ISSN:0975-9646

Review Paper on Bitcoin a Secured Transaction over p2p Network.

Unnati A. Dabre[#], Prof. Dr. Prashant V. Ingole[*]

[#]*M.E Student., CSE Department,*
G.H. Raisoni College of Engineering and Management,
S.G.B.A.U. University, Amravati, India
[*]*Principal, G.H. Raisoni College of Engineering and Management,*
S.G.B.A.U. University, Amravati, India

***Abstract*—In online transaction it always requires intermediate parties, like PayPal or MasterCard. Security of transaction process is difficult to implement. There is no privacy of information as the information passes through the internet and it may be accessed by strangers. For more secure transaction which does not involve third party intermediary, a new concept of Bitcoin is introduced. Bitcoin is a digital or virtual currency that uses peer-to-peer technology to facilitate instant payments. Bitcoin is a type of alternative currency known as a crypto currency, which uses cryptography for security, making it difficult to counterfeit. Bitcoin issuance and transactions are carried out collectively by the network, with no central authority. Storage and transfer of money safely, securely, cheaply and quickly to the customers anywhere in the world is possible with the introduction of Bitcoin. Bitcoin is an open-source, peer-to-peer digital currency. Among many other things, what makes Bitcoin unique is that it is the world's first completely decentralized digital-payments system.**

***Keywords*— Bitcoin, Payment transaction, virtual currency, third party transaction, Bitcoin wallet, digital signature, network security.**

I. INTRODUCTION

A peer-to-peer (P2P) network is a type of decentralized and distributed network architecture in which individual nodes in the network (called *"peers"*) act as both suppliers and consumers of resources, in contrast to the centralized client–server model where client nodes request access to resources provided by central servers online transactions always need a trusted third-party Intermediary. Commerce on the Internet has come to trust almost on financial institutions serving as trusted third parties to process electronic payments. The cost of mediation increases transaction costs, Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party. What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. For example, if Alice wanted to send $200 to Bob using the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders' balances. In the above transaction the Intermediaries, PayPal deducts the amount $200 from Alice account and adds it to Bob's account. Digital money could be spent twice, without such intermediaries. Imagine that, there are no intermediaries with ledgers. In this case digital cash is simply a computer file. Transaction of sending $200 between Alice and Bob is possible by attaching a money file to a message. But as in the case of email, sending an attachment to someone does not remove it from the sender's computer. The copy of the money file would be retained with Alice after she had sent it to Bob. Alice then could easily send the *same* $200 to anyone other she wants. In the field of computer science, this is known as the "double-spending" problem. Until Bitcoin it could only be solved by employing a ledger-keeping trusted third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. [1][2]

II. OPERATION

If Alice sends some bitcoins to Bob, that transaction will have three pieces of information 1)An input- This is a record of which bitcoin address was used to send the bitcoins to Alice in the first place. 2) An amount- This is the amount of bitcoins that Alice is sending to Bob. 3)An output- This is Bob's bitcoin address. Every transaction that takes place in the Bitcoin economy is registered in a public, distributed ledger, which is called the block chain. The block chain is now the base to identify that the Bitcoin haven't previously spent. Every new transactions are checked against the block chain created at the time of first transaction to ensure that the same bitcoins haven't been spent earlier, thus eliminating the double-spending problem. The place of intermediary in case of Bitcoin is takes the global peer-to-peer network which is composed of thousands of users. Alice and Bob can transact without PayPal by using the Bitcoin. One thing to be noted that, the transactions on the Bitcoin network are not

denominated in currencies like dollars or Euros as the case was in on PayPal. The transactions are now denominated in Bitcoins. This makes Bitcoin a virtual currency in addition to a decentralized payments network. As in the case of conventional currencies the value of the Bitcoin is not derived from gold or government fiat, but from the value that people assign to it. On an open market, the dollar value of a bitcoin is determined, as is the exchange rate between different world currencies.[1][5]

A. Transaction Process of Bitcoin.

As already stated the trusted third-party intermediary is always required for online transactions. For example, if Alice wanted to send $200 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard.

Let us define an electronic coin as a chain of digital signatures. Each owner now, transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of transactions. When someone looks at Alice's public key, he/she can verify that the transaction was indeed signed with her private key, that it is an authentic exchange, and funds are transferred to Bob and he is now the new owner of the funds. This transaction is one of the 'block' of the block chain. In this way the transaction and the transfer of the ownership of the Bitcoin is recorded, time stamped and displayed. It is ensured by Public-key cryptography that all computer systems in the network have consistently updated and verified records of all such transactions within the Bitcoin network, which prevents fraud and double-spending.

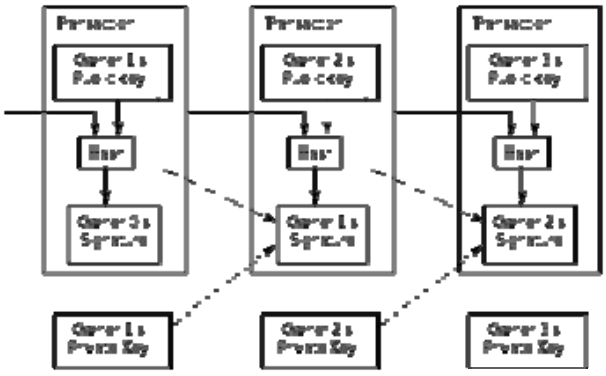

Fig. 1 Transaction process of Bitcoin.[1]

It is already discussed that the Bitcoin is a peer-to-peer network, hence there is no central authority charged with either creating currency units or in the verification of transactions. This network, thus created depends on users who logged by providing their computing power to does the reconciliation of transactions. These users are called as 'miners' since these users are rewarded for their work with newly created Bitcoins. In this way the Bitcoins are mined or say created as thousands of dispersed computers solve complex math problems and this in turn verify the transactions in the block chain.[1][4]

B. Avoiding Double-Spending

It is to be noted that, for the Bitcoin network there is not required to set up the 'Account'. No e-mail Id, username or passwords are required to hold or spend the Bitcoins in the Bitcoin network. Every money balance is simply coordinated with an address and its two keys viz. public key and private key. Only these two keys are utilized when the transaction takes place and there is no need to register them anywhere in advance. The identities of the transaction parties are secured. The transaction does not need to know the identity of money sender and the receiver in the same way that a shop keeper does not know a cash-paying customer's name.

Each person involved in the transaction can have many such addresses, each with its own balance. This may make it very difficult to know which person owns what amount. In the example mentioned earlier Bob receives the Bitcoin from Alice and Charlie receives the Bitcoin from Bob. In order to protect the privacy, Bob can generate a new public-private key pair for each individual receiving transaction and the Bitcoin software is so developed as to encourage this behavior by default. In the example from above, when Charlie receives the bitcoins from Bob, he will not be able to identify who owned the bitcoins before Bob.

When some money is spent successfully more than ones, the problem of Double-spending arises. This double-spending is protected in Bitcoin by verifying each transaction added to the block chain verifies and ensures whether the input inputs for the transaction had been previously spent or not. The systems adapted by other electronic systems to prevent double-spending is to maintain a master authoritative source, which follows business rules for authorizing each transaction. Bitcoin uses a decentralized system as a preventative measure. In decentralized system consensus among nodes following the same protocol is substituted for a central authority. The risk of exposure to fraudulent double-spending goes on reducing as the transaction gain confirmations. [1][4]

C. Block chain

A block chain is a database of transaction which is shared by all nodes participating in a system based on the Bitcoin protocol. A full copy of a currency's block chain contains every transaction ever executed in the currency. With this information, one can find out how much value belonged to each address at any point in history. Every block contains a hash of the previous block. This has the effect of creating a chain of blocks from the genesis block to the current block. Each block is guaranteed to come after the previous block chronologically because the previous block's hash would otherwise not be known. Each block is also computationally impractical to modify once it has been in the chain for a while because every block after it would also have to be regenerated. These properties are what make double-spending of bitcoins very difficult. The block chain is the main innovation of Bitcoin.

A hash algorithm is used to disburse huge amount. The exactly same data always results in the same Hash. However if the data is modified/changed by even one bit will completely change the hash. Usual practice of writing the hashes is as hexadecimal, as they are large numbers, like all computer data. [1][3]

III. PRIVACY

The earlier banking model achieves a level of privacy by limiting access to information to the involved parties and the trusted third party. The importance to announce all transactions publicly precludes this method, but secrecy can still be maintained by breaking the flow of data in another place by keeping public keys anonymous. The people can see that someone is sending an amount to someone else, but without data linking the transaction to anyone. This is like stock exchanges, where data is released, and the time and size of individual trades, the "tape", is made publically available, but without displaying who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unrestricted with multiple-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

As it gives the privacy from third party, at the same time it is having one problem that bitcoin payments are irreversible as there is no third party authority. The only way to get a payment back is if the person who received the funds sends them back to sender. If a person ever lost access to his or her wallet permanently, then whatever Bitcoins contained in there would be lost to that person.

IV. BENEFITS

The reasons to make global use of bitcoin are as follows.

A. Easy and Fast Payments

Bitcoin payments can be done easily using an smartphone app, using software on a computer or online on the web. There is no need of a credit card or a PIN or for any documents to be signed. All that is usually required is only to know the address to which you are transferring amounts. As bitcoin is a decentralized payment system, payments and transfers are very fast, usually done in seconds to minutes. It will bypass banks which take days to weeks to complete transfers especially in case of international transfers.

B. Secure

The cryptography used in bitcoin remains transaction more secure. No other person/entity can make transfer or payments except owner of wallet. However security of using bitcoin totally depends upon on the users who have to take steps to protect their bitcoin wallet.

C. Offers Some Degree of Anonymity

The identities behind Bitcoin wallets are private. Wallets use addresses in transactions and these are also created privately. Using an address once for a single transaction ensures privacy and anonymity. However, Bitcoin transactions are public, traceable and are permanently stored on the Bitcoin network. IP addresses of users on the Bitcoin network can also be logged. Therefore, if a user employs a single address for multiple transactions, it is possible to initiate a trace and if the IP address of the user has been logged his or her identity may be uncovered. This can be prevented by using a different address for every different transaction and hiding a computer's IP address using a service like Tor. [4]

D. Low or No Transaction Fees

Banks and payment processing companies typically charge fees to conduct payments and fund transfers on customer’s behalf. With Bitcoin these charges are eliminated. To transfer money to family or friends requires zero fees. In cases where there are transaction fees, they are very low compared to bank charges. Bitcoin transaction fees are usually a voluntary fee to enable faster confirmation of your transaction. [4][5]

V. CONCLUSION

Bitcoin is totally new concept in transfer & payments, as it is new, it’s in the process of being understood and adopted by large numbers of consumer merchants & investors all over the world. As this process continues the reason to start using bitcoins grows rapidly. Many new finance companies are offering more professional and consumer friendly solutions to attract consumers. To make life fast & easy just like mail anybody in the world with computer or a mobile device with internet access can have a bitcoin address. With bitcoin address and bitcoin wallet it is possible to send and receive bitcoins anybody, anywhere in the world. In bitcoin network people can transact bitcoins with another directly on the internet without any central server or entity like government central bank, corporation & foundation that control network.

REFERENCE

[1] Nakamoto, S.: Bitcoin: *A peer-to-peer electronic cash system* (2009).
[2] Bitcoin.org/bitcoin.wiki/bitcoin.pdf.
[3] BlockChainandBlock Explorer- Online browsers of Bitcoin published transactions.
[4] Criss kose, Mike koss, *A bitcoin primer –Coin Lab* (1 Jan 2012)
[5] Jerry Brito, Andrea Castillo, *Bitcoin - A primer for policymaker*, Center Copyright © 2013.