Research on the Security of Blockchain Data- A Survey

- blockchain data directly affects the security of various applications of blockchain
- classification of blockchain data attacks

defenses of blockchain data

privacy
- data leakage
- through analysis
  - Finding Bitcoin Relations between Different Addresses
  - Tracking Special Transactions
  - Discovering the Rule of Transactions
- transaction
  - Transaction Characteristics
  - Transaction Rules
- identity privacy
  - Multiple Input Addresses
  - Multiple Output Addresses
  - Input Addresses and Change Address

availability
- abnormal or incor- rect access
  - eclipse attacks
    - Populating Tried and New Tables
    - Restarting the Victim
    - Selecting Outgoing Connections
    - Monopolizing the Eclipsed Victim
  - network traceability
    - IP address
    - topology
    - transmission information

integrity
- tampered
- selfish mining
  - does not publish the blocks
    - private fork
  - selfish mining strategy will get more benefits
- double-spending
  - computational power
  - Attacker Used the same Bitcoin to Trade with multiple Users at the same Time:
  - Attacker Used his own Computing Power to Launch an Attack
- block with- holding attacks
  - sabotage attack
  - do not have any mining blocks
  - not have any benefit
  - fork after withholding (FAW) attack

controllability
- manipulated by smart contract vulnerability
  - vulnerabilities of smart contracts
    - Smart Contract Vulnerability Summary
    - Errors in Encoding State Machines
    - Plaintext transmission
    - Misaligned Incentives

important open research directions

threats
- openness
  - exposes users' privacy
- Network attacks
- selfish mining attacks
- data will be tampered
- Smart contract vulnerabilities
- mining pool attacks
- miner attacks

surveys
- security and adversarial strategies of proof of work
- vulnerabilities of smart contracts
- summarized some cases of attacks

main contributions
- classification and summary
- attacks and defenses
- describe attacks and defenses
- research hotspots
- future research direc- tions