A SURVEY ON THE SECURITY AND PRIVACY OF BLOCKCHAIN SYSTEMS

Rajesh Kumar1, Ankita Sharad2, Poornima Nag3, Vivek Kumar Singh4, Smriti Kumari5, Shweta Kumari6

1,2,3*Department of IT, NIT Raipur*
4,5,6*Department of CSE, IIIT Senapati Manipur*

---***---

Abstract - Since when bitcoin make an entry in cryptocurrency which is based on blockchain technology gets so much popularity just from initial phase itself, now most of the cryptocurrency are moving towards blockchain framework and using different hashing function. In this advancement most of the works are now using blockchain technology from cryptocurrency to smart online retails platforms which has been used by Walmart. since its going to be most used term and popular technology most of the attackers are targeting and just by using some loopholes and any other technical glitches or any other way they are attacking over this technology. since its going to be future and everyone is concerned for its security and privacy, here we did a good comparison of many attacks already did on this blockchain frameworks and we summarize this attacks and we tried to give our own opinion to make it more reliable and flexible.

Key Words: Consensus, PoW, PoS, PoL, PoI, Bloch Chain, Hash Function

1.INTRODUCTION

Blockchain [1] can be describe as a collection of records which is interlinked [4] with each other with strongly resistant to alteration and it's protected using cryptography. Blockchain technology is a distributed database. In blockchain ecosystem each node [2,3] is said to be block which contains transaction details, transactions may be of any types depends of blockchain implementation. Blockchain has been getting popularity just when it came because it's not traceable [5] and its not alterable also, which means its more reliable than any other technology. Invented in 2008 with a paper published by author named as Satoshi Nakamoto . just stated with a concept for bitcoin [15] its framework has been designed for blockchain and getting popularization day by day till now many of the sector implements its own technology based on blockchain. It has been spread in many fields from academic [10] [11], industries [12], medical [13], economics[18], software engineering[19] smart contracts [16][18][19][and many more areas block chain technologies are implemented. This is secured just because of any transaction that has been done is stored in many nodes, so for intruder its impossible to hack all those nodes at a time an d also because of its decentralization. It's gaining popularization day by day, just by knowing per day millions of transactions are done over block chain mainly in bitcoins and ethereum field. since most of the block chain technologies are growing so fast and it has gain almost maximum users across the globe so its most likely to be attacked by attackers [9] and hackers, in recent years many big attacks happen in this field we will discuss in this paper and we make some comparison based on them. The reaming section of this paper is as follows section 2 describes overview of block chain technologies which includes consensus [7] [11] [12] [14] mechanism block propagation and synchronization [6] and also public and private key concept, section 3 covers technological developments with advantages and disadvantages of block chain section 4 describes attack cases and section 5 describes about security enhancements and finally section 6 gives you conclusion of the paper.

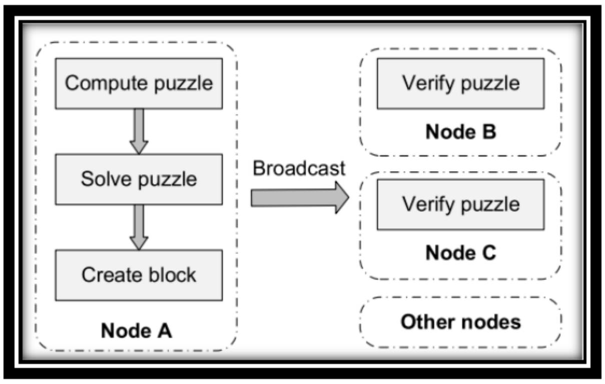


Fig -1: PoW consensus mechanism.

is document shows the suggested format and appearance of a manuscript prepared for SPIE journals. Accepted papers will be professionally typeset. This template is intended to be a tool to improve manuscript clarity for the reviewers. The final layout of the typeset paper will not match this template layout.

2. OVERVIEW OF BLOCKCHAIN TECHNOLOGIES

2.1. Consensus mechanism

2.1.1 PoW (Proof of work)

Every node has show that are doing lots of work in computational power[19] and in return of it they get some bitcoins in cryptocurrency form. So all ledgers all mutually agreed on it that this node is not malicious and all can trust on it and whoever wins the solving puzzle for any new transaction done over blockchain he may add new block to blockchain network. Best example for its Bitcoin and Ethereum.

2.1.2 PoS (proof of Stake)

Whoever put more stake in block to be added in blockchain network wins it and they will add this transaction in block chain network. Those ledgers or miners who solve most of the time first must have many cryptocurrencies for this in return.

So they may put more stake on it. There is a chance that any miner who is having more cryptocurrency put the maximum state in this, but if any malicious one will do that if somehow all others know about it, in future that particular miners will be removed from blockchain network and he lose all his bitcoins. so only valid and trustable ones put their stake in solving one block. so everyone is mutually agreed [21] on this type of consensus. a good example is ethereum.

2.1.3 PoC (Proof of Capacity)

Similar to previous ones in this whoever is having a maxing disk capacity will win it. Here also same as is applied as whoever is having most disk capacity [20] might not be intruder but if he any intruder with maximum disk capacity will took part in it and add any malicious block in blockchain then after knowing all about it reading one will kick out from the system and he lose all his precious currencies and credentials.

2.1.4 PoA (Proof of Authority)

In this type of consensus those blocks who made a good reputation in front of all reaming one's based on different parameters made by blockchain networks wins [14] it.

2.1.5 PoET (Proof of Elapsed Time)

It is developed by intel an in this all nodes create their own block wait for random time interval and whoever is having better progress time means whoever is having more patience win it.

2.1.6 PoD (Proof of Deposite)

Whoever is having maximum deposit wins the consensus.

2.2 Block propagation and synchronization

Each block in a blockchain is having a unique transaction details whose copies is distributed to all others blocks. If any new transaction happens in this blockchain environment, then to verify it it's a valid transaction all others blocks do consensus and whoever wins it add this block to this environment and make a copy with updated block details and send to all remaining blocks. this is how block propagation and synchronization happens.

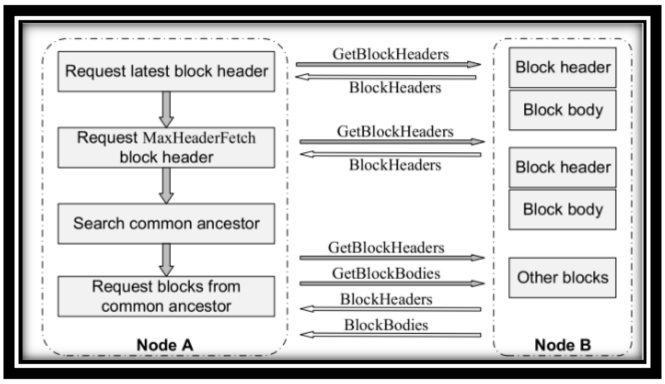


Fig -2: Block synchronization process between nodes

2.3 Public and private key concept

A node 'P' wants to sends a digital currency to node 'Q', initially p sends 2 bitcoins (let's assume for this example) to q then it creates a block which contain info regarding this transaction and now this transaction is encrypted with any hashing function and now p signs it with its own private key [22]. as a whole of this info a block is created which is digitally signed by p broadcast to all world (Reaming bocks) by using Q's public key [21], it reaches to Q's address and by its private key message has been decrypted. Here Public key you assume as Gmail id and private key as its password, in case of online wallets system you can assume public key as unique id for online wallets and its password as private key. Bitcoins [4] uses SHA256[8] and Ethereum uses ETHASH [18] hashing function.

3.TECHNOLOGY DEVELOPMENT

Bitcoins is having version one and version two means bitcoin 1.0 and bitcoin 2.0. Bitcoin comes into picture and it gets very popularity and within some years it makes a capital of more than 30 billion. Bitcoins 1.0 generally make cryptocurrencies enhancement in this era of version 1.o more than 800 cryptocurrency came in to market with net worth more than 60 billion is achieved. Now Facebook twitter and many bigger high tech companies also making their own cryptocurrency which shows its craze and it shows its more reliable. Blockchain 2.0 came with smart contracts and many other applications are like industry and academia and research. this is because of its advantages.

3.1 Advantages

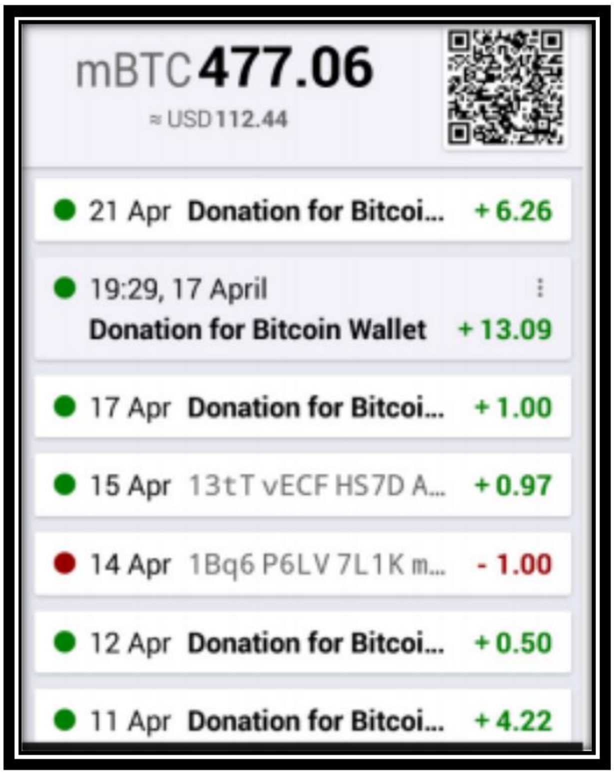
a) Decentralized and anonymous: when we send a money to other person

b) Secure and permission less: its more secured than banking one because banking servers can be hackable but this is not, even sending money sometimes requires permission in special cases like when withdrawing more than 1 lakh at sometimes is not permitted from banks but in cryptocurrency we can send and receive any number of amount and whatever it maybe.

c) Fast and global. Unlike in normal monetary function just for sending a money from one person to other we need to give other charges also but in blockchain we don't need to give any other charge for transaction and its faster than normal banking system. generally transferring money from one country to other took more than 3-4 days but in bitcoins it can max took 10 minutes for completing its transaction. so it's fast and globally accepted

d) Distributed: the main benefit of having a distributed network is like when any node got crashed we don't worry for data recovery because it can be recovered from other nodes. And also if any attackers want to attack or wants to alter any data he has to hacked most of the blocks at a time which is impossible.

e) Stability: once the data is written over a block can't be altered so it is stable even though any blocks get corrupted data can be achieved using other blocks of network.



mBTC 477.06
≈ USD 112.44

● 21 Apr Donation for Bitcoi... +6.26

● 19:29, 17 April
Donation for Bitcoin Wallet +13.09

● 17 Apr Donation for Bitcoi... +1.00

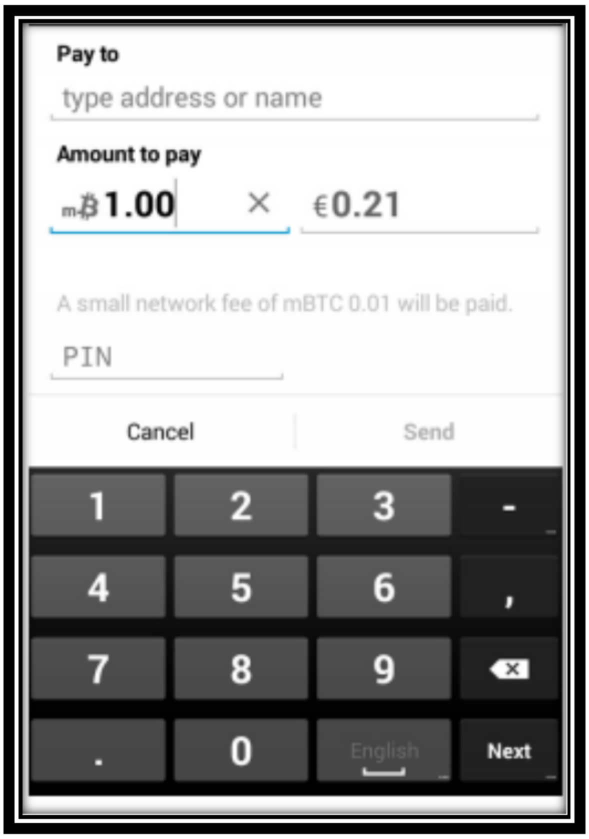
● 15 Apr 13tT vECF HS7D A... +0.97

● 14 Apr 1Bq6 P6LV 7L1K m... -1.00

● 12 Apr Donation for Bitcoi... +0.50

● 11 Apr Donation for Bitcoi... +4.22

Fig -3: Query Bitcoin transaction history



Pay to
type address or name

Amount to pay
m฿ 1.00 × €0.21

A small network fee of mBTC 0.01 will be paid.

PIN

Cancel Send

Fig - 4: Pay with Bitcoin

3.2 Disadvantages

a) Private keys: when anyone lose their private key in blockchain he may get lose all cryptocurrencies and data associated with that block id and it can’t be recoverable.

b) Inefficient: like in PoW context its very competitive and it may be possible that most knowledgeable and experienced person always solves first, so reaming ones who always make their efforts in solving this get ineffective

c) 51% attacks: Theoretically when a blockchain is hacked with maximum blocks data can be altered it means all transaction can be modified, but practically it’s impossible for an attacker to hack all this blocks at a same time which so highly encrypted.

4.Attack cases

4.1. Selfish mining attack

This type of attacks happens when a malicious miner wants to add a block to blockchain with its bad intention. like in PoS if a malicious ledger has more stake than other good miners, just because he has more stake he has given the priority based on PoS he may change or add malicious transactions to the original block.

4.2. DAO attack

In May 2016 an attack happened in the field of smart contract its developed using ethereum . it has been hacked within 20 days’ even though it has raised 150 million UD$ which is biggest till that date.

4.3. BGP hijacking attack

BGP stand for Border gateway protocols, in this type of attack if a malicious miner wants to control most of the node including network of blockchain they may slow down the speed of blockchain and also alter the transaction if he most of the time get wins in consensus.

4.4. Eclipse attack

In eclipse attack a victim can monopolize the incoming and outgoing connections

4.5. Liveness attack

This attack is done when any miners are busy in doing validation if transaction so malicious attackers delaying the speed of processing it. or it increases the computational time by accessing more number of nodes in control.

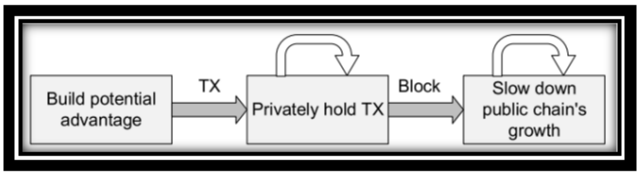


Fig -5: liveness attack process

5.SECURITY ENHANCEMENTS

5.1. SmartPool

smart pool is an secured version of bockchain technique. In this ledger conducts hashing computation for the task and return the share to smartpool. This is how miner gets it reward also and make it more securable. It has some more advantages as decentralization, efficiency and security.

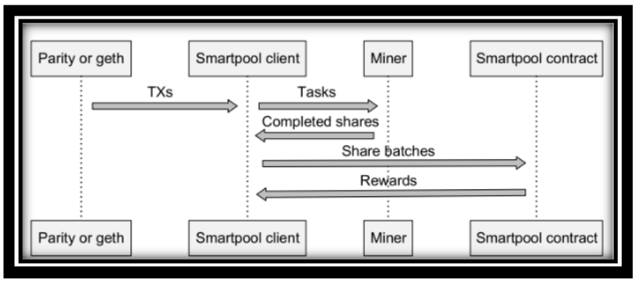


Fig -6: SmartPool's execution process

5.2. Quantitative framework

In this approach block chain stimulator an security model are used and stimulator acts as blockchain runnable whose inputs are arguments of consensus protocol and framework.

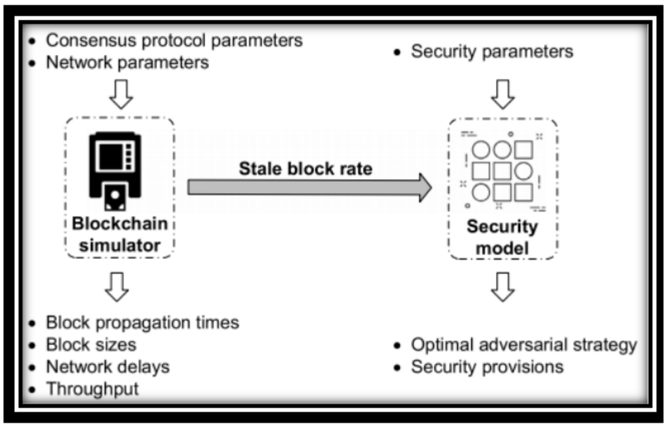


Fig - 7: Quantitative framework

5.3. Oyente

This is a technique in which smart contracts can be executed through analyzing with bytecode of it and it follow EVM model for running.

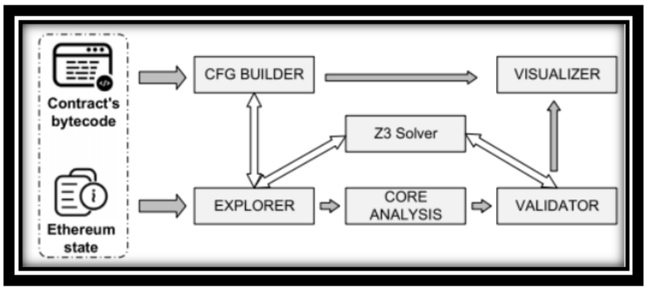


Fig - 8: Oyente's architecture design and execution process.

5.4. Hawk

In this novel approach privacy is being preserve using smart contracts. developers may code private smart contracts and it may be not necessarily to use code encryption.

5.5. Town Crier

This is also based on smart contract model through which it provides a robust security model through using. it achieves isolation among communication and running of Town crier.

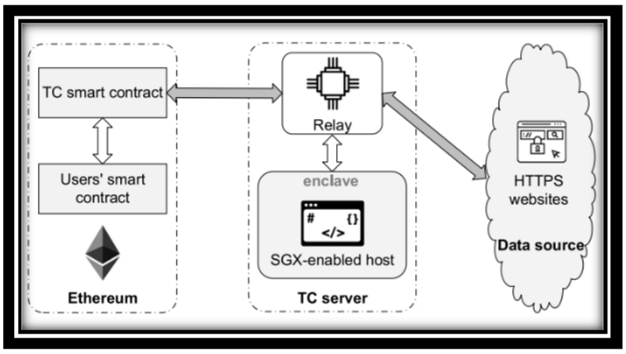


Fig - 9: Basic architecture of Town Crier environment.

6.CONCLUSION

In this survey paper we did a survey of various security and privacy issue of blockchain technologies and we give some suggested approach to solve it. and also we studied blockchain system and we represented it in a brief documented for future research purpose by doing it in a survey form.

REFERENCES

1. Zhou, Q., Huang, H., Zheng, Z. and Bian, J., 2020. Solutions to scalability of blockchain: A survey. IEEE Access, 8, pp.16440-16455.
2. Tripathi, Gautami, Mohd Abdul Ahad, and Sara Paiva. "S2HS- A blockchain based approach for smart healthcare system." In Healthcare, vol. 8, no. 1, p. 100391. Elsevier, 2020.
3. Lin, C., He, D., Huang, X., Xie, X. and Choo, K.K.R., 2020. Blockchain-based system for secure outsourcing of bilinear pairings. Information Sciences, 527, pp.590-601.
4. Bera, B., Saha, S., Das, A.K. and Vasilakos, A.V., 2020. Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System. IEEE Internet of Things Journal.
5. Xu, Yibin, and Yangyu Huang. "Segment blockchain: A size reduced storage mechanism for blockchain." IEEE Access 8 (2020): 17434-17441.
6. Elagin, V., Spirkina, A., Buinevich, M., & Vladyko, A. (2020). Technological Aspects of Blockchain Application for Vehicle-to-Network. Information, 11(10), 465.
7. Wan S, Li M, Liu G, Wang C. Recent advances in consensus protocols for blockchain: a survey. Wireless Networks. 2020 Nov;26(8):5579-93.
8. Páez, R., Pérez, M., Ramírez, G., Montes, J. and Bouvarel, L., 2020. An Architecture for Biometric Electronic Identification Document System Based on Blockchain. Future Internet, 12(1), p.10.
9. Khan, Prince Waqas, Yung-Cheol Byun, and Namje Park. "A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities." Electronics 9, no. 3 (2020): 484.
11. Wang, Eric Ke, Zuodong Liang, Chien-Ming Chen, Saru Kumari, and Muhammad Khurram Khan. "PoRX: A reputation incentive scheme for blockchain consensus of IIoT." Future Generation Computer Systems 102 (2020): 140-151.
12. Garay, Juan, and Aggelos Kiayias. "Sok: A consensus taxonomy in the blockchain era." Cryptographers' Track at the RSA Conference. Springer, Cham, 2020.
13. Miraz, Mahdi H. "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies." Advanced Applications of Blockchain Technology. Springer, Singapore, 2020. 141-159.
14. Bamakan, Seyed Mojtaba Hosseini, Amirhossein Motavali, and Alireza Babaei Bondarti. "A survey of blockchain consensus algorithms performance evaluation criteria." Expert Systems with Applications (2020): 113385.
15. Akyildirim, Erdinc, et al. "The development of bitcoin futures: Exploring the interactions between cryptocurrency derivatives."

Finance Research Letters 34 (2020): 101234.
16. Almasoud, Ahmed S., Farookh Khadeer Hussain, and Omar K. Hussain. "Smart contracts for blockchain-based reputation systems: A systematic literature review." Journal of Network and Computer Applications 170 (2020): 102814.
17. Hewa, Tharaka, Mika Ylianttila, and Madhusanka Liyanage. "Survey on blockchain based smart contracts: Applications, opportunities and challenges." Journal of Network and Computer Applications (2020): 102857.
18. De Giovanni, Pietro. "Blockchain and smart contracts in supply chain management: A game theoretic model." International Journal of Production Economics 228 (2020): 107855.
19. Omar, Ilhaam A., et al. "Ensuring protocol compliance and data t ransparency in clinical trials using Blockchain smart contracts." BMC Medical Research Methodology 20.1 (2020): 1-17.
19. Almasoud, Ahmed S., Farookh Khadeer Hussain, and Omar K. Hussain. "Smart contracts for blockchain-based reputation systems: A systematic literature review." Journal of Network and Computer Applications 170 (2020): 102814.
20. Taylor, Paul J., et al. "A systematic literature review of blockchain cyber security." Digital Communications and Networks 6.2 (2020): 147-156.
21. Wang, Qin, et al. "Blockchain for the IoT and industrial IoT: A review." Internet of Things 10 (2020): 100081.
22. Singh, Sachchidanand, and Nirmala Singh. "Blockchain: Future of financial and cyber security." 2016 2nd international conference on contemporary computing and informatics (IC3I). IEEE, 2016.
23. Rajesh Kumar,Harsh Sinha,Ankita Sharad,Rupali Sahu,"A Case Study on Software Defect Prediction", International Research Journal of Engineering and Technology (IRJET),e-ISSN: 2395-0056,p-ISSN: 2395-0072,Volume.8,Issue 12,pp.1348-1352,30 December 2021
24. Rajesh Kumar, Varun Pramod Bhartiya,Dhananjay Singh,Pavan Rathoriya,Jagmohan Sahu,"PALM PRINT RECOGNITION AND AUTHENTICATION USING DIGITAL IMAGE PROCESSING", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.9, Issue 12, pp.b486-b493,14 December 2021
25. Kumar, Rajesh, Jaykumar Lachure, and Rajesh Doriya. "Use of Hybrid ECC to enhance Security and Privacy with Data Deduplication." In 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 934-941. IEEE, 2021