Security Attacks on Blockchain

Kameswara Rao Kesavarapu
Oracle ERP & IoT Consultant
Block 37, Flat 401
Rain Tree Park, KPHB
Hyderabad-500072

V. Prasanna Venkatesan, PhD
Professor
Department of Banking Technology
Pondicherry University
Puducherry-605014

ABSTRACT
Many organizations are considering the adoption of blockchain technology as they believe that hacking the blockchain environment is extremely difficult as information stored on the blockchains use various cryptographic techniques to validate transactions and store them securely. But like other technologies, blockchains are also susceptible to attacks. In this paper, discussed about different types of consensus mechanisms that are used in validating the transactions of a blockchain network. This paper also focuses on key cryptography techniques that are often used in blockchain. This paper highlights security vulnerabilities and various noteworthy attacks that took place in blockchain environment.

General Terms
Blockchain

Keywords
Proof of Work, Proof of Stake, Cryptography, Bitcoin, Ethereum, Blockchain, Security Vulnerabilities.

1. INTRODUCTION
Blockchain is fundamentally a distributed tamper proof ledger that stores information in a secured way using cryptography. The first block in the block chain is called as "Genesis" block. Each block has a link to its previous block such that all the blocks are chained together. Any new transaction is added to the block only when a minimum of 51% of participating nodes validate and approve the transactions through consensus mechanism such as Proof of Work. The node that validates the transaction is called a miner who may get rewarded for the work done. Once a block is approved, all the other participant nodes in the blockchain update their ledger copy. This entire process makes blockchain a secure record store.

2. CONSENSUS
One of the key security aspects of blockchain is Consensus where hundreds or even thousands of nodes validate a transaction and ensure that the same copy of ledger is maintained across the blockchain network. This needs lot of computing power and even the most powerful blockchain can process somewhere around 40 to 50 transactions per second which is way lower than the current processing speed of modern payment networks which can scale up to 70000 transactions. Although Proof Of work and Proof of Stake are the most popular consensus algorithms that are used in various blockchains, there are many other powerful consensus algorithms that are invented in the recent past which are widely considered across the globe such as Practical Byzantine Fault Tolerance, Delegated Proof of Stake, Directed Acyclic Graph.

2.1 Proof of Work
Satoshi Nakamoto who is considered as father of blockchain has applied 'Proof of Work' consensus technique for Bitcoin that is currently using more than 10000 nodes to validate transactions and blocks. Anyone who wants to become a miner can install Bitcoin full node program in their system and start validating the transactions.

The Proof of Work algorithm is designed based on a concept called 'Scarcity' of computational resources. Miners in the blockchain compete to solve a mathematical cryptographic problem using machines that has good computation power which keeps on guessing to find the right answer that is acceptable across the network. The one who cracks the problem first will create the new node and incentivized for the work done.Computational resources are scarce in nature and Proof of Work exploits this reason by selecting a problem that can be solved only by guessing. Whoever guesses the right answer first gets incentivized. To increase their chance to win, miners can run as many mining equipment as possible. Since miners need to spend a lot of money for buying and maintaining these machines, no individual miner may have the capacity to maintain huge number of machines just to control the entire blockchain network and win the incentive which could be much lesser than the investment. Proof of work algorithm assumes that no individual can control more than 50% of network resources. Trying to attack a Proof of Work network is very expensive and the hacker need more money than he can steal from the network.

2.2 Proof of Stake
Proof of stake is an alternative consensus mechanism that allows a node to create a new block in the blockchain by paying a transaction fee for validating the transactions. The Proof of Stake algorithm is designed based on a concept called 'Scarcity' of the given cryptocurrency. Ethereum (second largest blockchain) is planning to switch from 'Proof of Work' consensus to 'Proof of Stake'.

In Proof of Stake, the block producers are called as validators rather than miners. Validators must put down their stake or do some deposit to participate in the process of block creation. In Proof of Stake, the creator of new block is chosen in a deterministic way by a selection algorithm that takes their stake into account. Once the validator is chosen, they have the exclusive rights to validate and create a new block. The other validators don't waste their energy as they need not compete with others in solving the puzzle. This will reduce the energy consumption dramatically when compared to Proof of work process which makes it more scalable and sustainable consensus mechanism. If the validator indulges in any form of cheating, they will lose their deposited stake immediately. This process ensures that the validator behaves honestly. Proof of Stake algorithm assumes that no individual can control more than 50% of a cryptocurrency.

2.3 Proof of Work vs Proof of Stake

Proof of Work is one of the well proven consensus protocol that went live with Bitcoin in 2009. Although there were few successful hacks against smart contracts written on top of blockchain, no one could exploit Proof of Work itself which shows the robustness and security of this protocol. However, there are few shortcomings to Proof of Work protocol such as low processing capability, need for huge computing power and specialized mining rigs due to which the blockchain community had started working on other alternatives and one of the great outcomes of it was 'Proof of Stake'. In Proof of Stake model, there is no need for someone to have specialized hardware and huge computing power to be a miner. Due to this requirement of huge computational power and equipment in Proof of Work, majority of the processing power comes from large datacenters in countries where electricity is very cheap. For e.g., In Bitcoin network, nearly 80 percentage of processing power resides in 6 major data centers in china. This kills one of the most important aspects of blockchain i.e., decentralization. To be a validator in Proof of Stake, one needs to have cryptocurrency to stake as this model rewards the nodes with most money staked and not the one with huge computational power. Decentralization and speed are the biggest motives to move from Proof of Work to Proof of Stake.

Consensus plays a vital role in verifying whether the transactions in the pool are valid or not thereby creates a new block to the existing chain. One of the key aspects of blockchain is immutability and it is achieved through Consensus. The other key element which makes blockchain secure and immutable is Cryptography. Messages are sent securely between two parties using various Cryptography techniques in the presence of bad actors such as hackers who may want to corrupt the message.

3. CRYPTOGRAPHY

Blockchain became so popular as it eliminates the need of a third party as intermediary to create trusted transactions and records. A layer of trust between trustless parties is created in Blockchain by storing the information in blocks using cryptography techniques such that only the user with right key and cryptographic signature can access it.

3.1 Key Concepts

There are four key elements that everyone should be aware of in Cryptography – Secret, Key, Function and Cipher. Secret is nothing but a piece of information that is to be protected. Key is a piece of data that is used for encrypting this information and decrypting when needed. Function is the mechanism that does this encryption for us by taking Secret and Key as inputs. The output of the function is referred to as Cipher.

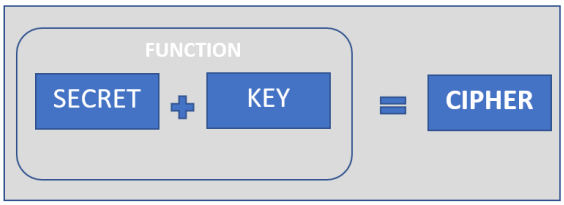

Fig. 1 Key Terms in Cryptography

3.2 Public Key Cryptography

In Public Key Cryptography, a private key and a public key are used for digital signatures and encryption. As the name says Public keys are publicly known to everyone whereas private key is of utmost secret.

If A wants to send a message to B, A will encrypt this message(secret) with public key of B and share the cipher with B so that only B can decrypt the cipher with his private key. If any unauthorized user tries to decrypt this message with his private key, it doesn't work. To ensure B that the message does really come from A, a digital signature is created on top of the message with A's private key. Now B will use the public key of A to authenticate whether the message had really come from A and not tampered since then. If someone else tries to personify A and sends this message to B, B can find it very easily as the public key of A doesn't work here and B realizes that the message is not signed by A. If A wants to pay 3 bitcoins to someone, it is very easy to authenticate whether the message had really come from A or not and then it is equally easy to protect this message from hackers or bad actors in the network such that it cannot be tampered. Blockchains use public key cryptography extensively on transactions for verifying the identity of the creator and to ensure that data is not modified since signing.

3.3 Zero-Knowledge Proof

This is a technique where one person can prove to other that given statement is true without revealing any additional information. For e.g., a Zero-Knowledge Proof(ZKP) allows a user to prove that he is of a certain age without revealing his actual age. In financial services industry, ZKP will help in improving confidentiality in a public ledger which is one of their biggest obstacles. ING is a multinational bank which had added a 'Range' factor to their blockchain solution such that it allow users to prove he has a secret number which lies in a known range. For e.g., a mortgage applicant could prove that his salary is within a specific range without revealing his exact salary. One of the use case for ZKPs in blockchain is When a user makes a transfer request of some bitcoins (or money) from his account to another, the blockchain needs to ensure that the sender has enough money in his account to process this request without worrying about who this user is and how much money does he has in his account. Anonymity/Privacy is one of the key requirements in blockchains and this can be achieved through ZKPs.

3.4 Hash Functions

A Hash Function takes any input and generate a fixed size output which is also called as Hash. Even a minor change in the input changes the Hash output dramatically. It is very difficult to guess the input based on hash output. This technology helps us to condense the message of any size into a small piece of data. Hash functions belong to one-way cryptographic function category.

A simple use case that can explain the significance of Hash Function is to store the passwords in the form of a Hash rather than storing it as is in the database so that it can never be corrupted or stolen by a hacker and at the same time authentication of the password still happens correctly. Every time a user enters the password, the hash of the entered password gets generated and compared with the original one in the database. If both matches, it is an authentic login otherwise the system concludes that the user had entered the wrong password. One other classic example is self-driving cars. Every time the user starts his self-driving car, it can generate a hash out of its current source code and authenticate

it with original hash that is stored in the blockchain maintained by a central authority or car company. If the authentication fails, it may not be safe anymore to drive this car as the software might have been compromised by a hacker.

Cryptographic hashes are used to chain the blocks in a blockchain such that even if one block gets hacked the link breaks from the subsequent block so that it is easy for any validating node to find the discrepancy immediately and reject the change.

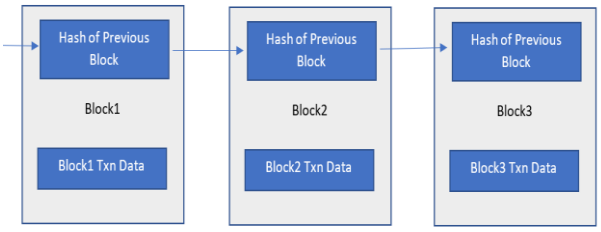

Fig. 2 Simple Blockchain Structure

Tampering the data in any of the block regenerates a new hash for that block there by destroys the link to next subsequent blocks.

To create a new block, a hash needs to be generated by combining the data in the block with a random number called 'Nonce'. For e.g., In a specific blockchain, there could be a protocol to generate a hash starting with four leading zeros (mathematical puzzle). To do that, miners keep on guessing for a nonce value until a hash gets generated with four leading zeros by using huge computational power. The miner who cracks this first wins an incentive.

Although blockchain can resist traditional cyber-attacks with various cryptography and consensus techniques, hackers are coming up with new techniques to attack blockchain's security and making them vulnerable.

4. SECURITY ATTACKS

Blockchain follows a completely different approach to validate transactions and store the information. Blockchain ensures security by doing incredible amount of repetition. A smart contract is a piece of code that runs on blockchain. In blockchain environment, smart contracts often call other smart contracts. Due to this very nature, one should be very careful while calling other smart contracts so that any security vulnerabilities from other smart contracts doesn't get inherited.

Blockchain is a decentralized distributed system that runs on untrusted hardware. In traditional environment, the primary goal of cyber security is to ensure hackers and untrusted parties not to enter the network whereas security in blockchain is provided by ensuring that same ledger is maintained across nodes and each block is immutable from making any updates.

Here are the few attacks that can be launched against blockchain:

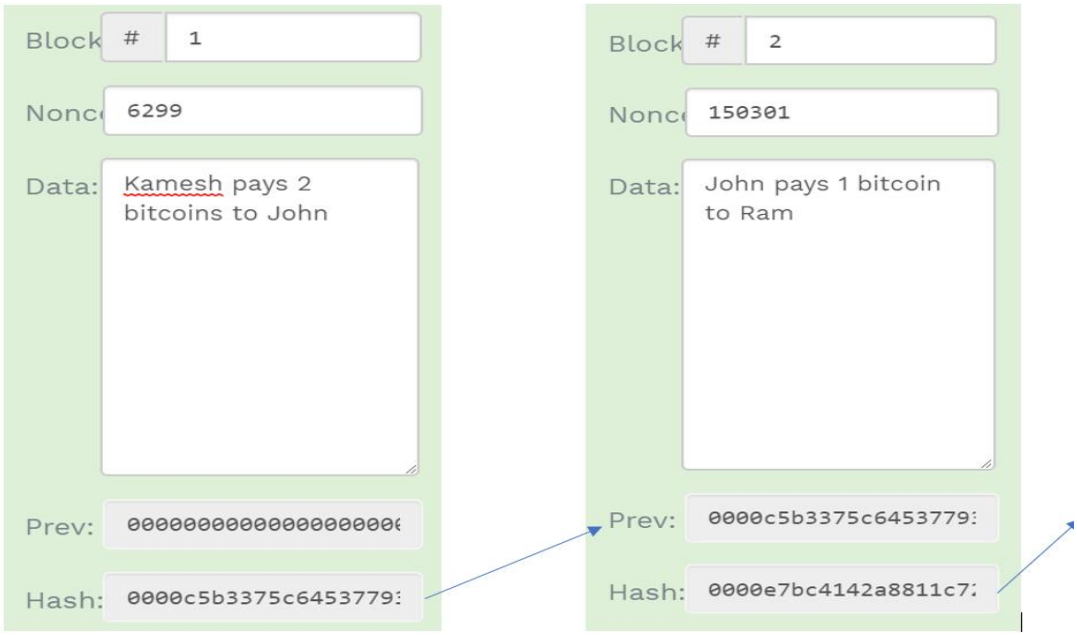

Fig. 3 Blockchain with Hash Link to previous Hash

4.1 Denial-of-Service

This is one common form of attack where the hacker floods the target system in such a fashion that the system can no more serve its users. A Denial-of-Service(DoS) attack in blockchain involves submitting more transactions than it can handle. Another way of DoS attack in blockchain network is to send bogus traffic to other peer nodes by taking control of one or more nodes in the network. This will slowly congest the entire network and the genuine transactions may not get executed as all the nodes are busy validating bogus traffic.

4.2 Endpoint Security Attacks

Endpoints are the platforms where human beings interact with the system. In traditional environment, endpoints are under the control of the enterprise whereas in blockchain environment end users and miners use their own systems to access the services of blockchain. To access blockchain, one need to have private key handy. Hackers steal user's keys by various means such as attacking their email accounts or laptops. Mt. GoX exchange, one of the largest bitcoin exchange in 2014, was hacked by getting access to a computer that belongs to an auditor of that company. The bad actor used

the access to alter the value of a bitcoin to once cent and then transferred around 2000 bitcoins from customer accounts.

4.3 Code Vulnerabilities

Anyone can develop a smart contract that can run on top of a blockchain and a small loophole in the underlying platform or smart contract can have wide reaching consequences. There was a big hack discovered against bitcoin network due to an integer overflow vulnerability in 2010. Around 92 billion bitcoins were received by two addresses because of a small flaw in the code that was used for checking transactions where the developer had not anticipated such a huge number that came into picture when summed, that ended up in overflow of integer. A hacker exploited a flaw in the Parity multi-signature wallet on the Ethereum blockchain and drained 3 massive wallets of worth $31,000,000 of Ether. This exploit was possible not because of a vulnerability in Parity or Ethereum rather due to a vulnerability in the smart contract code given by Parity client to deploy multi-signature wallets for their users. The hacker found a small bug in the smart contract code that allowed him to re-initialize the wallet, that allowed him to set himself as the new owner and run away with everything in the wallet. Ethereum had to do a hard fork to nullify this attack.

4.4 Sybil Attacks

This is an attack where the hacker pretends as many nodes in the blockchain at the same time. When the hacker takes charge of major percentage of peer nodes in the blockchain network, every transaction gets accepted as the bad actor owns majority of the nodes. It is very difficult to do a Sybil attack on a longer blockchain network such as bitcoin as huge computing power is required to do this.

4.5 Eclipse Attacks

Rather than attacking the entire network at once as in Sybil attack, the hacker attacks few specific nodes in Eclipse attack. The bad actor attacks specific nodes and eclipse them from the network. The hacker sends a transaction showing proof of payment to this victim node(s) and then sends another transaction to the entire network using the same tokens.

4.6 Routing Attacks

Routing attack primarily comprises of two separate attacks. The first one is 'Partitioning attack' where the malicious internet service provider(ISP) partitions the blockchain network into two or more groups by hijacking few important network points. The second step is 'Delay Attack' in which the malicious ISP delays the block propagation that makes the blockchain network susceptible to double spending.

Since 2017, Hackers had stolen nearly $1 billion worth of cryptocurrency. Here is the list of major hacks that took place in the last 2 years.

5. RESEARCH OPPORTUNITIES

There are various research opportunities that are available to confront security attacks in blockchain.

- Establishment of Network Architecture
- Transaction Reversibility
- Faster Transaction Verification
- Ability to restrict access
- Cryptanalysis
- Anonymity
- Data mining Security
- Security Modelling

6. CONCLUSION

Decentralized blockchain networks will surely enhance the security over centralized systems but at the same time it is important to understand that the blockchain networks are not completely immune to cyber-attacks. With security best practices and proper governance strategy, majority of these security attacks can be eliminated, or the damage can be mitigated.

7. REFERENCES

[1] Linux Foundation, "Blockchain: Understanding Its Uses and Implications," 2018.

[2] Michael del Castillo & Bailey Reutzel, "$100 Billion Controversy: XRP's Surge Raises Hard Questions for Ripple," *coindesk.com*, Jan 2018.

[3] Emilio Janus, "BITCOIN PUBLIC FULL NODE COUNT SURPASSES 10,000," *bitcoinist.com*, Nov 2018.

[4] Alyssa Hertig, "Ethereum's Big Switch: The New Roadmap to Proof-of-Stake," *coindesk.com*, May 2017.

[5] Tommy Koens, Coen Ramaekers and Cees van Wijk, "Efficient Zero-Knowledge Range Proofs in Ethereum," 2015.

[6] Ehab Zaghloul, "Beginners Guide on Blockchain Security Attacks Part 1—Network," *medium.com*, July 2018.

[7] Andrew Norry, "The History of the Mt Gox Hack: Bitcoin's Biggest Heist," *blockonomi.com*, Nov 2018.

[8] Admin, "Value overflow incident," *en.bitcoin.it*, July 2016.

[9] Haseeb Qureshi, "A hacker stole $31M of Ether—how it happened, and what it means for Ethereum," *medium.freecodecamp.org*, July 2017