A Review On Security Aspects Of Bitcoins And Blockchain Technology

Ritu Shree[1], Priyanka Sharma[2]

[1, 2] Dept of Information Technology & Telecommunication

[1, 2] Raksha Shakti University, Ahmedabad, Gujarat -380016

Abstract- *Bitcoin technology as knowtoday has grown vastly due to its security, scalability as well as being an independent crypto currency that does not rely upon conversion and inflation of international borders. All in all, Bitcoin currency is a decentralized platform where no one organization or state is responsible for its control and circulation. This characteristic makes Bitcoin technology so vastly used in large business, but the question arises, how secure is bitcoin currency? The motivation of this literature review is to look into various research papers to help in investigating this question. The area of concern in this paper is to look at Bitcoin technology and presentthe overview on security and privacy aspects of Bitcoin. This paper provides an overview of blockchaintechnology and overview of algorithms used in different blockchains. Furthermore, technical challenges and recent advances are briefly listed.*

Keywords- Blockchain, Bitcoin, crypto currency, decentralization.

I. INTRODUCTION

Nowadays *crypto currency*has become a catchword in industries.Bitcoin has emerged as one of the most successful crypto currency, and has gained a large success with its capital market reaching 10 billion dollars in 2016 [1]. Transactions in Bitcoinnetwork occurs without involving any third party.

Digital transactions and online trading are gaining a lot of interest in e-commerce society. In such electronic payment systems, the consensus is reached via a trusted centralized authority that may appear as a bank, a Chartered Accountant (CA), a notary, or any other trusted service. The use of such third party authorities as an authenticator increases the cost of trading because a nominal fee is deducted as a payment or commission by these third parties. Bitcoin is removing these overhead extra charges and has completely allowed the transactions to be a decentralized. The core technology to build Bitcoin is *blockchain*, which was first proposed in 2008 and implemented in 2009 [2]. Blockchainis regarded as a public ledger and all transactions are stored in a list of blocks. This chain grows by appending the blocksthat holds the transactions information to it continuously. Asymmetric cryptography and distributed consensus algorithms have been implemented for user security and ledger consistency. The blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, blockchain can greatly save the cost and improvethe efficiency.As the payment is done without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment additionally, it can also be applied into other fields including smart contracts.

II. CENTRALIZED DIGITAL CURRENCIES

In a centralized scenario, there is a third party authenticator that will authenticate all the transactions. One eg.is a Bank: the bank issues coins with unique serial numbers and maintains a ledger including all ownerships, i.e., the mapping between user accounts and serial numbers. Assume Alice want to transfer a coin to Bob. In order todo so—in an extremely simple approach—she could generate a digitally signed contract stating

"I transfer one coin to Bob" and broadcast it publicly. Following Bitcoin terminology, such a contract may be called *transaction*.Transmitting a coin would then consist of Alice signing and announcing a transaction of the following form: "I transfer coin '12' to Bob". Bob verifies the ownership of coin '12' by asking the bank. If the transaction is true and Bob accepts the transaction, the bank bring up-to-date its ledger. Simultaneously the owner of the coin changes from Alice to Bob. All the transaction activities are preserved by the third party. Dependency of users on third party is the important criteria here. Bitcoingoals for eliminating the third party dependency, by which one gets rid of the central bank. For this, mechanisms are necessary to create coins in a distributed setting, and to store and accomplish the ledger in a distributed way. Task is to achieve consensus on existing coins and their possession without a third party instance, and without common trust relationships between participants.

III. DECENTRALIZING THE DIGITAL CURRENCY

So, how can we eliminate the central bank? Bitcoin had removed this dependency: in a sense, everyone is the bank. That is, every participant have a copy of the transaction record which earlier was to be stored at the banks.In Bitcoin, the so-called *block chain* takes the role of this distributed ledger. But, distributed storage of multiple copies of the block chain opens up new possibilities for users to cheat. Several drawbacks had evolved from this technology also.

EveryBitcoin transactions are communicated to all participants in the network. The participants need to be lawful.All the transactions are documented in a form known as block. The puzzle used in the proof of work-based distributed validation process consists of calculating a hash value thus formed block and adjusting a nonce in such a way that the hash value is lower than or equal to a assured*target* value. Once one contributor has found such a nonce, the block with the that nonce will be distributed in the network, and contributors will update their local copy of the blockchain[2].Solving the puzzle is computationally difficult task and requires a lot of computational resources. Bitcoin uses the SHA-256 hash functions.

IV. BLOCK CHAIN

Blockchain is the foundation of Bitcoin and has gained huge attentionsnow days. Blockchain basically is an immutable ledger which facilitates transactions to occur in a decentralized manner. Application based on Blockchain are growing up, and covering various fields that includes financial sectors, reputation system, Internet of Things (IoT), and lot many. Still, there are fewchallenges of blockchain technology that needs to be resolved such as scalability and security. We describe an overview of blockchainarchitecture andsome classic consensus algorithms used in blockchains.

(A) Few Characteristics of Blockchain

1. Decentralization

In traditional centralized transactionsystems, each transaction were validated through the central or third party trustedagencies like banks, certainlythis results in paying some cost to the third party and hence needs to be dependent upon them. But in case of to decentralize system, no third party is required for the task to be done. Block chain allowsworking in decentralized fashion. Data consistencies in distributed environment are maintained by Consensus algorithms in Block chain.

2. Persistency

Every transactionis validated by the honest miners. They are paid some intensives for this work. Invalid transactions are not admitted in the block chain by the miners. Once the valid transactions are recorded in the block chain, it is quite impossible to roll back the process. It can neither be edited nor deleted from the block chain. Blocks which are carrying invalid transactions can be discovered quickly.

3. *Anonymity*

Interaction among users of block chain occur with a generated address, that will not reveal the real identity of the user. Hence the user name is not disclose publically. They interact with each other by some generated random address.

4. Auditability

Bitcoinblockchain keeps the data about userBalances. Everytransaction needs to refer to some previousunspent transactions. Oncecurrenttransaction isrecorded into the blockchain, the state of those referredunspent transactions switch from unspent to spent. Sotransactions could be easily verified and tracked.

(B) Types of Blockchain System

Blockchain systems are categorized basically intothree types: Public blockchain, Private blockchain and Consortium blockchain.As name indicates, in public blockchain, everyone can see the records and canparticipate in the consensus process and all decisions making processes. Contrarily, In Consortium blockchain, only a group of few pre-selected nodes will participate in the consensus process. In case of privateblockchain, only nodes from few specific

Organizations will be able to join the consensus process. Because of this feature,a private blockchain is considered as centralized network rather than decentralized one as the central organization is controlling the process.In case of consortium blockchain , that is built by many organizations isconsidered as partially decentralized as small portion of selected nodes will participate in the consensus process.

(C)*Consensus Algorithms*

1. PoW (Proof of work)

In PoW, each node calculates the hash value of block header. Nonce is one field present in the block header. Nonce are frequently changed by the miners to get the different hash values. The calculated value must needs to be less than certain target value for consensus. . Correctness of hash values. The validated new block is then appended to their own blockchains by the miners. Miners are the nodes that calculate the hash values. Calculation of hash values needs very high power computational resources.

2. PoS(Proff of Stake)

PoS (Proof of stake) is another alternative of PoW where less energy is required.Miners in PoS have to prove the possession of the amountof money. It is supposed that people with more currenciesare less likely to attack on network. The assortment based on account balance is quite partial because the richest person is guaranteed to be governing in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to falsify the next block. It uses a formula that looks for the lowest hash value in combination with the size of the stake. As Compared to PoW, PoS saves more energy and is more effective. Unluckily, as the mining cost is almost zero, attacks are more easily possible.

3. PBFT (Practical byzantine fault tolerance)

A new block is resolute in a round. In each round, a primary would be nominated according to some rules. And it is responsible forexecuting the transaction. The whole process could be distributed into three phase: *pre-prepared, prepared* and *commit*. In every phase, a node will enter into next phase if it has received votes from over 2/3 of all other nodes in the network. So basic thing is that, PBFT requires every
Node should be known to the network.

V. ATTACKS ON BITCOIN SYSTEM

Double spending, is very common Attack present in Bitcoinsystem.The other area includes a wide range of Wallet Attacks (Client-side security), Network Attacks (DDoS Sybil and eclipse) and Mining Attacks(Block Withholding, bilberry).

1. Double Spending and Race Attack

In This Attack, the dishonest Client will spend the same coins in multiple transactions, and will try to attempt two conflicting transactions. By doing this they will try to earn by other means. This attack is generally done on merchants or sellers. The adverse effect is that sellers lose their products. The honest user will drive away from the network. And the block chain forks will be created frequently that will adversely affect the performance.

Possible countermeasures Inserting observers in the network can reduce the miscommunication gap, Provision of Double spending Alert among peers should be implemented, and the known nearby peers should notify the merchant about on-going double spending attacks.

2. Finney attack

Fraudulent minerwill broadcast a selected blockfor committing the doublespendingattack as soon asit receives product from amerchant.

Possible countermeasures-Merchants or sellers should wait for multi-confirmation messages or messages from several nodes of the network before completing a transaction.

3. > 50% hashpower or Goldfinger

In this Attack, the attacker will try to consume the computational power in other means and will try to not be used fully by the original miners. Mostly The adversarywill control more than > 50% of computational power in the Bitcoinnetwork. The consequence of this attack will drive away the miners working alone or within small mining pools. It will weakens the effectiveness of consensus protocol, DoS is one main consequence of this attack.

Possible countermeasures

Inserting observers in the network,communicating double spending alerts among peers,disincentive large mining pools.

4. Block discarding or Selfish mining

In this Attack the fraudulent miner (or mining pool) withholds the processedBlock in order to earn inappropriate incentives. This will cause the race conditionsby creating forks, waste thecomputational power of the honest miners.

Possible countermeasures

Zero Block technique, timestamp basedTechniques such as freshness preferred.

5. *Bribery attacks*

In this attack the adversary pay money toMiners to mine on theirbehalf. The only intention is to earn extra incentives and make fool to the original nodes.

Possible countermeasures-One should increase the rewards for honest miners so that everyone should bend towards honesty, try to aware the miners that bribery might cause the long-term losses to the dishonest miners

6. SybilAttack

In this attack the adversary or fraudulent user will create multiple virtual identities in theNetwork for their personal means.

Possible countermeasures

Xim (a two-party mixing protocol) can be applied to overcome this attack.

VI. POSSIBLE FUTURE DIRECTIONS

(A) *Blockchain testing*

Blockchain testing can be separated into two phases:*standardization phase* and *testing phase*. In standardizationphase, all standardsneed to be fulfilled and agreed. When ablockchain is created, it will be tested with the agreed normsto valid if the blockchain works well as developer'sentitlement. Asfor testing phase, blockchain testing needs to be accomplished with different standards. For example, an user who is in chargeof online retail business upkeeps about the throughput of theblockchain, so the investigation needs to test the average timefrom a user refer a transaction to the transaction is packed intothe blockchain, capability for a blockchain block and etc.

(B) *Stop the tendency to centralization*

Blockchain is planned to be a decentralized system. But, there is a tendency that miners are centralized in the mining pool.Up to now, the top 5 mining pools altogether owns greater than 51% of the overall hash power in the Bitcoin network. Beside from that, selfish mining strategy indicates that pools withover 25% of total computing power can get more revenue than unbiased share. Rational miners would be fascinated into theselfish pool and lastly the pool could easily beat 51% ofthe total power. As the blockchain is not proposed to serve afew organizations, some methods can be proposed to solvethis problem.

(C) *Blockchain Applications*

Presently most blockchains are used in the commercial domain,more and more applications for different fields are appearing. Traditional industries can take blockchain into consideration and apply blockchain into their fields to improve their systems. For example, user status can be stored on blockchain. Simultaneously, the up-and-coming industry can make use of blockchain to increase performance. A smart contract is a electronic transaction protocol that executes the terms of a contract. It has been planned for long time and now this idea can be implemented with blockchain. In blockchain, smart contract is a small code that can be executed by miners itself. Smart contract has transformative prospective in various fields like financial services and IoT.

VII. CONCLUSION

Blockchain has shown its potential for transforming traditional industry with its key characteristics like decentralization, persistency, anonymity and auditability.

We had listed some challenges and problems that will obstruct blockchain development and summarized some existing approaches for solving these problems. Some possible future directions are also proposed. Nowadays blockchainbased applications are bouncing up.Simultaneously we had describeb some features of bitcoins. Bitcoins had now revealed as a popular digital currency in the market. Though, the fame of Bitcoin has attracted criminals to use Bitcoin network for their self-seeking reasons and benefits. Today we have nearly 700 different crypto currencies in action; nevertheless, the outstanding popularity of Bitcoin makes this currency favourite for hackers.

VIII. ACKNOWLEDGEMENT

We would like to thank our institute to grant permission to perform our research work on such topics and providing all the required materials to us. I would like to thank my parents and friends for their constant support and encouragement

REFERENCES

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

[2] Bitcoin and Beyond: A Technical Survey onDecentralized Digital CurrenciesFlorian Tschorsch and BjörnScheuermann

[3] An Overview of Blockchain Technology:Architecture, Consensus, and Future TrendsZibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3

[4] A Survey on Security and Privacy Issues of BitcoinMauro

Conti, Senior Member, IEEE, Sandeep Kumar E, Member, IEEE, ChhaganLal, Member, IEEE,SushmitaRuj, Senior Member, IEEE