International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

A Survey on Bitcoin –The Blockchain

Mrs. Sonam Patil, Mr. Chetan Awati, Mrs. Arati Gaikwad
Department of Information Technology, D Y Patil College of Engineering Akurdi, Pune Assistant Professor
Department of Technology, Shivaji University, Kolhapur Assistant Professor
Department of Information Technology, D Y Patil College of Engineering, Akurdi, Pune Assistant Professor
Email: skh9624@gmail.com, chetan.awati@gmail.com, aratig.2010@gmail.com

Abstract-Blockchain is a platform for executing transactional services. The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. It is spanned over multiple organizations or individuals who may not trust each other. Blockchain technology enables distributed public ledgers that hold immutable data in a secure and encrypted way and ensure that transactions can never be altered. An append-only shared ledger of digitally signed and encrypted transactions replicated across a network of peer nodes By allowing digital information to be distributed but not copied, blockchain technology created the backbone of a new type of internet. This technology is specifically devised for the digital currency, Bitcoin. More attempts are been made to be applied on blockchains. Blockchain has led a very high impact on the lifestyles of all human beings. This paper will give a survey of what is bitcoin, blockchain and its applications.

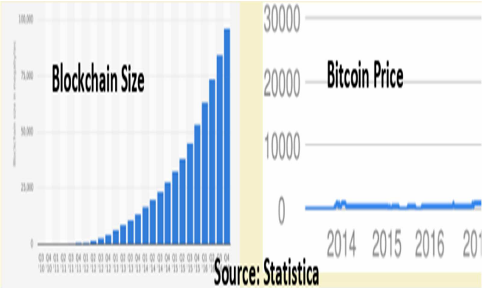
Index Terms-Blockchain, bitcoin, cryptocurrency, decentralized.

1. INTRODUCTION

A blockchain is a distributed ledger capable of maintaining an immutable log of transactions happening in a network. It is a platform for executing transactional services. This Technology has attracted significant scientific interest in may research areas including Internet of Things, Security and so on. It is a decentralized computation and information sharing platform that enables multiple authoritative domains, which do not trust each other to cooperate in a rational decision making process. In a decentralized system there are multiple points for coordination whereas in a distributed system everyone collectively execute the job. Every node in the system maintains a local copy of the global data sheet. Blockchain plays a role like a public ledger. We need to ensure proper protocols for commitment during each valid transaction, local copies are consistent and updated, data is tamper proof and authentic. A block in a blockchain is a container data structure that contains a series of transactions. Blockchain and Bitcoin are two different things. Bitcoin is a Cryptocurrency put forth in 2009. It is the first blockchain application, permissionless – Open to anyone. Consensus achieved through 'Proof of Work' and requires mining - resource intensive.

2. BITCOIN

The Bitcoin was invented by an unknown group or person under the pseudonym Satoshi Nakamoto as stated in "Bitcoin: A peer-to-peer electronic cash system." a research study completed after the UnitedStates Subprime mortgage crisis [1] in 2008. CNNMoney [2] define Bitcoin as "…a new currency that was created in 2009 by an unknown person using the aliasSatoshi Nakamoto. Transactions are made with no middle men. There are no transaction fees and no need to give your real name. Wikipedia, on the other hand describe Bitcoin as "… a worldwide cryptocurrency and digital payment system called the first decentralized digital currency, as the system works without a central repository or single administrator [3]." Bitcoins are generated during the mining – each time a user discovers anew block. The rate of block creation is adjusted every 2016 blocks to aim for aconstant two week adjustment period.The number of bitcoins generated per block is set todecreasegeometrically, with a 50% reduction for every 210,000 blocks, orapproximately 4 years.Thus, we can infer that Bitcoin is a cryptocurrency and digital payment system that is decentralized with no middle men and no transaction fees, however the miners will get their reward if they can prove the transaction, otherwise known as proof of work (PoW) or Proof of Stake (PoS).



Source: Statistica

Fig. 3.1 Bitcoinblockchain size

3. ACTORS IN A BLOCKCHAIN SOLUTION

1. Blockchain Architect: Responsible for the architecture & design of the blockchain solution.
2. Blockchain user: The business user working in the business network is not aware of the blockchain.
3. Blockchain Regulator: It has an overall responsibility in a business network. The regulators may require broad access to the ledgers contents.
4. Blockchain Developer: The application developer and smart contracts that interact with blockchain and are used by blockchain users.
5. Blockchain operator: It manages and monitors the blockchain network. Each network has a blockchain operator.
6. Membership services: It manages different types of certificates which are required to run a permissioned blockchain.
7. Traditional processing platform: An existing computer system which may be used by the blockchain to augment processing. This system may also need to initiate requests into the blockchain.
8. Traditional data sources: An existing data system which may provide data to influence the behavior of smart contracts.

4. BITCOIN VALUE PROPOSITION

The last few years have seen a lot of interest in Bitcoin and cryptocurrencies in general used as a cross-country, untraceable currency which is not under the control of any government and hence free from regulation. The Bitcoin blockchain size as of December 2017 is approximately 149 GB as shown in figure 3.1. A block may contain multiple transactions

5. BITCOIN BASICS-SENDING PAYMENT

Consider 3 users A, B and C. Need to ensure that C cannot spend A’s bitcoins by creating transactions in A’s name. Bitcoin uses public key cryptography to make and verify digital signatures. Each person has one or more addresses each with an associated pair of public and private keys (may hold in the bitcoin wallet). An example of transaction is as given below:

a. A wish to transfer some bitcoin to B. A can sign a transaction with its private key. Anyone can validate the transaction with A’s public key
b. A wants to send bitcoin to B. B sends its address to A, A adds B’s address and the amount of bitcoins to transfer in a “transaction” message. A signs the transaction with its private key, and announces its public key for signature verification. Alice broadcasts the transaction on the Bitcoin network for all to view
c. Same bitcoin is used for more than one transactions.

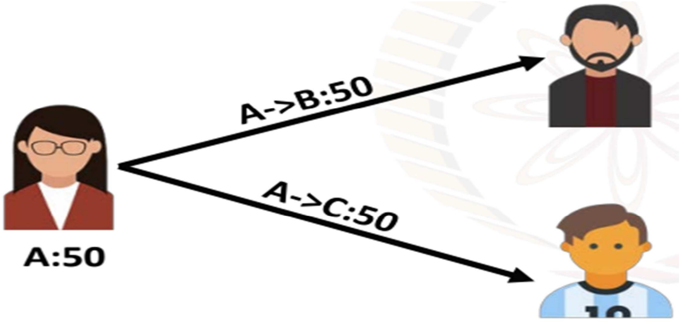


Fig. 5.1 Transaction

Table 1. Technical Terms

Term	Description
Decentralized	The system that stores data across the network.
Miner	Miner Transaction verifier
Hash	One-way hash function to check the integrity of a transaction or message.
Wallet	Securely manages a user’s security credentials

6. CONCLUSION

We have defined what a Blockchain is and also clarified the differences between Blockchain and Bitcoin.

Acknowledgments

I would like to express my sincere gratitude to Mr.C.J.Awati who guided and supported to me in this work. Also I am thankful to all those who have supported and helped me in the completion of this work.

(A.1)

REFERENCES

[1] Hyperledger,"AboutHyperledger",https://www.hyperledger.org
[2] CNNMoney "What is Bitcoin"http://money.cnn.com/infographic/technology/what-is-Bitcoin/
[3] Wikipedia, "Bitcoin",https://en.wikipedia.org/wiki/Bitcoin.
[4] Blockchain: Challenges and applications. 2018 International Conference on Information Networking (ICOIN), Electronic ISBN: 978-1-5386-2290-2, USB ISBN: 978-1-5386-2289-6
[5] https://drive.google.com/file/d/18CyN6ugil4xEJzGPjKWpwWe_s9WNf7tj/view