Digital Assets Technology - Blockchain

Adithya R[1], Barath Kumar S[2], Bhalahariharan V[3], Suivthavani P[4]
[1, 2, 3, 4] Dept of Computer Science
[1, 2, 3, 4] Sri Shakthi Institute of Engineering and Technology

Abstract- *The technology that is used for having some kind of digital asset is blockchain. A blockchain is distributed server environment of the public leger which maintains records of all transactions that is participated between parties. Each transaction is maintained in a public ledger which is regularly monitored by most of participants in the system. The main objective for blockchain establishment is to create a centralized environment where leger is maintained by multiple users at a time through internet.*

I. INTRODUCTION

A blockchain is typically a distributed database of records or public ledger of all digital events that have been executed and shared among participating parties. Each and every transaction in the public ledger is verified by agreement of most of the participants in the system. Once entered information can never be erased. The blockchain contains a certain verifiable record of every single transaction that have ever made. To make use of a basic analogy, it is easy to take a cookie from a cookie jar, kept in a secluded place than stealing the cookie from a cookie jar kept in a market place, being observed by thousands of people. This may be bit doggy but many have experienced this earlier Internet works in distributed consensus manner which is more similar to blockchain . So this might be a digital asset for future.

II. HISTORY OF BLOCKCHAIN

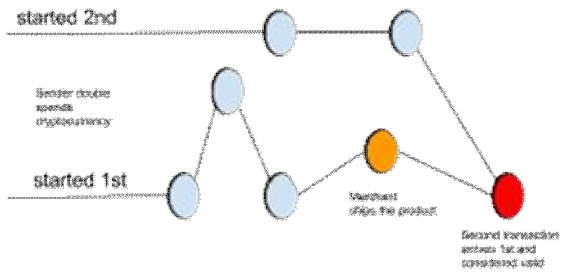
In year 2008, an individual or group writing under the name of Satoshi Nakamoto published a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System". This paper describes a peer-to-peer version of the electronic cash that would allow online payments to be sent directly from one party to another without make use of a financial institution. Bitcoin was the first realization of this concept. Now word cryptocurrencies is the label that is used to describe all networks and mediums of exchange that uses cryptography to secure transactions-as against those systems where the transactions are channeled through a centralized trusted entity. However Satoshi Nakamoto remains anonymous since beginning but his their idea is getting popular and popular.

III. HOW DOES BLOCKCHAIN WORK

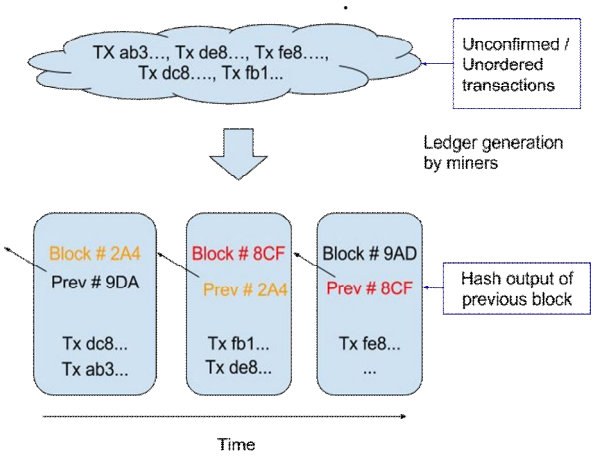
The blockchain technology is applicable to anydigital asset transaction exchanged online. Internet commerce is exclusively attached to the financial institutions serving as the trusted third party who process and mediate any electronic transaction. The role of trusted third party is to validate, safeguard and preserve transactions. A certain percentage of fraud is unavoidable in online transactions and that needs mediation by financial transactions. This results in high transaction costs. Let us take blockchain implemented cryptocurrency ***BITCOIN*** as an example. Bitcoin uses cryptographic proof instead of the trust in the third party for two willing parties to execute an online transaction over the Internet. Each transaction is protected through a digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to spend money, owner of the cryptocurrency needs to prove the ownership of the "private key". The entity receiving the digital currency verifies the digital signature –thus ownership of corresponding "private key"--on the transaction using the "public key" of the sender. Each transaction is broadcast to every node in the Bitcoin network and is then recorded in apublic ledger after verification. Every single transaction needs to be verified for validity before it is recorded in the public ledger. Verifying node needs to ensure two things before recording any transaction:

1. Spender owns the cryptocurrency—digital signature verification on the transaction.
2. Spender has sufficient cryptocurrency in his/her account: checking every transactionagainst spender's account ("public key") in the ledger to make sure that he/she hassufficient balance in his/her account.

However, there is question of maintaining the order of these transactions that are broadcast toevery other node in the Bitcoin peer-to-peer network. The transactions do not come in order inwhich they are generated and hence there is need for a system to make sure that double-spending of the cryptocurrency does not occur. Considering that the transactions are passed node by node through the Bitcoin network, there is no guarantee that orders in which they are received at a node are the same order in which these transactions were generated.



This means that there is need to develop a mechanism so that the entire Bitcoin network can agree regarding the order of transactions, which is a daunting task in a distributed System



The Bitcoin solved this problem by a mechanism that is now popularly known as Blockchain technology. The Bitcoin system orders transactions by placing them in groups called blocks and then linking these blocks through what is called Blockchain. The transactions in one block are considered to have happened at the same time. These blocks are linked to each-other (like a chain) in a proper linear, chronological order with every block containing the hash of the previous block. There still remains one problem. Any node in the network can collect unconfirmed transactions and create a block and then broadcasts it to rest of the network as a suggestion as to which block should be the next one in the blockchain. How does the network decide which block should be next in the blockchain? There can be multiple blocks created by different nodes at the same time. One can't rely on the order since blocks can arrive at different orders at different points in the network.

Bitcoin solves this problem by introducing a mathematical puzzle: each block will be accepted in the blockchain provided it contains an answer to a very special mathematical problem. This is also known as "proof of work"—node generating a block needs to prove that it has put enough computing resources to solve a mathematical puzzle. For instance, a node can be required to find a "nonce" which when hashed with transactions and hash of previous block produces a hash with certain number of leading zeros. The average effort required is exponential in the number of zero bits required but verification process is very simple and can be done by executing a single hash.

IV. BUSINESS VIEW

Blockchain technology is finding applications in both financial and non-financial areas that traditionally relied on a third trusted online entity to validate and safeguard online transactions of digital assets. There was another application "Smart Contracts" that was invented in year 1994 by Nick Szabo. It was a great idea to automatically execute contracts between participating parties. However, it did not find usage until the notion of crypto currencies or programmable payments came into existence. Now two programs blockchain and smart contract can work together to trigger payments when a preprogrammed condition of a contractual agreement is triggered. Smart Contracts are really the killer application of the cryptocurrency world. Smart contracts are contracts which are automatically enforced by computer protocols. Using blockchain technology it has become much more easier to register, verify and execute Smart Contracts. Open source companies like Ethereum and Codiusare enabling Smart Contracts using blockchain technology. Many companies which operate on bitcoin and blockchain technologies are supporting Smart Contracts. Many cases where assets are transferred only on meeting certain conditions which require Lawyers to create a contract and Banks to provide Escrow service can be replaced by Smart Contracts.

V. CHALLENGES

BlockChain is a promising breakthrough technology. As we described before, there are vast array of applications or problems that can be solved using BlockChain based technology. That spans from Financial (remittance to investment banking) to non-financial applications like Notary services. Most of these are radical innovations. As it happens with adoption with radical innovations, there are significant risks of adoption.

Behavior change: Change is constant, but there is resistance to change. In the world of a non-tangible trusted third party, that BlockChain presents, customers need to get used to the fact that there electronic transactions are safe, secured and complete. The present day intermediaries like Visa or Mastercard (in case of a credit cards) will also go through change roles and responsibility. We envision that they will also invest and move their platforms to be BlockChain-based.

They will continue to provide the customer relationship kind of services.

Government Regulations: In the new world of BlockChain-based transactions, Government agencies like FTC, SEC, etc may slow down the adoption by introducing new laws to monitor and regulate the industry for compliance. In USA, this may in a way help adoption as these agencies carry customer trust. In more controlled economies like in China, the adoption will face significant headwind.

Quantum Computing : The basis of BlockChain technology relies on the very fact that it is mathematically impossible for a single party to game the system due to lack of needed compute power. But with the advent of Quantum Computers (in future), the cryptographic keys may be easy enough to crack through sheer brute force approach within a reasonable time. This will bring the whole system to its knee. The counter-argument would be for keys to become even stronger so that they may not
be easy to crack.

VI. CONCLUSION

The distributed ledger functionality coupled with security of BlockChain, makes it very attractivetechnology to solve the current Financial as well as non-financial business problems.

There is enormous interest in BlockChain based business applications and hence numerous Startups working on them. The adoption definitely faces strong headwind as described before. The large Financial institutions like Visa, Mastercard, Banks, NASDAQ, etc., are investing in exploring application of current business models on BlockChain. In fact, some of them are searching for the new business models in the world of BlockChain. Some would like to stay ahead of the curve in terms of transformed regulatory environments of BlockChain.

To conclude, we envision BlockChain to go through slow adoption due to the risks associated. Most of the Startups will fail with few winners. We should be seeing significant adoption in a decade or two.

REFERENCES

[1] Bitcoin: A Peer-to-peer Electronic Cash System
[2] Smart Contracts: Nick Szabo
[3] Formalizing and Securing Relationships on Public Networks: Nick Szabo
[4] Introduction To Smart Contracts
[5] The Ultimate List of Bitcoin and Blockchain White Papers
[6] Bitcoin Tutorial
[7] A Risk-Based View of Why Banks are Experimenting with Bitcoin and the Block
[8] Blockchain:The Information Technology of The Future
[9] Bitcoin 2.0 Applications
[10] Beyond Bitcoin:How the Blockchain Can Power a New Generation of Enterprise Software
[11] Forget Bitcoin-What is the Blockchain and Why Should You Care?