International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Exploiting Cryptocurrencies Toward Bitcoin Exchanges And Provided Solution For Current Problems

A. Punyavardhan Raj[a*], *G. Nithin*[b], *A. Sai Bharath*[c], *Ch. Abhishek*[d], *B. Prasanth Kumar*[e],

Department of CSE, GMR Institute of Technology, Rajam, AP-532127, India

ABSTRACT

The concept of Bitcoin first came into creation in 2008, as a response to the Great Financial Crisis, and the world of finances relies upon banks for all kinds of financial transactions as intermediaries. Nowadays security has become the biggest issue throughout the world, due to increase in technology there are huge benefits with it, but along with it there are loop holes too. Using these loop holes hackers or any bad actors are being benefitted other than the beneficiaries' these bad actors call these loop holes as vulnerabilities. These vulnerabilities will lie in every software and hardware to provide few beneficial features to the users, rectifying these vulnerabilities are the biggest tasks for most of the cyber security officers. Hackers mostly target financial sectors to help themselves benefitted soon. For being secure from these various attacks banking sectors are doing their best. To avoid these struggles either to the banking sectors side or to the user side there introduced a digital currency called bitcoin by the unidentified person or a group called 'Satoshi Nakamoto' this currency is purely decentralized and completely eliminates the centralized system in which these banks are working. This cryptocurrency work on its own consensuses, which made its existence so mandatory and trust worthy. It works on the blockchain technology which is termed as its backbone to the entire bitcoin network. As this network runs on blockchain technology it is impossible to hack the network, to do this the one who hacks the network needs to gain control over 51% of the entire network which is highly impossible. Even though there are few loop holes existed in the network, as there is a known way is closed then these intruders will find a new way to get control over it and such cases are there in bitcoin. As bitcoin is a decentralized and completely open to each and every onein this world, anyone can be as a miner in this network. In such cases the hacker may breach into the data of any miner in the network and can get some crucial information, if not he may gain control over the node or the miner's computer, which may lead to network corporatization which will gradually makes the network to fall and slowly disappears. In the same way there are few services provided by the bitcoin network to the user's that are non-miners in the network, which further lead a way to hackers to have a chance to get hacked. Those services are hot storages, cold storages, hybrid storages, services will store the user's private key, which is impossible to user to remember as it is in the hash form. And we came up with another vulnerability that is with mempool, where all the unvalidated transactions exit in the network, and we tried to reduce the waiting time even difficulty level is high and also may some effort towards reducing the computational power of the miner in the network.

Keywords: Cryptocurrency, Centralization, Mempool, Merkel root, Vulnerability.

1.Introduction

Bitcoin is termed in the year 2009, it is introduced to this world through a paper to which Satoshi Nakamoto is the main author. When it also given a solution to the double spending problem in decentralized applications. This has acquired a wide range popularity such that the current bitcoin value is 1.6 million in INR where the user needs to pay that amount to own a bitcoin these days. There is independence and no rules while sharing the data of the network without any fear. There is no chance of manipulating the data or a database of the network, bitcoin network uses SHA256 algorithm to encrypt the data, in few encryptions the generated hash can be reversed by various techniques but this SHA256 cannot be reversed and trying for it is a lot of problematic and resource consuming. Most of the networks of various cryptocurrencies like Litecoin, Ethereum, Dogecoin, etc. The backbone of the bitcoin is blockchain, it has various number of consensus where these consensuses are used based on the type of application is developed using blockchain. In bitcoin Proof of Work, Proof of Stack and Proof of Storage are used to maintain the network secured. In those consensuses Proof of work plays the vital role. Using this consensus only the miner who successfully mines a block using his resources will be rewarded with bitcoins. This reward will be varying for every 4 years this mechanism is called Halving. This is because for every successful mining of a block a bitcoin will be generated and for generating such bitcoins a miner is rewarded with 50BTC in the year 2009 but in the year 2013 the reward is halved that is 25BTC and later on it is 12.5BTC and soon, currently the reward is at 6.25BTC later in the year 2023 this will be again halved and drops to 3.12BTC. If this process continues by the year 2140 the reward will be 0BTC by that time 21million BTC will be generated and that is the final count of total bitcoins in the network, these will be rotated over the network and used as a digital currency. Due to this technique most of the users are considering this bitcoin as a digital asset and this will be making the new virtual asset. These bitcoins are now being used by most of the people in every corner of the world, but unfortunately this digital currency is mostly used to buy sedative drugs, illegal weapons and for many more illegal activities online. These bitcoin transactions are mostly found in dark web where all these activities are held secretly. As the details of the user who is making the transaction is completely unidentified and the user is most secured even his activities are malicious and illegal. The main agenda of this bitcoin is to send digital money over internet throughout the world without any centralized authorities like Banks. This allows users to save user charges and transfer fees that are being laid by the banks on the user for utilizing their services. At the same there will be no idea of taking loan over the network because the user who is in this network will be able to generate his own currency in the name of BTC. This allows users save a lot and trust worthy. The total network is not at all maintained by any authority, it is under every miner and user, each and every transaction details are visible and allowed to check just for fun by any user of the network or out of the network. This bitcoin network runs on nodes which are indirectly miners, each miner is validated by confirming weather they are having perfect equipment to mine the blocks of the network. Miner is rewarded due to many his investment and maintaining his equipment, network doesn't provide any facility to do the work over network the miner need to maintain all those so to make it easy a miner is rewarded with BTC along with transaction fee of each transaction in the block that he had mined. This mining will consume huge electricity and more computational power of the computers which is very expensive. To maintain all these in the single movement the miner needs to be rewarded in which it turned everything into an enthusiastic method for active participation of the miners. Even though there is a vulnerability which is mempool waiting time. A user needs to wait minimum of 10 minutes which is a huge time. If a hacker manages to get control over 51% of the network, then this waiting time is more than enough to drop all the bitcoin value to zero. Thiscannot affect the network security but it effects the users and miners only. Blockchain provides us ahigh-level security to our data, blockchain is being used in various sectors like health care centres, finance, agriculture, industries, etc. This technology will be the revolutionary technology in future.

There are some applications which are developed using blockchain, these applications are called as Dapps in general, those applications are developed in various sectors like web browsers like Brave, mining applications like pi and some of the routine applications like Uniswap, Pancake Swap, 1Inch, Aave, etc. These applications are developed to replace some of the routine application which are developed based on web 2.0. Now all these Dapps are developed using web 3.0 technology where this is the completely new version of web applications, it is the most secure and powerful technology which enables us to do any activity securely because the behind one is blockchain.

2.Related works

In this paper we came up with a solution for existing vulnerabilities. These can also be called as drawbacks of bitcoin those are 1) It takes much time for making a transaction, 2) Transaction fees are high, 3) Power consumption is more. All these three are making bitcoin a bit lower. Due to these drawbacks few more cryptocurrencies are generated by solving above drawbacks. Some of those cryptocurrencies that are created to solve the bitcoin drawbacks are Ethereum, Litecoin and few more. So, we came up with a solution for the drawback 2, 3, that is high transaction fees and high-power consumption. We do have a solution for 1st drawback too but there is consensus that doesn't allow us to make that solution to be implemented, that consensus is 'No new block should be added to the network less than 10 minutes.' The miner who violets this consensus will be penalised with value equal to the reward he gains by the mining a block. This consensus is made so mandatory because, there are some miners who are able to set up all the computers with high computational power which can mine a block less than 10 minutes for sure but based on the difficulty level. So due to his high computational powered computers only those miners are able to get reward remaining will be useless even they consume their computational power, to reduce this misunderstanding and to make each and every miner to involve in this mining they made this consensus so mandatory. So, one of the drawbacks cannot be solved until or unless this consensus is lifted or altered a bit to make the transactions faster. In this project we have done everything from scratch that we, have created a virtual network which is nearly equal to bitcoin network which is capable of allotting four miner at a time. We built a network using python script which is work is working all perfectly in vscode. The entire network works on single python script that is blockchain.py, remaining scripts are linked to this network. The total backend work is linked with flask so that connect the frontend and backend with good looking network, it consists of home page, block page, transactions pages, mempool page and wallet page. These pages will display the transactions that are in waiting list and the verified transactions and also works with input data like creating a new transaction.

This is project created a huge amount of bitcoin transactions data and given each transaction data as a new transaction to the input state of the network later it performs some mathematical calculations that and just in calculation time the transaction will be validated, without waiting for 10 minutes just like bitcoin network. All the pending transactions will appear in mempool and when a transaction is validated that transaction will be removed from mempool page and updates its status in the block page and transaction page.Most of the data is generated by the account holders and this validated by miners, In the significant way the validated data will be added to each and every node in the network, this data will be transferred to the miner who will join later on. At this segment we made small change related to security, there are few chances of hacking the network but which is impossible currently, but not 100% so, the only way left to do so is corrupting network nodes slowly. There might be a chance of add malicious content in hash form to the data that a corrupted miner and when a newly added miner requests for data he might also receive that corrupted data, due to this corrupted data the newly added miner will also be compromised. If this process continues the hacker might reach control over 51% of the network which makes the network to collapse soon. To avoid this, we may small change that the data which is requested from the new miner will be sent throughout the network then the nearby miner will send the first half data to the new miner, as the new miner received the first half an alert will be sent to the network again, this notifies the next near miner so that he sends the next half data to the requested miner. If the miner receives the data in correct order and the entire consensus is interlinked correctly then the miner will be in safe zone and the miners who sent the data to the new miner are genuine to the network working properly. This technique will reduce pressure on the network and will help to validate weather the miner is genuine or not.

3. Materials and methods

Receiver's details:

This contains all the details like beneficiary name, account number and his public address, but all this data is completely computed combinedly that generates a public key which allows the sender to send the specified amount in the network.

Private Key:

This is a secret key which is used to validate the user is genuine or not, if the user fails to protect the key will lose all his control of his BTC's, this has to be very much confidential.

Public Key:

This is generated to represent the public identification of the user in the network, using this key only the sender will identify the address for sending the amount which is required.

SHA256(SECURE HASH ALGORITHM):

This is a cryptographic algorithm which is used to safe guard the data which is being transmitted in the network. This is an hashing cryptography it is created by NSA which is different from various hashing functions. This algorithm is an irreversible algorithm, it cannot be changed into plan text once hashed. This is the key feature of this algorithm.

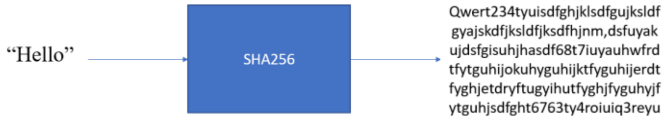
"Hello"
SHA256
Qwert234tyuisdfghjklsdfgujksldf
gyajskdfjksldfjksdfhjnm,dsfuyak
ujdsfgisuhjhasdf68t7iuyauhwfrd
tfytguhijokuhyguhijktfyguhijerdt
fyghjetdryftugyihutfyghjfyguhyjf
ytguhjsdfght6763ty4roiuiq3reyu

Fig-1: SHA256

Signature:

This is used to validate weather the initiated transaction is genuine or not, this follows few steps like weather the user who initiated this transaction is genuine or not and does this user has enough balance to initiate this transaction.

Mempool:

This is short for memory pool, this used to store all the unverified or the transactions yet to be verified in the network, this is not stigmatic storage class once a transaction in this storage is verified it will be removed automatically. This is place where most of the miners pick up the transactions based on the transaction fee.

Nonce:

It is a random value chosen with a fixed length of 32 bits. This is to be decoded that means a miner needs to find the ingredients that are used to generate this nonce value like difficulty level, size of the block and soon. If this value is matched with the miners guessed value, then the transaction is valid and a bitcoin is generated successfully.

Transaction Verification:

Every transaction in the block is verified using computational calculations by the software and some of the preferred hardware section of the miner. It completely involves in guessing the values that is number of zeros present in the nonce value, if found exact same value then the transaction is verified.

Miner:

The user who mines a block using computational power and hardware that are required and generates bitcoins according to the bitcoin network consensuses. Miners receive the reward based on Halving and Block frequency.This can also be called a bitcoin monetary policy.

Halving:

This a process in which the reward for generating a bitcoin or validating a block in the network will be rewarded this reward will be given to the miner who are able to mine that block, in this process the reward will be halved for every four years to make bitcoins limited. By the year 2140, the reward value will be 0 and the total generated bitcoins will be a 21million BTC.The current value of BTC in the market is 17,24,306 INR.

Block Frequency:

The average time required to add a verified block to the network is called block frequency. Currently the block frequency in the network is 1BTC/10mins, that means one block will be added to the network for every 10 minutes on an avarege.

Mining pools:

Group of miners in the network will work combinedly to benefit themselves in those pools any miner can contribute any amount of computational power so that his share will be calculated and given when the reward is given.CPU is a mining pool that is <= 10MH/s.GPU is a mining pool which is = 1GH/s.ASIC is a mining pool that is >1000GH/s(ASIC is short for Application Specific Integrated Circuit)One who uses ASIC for mining will have more chances to win a reward.

Block:

It is container of transaction for limited number of transactions where no new transaction can be added or removed from the block once done. All these transactions are verified by the miners and this mined block will be added to the network.

Block consists of:

Version – This gives the type of block added to the chain.
previous hash – The chaining of every block done here, links the new block to the previous block.
Merkle root - It is the combined hash value of each transaction hash value in the block.
Timestamp – Time will be stamped on the block when it is generated and it is immutable.
Difficultylevel – Based on this value the hash is estimated to be solved in an estimated time.
header - The above details are added and hashed to a single value which acts as a block hash.

Proof of work (PoW):

It is sure consensus that is to monitored. This is the most valued consensus by the miners through which the miners are rewarded by successful mining. It is proof for the work done by the miners in the network.

Proof of Stake (PoS):

This also one of the consensuses in blockchain technology in which it has very small role in the bitcoin network nearly negligible.

Blockchain Features:

1) **Hash Cryptography** – It is a unique cryptography algorithm where SHA256 is used to generate a hexadecimalnumber (0 to 9 and A to F).
2) **Immutable leger –** It is unaltered or modified or deleted once it is added into the chain, it is one of the key features in blockchain regarding security.
3) **Distributed P2P Network –** It is an open network in which every one of the networks will have a copy of every transaction in the network, but it keeps all the data inside the block in a hash format.
4) **Consensus Protocol –** Every transaction will follow a definite protocol for security and privacy issues, misleading this may cause a penalty for the misusers.
5) **Mining –** This is the validation process in the bitcoin network, which is the toughest process in the network, where the miner uses more computational power based on the difficulty of the block, which may sometimes lead to high expenses.

4. Results and discussions

The vulnerabilities that are currently existing in bitcoin are slow transactions, inconsistency of bitcoin value in the market, and high transaction fees. These are the technical problems that are faced by the normal customers of bitcoin buyers, they are slowly converting it into a digital asset but there are some other conflicts among bitcoin miners. As there is an increase in miners in the network there is huge competition, this led to consuming huge computational power for miners. This conflict is reduced to some extent by using the concept of mining pools without losing or violating the consensus of bitcoin. This minute change in the network will be reflecting some results by reducing the computational power by 0.00039 by adding additional miners for a single block and sharing the entire data of the network by two miners with the new miner, this made the new miner receive the data accurately and within no time so that the new miner can easily validate whether the received data is genuine or not.

5. Conclusion and future scope

5.1. Conclusion

In this project we have cleared some issues with the computational power related and one related to security. Step by step process and validation is done in practical way and proved it and it is done we have used python and flask to demonstrate all the solution that we have explained throughout this paper and everything is done with proper care and required knowledge. This improves the security patches and reduced some computational pressure over the miners without crossing the consensuses.

5.2. Future scope

This project may be validated for various future aspects in bitcoin network as the changes that are made are the current problems solution and these can be applied in any time line of this network, there is requirements to make this project work on any computer it works smooth and less power consuming when compared to other applications and software's.

.

Acknowledgements

It is over pleasure to work with our guide Dr. V. Vasuda Rani who encouraged us to do this project and helped us in each and every aspect of our difficult times and showed us a way to make this project up to this extent, all the effort we have kept on this project is according to her guidance and instructions and this project helped us a lot in working with a worlds new technologies that is blockchain it gave us a lot of knowledge and we are here with the knowledge that we have gained through this project.

REFERENCES

[1] K. Oosthoek and C. Doerr, "Cyber Security Threats to Bitcoin Exchanges: Adversary Exploitation and Laundering Techniques," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1616- 1628, June 2021.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] S. Phetsouvanh, F. Oggier, and A. Datta, "EGRET: Extortion Graph Exploration Techniques in the Bitcoin Network," 2018 IEEE International Conference on Data Mining Workshops (ICDMW).

[3] Z. Fang, M. Xu, S. Xu, and T. Hu, "A Framework for Predicting Data Breach Risk: Leveraging Dependence to Cope With Sparsity," in IEEE Transactions on Information Forensics and Security.R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] R. Xiao, W. Ren, T. Zhu, and K. -K. R. Choo, "A Mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain," in IEEE Transactions on Dependable and Secure Computing.

[5] Mendi, Arif & Erol, Tolga & Şafak, Emre. (2020). Generating a Blockchain Smart Contract Application Framework. Advances in Science Technology and Engineering Systems Journal.

[6] H. N. Chua, J. S. The and A. Herbland, "Identifying the Effect of Data Breach Publicity on Information Security Awareness Using Hierarchical Regression".

[7] Cheng, Long, Fang Liu, and Danfeng Yao. "Enterprise data breach: causes, challenges, prevention, and future directions." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery.

[8] M. Xu, K. M. Schweitzer, R. M. Bateman, and S. Xu, "Modeling and Predicting Cyber Hacking Breaches," in IEEE Transactions on Information Forensics and Security.

[9] T. Phaladisailoed and T. Numnonda, "Machine Learning Models Comparison for Bitcoin Price Prediction," 2018 10th International Conference on Information Technology and Electrical Engineering (ICEE).

[10] T. Miseta and A. Vathy-Fogarassy, "The Effect of the Different Data Aggregation Methods and their Detail Levels to the Prediction of Bitcoin's Exchange Rate," 2019 IEEE International Work Conference on Bioinspired Intelligence (IWOBI).

[11] P. -W. Chen, B. -S. Jiang and C. -H. Wang, "Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet," 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).

[12] A. Gifari, B. Anggorojati, and S. Yazid, "On preventing bitcoin transaction from money laundering in Indonesia: Analysis and recommendation on regulations," 2017 International Workshop on Big Data and Information Security (IWBIS).

[13] Ajith GS Master of Computer Application. Bitcoin security - Anti-Dust Attack. Proceedings of the National Conference on Emerging Computer Applications (NCECA)-2022.

[14] E. Badawi, G. -V. Jourdan, G. Bochmann and I. -V. Out, "An Automatic Detection and Analysis of the Bitcoin Generator Scam," 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

[15] Sallal, Muntadher, et al. "Security and performance evaluation of master node protocolbased reputation blockchain in the bitcoin network." Blockchain: Research and Applications 3.1 (2022): 100048.

[16] Caporale, Guglielmo Maria, et al. "Cyber-attacks, spillovers and contagion in the cryptocurrency markets." Journal of International Financial Markets, Institutions and Money (2021).

[17] Groby, Klaus & Dufitinema, Josephine & Sapkota, Niranjan & Kolari, James W., 2022. " What's the expected loss when Bitcoin is under cyberattack? A fractal process analysis," Journal of International Financial Markets, Institutions and Money, Elsevier, vol. 77(C).

[18] R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep delved study into legality, ransomware, underground web and bitcoin wallet," 2016 International Conference on Computing, Communication, and Automation (ICCCA).

[19] C. Y. Kim and K. Lee, "Risk Management to Cryptocurrency Exchange and Investors Guidelines to Prevent Potential Threats," 2018 International Conference on Platform Technology and Service (Platon).

[20] Q. Hum et al., "CoinWatch: A Clone-Based Approach For Detecting Vulnerabilities in Cryptocurrencies," 2020 IEEE International Conference on Blockchain (Blockchain), 2020, pp. 1725.00011.

[21] K. Oosthoek and C. Doerr, "From Hodl to Heist: Analysis of Cyber Security Threats to Bitcoin Exchanges," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-9, 9169412.

[22] S. Mercan, E. Erdin, and K. Akkaya, "Improving Transaction Success Rate via Smart Gateway Selection in Cryptocurrency Payment Channel Networks," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-3, 9169458.

[23] S. Yoo, S. Kim, J. Joy, and M. Gerla, "Promoting Cooperative Strategies on Proof-of-Work Blockchain," 2018 International Joint Conference on Neural Networks (IJCNN), 2018, pp. 1-8, 8489267.

[24] Andani, R., Ali, Y., & Inkiriwang, F. F. W. Stages of Human Resource Planning for National Cyber and Crypto Agency to Support Defense.

[25] Alfieri, C. (2022). Cryptocurrency and National Security. *International Journal on Criminology, https://www. criminologyjournal.*

[26] Guo, F., Huang, X., & Yung, M. (2019). *Information security and cryptology*. Springer International Publishing.

[27] Ramos, S., Melon, L., & Ellul, J. (2022, June). Exploring Blockchains Cyber Security Techno-Regulatory Gap. An Application to Crypto-Asset Regulation in the EU. In *10th Graduate Conference in Law and Technology, Sciences Po (2022)*.

[28] Mohanta, B. K., Satapathy, U., Panda, S. S., & Jena, D. (2019, December). A novel approach to solve security and privacy issues for iot applications using blockchain. In *2019 International Conference on Information Technology (ICIT)* (pp. 394-399). IEEE.

[29] Bhaskar, N. D., & Chuen, D. L. K. (2015). Bitcoin mining technology. In *Handbook of digital currency* (pp. 45-65). Academic Press.

[30] Wang, Q., & Su, M. (2020). Integrating blockchain technology into the energy sector—from theory of blockchain to research and application of energy blockchain. *Computer Science Review*, *37*, 100275.