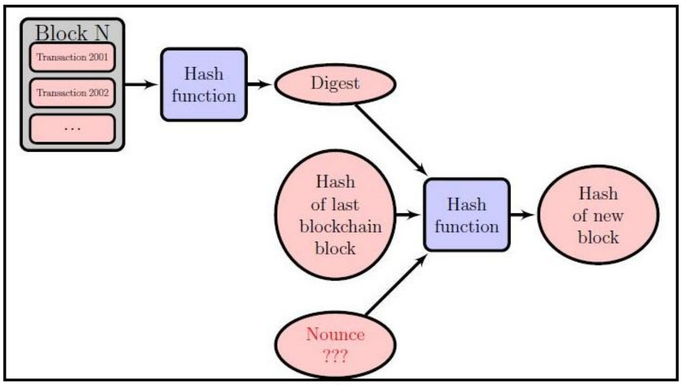

FIGURE 2: BlockChain Updating process

After the initial verification of the signed transaction a group of nodes also known as miners compete to record the transaction in a public ledger. Theses ledgers keep track of all the transactions that have been processed on the network in a chronological order. To determine the winning miner that will update the blockchain a predefined process known as proof of work is used. Proof of work consists of finding a byte string called as nounce which when combined with the transaction gives a hash value that has a specific property. In this case the hash should have a predetermined number of leading zeros. The miners first group the transactions that have been broadcasted since the last record on the blockchain in order to find solution. The block consisting of all new transactions is then used as the input to the cryptographic hash function to obtain digest. The digest together with a nounce and the hash of the previous block on the blockchain is feed as the input to another hash function to get the hash value which will be recorded in the blockchain. The first miner that finds the nounce broadcasts the information on the network and all the ledgers are updated. Since proof of work, uses one way cryptographic hash function finding such a nounce can only be possible by actually calculating the hash of the block for all possible nounce till the desired hash is obtained. It is therefore difficult to find a nounce that gives the desired output but it’s easy to verify it. The other nodes on the network can verify that the creator of the block has solved the proof of work as the nounce is the part of the broadcasted block that will eventually be updated on the blockchain. The miner who successfully carries out the proof of work process is incentivized. In most cases the reward is a predetermined amount of newly minted bitcoins and in rest of the cases the award is voluntary transaction fee that are paid by the creator of the transaction to the miner for processing and clearing their transactions. In this way the transactions are created and processed in a decentralized manner without the need for central third party.

6. BITCOIN SYSTEM ROBUSTNESS AGAINST SECURITY THREATS

Every transaction system that enters into the internet domain has to face and deal with two classical security threats. The first is fraud and bitcoin system deals with it by assuming that almost all the nodes on the network are honest and it excludes third party. By allowing nodes to transact directly the control of the whole system is decentralized thus reducing the chances of fraud by third parties. The nodes also check the validity of each and every transaction created by the sender using digital signatures. The second threats is Double spending when two or more transactions attempt to transfer the same coins multiple times then it is called as double spending attack . Bitcoin system uses peer to peer network to solve the problem of double pending whether it is done intentionally or by mistake. The peer to peer network keeps all the nodes updated about all the transactions that have taken place in the system .The network timestamp transaction by hashing them into an ongoing chain of block chain using hash based proof of work. The records that are generated by using proof of work cannot be altered without re finding the solution which are computationally time consuming to find and as long as the majority of the nodes are honest and controls maximum CPU power it is impossible for the attacker to find the solution. The transactions are accepted sequentially which guarantees that duplicated transactions are not accepted. The first transaction that is recorded on the blockchain is processed and subsequent transaction that claims same bitcoins is rejected and thereby removing any possibility of double spending attack.

7. ADVANTAGES OF USING BITCOIN

The bitcoin system facilitates its users with number of varied advantages. These advantages are

7.1. Information transparency

Bitcoin uses block chain to record all the transactions processed on the network that allow nodes to verify the transaction anytime.

7.2. No Trusted Third-party Interruptions

The most widely publicized benefit of bitcoin is that no banks and financial intermediaries are involved to process transactions therefore it provided greater degree of freedom to its users.

7.3 Global payments

Bitcoin can be used to do transactions globally without paying any extra processing fees and these transactions are almost processed immediately.

7.4 User Anonymity

Bitcoin purchases and transactions are never associated with the person identity and hence these can never be tracked back. In fact, the anonymous Bitcoin address that is generated for user purchases changes with each transaction.

7.5 No Risk of charge back

Bitcoin transactions are non reversible and once the transaction is processed the ownership of the coins changes and there is no risk involved when receiving bitcoins.

7.6 Transactions are non taxable

There is no way for third parties to keep track of the transactions no sales tax is added onto any purchase.

7.7 Low Transaction Fees

Bitcoin transaction uses peer to peer protocol and there is no intermediary party involved in the processing of the transaction and hence the transaction cost s very low.

7.8 Low risk of theft

Bitcoin ownership can only be changed by the owner or when they are sent to other person account and therefore there is no risk of getting bitcoins stolen from the wallet.

8. DISADVANTAGES OF BITCOIN

8.1 Untraceable

This feature of bitcoin attracts the attention of the criminals and criminals can use bitcoin for the illegal buying of goods such as drugs and arms and ammunition as the transactions are not associated with the directly people making them untraceable.

8.2 Wallets Can Be Lost

Bitcoins are stored in the form of transactions on the owners hard disk and if the hard disk crashes or is attacked by the virus there is no way to recover the lost bitcoins.

8.3 No Buyer Protection

When goods are bought using Bitcoins, and the seller doesn’t send the promised goods, the buyer of the goods is not able to do anything as these transactions are non reversible.

8.4 No Valuation Guarantee

There is no central authority that keeps the value of the bitcoin regulated. If the maximum number nodes on the network decide to dump the bitcoin its value will be degraded immensely which will incur a huge loss to the person who have invested large money on it.

8.5 No Physical Form

Bitcoins do not have a physical form and hence cannot be used in physical stores. It would always have to be converted to other currencies.

9. Conclusion

We have explored the first decentralized payment system Bitcoin that uses peer to peer protocol and distributed timestamp service to keep track of every transaction. The transactions are processed using proof of work. The system effectively deals with all the security concerns and has successfully eliminated the need for third party. It has also encouraged small and casual transaction by reducing the transaction fees to almost negligible. Bitcoin system has used the basic cryptographic concepts in a new way to give us a new electronic payment system that is faster as well as cost effective. It efficiently makes use of the computation power to generate new bitcoins that can further be used to buy goods and services. Thus we can conclude that bitcoin is an emergent technology and it rapids growth in number of transactions proves that it will surely replace the conventionally currency transaction over internet.

References

[1] Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto October 31, 2008 www.cryptovest.co.uk

[2] Information Propagation in the Bitcoin Network, Christian Decker,_ Roger Watten hofer, 13-th IEEE International Conference on Peer-to-Peer Computing.

[3] Introduction to Bitcoin: Unique Bitcoin features, Jonathann Levin ,University of Oxford, Department of Economics

[4] Majority is not Enough: Bitcoin Mining is Vulnerable, Ittay Eyal and Emin Gun Sirer Department of Computer Science, Cornell University,ittay.eyal@cornell.edu,15 Nov 2013.

[5] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar. On bitcoin and red balloons. In Proc. of Electronic Commerce, 2012.

[6] Matthew Elias. Bitcoin: Tempering the digital ring of gyges or implausible pecuniary privacy. SSRN 1937769, 2011.

[7] Ilja Gerhardt and Timo Hanke. Homomorphic payment addresses and the pay-to-contract protocol. CoRR, abs/1212.3257, 2012.

[8] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. 2013.

[9] F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system In Proc. of the Conference on Social Computing (socialcom), 2011.