Blockchain & Cybersecurity

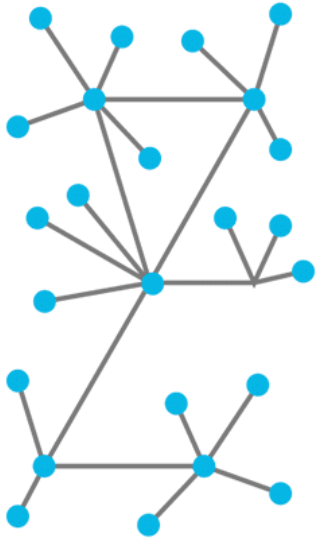
Enhancing security through decentralization

What is Blockchain?

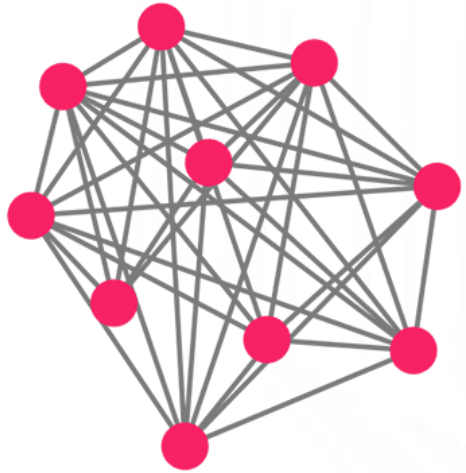
Blockchain is a special kind of Database

Centralized

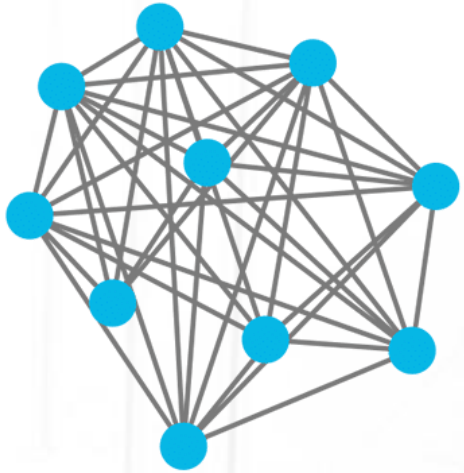
Decentralized



Distributed Ledgers



Permissioned

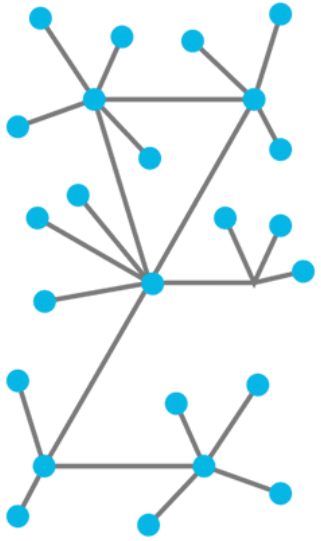


Permissionless

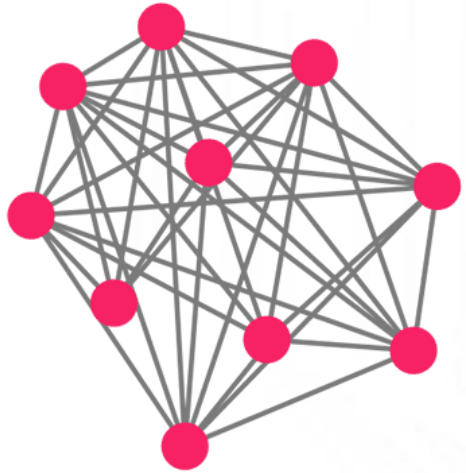
Blockchain is a Distributed Ledger

Centralized

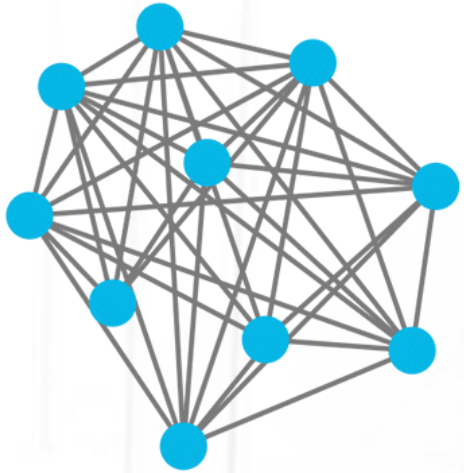
Decentralized



Distributed Ledgers

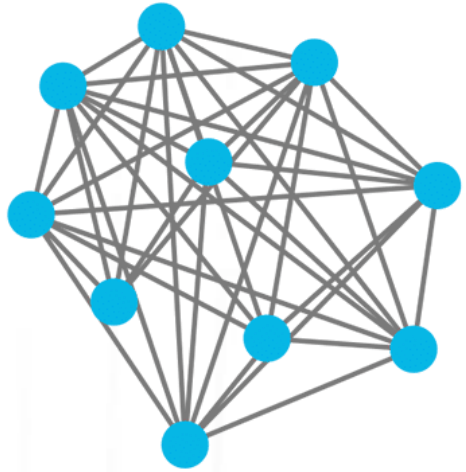


Permissioned



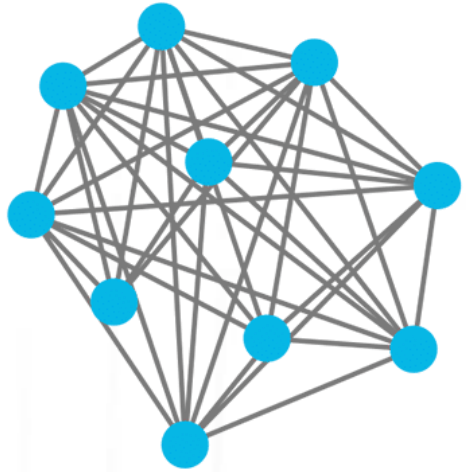
Permissionless

Benefits of Blockchain



- Peer to Peer
- Each node has direct connections to other nodes
- Trustless – No central authority
  - No worry about manipulation
  - No transaction cuts
  - Privacy

Benefits of Blockchain



- Data Integrity
- Disclaimer: Blockchain ensures data integrity of database, not data input
- Entire network maintains same data across different nodes
  - Stores hash of file instead of actual file
  - Each file results in a different hash → exact representation
- If I hack into one and change the data → Rest of network reject the anomaly
- Depending on consensus algorithm, can tolerate <50% compromised systems.
  - Previously, single point of failure → Just need to hack into 1

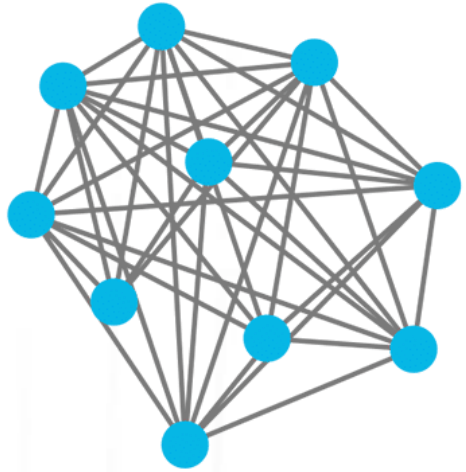
How is a Blockchain Fraud-proof?

- Each Block has a hash called the Block hash
  - This hash is defined by the data inside that block
- Each Block hash is determined by the previous Block hash
- This forms a chain of blocks, all linked together
- Changed data from existing blocks will be rejected by the rest of the nodes
- Demo

Benefits of Blockchain

- Transparency and Auditability
- Data on the blockchain is available to everyone
  - Permissioned: Only nodes in the blockchain
  - Permissionless: Anyone, even those not in the blockchain
- Data is transparent and easily auditable
- Hard to cheat participants when everything is auditable
- Data Privacy ➔ Zero Knowledge proofs

Benefits of Blockchain



- High Availability
- As long as one node is online, the system continues to work
  - Nodes will be reconnected to this node when back online
- Even if all nodes are offline, data is not lost
  - Each node still retains copy of data
- Previously, DDoS single point of failure, now Attacker needs to DDoS all nodes
  - Much more difficult

Benefits of Blockchain

- Faster and Cheaper than traditional processes (Using Smart Contracts)
- Smart contracts require Blockchain for Fraud-proof attributes
  - We don’t want contract to be manipulated after activated
- Can streamline verification, reconciliation, clearance and other business processes

Cybersecurity Impacts

Data Security

- Data integrity for sensitive information
- ”Our goal is to provide every Soldier...Marine the confidence that they can rely on the information they see and the equipment they operate without fear that it has been manipulated by an outside force,”

guardtime FEDERAL

LOCKHEED MARTIN

IoT

- Currently, IoT data requests are aggregated into a single point of trust
  - The calling device is inherently trusted
  - Single point of Failure
- Blockchain allows IoT devices to form group consensus of normality
  - Each IoT device has a record of each other's activity
  - Trust is distributed to all devices
  - Able to quarantine IoT devices that behave abnormally

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

CHRONICLED

Authentication Protocols

- Decentralised Certificate Authorities
  - Centralised CAs run risk of compromise, internal misuse or mistakes
  - Decentralising the certificate signing process with multiple parties reduce risk
- Storing PKI Certificates on Blockchain
  - SSL keys on devices directly authenticate with validated certificates
  - Fake certificates will not be verified due to auditability and immutability of Blockchain

ethereum

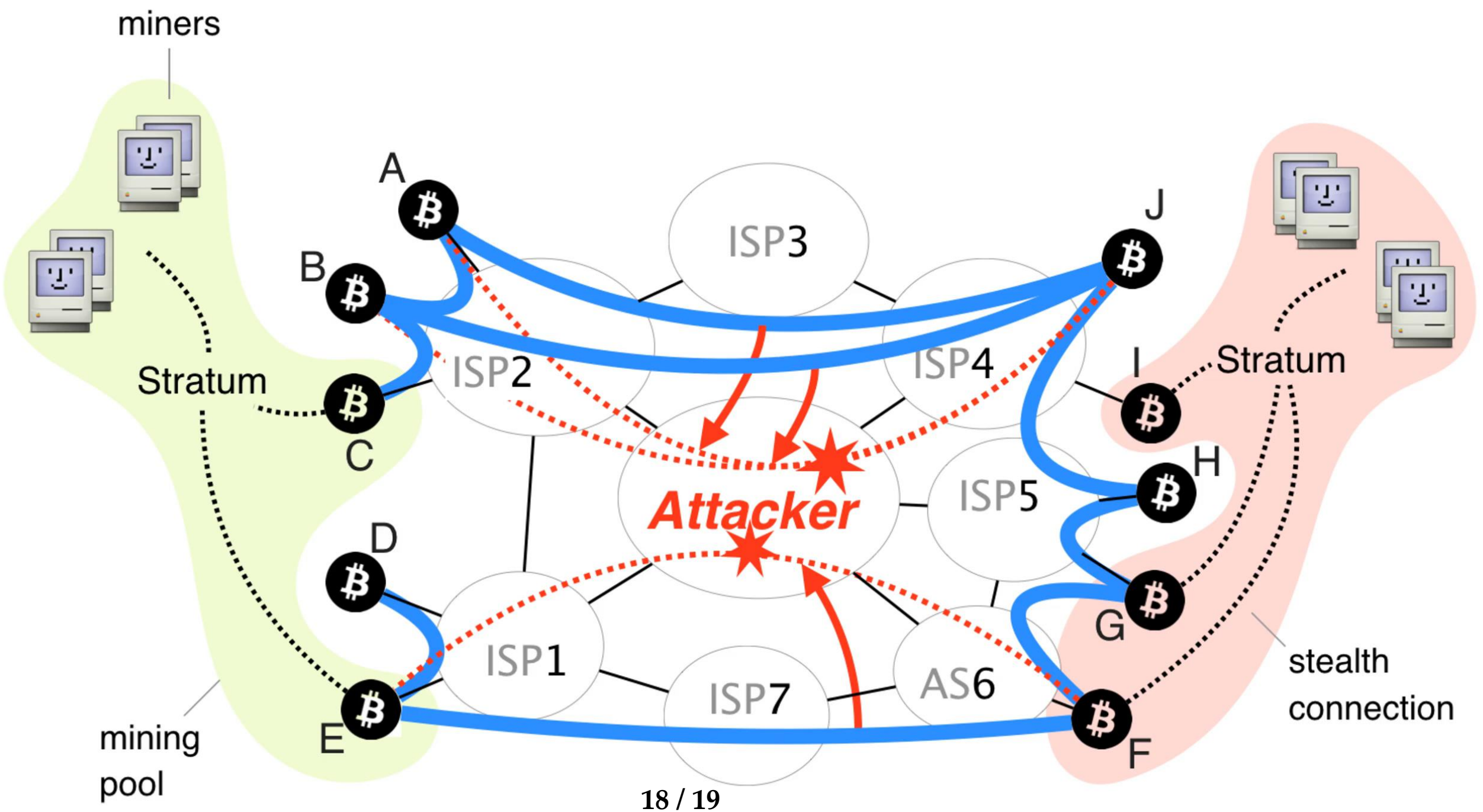
Pentesting

Smart Contracts

- With database secured, viable attack vector → Input of data
  - Injections
  - Social Engineering
  - Logic Manipulation
- Smart Contracts execute automatically
  - If compromised, Attacker will directly receive the reward
  - Due to Blockchain, once reward is sent, it cannot be reversed
- Smart Contracts → Future?
  - Pentesting and Code Audits become more important than ever

Blockchain Network

- Nodes are reliant on incoming communication from other nodes
  - Bitcoin has 8 connections, Ethereum has 13
- If communication from nodes are malicious, can influence data recorded
- If executed on large enough scale, can partition entire networks
  - Requires hijacking of Autonomous Systems (AS) or Border Gateway Protocol (BGP)
    - AS contains the information sent out
    - BGP determines the routing of information


miners
A
B
C
D
E
F
G
H
I
J
ISP1
ISP2
ISP3
ISP4
ISP5
ISP7
AS6
Attacker
Stratum
Stratum
mining
pool
stealth
connection

If you are interested to learn more…

- HITB GSEC 2018
- 31 August, 4.30pm - 5.00pm
- Blockchain & Smart Contract Attack Vectors
- InterContinental® Singapore

Food for thought

- Countries and Companies have invested in Blockchain solutions
- Smart Contracts looks set to streamline various industries
- Singapore has already started using Blockchain (PSA, IMDA, SQ etc)

- Can we afford to ignore this? What would happen to the adopters and industries?
- Can we secure our future? Or will we be reliant on others?