Blockchain Professional Course

Attacks over Blockchain

51% Attack

- It states that group of miners controlling more than 50% of the network's mining hashrate, or computing power can take over the network.
- It is a speculative attack described over Bitcoin blockchain.
- Bitcoin Gold, at the time one of the top 30 cryptocurrencies, suffered a 51% attack and lost $18 million.
- Potential damage could be
    - The attackers would be able to prevent new transactions gaining confirmations, allowing them to halt payments between users.
    - Attackers would also be able to reverse the transactions that were confirmed while they were in control of the blockchain network, meaning they could double-spend coins.
- The mining pool ghash.io was briefly exceeding 50% of the bitcoin network computing power in July 2014, leading the pool to commit to reducing its share of the network voluntarily.

Eclipse Attack

- This attack is based on Distributed application architecture that partitions tasks or workloads among peers without the need for a central coordinating server or stable hosts.
- Cripple a node in such a way that it can not talk to other nodes in the network.
- This attack is possible due to design strategy flaws in the Blockchain such Peer's identity and Peer Selection Strategy.
- Currently, Bitcoin has eight outgoing connections, and Ethereum has 13 which implies one node in Bitcoin only has a view for eight nodes connected to it.
- So one node in Bitcoin has to depend on the other 8 for the complete view of the network which can be taken advantage by the hacker.
- Potential damage could be:
  - Double spending;
  - Attacks against second layer protocols, e.g., an attacker can obtain the products/services without paying by tricking his victims into thinking that the payment channel is still open while the non-eclipsed part of the network sees that payment channel is closed.
  - Smart contracts also may be attackable if users see inconsistent views of the blockchain.

Sybil Attack

- In a Sybil attack, the attacker attempts to fill the network with clients nodes that they control, if this happens then you would be most likely to connect with attacker nodes.
- Bitcoin never keeps a count of nodes for anything, If the attacker completely isolates a node from the honest network than it can help the attacker in the execution of other attacks.
- Potential damage could be:
  - Attacker refuse the relay blocks
  - Attacker only relay blocks which he creates.

Timejacking Attack

- Timejacking attack is an extension of the Sybil attack.
- Each node internally maintains a network time counter.
- The counter is based on the median time of a node's peers which is sent in the version message when peers connect.
- The network time counter reverts to the system time if the median time differs by more than 70 minutes from the system time.
- Potential Damage could be:
    - An attacker could potentially slow down or speed up a node's network time counter by connecting multiple peers and reporting inaccurate timestamps.
    - Since the time value can be distorted by at most 70 minutes, the difference between the nodes would be 140 minutes.

THANK YOU

For more information contact
info@we2blocks.com