International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

A Block Chain Based Framework to Enhance Security against Cyber Attacks

Vani Rajasekar, J. Premalatha, K. Sathya

Abstract— Block chain has drawn major attention recently in the area of cyber security. Till to date many detection techniques and protection mechanisms have been proposed to enhance the security. In this paper we have proposed an overview of distributed ledger framework, block chain to defense against the cyber attacks. We here present a comprehensive overview of block chain architecture and some major algorithms used in different block chains. The future trends of block chain technology in the applications such as IoT security, E-voting, Banking sector has also coined out in this paper.

Keywords: Block chain, ledger, decentralized, cyber attacks, security and privacy

.

I. INTRODUCTION

Block chain is a decentralized ledger or data structure contains a cryptographically verifiable data list. The buzzword crypto currency has enjoyed its huge marketing from 2016[1]. The main advantage of block chain is the centralization of data. The block chain contains a distributed public ledger where all users have same data that can be used for high value use cases such as crypto currency. The future research on block chain emphasizes the security and privacy. In 2008, Satoshi Nakamato identified Bitcoin, which is used to make transactions without the bank acting as a third party. But the privacy and security of this bitcoin technology in provable manner [2].

Block chain contains various blocks; each block is built on the top of previous block. The network miners will does the job of building a block along with signature and merkle root. It is difficult for the attacker to tamper the blocks and modify the data present in it. Bitcoin has find its major application in the emerging trends such as peer-peer transactions, end to end cloud storage, distributed record keeping, Iot Security, etc. Despite of all existing technologies, this paper proposes a block chain based framework for data protection. Main contributions are listed as follows,

1. The proposed framework is consensus based and it enhances the security compared to the entire existing framework.
2. The proposed framework increases the self defensive capabilities against cyber attackers who can never be able to hack or modify the data.
3. Block chain can be used to overcome the problems of fraudulent results
4. Block chain can be used to provide the trusted records of events in health insurance.

ADVANTAGES OF BLOCK CHAIN

A. *Immutable:* Difficult for the attacker to tamper or alter the data

B. *Irreversible:* Signature enables the user to provide irreversible which prevents double spending

C. *Resilient:* It ensures high security against major attacks

D. *Distributed system:* The ledger contains the data copy will be present with all members

E. *No centralized authority:* It is a peer to peer system does not depend on central server to initiate the transaction.

II. HISTORY AND EVALUATION

After the invention of Satoshi Nakamoto's Bit coin has become the most popular and used crypto currency. The anomalies of bitcoin are

1. *Time Taking:* Even though Bit coin is a emerging technology, the time taken to validate the same is not taken into account.
2. *Asset:* It was primarily built as a currency; it cannot be applied as assets.

The miners of block chain technology has identified many technologies, some of the examples are cite here,

A. Colored coins:

The technology that can be used as an digital asset other than bitcoin is considered as "tokens", it can be considered as meta data for representation of shares, properties and other instances.

B. Ethereum block chain:

It is one of the emerging technologies that is known as "smart contracts", the algorithm that is used for smart contracts is slightly different that of bitcoin, smart contracts uses small computer programs that accounts for transaction between clinet and server.

Manuscript published on November 30, 2019.
* Correspondence Author
Vani Rajasekar*, Dept of CSE, Kongu Engineering College, Erode, Tamil Nadu, India.(Email: vanikecit@gmail.com)
J. Premalatha, Dept of IT, Kongu Engineering College, Erode Tamil Nadu, India. .(Email: : jprem@kongu.ac.in)
K. Sathya, Dept of CT/UG, Kongu Engineering College, Erode, India, Tamil Nadu, India. .(Email: pearlhoods@gmail.com)

This technology plays a major role in IBM and Amazon.

C. Hyperledger block chain:

Linux foundation started a umbrella project in the year 2015[3], the purpose of this is to develop the collaborative development of block chain based distributed ledgers and it contains four platforms Iroha, Fabric, Burrow and Sawtooth.

In this IBM owns Fabric and Intel owns Sawtooth project of hyperledger.

III BLOCK CHAIN ARCHITECTURE

It is a sequence of blocks contains a complete transaction list of public ledger [4]. The first block in the block chain is called genesis block which has no parent block. Fig.1 represents the overall architecture of block chain. Each block contains a block header, parent block hash, transaction counter.

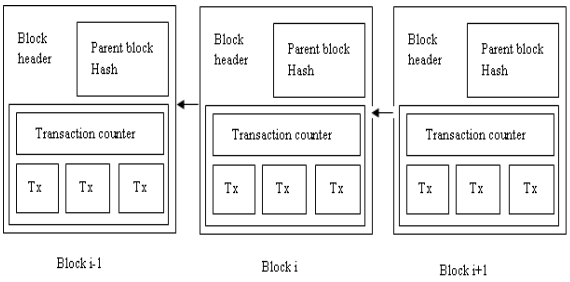

Fig.1. Block Chain Architecture

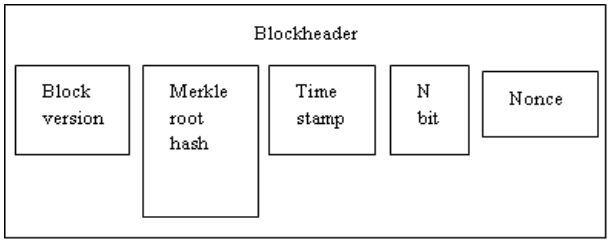

Fig.2. Block Header Structure

The above mentioned Fig.2 represents the typical structure of block header which contains

1. Block version: which indicates what version of rules to be followed for the block chain
2. Merkle root: Indicates the hash value of transactions.
3. Time stamp: Represents the current time in seconds
4. N bit: Represents target threshold of hash value
5. Nonce: Which is usually a 4 byte field starts with 0. It increases for every hash calculation

IV WORKING MECHANISM OF BLOCK CHAIN BASED FRAMEWORK

In the block chain frame work, the data are usually stored in ledger by means of connected blocks that exists in a distributed manner. The frame work contains a following section for secure transmission, verification, access and storage of data.

A. Data Encryption and Broadcast

Each node in the network contains public key and private key. Private Key is the node's private information that is used to verify the identity whereas public key is the main accessible information available in the network. Each meter node is given the public key, private key, consensus algorithm, and data blocks. The meter node takes the plain text and identifies the cipher text using encryption algorithm which also identifies the hash code of the data block using SHA message digest algorithm. The encrypted data again is then broadcast to all other nodes in the network. The fig. 3 depicts the process of encryption and broadcast in block chain.

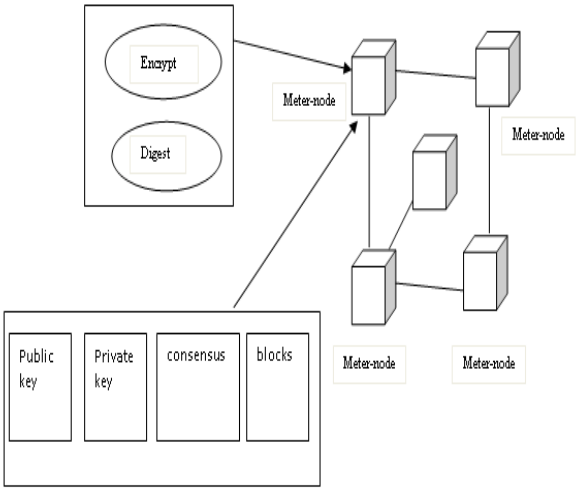

Fig.3. Encryption and broadcast in secure frame work

B. Data decryption and verification

The meter node which receives the encrypted broadcast information needs to decrypt the data and display the result. For the decrypted plain text again the message digest value is calculated and resulted hash value is verified with the sent value, if matches data can be accessed, stored and modified by the user else the data will not be able to access.

V PERFORMANCE COMPARISON OF PROTECTION FRAME WORK AGAINST CYBER ATTACKS

In this section overview of block chain is compared with respect to three key observations. Firstly the proposed framework is applied to power systems that need the security. Secondly the proposed framework can be used in modern applications that are beyond the power systems. Thirdly the proposed frame work is more secure to store and access the data. The framework explained by Liang[5], depicts that the proposed framework ensures security by resist against the information disclosure.

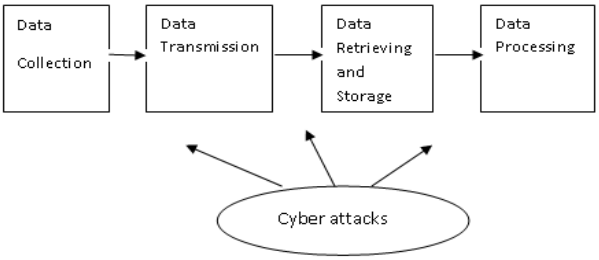

Fig.4. (a) Existing framework prone to attack.

The fig 4.(a) represents the existing information system that prone to cyber attacks

where as the fig 4.(b) depicts the block chain based distributed framework that ensures security against cyber attackers and other security attacks.

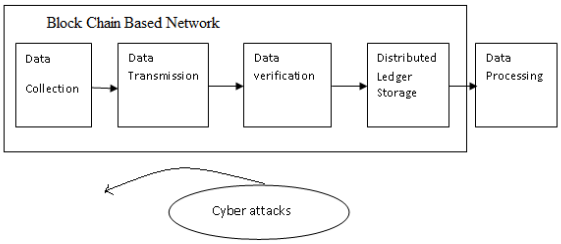

Fig.4. (b) Block chain framework against cyber attacks

The table 1 shows the technology comparisons of block chain in bit coin system and block chain in distributed frame work against cyber attack. One notable thing is that bit coin is proposed to "double spending attack" in which a bit coin spends one ticket twice. Another important hazard is "51%attack" in this the attacker can be able to take the major control of the node in the network that produces false result. And researchers have coined that the 51%attack is most hazardous and it results in major security threats.

Table I. Review on technology comparisions

Items	Block chain in Bit Coin	Block chain in Distributed Frame work
Double spending attack	Threat	Not exists
51% attack	Threat	Not exists
Chain connection speed	Slower	Much faster
Transaction relationship	Continuously, Related	Independent, unrelated
Transaction money	Money	Collected measurement

VI CHALLENGES OF BLOCK CHAIN

Despite the great advantages of block chain, it faces countable number of challenges. Some major challenges are listed below.

A. Scalability

As day by day the amount of transactions are increased considerably. Each meter node in the network has to store all the transactions, due to the block size and time to create block, bit coin is able to process only 7 transactions per second which cannot be able to process all the huge number of transactions in real time applications. The scalability can be optimized in two ways

1. Storage optimization of block chain
2. Redesigning block chain

B. Privacy

In the block chain architecture private and public keys are transferred without any real identity exposure hence it does not ensures transactional privacy [5]. Recent study has also revealed that bit coin is prone to privacy leakage [6]. Multiple methods are proposed in real time to enhance the security by overcoming the above mentioned security breaches.

C. Selfish mining

As said by Eyal and Sirer[7] block chain is susceptible to selfish mining attack, because if small portion of hash is known by the attacker he can be able to compromise the entire system. And based on this selfish mining attack many attacks such as mining attacks, network level ellipse attacks have been identified in this emerging technology. One idea that is proposed to overcome this is Zero block

VII FUTURE TRENDS & RESULTS

Block chain has found its major challenges in the field of IoT, centralization, big data analytics, E-voting, etc.

A. Iot Applications

Iot has attracted much attention from academics and industries which is a major component of information systems. Industrial Iot has found its applications for major energy demand in the area of energy harvesting, wireless power transfer, vehicle to grid. The P2P energy trading scenarios in the following areas

1. Microgrids
2. Energy harvesting networks
3. Vehicle to grid networks

B. E-Voting system

It acts as the major active research for decades; block chain provides the transparency and flexibility for electronic systems. Block chain ensures smart contracts in electronic voting that includes secure and cost-effective election. It offers i) Identify the roles that involved in agreement ii) Agreement process or (Election process) iii) The transactions. It enables easy and fast transactions on electronic systems. It also emerges with the technology such as Smart contract for board room voting, Digital voting, Net vote, etc.

C. Financial applications

Traditional and financial institutions have taken this block chain technology to enhance their financial needs. According to the research Arcade city[8], a ride sharing startups that offers an market place in this case drivers connect directly with the market place by leveraging the secure block chain network

VIII CONCLUSION

Block chain has still its research demand in the arena of many real time applications. Many researchers in the field of cryptography and security has come forward to bring this technology to newer highs. In this paper we present a comprehensive overview of block chain technology along with distributed ledger to protect against cyber attacks. From the review of literatures we have analyzed and compared the features of bit coin with distributed ledger framework. Furthermore we have listed some challenges and future directions for the applications of block chain. We have a plan to do more in depth research in the block chain security and its applications in future

REFERENCES

1. State of blockchain q1 2016: Blockchain funding overtakes bitcoin," 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1-2016/

2. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, KirillLevchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. “A fistful of bitcoins: characterizing payments among men with no names”. In Proceedings of the 2013 conference on Internet measurement conference, pages 127–140. ACM, 2013.
3. D. Lee Kuo Chuen, Ed., “Handbook of Digital Currency”, 1st ed. Elsevier, 2015. [Online]. Available:http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170
4. G. Liang, J. Zhao, F. Luo, S.R. Weller, and Z. Dong. “A review of false data injection attacks against
5. modern power systems,” IEEE Trans. Smart Grid, vol. 8, no. 4, pp. 1630 – 1638, Jul. 2017
6. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M.Voelker, and S. Savage, “A fistful of bitcoins: Characterizing payments among men with no names,” in Proceedings of the 2013 Conference on Internet Measurement Conference (IMC’13), New York, NY, USA, 2013.
7. J. Barcelo, “User privacy in the public bitcoin blockchain,” 2014.
8. I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp. 436–454.
9. “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. [Online]. Available: http://www.coindesk.com/state-of-blockchain-q1-2016/
10. S. King, “Primecoin: Cryptocurrency with prime number proof-ofwork,”July 7th, 2013.
11. S. Solat and M. Potop-Butucaru, “ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin,” Sorbonne Universites, UPMC University of aris 6, Technical Report, May 2016
12. Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018..

AUTHORS PROFILE

Vani Rajasekar completed her B.Tech(IT), M.Tech (Information and cyberwarefare) in department of IT Kongu engineering college. She is pursuing her PhD (Information and Communication Engineering) in the area of Network security. Presently she is working as assistant professor in the department of CSE Kongu engineering college for past 3 years. Her area of interest includes Network security, Cryptography and Wireless networks.

Dr.J.Premalatha completed BE(ECE), ME(CSE), PhD(Information and Communication Engineering). She is working as professor in the department of IT Kongu engineering college. Her teaching experience is 28 years. Her area of interest includes Network security, Cryptography, Computer networks and Database Management system

K.Sathya completed her B.Tech(IT), M.Tech (Information and cyberwarefare) in dept of IT Kongu engineering college. She is pursuing her PhD (Information and Communication Engineering) in the area of Network security. Presently she is working as assistant professor in the department of CT/UG Kongu engineering college for past 3 years. Her area of interest includes Network security, Computer networks.