HOW SECURE IS BITCOIN AND ETHEREUM BLOCKCHAIN?

Ajay Singh, Sandeep Shukla

MINING POOL ATTACK
- Selfish Mining
- Fork After Withholding
- Bribery Attack

Double Spending Attack
- Finney Attack
- Brute-force Attack
- Balance Attack

MINING POOL ATTACK
- Miners act maliciously to get unfair rewards

Client Side Security Threats
- Wallet Theft
- Installation of Buggy Software
- Incorrect Usage

Spending the same set of bitcoins in two different transactions

Hash of Predecessor
- Backward Compatibility
- Freshness Preferred

Cold Wallet
- Blue Wallet
- BitGo

BitCoin Network Attack
- Code Vulnerability
- DDOS
- Sybil Attack
- Eclipse Attack
- Tampering

Attacks due to flaw in design and implementation of the protocol.

Ref: IEEE A Survey on Security and Privacy Issues of Bitcoin