IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-6, Issue-12, 2018 E-ISSN: 2347-2693

Issues and Challenges with Blockchain: A Survey

Divyakant Meva

Faculty of Computer Applications, Marwadi University, Rajkot, India

*Corresponding Author: divyakantmeva@gmail.com, Tel.: +91-98259-51824

Available online at: www.ijcseonline.org

Accepted: 19/Dec/2018, Published: 31/Dec/2018

Abstract- Blockchain is one of the latest trends in Information Technology domain. It has changed a way of thinking for IT professional. Companies are focusing on implementation of blockchain with their services to ensure security and reliability. Still they are facing challenges and issues for development and implementation of blockchain based services. This paper discusses those issues and challenges to be considered in development and implementation.

***Keywords*—**Blockchain, Smart contracts, Issues and Challenges (key words)

I. INTRODUCTION

When we talk about blockchain, first thing which comes to our mind is Bitcoin. This crypto currency was first one to use concept of blockchain for implementation purpose in the year of 2009. Bitcoin brought the concept of blockchain and smart contracts in to the knowledge of every one.

Stuart Haber and W. Scott Sternest started first work on a cryptographically secured chain of blocks in 1991 and continued till the mid 2000's. It was Satoshi Nakamoto who conceptualized first blockchain in 2008 and then it as a core component of Bitcoin.

A. Blockchain

Blockchain is not just one concept, but combination of multiple concepts like cryptography, mathematics, networking, distributed consensus technology, algorithms etc. [1].It is trying to solve problems with distributed database synchronization with distributed consensus. The characteristics of Blockchain technology are:

1. Transparent
2. Distributed
3. Autonomy
4. Immutable
5. Anonymity
6. Open source

B. Smart contract

The term smart contract is a bit confusing as neither this is smart nor is a legal contract. Smart contract is a code running on top of the blockchain technology containing a set of rules with which parties under that contract will agree to interact with each other.

If the defined rules meet, the agreement will automatically be enforced. The code verifies, facilitates and enforces performance of agreement or transaction.

This is one of the simplest forms of decentralized automation. Smart contracts reduce transaction cost. Characteristics of smart contracts are:

1. Self executing
2. Self verifying
3. Tamper resistant

After taking introduction to blockchain, the section II gives idea about working of blockchain. Section III focuses on working of smart contracts. Section IV then discusses issues related with blockchain. Section V gives idea about challenges related with blockchain. At the end, section VI concludes the discussion on issues and challenges related with blockchain.

II. WORKING OF BLOCKCHAIN

Here are the important concepts of working of blockchain:

1. The record: It can be any information or a deal
2. The Block: It is bundle of records
3. The chain: When all the blocks are linked together, it forms a chain

The process steps:

1. Ina trade, record is created; Mr. X is selling three of his coins to Mr. Y for 2000 Rs. This record lists details including digital signature from each participating party.
2. This record will be checked on to network. The nodes – computers on network, will check the details of record or trade, to assure validity of the trade

3. The record or trade which has been accepted or assured by network is now added to a block. Every block will contain a unique code which is called hash. It is containing hash of the previous block of the chain.
4. In this step, block is now added to the blockchain. The hash code will connect the blocks in specific order.

In this process, hash code will keep the record safe. Irrespective of the record size, hash code will have the same size for each record.

Any change to the original record will generate new hash. And to assure the security of the data, the person is required to change the hash of previous records also. Ultimately this will change the whole set of hash. So, hash will say directly that the data has been changed or not. In this way, it will assure security of the records.

III. WORKING OF SMART CONTRACT

Here are some basic steps in smart contract:

1. An option contract between parties is written as code into the blockchain. The individuals involved are anonymous, but the contract is public ledger
2. A triggering event like expiration date and strike price is hit and the contract executes itself according to the coded terms.
3. Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actor's position.

Smart contracts achieves following benefits for the actor:

1. Autonomy
2. Trust
3. Backup
4. Safety
5. Speed
6. Savings
7. Accuracy

IV. ISSUES RELATED WITH BLOCKCHAIN

Every technology will have its own limitations and problems / issues. Blockchain is said to be overhyped by some of the critics. Few of the issues are explained in short here:

A. Complexity

Blockchain has completely new set of vocabulary. It has adopted cryptography as the major player and this step indeed is making blockchain a complex technology.

B. Network size

Blockchain like other distributed technology is antifragile - responding to attacks and growing stronger.

Blockchain has large number of users. If blockchain is not supporting a robust network with widespread grid of nodes, getting full benefits will be impossible.

C. Transaction cost and network speed

By taking example of Bitcoin, in late 2016, it was possible to process seven transactions per second. The cost of each transaction was about $0.20 and it was able to store 80 bytes of data.

Also it requires adding detail to each and every node of the network and performing hash calculations, so it heavily uses network speed.

D. Human error

For considering blockchain as database, it requires to have high quality information as an input. The information going to be stored on blockchain may not be trustworthy, so each event should be recorded accurately. Otherwise the phrase 'Garbage in – Garbage out' will be true.

E. Politics

Blockchain provide an opportunity for digitizing e-governance models. Miners are forming another kind of incentivized e-governance model. Because of this, there are chances to have public disagreements among different sectors of community. It is notable feature and clears relation with 'forking' a blockchain.

This kind of discussion will be clearly technical and in some cases, will be heated but really informative for those who are interested in mixing of democracy and consensus.

F. Interoperability

Blockchain networks have been divided into categories like private, public and consortium. Each of these has its own advantages and disadvantages based on application requirement. One blockchain may not be enough as there is not a single solution which fits for all categories of problems. Consensus mechanism will vary from one industry to another. Other aspects like privacy, centralization and economy will also vary from one to another industry.

The blockchains of different kinds cannot communicate with each other at this stage. To solve this problem, you need to have various cross-chain technologies for interconnection [2].

G. Data malleability

Data malleability is a latent issue in the Blockchain technology. The signatures don't provide surety about the ownership of the Bitcoin transferred in a transaction. An attacker can modify it and then rebroadcast a transaction which can create problems with transaction confirmation [3][4].

H. Authentication
An issue related to the Blockchain transactions is the authentication. An example of event with the authentication is the known case in Mt. Gox [5] when the storage of customer private keys was attacked and stolen.

I. Wasted resources
The energy spent of mining in the Bitcoin network was $15 million per day as per data in 2015 [6]. The waste in the Bitcoin is because of the Proof-of-Work effort. Here, the probability of mining a block will be depending on the work done by the miner [3].

J. Usability
Here usability is an issue because Bitcoin API is less user-friendly in comparison of the other latest APIs [3][6].

V. CHALLENGES RELATED WITH BLOCKCHAIN

Though blockchain has given strong support to manage security, still blockchain technology is facing challenges. Some of the challenges have been described here:

A. Scalability
There is an increase in blockchain usage volume and rise in the number of transactions occurring daily basis, blockchain has become huge in size. Transactions are stored in nodes for getting validation. First, the current transaction source needs to be validated before transaction itself. The block size restriction and time break required to produce new block plays a major role in not satisfying requirement for the simultaneous processing of millions of transactions in real time environment. In few cases, size of block may also create issue in delay of transaction [7].

B. Privacy leakage
Main vulnerability of blockchain is leakage of transaction privacy because the balances and details of public keys will be visible to each and every one available on network. One suggested solution is to get anonymity in blockchain. This can be classified in anonymous solution and mixing solution [2].

C. Selfish mining
It is a major challenge in blockchains. A block is vulnerable of cheating even if a small part of hashing power is used. Here, the miner keeps with him the mined block with no broadcasting on network and will create a private branch which will be broadcasted after meeting certain requirements.
Due to this, legitimate miners will waste time and resources and private chain will be mined by selfish miners [2].

D. Personal Identifiable Information (PII)
The myth related to blockchain and identity is that blockchain provides ideal distributed alternative instead of centralized database storage for Personal Identifiable Information.

Blockchain can technically support placing Personal Identifiable Information on chain or used to create attestation on the chain which points to off-chain for Personal Identifiable Information storage.

Elmagharaby and Losavio discussed about Personal Identifiable Information from the viewpoint of communication and location privacy [8].

E. Security
Security refers to the terms like integrity, availability and confidentiality. As all knows, confidentiality will be low in distributed networks, as well as integrity is also a major concern. In this case, availability will be not an issue as replication is there. Another major concern is 51% majority attack. In this case, one miner can get full control of the chain. Also there will be challenges like prevention from DDoS attack, Trojans and viruses from adware etc. [9]

F. Fork problems
It is related with decentralized node version, as well as agreements when the software update. This is very crucial as it involves a wide range in blockchain.

There are basically two types of forks – hard fork and soft fork.

When systems comes with new agreement or version, and if it is not compatible with older version, then the older nodes cannot be agree with mining of new nodes. And this makes one chain in to two. This is called hard fork.

When systems comes with new agreement or version, and if it is not compatible with older version, then the new nodes cannot be agree with mining of older nodes. Older nodes and new nodes still continue to work on the same chain. This is called soft fork.

Soft fork makes the older nodes unaware about consensus rule changes. Also it will not affect stability and effectiveness as both types of nodes are on single chain [8].

G. Time confirmation
Bitcoin transaction takes only one hour in comparison of traditional transaction which takes almost 2 to 3 days for confirmation. Still it is more compared to the expectation. Lighting network can be the solution to this.

H. Regulation problems
The major challenge in case of blockchain implementation is rules and regulations of various countries. The concept of decentralized structure will make the control of central bank

weak from the viewpoint of economic policy and money transactions amounts. Concerned authority need to pay attention on research on this issue and identify new strategy and formulating new policies.

I. Integrated cost

Another important challenge here is high cost for replacing existing system with blockchain based new system. This involves cost in terms of time and money as well. The infrastructure requirements will get changed. Ensure that new system brings economical benefits along with meeting other requirements.

J. Energy consumption

Blockchain works on Proof-of-Work (PoW) mechanism for validation of transaction. PoW requires too much complex mathematical computations to validate transaction. These calculations require large amount of energy to provide power to computers doing this task.

This much of energy requirement in operation is curb to many organizations which are now thinking for some other sources of energy or other sustainable methods of doing business.

K. Public perception

Most of the people are still unaware of existence and usage of this technology. This technology is revolutionary changes in industry, but the knowledge about this distributed ledger technology is limited to only those who are involved in this process.

When we talk about blockchain, people will only think about Bitcoin and other cryptocurrency. And people think about this currency as a way of money laundering, black market and other illegal task.

So, it is must that people should understand difference between Bitcoin and Blockchain and negative undertones about blockchain.

L. Technical maturity

Blockchain technology is yet to be mature. It is easily susceptible to the problems like capacity, system failure, non-predicted bugs, and the most important; it is going to be used by technically unsophisticated users.

M. Integration barriers

Let us take example of CRM in telecommunications field. Here starting from taking order and completing with generation of bill, every system is using different format of data and model for storing information. These systems will work in isolation and process the information to meet certain objectives. The major challenge here is about the integration of one system with other business system.

Though blockchain will offer solution, but the architecture should be re-designed for such kind of system. The organization has to make evaluation that which part of system will be working closely with blockchain.

VI. CONCLUSION

The author has tried to accumulate as many as issues and challenges related to blockchain technology. It has not been proved that every issue and challenge persist forever. Some of the issues and challenges have been tried to pay attention and partially been solved. Still some issues like technical maturity, public perception, politics, and regulations are tough to resolve as they involve human and governance aspects. When there is case of technical matter, it can be solved with some alternative technology or proven solutions. But to deal with public, regulation and political aspects, it will take time.

REFERENCES

[1] Iuon-Chang Lin, Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges", International Journal of Network Security, Vol 19, No. 5, pp. 653-659, 2017

[2] Jacek Bastin," Blockchain technology issues and solutions: a complete overview", 2018

[3] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander, "Where Is Current Research on Blockchain Technology? -A Systematic Review ", PloS one Vol. 11, 10 ,2016

[4] Tobias Bamert, Christian Decker, Roger Wattenhofer, Samuel Welten," Bluewallet: The secure bitcoin wallet", International Workshop on Security and Trust Management. Springer, pp 65–80, 2014

[5] Joppe W Bos, J Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow, "Elliptic curve cryptography in practice", International Conference on Financial Cryptography and Data Security, Springer, pp.157–175, 2014

[6] Melanie Swan, "Blockchain: Blueprint for a new economy", O'Reilly Media, Inc., 2015

[7] Zibin Zheng ,Shaoan Xie, Hong-Ning Dai, "Blockchain challenges and opportunities: a survey", International Journal of Web and Grid Services, Vol. 14, No. 4, pp. 352-375, 2018

[8] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety,security and privacy", Journal of Advanced Research, Vol. 5, pp. 491-497, 2014

[9] Archana Prashanth Joshi, Meng Han_ and Yan Wang, "A survey on security and privacy issues of blockchain technology", Mathematical Foundations of Computing, Vol. 1, No. 2, pp. 121-147, 2018

Authors Profile

Dr. Divyakant Meva pursed Master of Computer Applications from Saurashtra University, India in 2002 and Ph.D. from Saurashtra University, India in year 2015. He is currently working as Associate Professor in Faculty of Computer Applications, Marwadi University, India since 2010. He is a member of CSI since 2013. He has published more than 20 research papers in reputed national and international journals. His main research work focuses on Biometrics, Blockchain, Cyber Security and Artificial Intelligence. He has 16 years of teaching experience and 5 years of Research Experience.

