Cryptography: Blockchain Technology

Mr. Krushna K. Dakale
Department of Master of Computer Application
MGM Jawaharlal Nehru engineering collage ,Aurangabad, MH,India

Abstract- *Block chain is a decentralized transaction and data management technology developed first for Bit coin crypto currency. The interest in Block chain technology has been increasing since The idea was coined in 2008. The reason for the interest in Block chain is its central attributes That provides security, anonymity and data integrity without any third party organization In control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations. In this research, we have conducted a systematic mapping study with the goal of collecting all relevant research On Blockchain technology. Our objective is to understand the current research topics, challenges And future directions regarding Blockchain technology from the technical perspective. We have extracted 41 primary papers from scientific databases. The results show that Focus in over 80% of the papers is on Bitcoin system and less than 20% deals with otherBlockchain applications including e.g. smart contracts and licensing. The majority of Research is focusing on revealing and improving limitations of Blockchain from privacy and Security perspectives, but many of the proposed solutions lack concrete evaluation on their Effectiveness. Many other Block chain scalability related challenges including throughput And latency has been left unstudied. On the basis of this study, recommendations on Future research directions are provided for researchers.*

Keywords- Blockchain, Bitcoin, Currency, Cryptography.

I. INTRODUCTION

Currency transactions between persons or companies are often centralized and controlled by aThird party organization. Making a digital payment or currency transfer requires a bank orCredit card provider as a middleman to complete the transaction. In addition, a transaction Causes a fee from a bank or a credit card company. The same process applies also in several Other domains, such as games, music, software etc. The transaction system is typically centralized, and all data and information are controlled and managed by a third party organization, Rather than the two principal entities involved in the transaction. Block chain technology has been developed to solve this issue. The goal of Blockchain technology is to create a decentralized. Environment where no third party is in control of the transactions and data.

Block chain is a distributed database solution that maintains a continuously growing list of Data records that are confirmed by the nodes participating in it. The data is recorded in a public Ledger, includinsg information of every transaction ever completed. Blockchain is a decentralized.

Solution which does not require any third party organization in the middle. The information About every transaction ever completed in Blockchain is shared and available to all nodes. This attribute makes the system more transparent than centralized transactions involving aThird party. In addition, the nodes in Blockchain are all anonymous, which makes it more Secure for other nodes to confirm the transactions. Bitcoin was the first application that introduced Blockchain technology. Bitcoin created a decentralized environment for cryptocurrency,Where the participants can buy and exchange goods with digital money.

II. BACKGROUND

Blockchain, mostly known as the technology running the Bitcoin cryptocurrency, is a public ledger system maintaining the integrity of transaction data Blockchain technology was first used when the Bitcoin crypto currency was introduced. To this day, Bitcoin is still the most commonly used application using Blockchain technology Bitcoin is a decentralized digital.Currency payment system that consists of a public transaction ledger called Blockchain The Essential feature of Bitcoin is the maintainability of the value of the currency without any organization or governmental administration in control.

Blockchain is the decentralized managing technique of Bitcoin, designed for issuing and Transferring money for the users of the Bitcoin currency. This technique can support the public Ledger of all Bitcoin transactions that have ever been executed, without any control of a third Party organization

Blockchain technology has also some technical challenges and limitations that have been Identified. Swan presents seven technical challenges and limitations for the adaptation of Blockchain technology in the future:

• Throughput: The potential throughput of issues in the Bitcoin network is currently maximized to 7tps (transactions per second).Other transaction processing networks are VISA

(2,000tps) and Twitter (5,000tps).When the frequency of transactions in Blockchain Increases to similar levels, the throughput of the Blockchain network needs to be improved.

• Latency: To create sufficient security for a Bitcoin transaction block, it takes currently Roughly 10 minutes to complete one transaction. To achieve efficiency in security, more time has to be spent on a block, because it has to outweigh the cost of double spending attacks. Double-spending is the result of successful spending of money more than once. Bitcoin protects against double spending by verifying each transaction added to the block chain, to ensure that the inputs for the transaction have not been spent previously. This makes latency a big issue in Blockchain currently. Making a block and confirming the transaction should happen in seconds, while maintaining security. To complete a transaction e.g. in VISA takes only a few seconds, which is a huge advantage compared to Blockchain.

• Size and bandwidth: At the moment, the size of a Blockchain in the Bitcoin network is over 50,000MB (February 2016).When the throughput increases to the levels of VISA, Blockchain could grow 214PB in each year. The Bitcoin community assumes that the size of one block is 1MB and a block is created every tenminutes. Therefore, there is a limitation in the number of transactions that can be handled (on average 500 transaction in one block) . If the Blockchain needs to control more transactions; the size and bandwidth issues have to be solved.

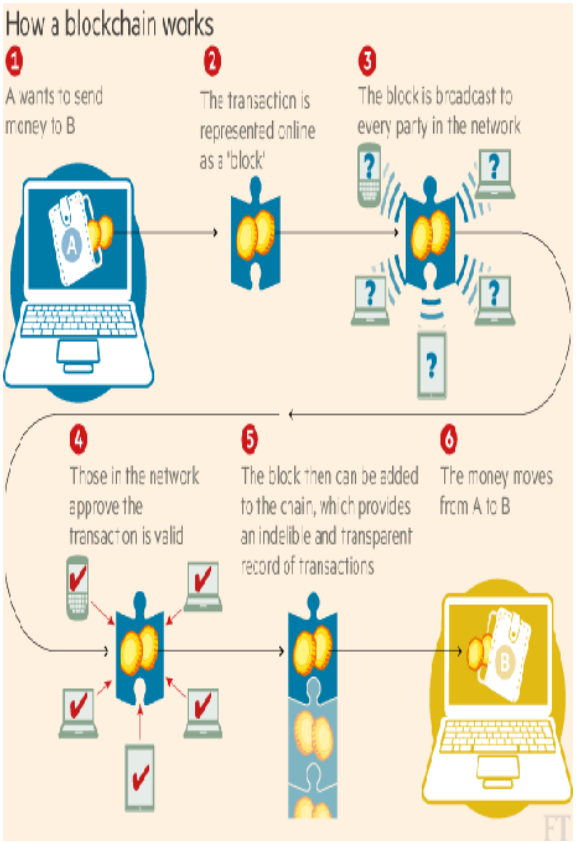
• Security: The current Blockchain has a possibility of a 51% attack. In a 51% attack a single Entity would have full control.

• Wasted resources: Mining Bitcoin wastes huge amounts of energy ($15million/day). The waste in Bitcoin is caused by the Proof-of-Work effort. There are some alternatives in industry Fields, such as proof-of-stake. With Proof-of-Work, the probability of mining a block Depends on the work done by the miner. However, in Proof-of-Stake, the resource that is compared is the amount of Bitcoin a miner holds . For example, someone holding 1% of the Bitcoin can mine 1% of the "Proof-of-Stake blocks" . The issue with wasted Resources need to be solved to have more efficient mining in Blockchain.

• Usability: The Bitcoin API for developing services is difficult to use. There is a need to Develop a more developer-friendlyAPI for Blockchain. This could resemble REST APIs.

• Versioning, hard forks, multiple chains: A small chain that consists of a small number of Nodes have a higher possibility of a 51% attack. Another issue emerges when chains are split for administrative or versioning purposes.

How to work Blockchain Technology:



Advantages:

Process Integrity: Due to Security reason, this program with made in such a way that any block or even a transaction that add to the chain cannot edit which ultimately provides a very high range of security.

Traceability: The format of Blockchain Designs in such a way it can easily locate any problem and correct if there is any.

Security: Blockchain Technology is highly secure because of the reason is and every indivusal who enter into Blockchain Network is provide with the unique identity which linked his account. This ensures that the owner of the account himself is operating the Transaction. The Block Encryption in the chain make it tougher for any hacker to the distribute the traditional setup of the chain

Fast Processing: Before the invention of the Blockcahin, the Traditional Banking Organization take a lot of time in a processing and initiating the transaction but after blockchain technology speed of the transaction is the increase to very high extend.

Disadvantages:

Power used: The Consumption of the power in the Blockchain Technology is a comparatively high as in a particular year the power consumption of Bitcoin miner was alone more than the per capital Power consumption of 159 indivusal country.

Cost: As per the Studies as an average cost of bitcion transaction is $50-$160 and most of this cost is coverd by the energy consumption. They are very fever chances That this issue can be resolved by the achievement in the technology.

III. CONCLUSION

This paper discussed the Blockchain technology is the secure to transaction money .goal of the Blockchain technology is to provide anonymity, security, privacy and trassnpermcy to this entire user.

However this attribute set up a lot of technical challenges and limitation that need to be addressed.

REFERENCES

[1] Where Is Current Research on Bolckchain Technology? – A Systematic Review by kari smolander Lappeenranta university of Technology.
[2] WWW.google.com