Blockchain Technology

Miss. Amruta P. Deshmukh [1], Prof. V. B. Gadicha[2]
[1]Dept of Computer Science and Engineering
[2]HOD, Dept of Computer Science and Engineering
[1, 2] P. R. Pote COET Amravati, Maharashtra, India

Abstract- *Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The interest in Blockchain technology has been increasing since the idea was coined in 2008. The reason for the interest in blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and especially form the perspective for technical challenges and limitations. Our objective is to understand the current research topic, challenges and future directions regarding Blockchain technology form the technical perspective. A blockchain is essentially a distributed database of records or public ledger of all transaction or digital event that have been executed and shared among participating parties. Each transaction in the public ledger is verified consensus of a majority of the participant in the system. And once entered, information can never be erased.*

Keywords- Bitcoin, Blockchain technology, cryptocurrency,

I. INTRODUCTION

The blockchain is the publicly verifiable, distributed transaction ledger that secure the Bitcoin network against double-spending, forgery and reversed transaction. The block chain is a data structure that consists of time ordered, linked blocks that contain a number of transaction. The blocks are linked in the sense that each block includes the ID of the previous block in the chain. ID of each block itself is the cryptographic hash of its contents. thus it becomes apparent that each block depend on the previous block thus forming a chain that in order to be recreated all blocks leading to the current one will have to be recreated as well.

Bitcoin is the most popular example that is intrinsically tied to blockchain technology. To make the function of the blockchain more apparent let us look at the following scenario: User Bob want to send an amount of bitcoin let's assume 1.5 BTC in this example to user Alice.Bob makes a transaction referencing a number of previous truncations called input in the Bitcoin protocol whose value sums to 1.5 BTC, and the addressed to Alice[3]. This transactionis broadcast to Bitcoin network. Now the network node have to confirm that, the referred input does, firstly indeed belong to Bob and secondly it is unspent, i.e has not been referenced as the input of a previous transaction. Once this confirmation is granted the ownership of 1.5 BTC is transferred for Bob to Alice. Now Alice can proceed to provide the service that Bob is paying for.

History of Bitcoin:

The 2008 financial crisis caused a lot of people to lose trust in banks as trusted third parties. Many questioned whether banks were the best guardians of the global financial system. Bad investment decisions by major banks had proved catastrophic, with rippling consequences Bitcoin was a "peer-to-peer electronic cash system." It would allow for online payments [to move] from one party to another without going through a financial institution."

Bitcoin is a decentralized, public ledger. There is no trusted third party controlling the ledger. Anyone with bitcoin can participate in the network, send and receive bitcoin, and even hold a copy of this ledger if they want to. In that sense, the ledger is "trustless" and transparent[2].It has grown in popularity since then.

–**2008**

• August 18 Domain name "bitcoin.org" registered
• October 31 Bitcoin design paper published
• November 09 Bitcoin project registered atSourceForge.net

–**2009**

• January 3 Genesis block established at 18:15:05GMT
• January 9 Bitcoin v0.1 released and announced on the cryptography mailing list
• January 12 First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

The popularity of the Bitcoin has never ceased to increase since then.A bitcoin or a transaction can't be changed, erased, copied, or forged – everybody would know.

II. PROPOSE WORK

There are three principal technologies that combine to create a blockchain. These technologies are: 1) private key cryptography, 2) a distributed network with a shared ledger and 3) an incentive to service the network's transactions, record-keeping and security.

The following is an explanation of how these technologies work together to secure digital relationships.

2.1 Cryptographic keys

Two people wish to transact over the internet. Each of them holds a private key and a public key. The main purpose of this component of blockchain technology is to create a secure digital identity reference. Identity is based on possession of a combination of private and public cryptographic keys. The combination of these keys can be seen as a dexterous form of consent, creating an extremely useful digital signature[2]. this digital signature provides strong control of ownership.

2.1.1 Identitys

But strong control of ownership is not enough to secure digital relationships. While authentication is solved, it must be combined with a means of approving transactions and permissions (authorisation).

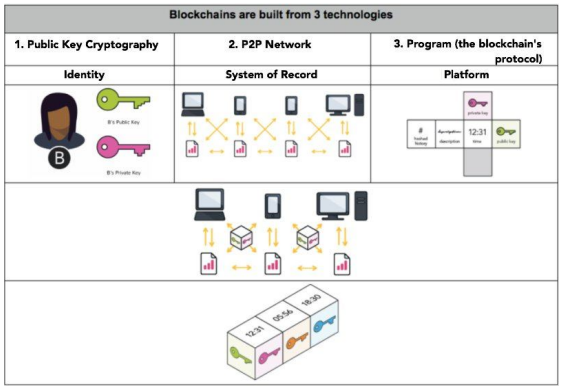

Figure 2.1: Combination of three technology

2.2 A Distributed Network

The benefit and need for a distributed network can be understood by the 'if a tree falls in the forest' thought experiment. In short, the size of the network is important to secure the network[1]. That is one of the bitcoin blockchain's most attractive qualities -- it is so large and has amassed so much computing power. At time of writing, bitcoin is secured by 3,500,000 TH/s, more than the 10,000 largest banks in the world combined. Ethereum, which is still more immature, is secured by about 12.5 TH/s, more than Google and it is only two years old and still basically in test mode.

2.2.1 System of record

When cryptographic keys are combined with this network, a super useful form of digital interactions emerges. The process begins with A taking their private key, making an announcement of some sort -- in the case of bitcoin, that you are sending a sum of the crypto-currency and attach it to B's public key.

2.2.2 Protocol

A block - containing a digital signature, timestamp and relevant information is then broadcast to all nodes in the network.

2.3 Network servicing protocol

The type, amount and verification can be different for each blockchain. It is a matter of the blockchain's protocol - or rules for what is and is not a valid transaction, or a valid creation of a new block. The process of verification can be tailored for each blockchain. Any needed rules and incentives can be created when enough nodes arrive at a consensus on how transactions ought to be verified.

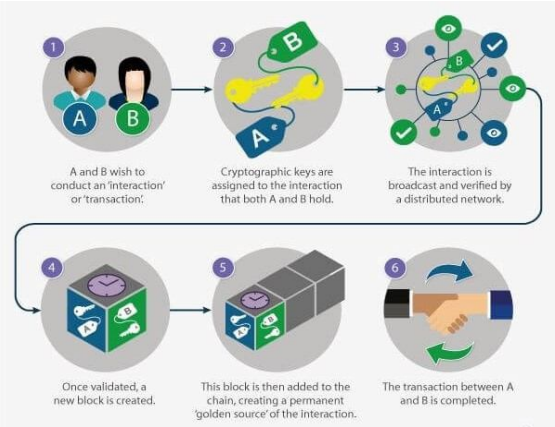

Figure 2.2: Working of blockchain technology

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.

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 transaction against spender's account ("public key") in the ledger to make sure that he/she has sufficient balance in his/her account.

III. BLOCKCHAIN TECHNOLOGY USE CASES IN FINANCIAL SERVICES

One of the most discussed topics in the financial services industry today is blockchain technology.

1. Blockchain technology – speeding up and simplifying cross-border payments

The transfer of value has always been an expensive and slow process. This is particularly true for cross-border payments. Blockchain technology is able to speed up and simplify this process - and also reduces the costs significantly.

2. Blockchain technology – the future of share trading

Share trading will soon be impacted by blockchain technology. Utilizing blockchain technology allows for greater trade accuracy, and a shorter settlement process

3. Blockchain technology – the benefits of smart contracts

One of the most promising applications of blockchain technology is the smart contract. It can execute commercial transactions and agreements automatically. It also enforces the obligations of all parties in a contract – without the added expense of a middleman.

4. Blockchain technology – how to improve online identity management

When identity management is moved to blockchain technology, users are able to choose how to identify themselves and who will be informed. They still need to register their identity on the blockchain somehow, but after that, they can re-use that identification for other services.

5. Blockchain technology – loyalty and rewards

Blockchain technology offers many benefits, including transparency and traceability of transactions. This will help banks and insurers to create a more captivating loyalty and rewards program that fits 24/7 performance management and enhances engagement.

IV. CHARACTERISTICS OF BLOCKCHAIN

- Very secure due to use of crypto-currency
- Capable of near real-time synchronization or settlement
- Very low transaction costs
- A peer-to-peer network for discovery and communication
- Typically based on open source software-changes are developed by the community
- Transparency and traceability of transaction is typically superior to current systems but user identification may be weaker or nonexistent

V. LIMITATIONS OF BLOCKCHAIN

- Limited scalability of public blockchain
- The public blockchain processes 3-20 transaction per second
- VISA handles around 2000 transactions per second
- Improving transaction processing rate

VI. PRO'S AND CON'S OF BLOCKCHAIN

6.1 PRO'S OF BLOCKCHAIN

- Anything of value can be transferred and saved safely and confidentially without alteration
- Transaction areVerifiable by aVast, peer-to-peerGlobal network
- Crypto-currencies are not able to be "frozen" in the case of economic crisis
- There will on longer be the need for intermediaries such as bank, lawyers,
- Transactions are irreversible.

6.2 CON'S OF BLOCKCHAIN

- Scammers and other seedy characters can use the anonymity to their advantage to do evil.
- Hacks and manipulation can still occur
- The majority of government, offices, retailers, do not understand, let alone use/accept crypto-currencies as valid payment
- Many people are currently employed in institution that serve as intermediaries there will certainly be a lot of resistance
- Transactions are irreversible.

VII. CONCLUSION

Blockchain technology can be used to maintain a decentralized transaction ledger. many new application areas possible, both in finance and outside. whetherblockchain work in practice without crypto-currencies remains to be seen. Blockchain fits well with the decentralized architecture of the internet.

REFERENCES

[1] spectrum.ieee.org/telecom/internet/wall-street-firms-to-move-trillions-toblockchains-in-2018
[2] spectrum.ieee.org/computing/networks/blockchains-will-allow-rooftop-solarenergy-trading-for-fun-and-profit
[3] techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-theblockchain/
[4] http://ieeexplore.ieee.org/document/7996119/
[5] http://standards.ieee.org/news/2017/blockchain_adoption_in_the_pharmaceutical_enterprise.html
[6] http://www.telemedmag.com/article/new-kids-blockchain/
[7] http://ieeexplore.ieee.org/document/7968630/
[8] https://www.marketwatch.com/story/hundreds-of-millions-of-dollars-in-ethereumfrozen-in-accidental-coding-mistake-2017-11-07
[9] https://www.theregister.co.uk/2017/11/07/parity_wallet_destroys_280m_ethereum/
[10] https://standards.ieee.org/develop/project/825.html
[11] http://standards.ieee.org/about/sasb/iccom/IC17-012-01_SupplyChain_Trials.pdf
[12] https://standards.ieee.org/about/sasb/iccom/IC17-011 -01Connectivity_Harmonization_of_the_Digital_Citizen.pdf