Deep into Blockchain Series

Security in Blockchain Solutions

Presenter(s): Mohit , Sam & Dharmen

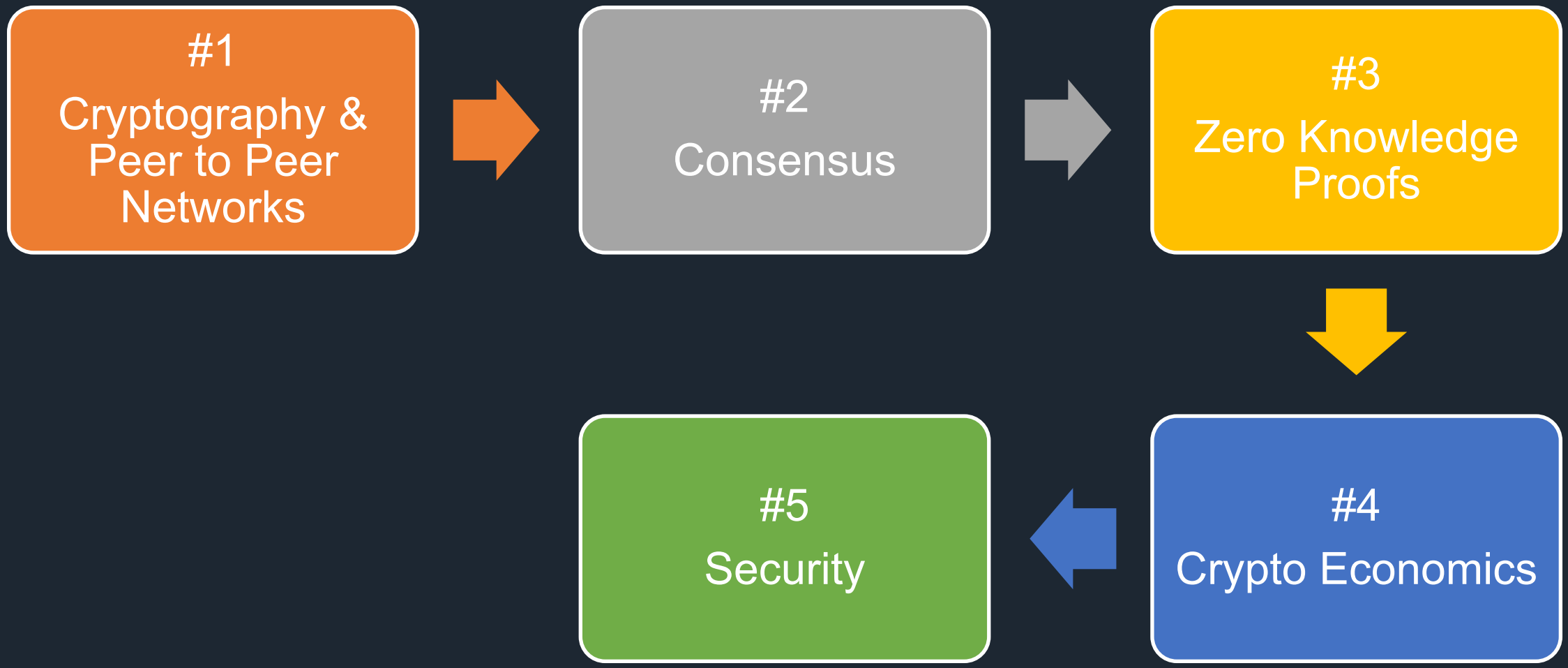
"A Blockchain-Powered platform is as secure and robust as it's consensus model."

Virtual Meet-up

dcentrum Community

Connect | Collaborate | Create

Meetup Series



Agenda

- ❑ Is your Blockchain Secure?
- ❑ How to ensure Confidentiality, Integrity and Availability of your DLT solution?
- ❑ What are traditional and non-traditional methods available to evaluate DLT security?
- ❑ Attacks and vulnerabilities of Public Blockchains and their mitigations
- ❑ What are DLT specific security considerations?

Our founding members

Deepak Bhattad

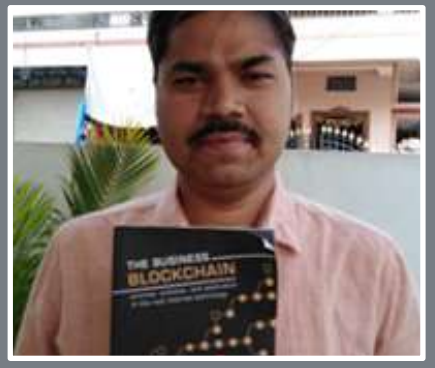
Dharmen Dhulla

Mahesh Wankhade

Mohit Bathla

Rishi Cherukuri

Sam Naidu



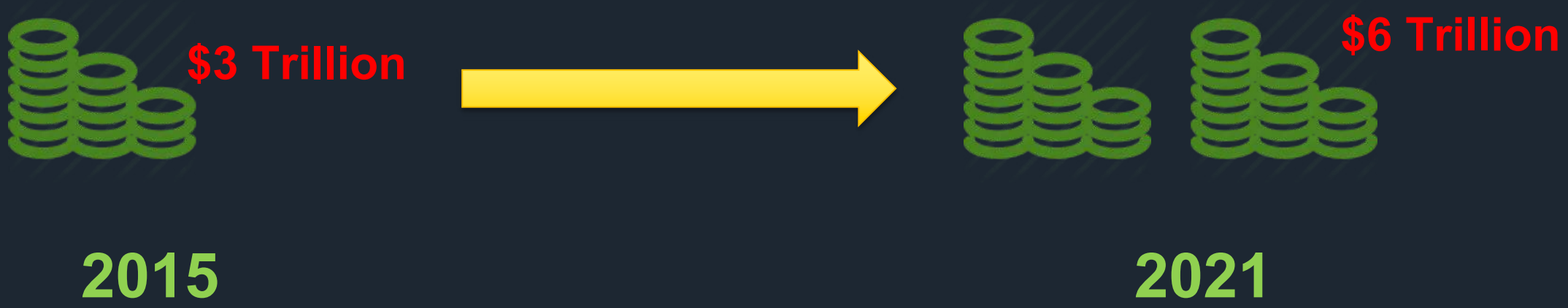
Sreenivas Chinni

7 Use Cases our community has executed

Krishi Chain	• A De-Centralized, Autonomous Marketplace for trading of agricultural commodities
Good Char	• Last mile donation tracking using Blockchain
B'Lock'	• Distributed Logistics with proof of origin and tracking etc
Identity Management	• Managing Self sovereign Identity on Blockchain
Cold Chain	• Bringing transparency to Cold Supply Chain (Vaccines, Food etc)
Smarter Law Violation Prevention System	• Focus on Traffic Violation Challan Management
LINQED	• Easy and trusted way to share unused assets paving path for truly shared economy

Impact
&
importance of Security
in Blockchain Solutions

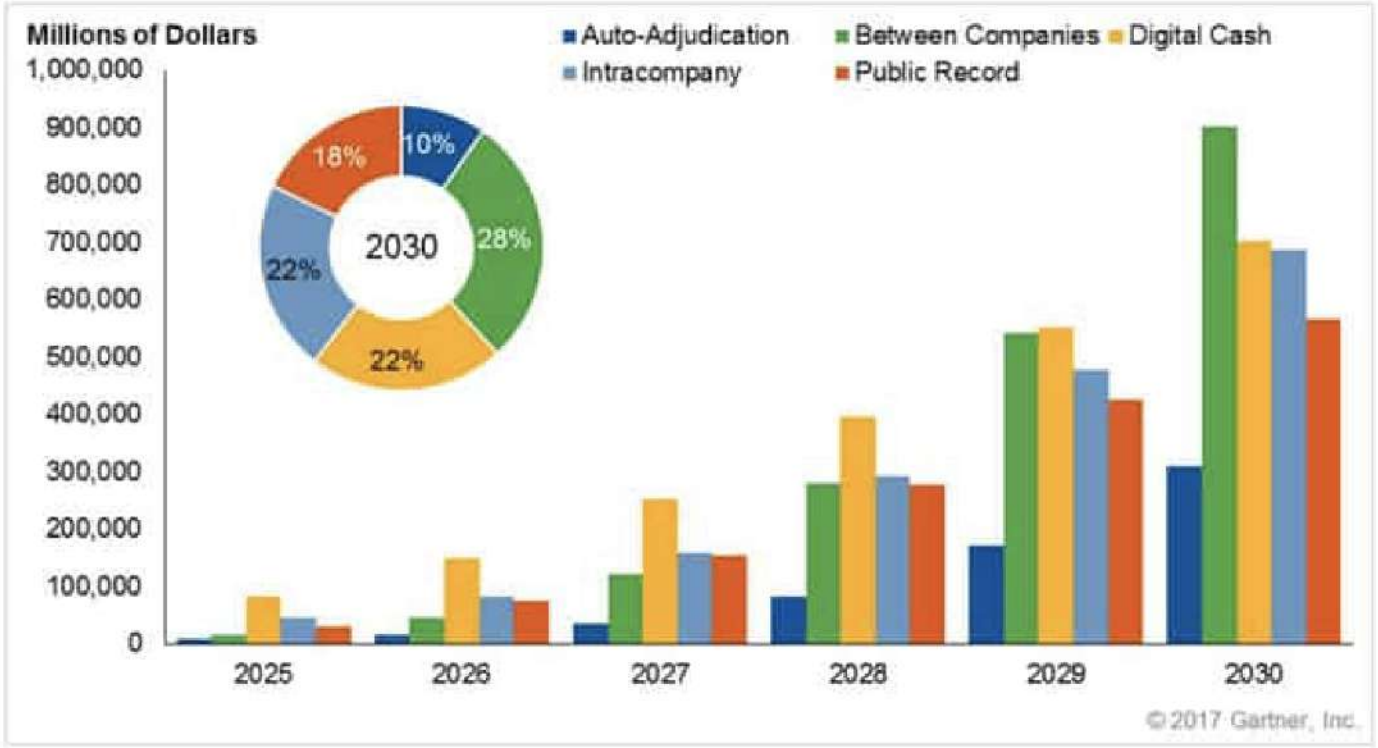
Cost of Cyber Crime



Source: Crime security ventur

Blockchain value addition by 2030

Business value-add of Blockchain - $176 billion by 2025, $3.1 trillion by 2030



Source: Forecast: Blockchain Business Value, Worldwide, 2017-2030

Gartner

Crypto Heists

2014 – Mt Gox

- Bitcoins worth $460 million were lost
- Vulnerability of private key storage was exploited by the attackers

2016 – DAO

- Ethers worth $60 million were lost
- Vulnerability in DAO Smart Contract was exploited by the attackers

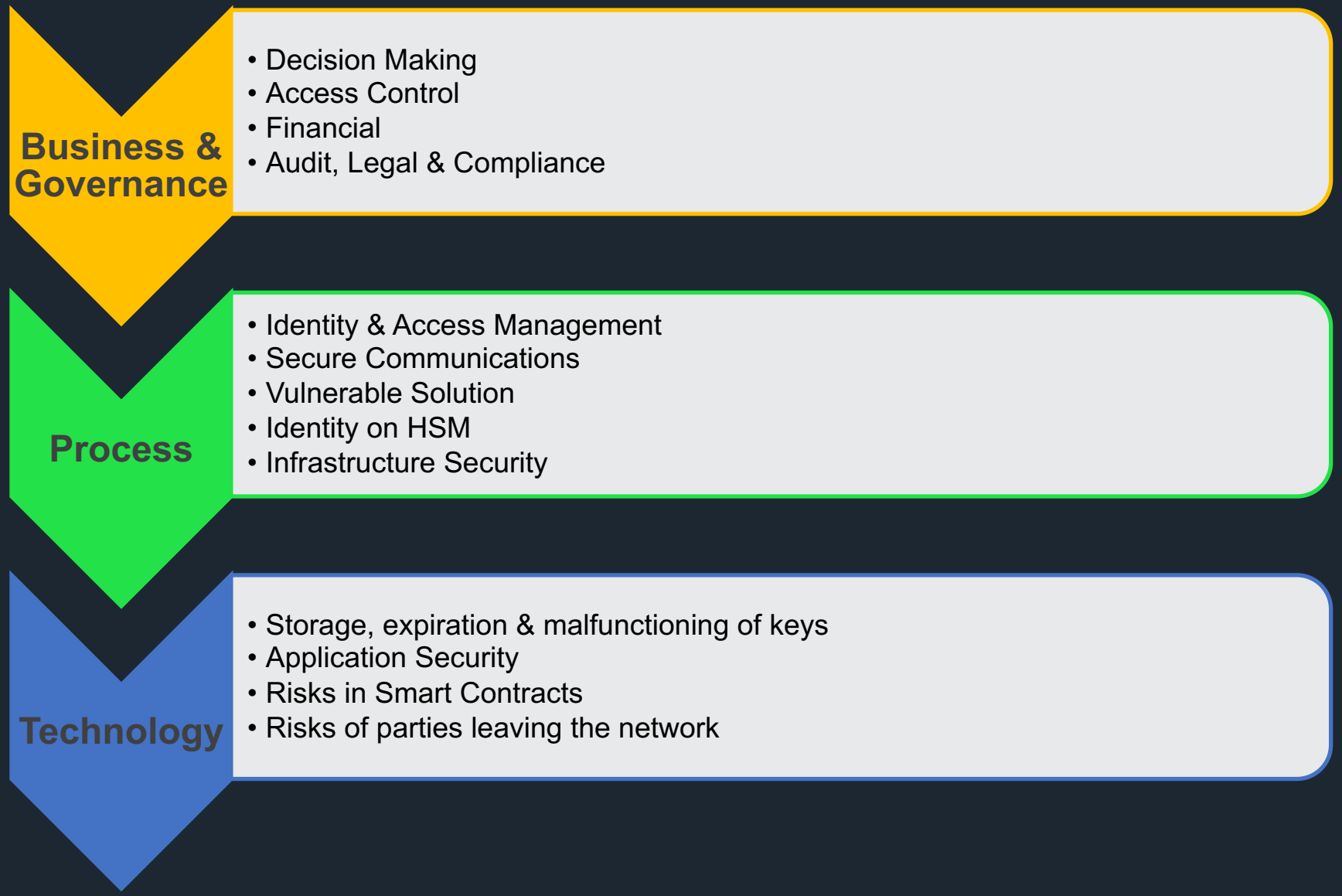
2017 – Bitfinax

- Bitcoins worth $72 million were lost
- Vulnerability in multi-signature wallets was exploited by the attackers

2019 – 51% attack on Ethereum Classic

- Ethereum Classic coins worth $1.1 million were lost
- 51% attack vulnerability was exploited by the attackers

Security Risks

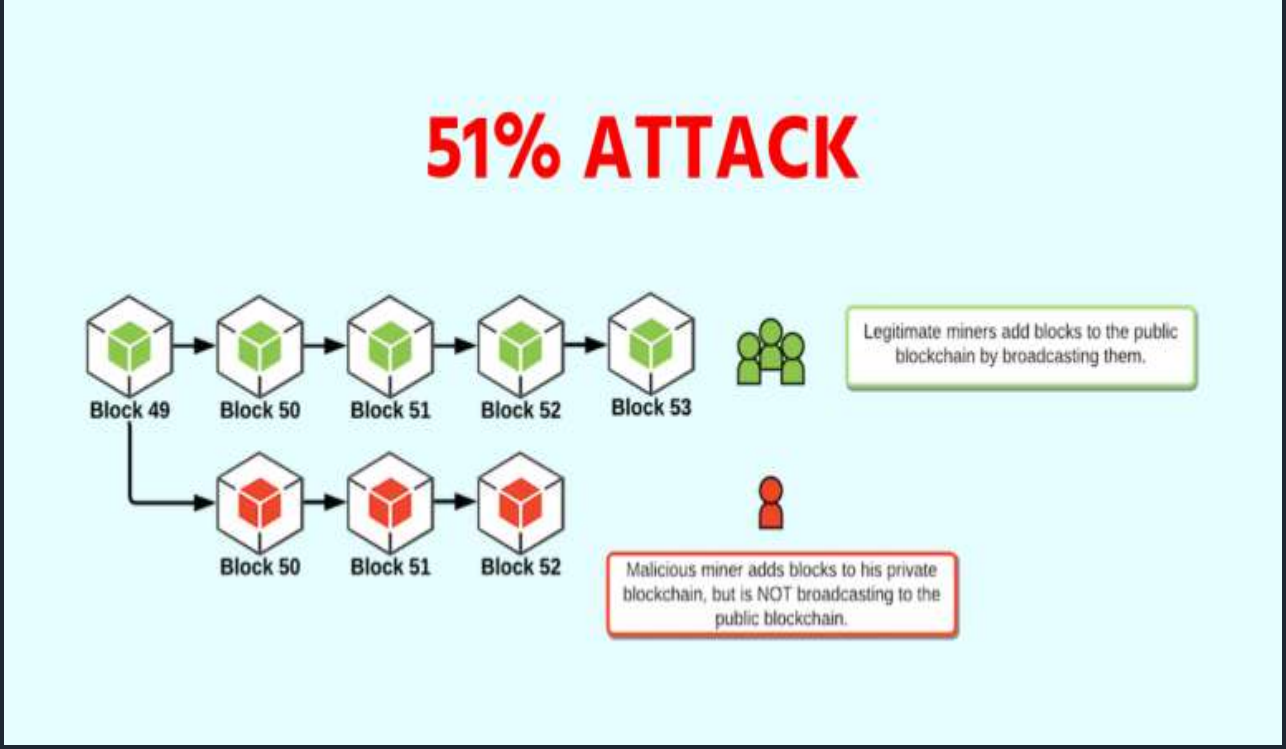


Possible attacks on Public Blockchains and Prevention mechanisms

Attacks & Vulnerabilities

- ❑ 51% Attack
- ❑ Sybil Attack
- ❑ Selfish Mining
- ❑ Eclipse Attack
- ❑ Routing Attack
- ❑ DoS Attacks
- ❑ Smart Contract Vulnerabilities and Security

51% Attack



Attack on the consensus algorithm

If an attacker controls 51% of a PoW blockchain's computational resources, they control the blockchain.

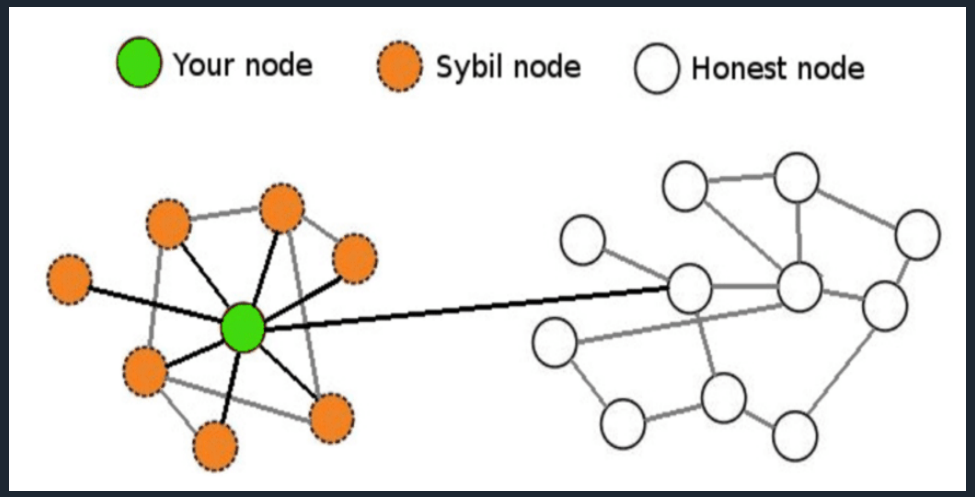
Possible Double-spend attacks

How to prevent it:

https://cryptotheheroes.wordpress.com/2019/01/25/is-the-blockchain-vulnerable-the-51-attack-case/

- Checkpointing
- PoS
- Coins built on top of other networks (ERC20)
- Interchain linking

Sybil attack



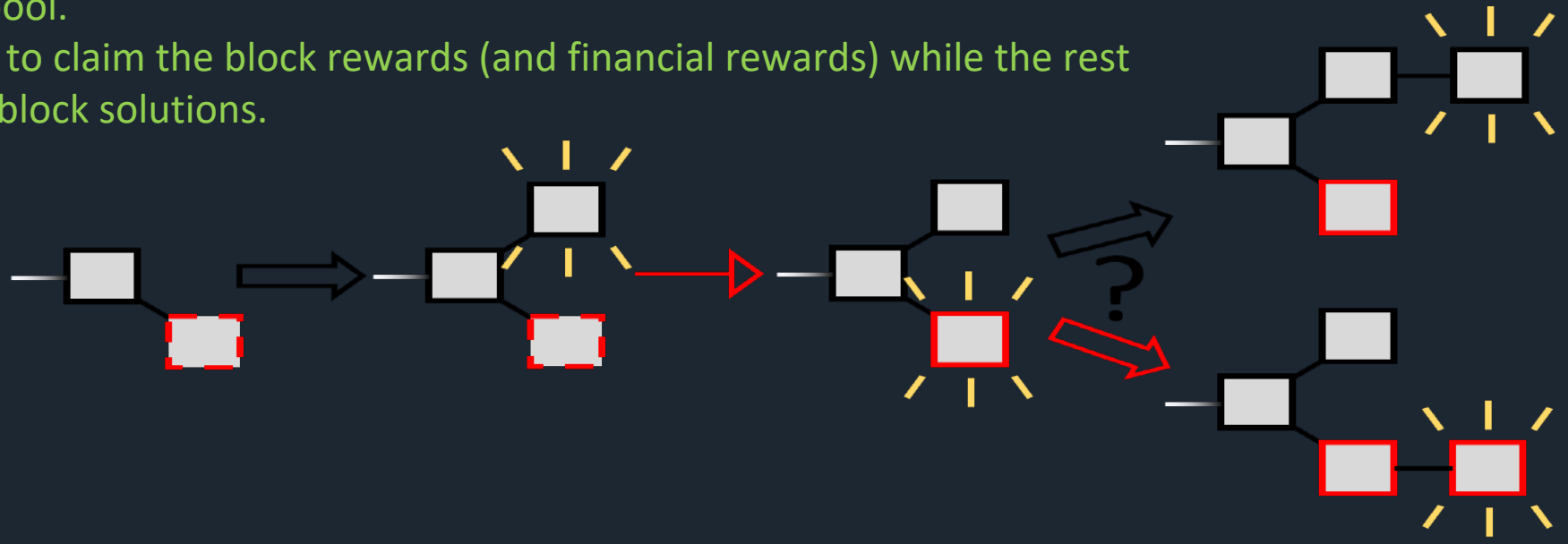
A Sybil attack is an attempt to control a peer network by creating multiple fake identities. These fake identities appear to be unique users.
A successful Sybil attack against a Blockchain or file transfer network would allow bad actors disproportionate control over the network.

How to prevent it:

1. Raise the cost to create a new identity/node:
   POW: more processing power, POS: more stake to contribute
2. Identity Verification:
   IP Address restriction, two-factored Authentication, Trust/reputation based

Selfish Mining

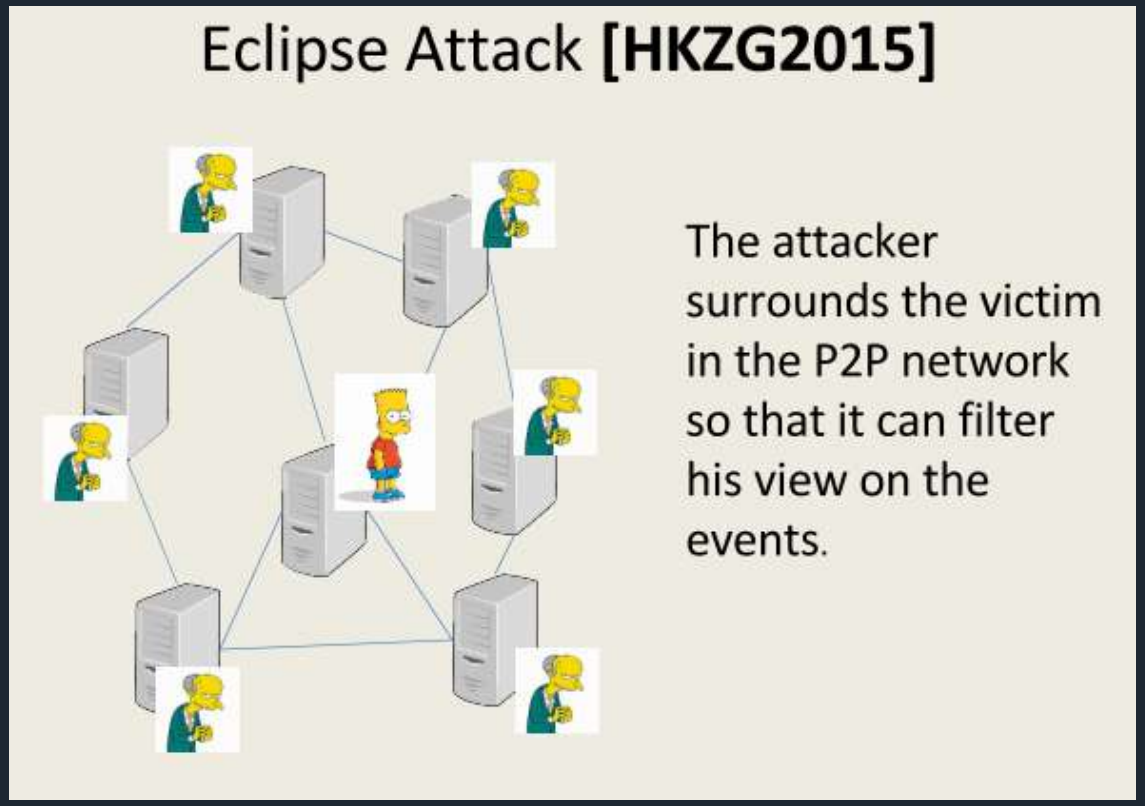
- Miner attempts to withhold a successfully validated block from being broadcast to the rest of the mining pool network.
- He continues to mine the next block, by demonstrating more proof-of-work compared to other miners in the mining pool.
- This allows the selfish miner to claim the block rewards (and financial rewards) while the rest of the network adopts their block solutions.



Solutions to prevent this:

1. Randomly assign miners to branches of the Blockchain when a fork occurs
2. Set threshold limits for mining pools on the network that would prevent selfish miners from gaining a significant advantages over other miners operating on the network.

Eclipse Attack



How to mitigate this:

1. Whitelisting
2. Random reconnections

Eclipse attacks are a type of network attack that aim at eclipsing certain nodes from the entire peer-to-peer network.
Monopolizes a node's connections so that it doesn't receive information from any nodes other than the attacking nodes.
In contrast to Sybil attacks, Eclipse attacks are mainly focused on attacking single nodes rather the entire network at once.

this attack can be used to leverage others
– Selfish mining
– 51% Attack
– Double spending

Routing Attack

Attacker intercepts messages propagating through the network and tampers with them before pushing them to their peers

Helpful to perform 51% attack, DoS attacks and double-spend attacks

How to mitigate this:

1. Network Statistics Monitoring
2. Encrypted Authenticated communications

DoS Attacks

Denial of Service attacks target the network's bottlenecks or single points of failure

- Transaction Flooding
- Block Forger DoS
- PoS and MSP DoS

Smart Contract Security:

Programming Vulnerabilities:

1. DoS attacks targeting loops or recursion
2. Race Conditions
3. Reentrancy
4. Randomness provided by Oracles
5. Integer Overflows/Underflows

Mitigation: Smart Contract Auditing

1. Expert Code Analysis
2. Vulnerability Scanning (Oyente)
3. Symbolic Execution
4. Taint Analysis (Mythril)
5. Test Coverage tools

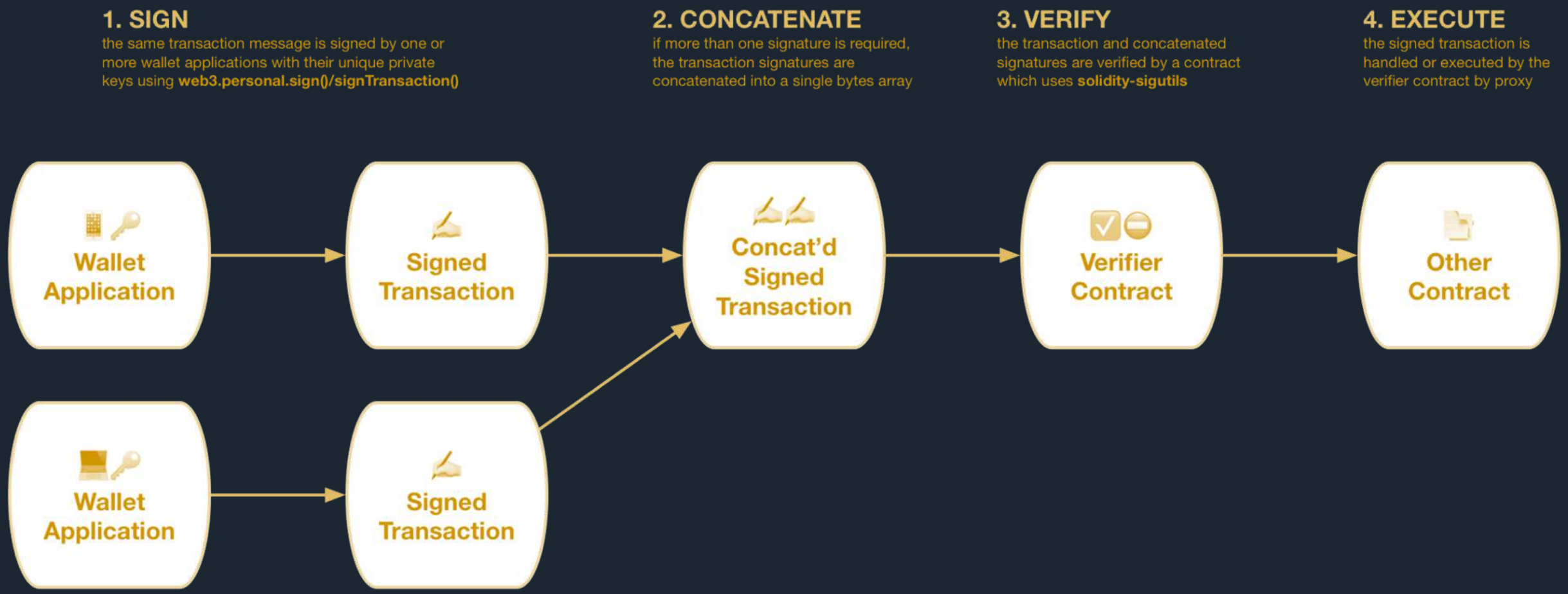
Other Risks:

1. Code is visible to everyone – IP can be reverse-Engineered, Data mining of transaction data to track details of sender, receiver
2. Cannot remove poorly designed smart contracts from Blockchain

Advanced Security Mechanisms

- ❑ Multi signatures
- ❑ Zero-Knowledge Proofs
- ❑ Anonymous Signatures (Stealth Addresses, Ring Signatures)
- ❑ Anonymizing crypto currency transactions - Mixing
- ❑ Multi Party Computation
- ❑ Confidential Transactions using Homomorphic Encryption

Multi Signatures



- Multi signatures can be enabled for Crypto Wallets

Zero Knowledge Proofs

ZKP can be used as a diligence, security, and verification tool in some of the most highly regulated industries like financial services, insurance, audit firms, and retail

Anonymization - Stealth Addresses (recipients)

Stealth addresses are designed to prevent public association of a transaction's output with a recipient's wallet address and conceal a transaction's actual **destination address**, thereby hiding the receiver's identity on a cryptocurrency network.

Stealth addresses are private, single-use addresses generated using the elliptic-curve Diffie-Hellman protocol.

Monero(XMR) implements stealth addresses for enabling private transactions

Anonymization - Ring Signatures (senders)

A ring signature is a digital signature that is created by a member of a group that each have their own keys. With this it will not be possible to determine the person in the group who has created the signature.

Monero(XMR) implements Ring Signatures

Anonymization – Mixers or Tumblers

A Cryptocurrency tumbler or cryptocurrency mixing service is a service offered to mix potentially identifiable (or 'tainted‘) cryptocurrency funds with others, so as to obscure the trail back to the fund's original source.
Tumblers have arisen to improve the anonymity of cryptocurrencies,
usually bitcoin (hence Bitcoin mixer), since the currencies provide a public ledger of all transactions.

BitcoinMixer - (Bitcoin, Litecoin and Ethereum)
BMCMixing (Bitcoin Monero Coin Mixing)

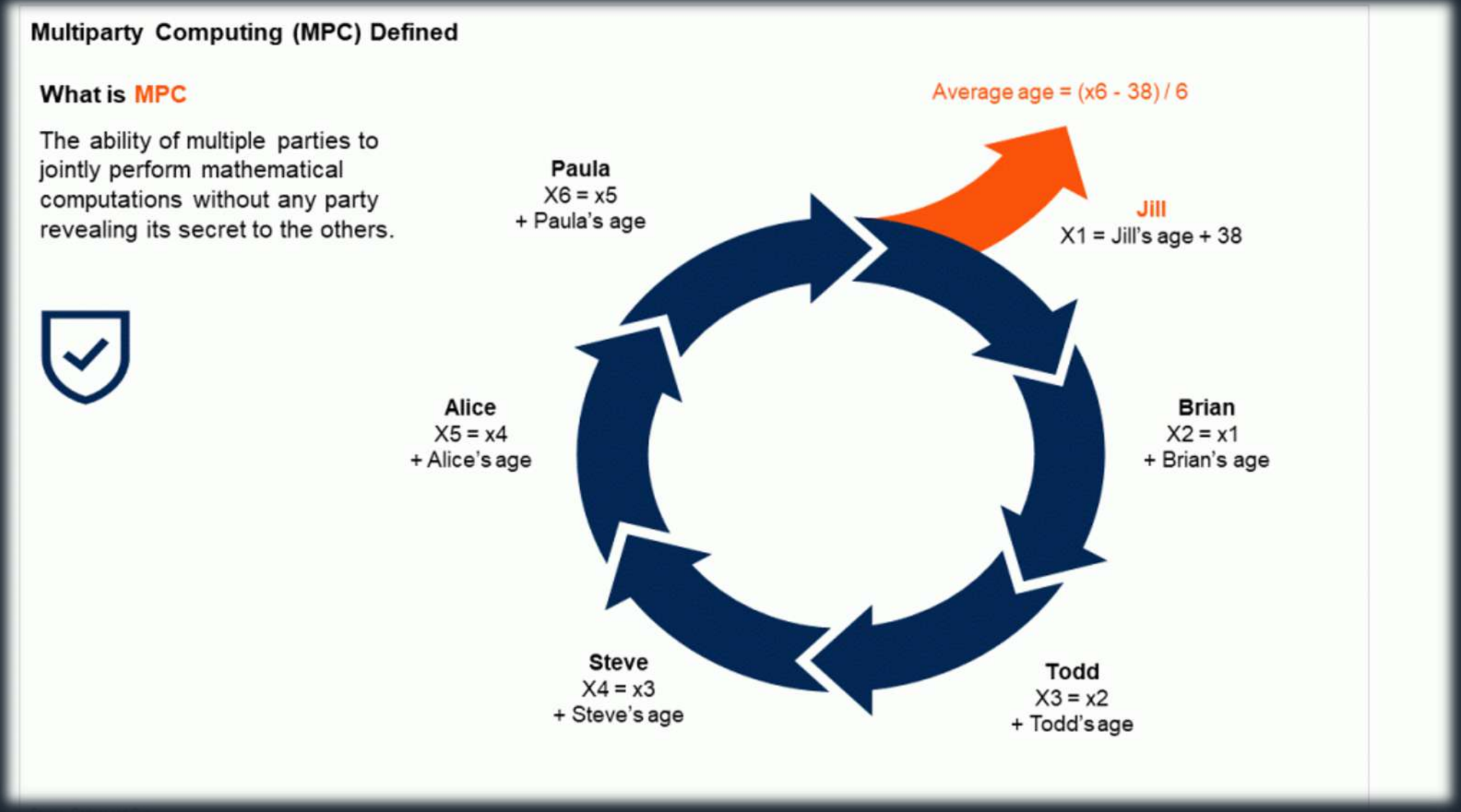
Confidential Transactions (CT)

Confidential transactions (CT) is a cryptographic protocol which results in the **amount value of a transaction** being encrypted.

This is accomplished by proving that the transaction value is within some set of values, all of which could have been a valid transaction (i.e. less than the amount in the user's account).

Using Homomorphic algorithms, ECC, Pederson Commitments, Ring Signatures etc

Multi Party Computation (MPC)



Blockchain Security in a Permissioned network

Overview

Blockchain

- ❑ How industries are adopting Blockchain for various use cases

Security

- ❑ How Blockchain Security is enforced in Permissioned network

Privacy & Confidentiality

- ❑ Authorized identities allowed to perform, share, audit transactions and ensure data privacy

Blockchain for Healthcare

Patient

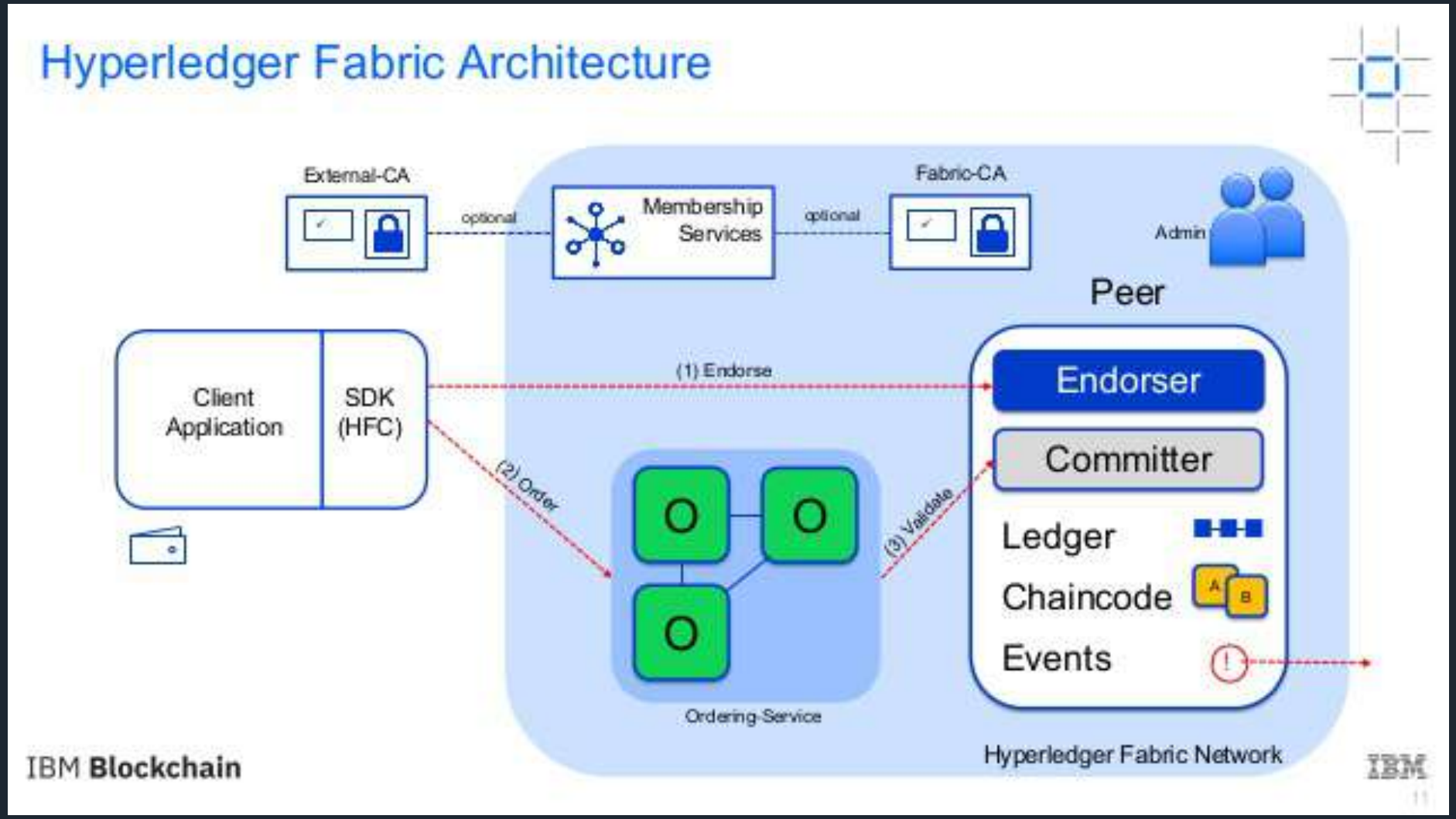
Doctor

Insurance

Pharmacy

Hospitals

Hyperledger Fabric Architecture

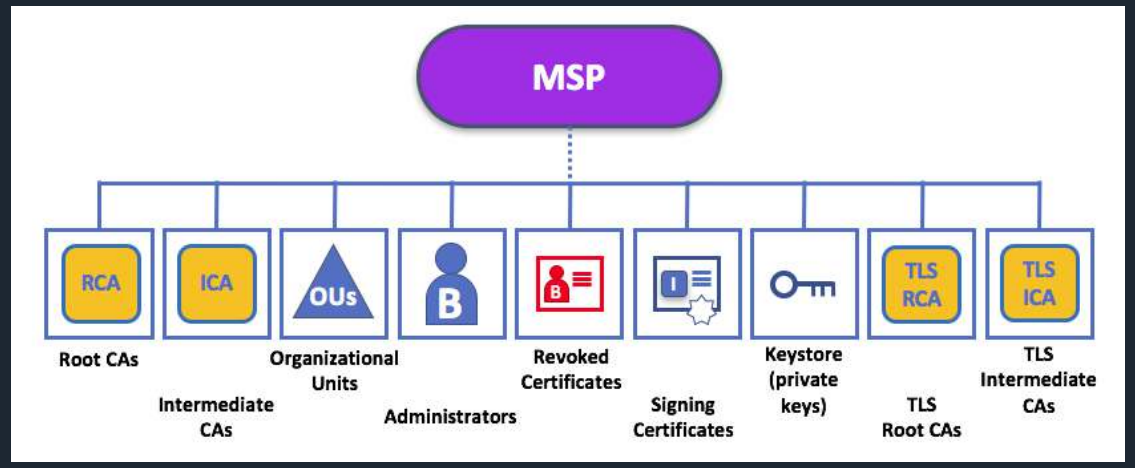


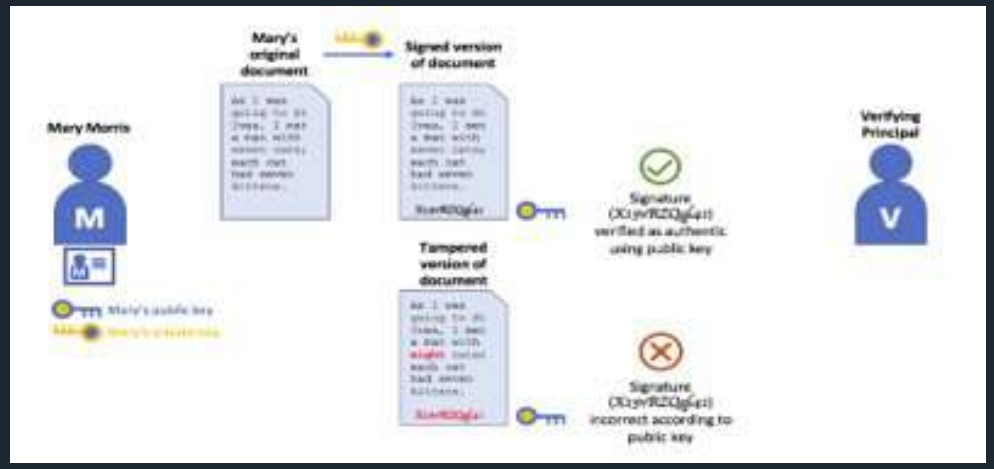
Security/Privacy & Confidentiality Features

- ❑ Identities, Membership and access control
- ❑ Application Level Encryption
- ❑ Privacy of transactions
- ❑ Chaincode Packaging
- ❑ Channels/Private Data collections
- ❑ SideDB/Off-chain
- ❑ Anonymous and unlinkable transactions (Identity Mixer)

"

Identity enforced





Four key elements of PKI

- Digital certificates
- Public and Private Keys
- Certificate Authorities
- Certificate Revocation Lists

Application Layer Encryption Support

Application sends all data encrypted

- ❑ Data not visible to peer in clear text
- ❑ Chaincode cannot validate the data easily

Encryption key using transient data field

- ❑ Chaincode can decrypt data but data stored is encrypted

Identity Mixer

Application sends all data encrypted

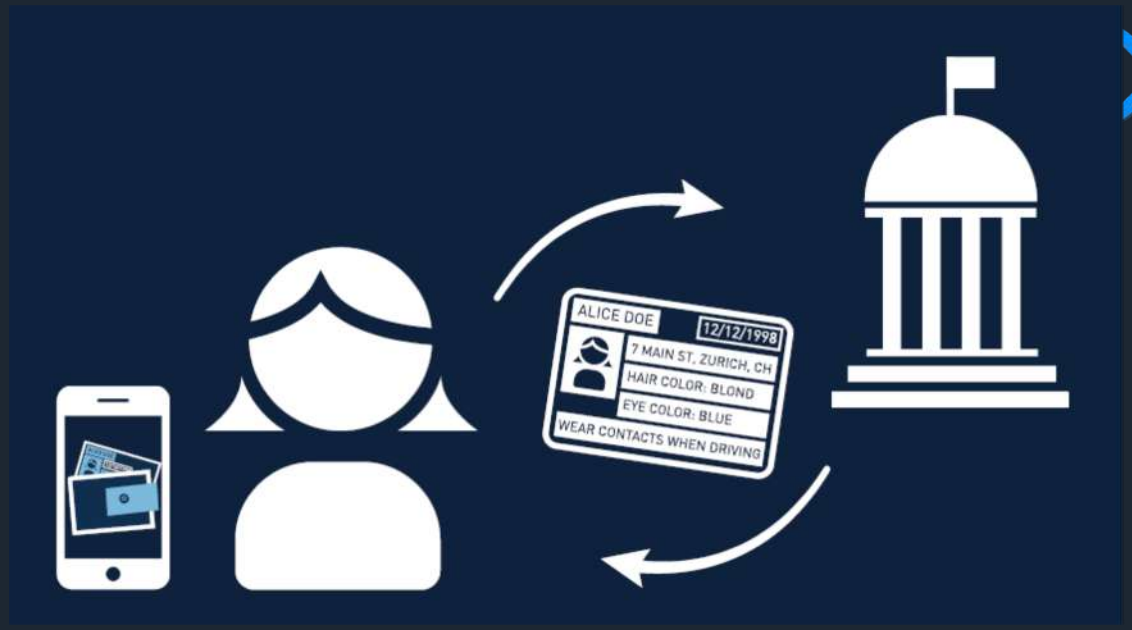
- Data not visible to peer in clear text
- Chaincode cannot validate the data easily

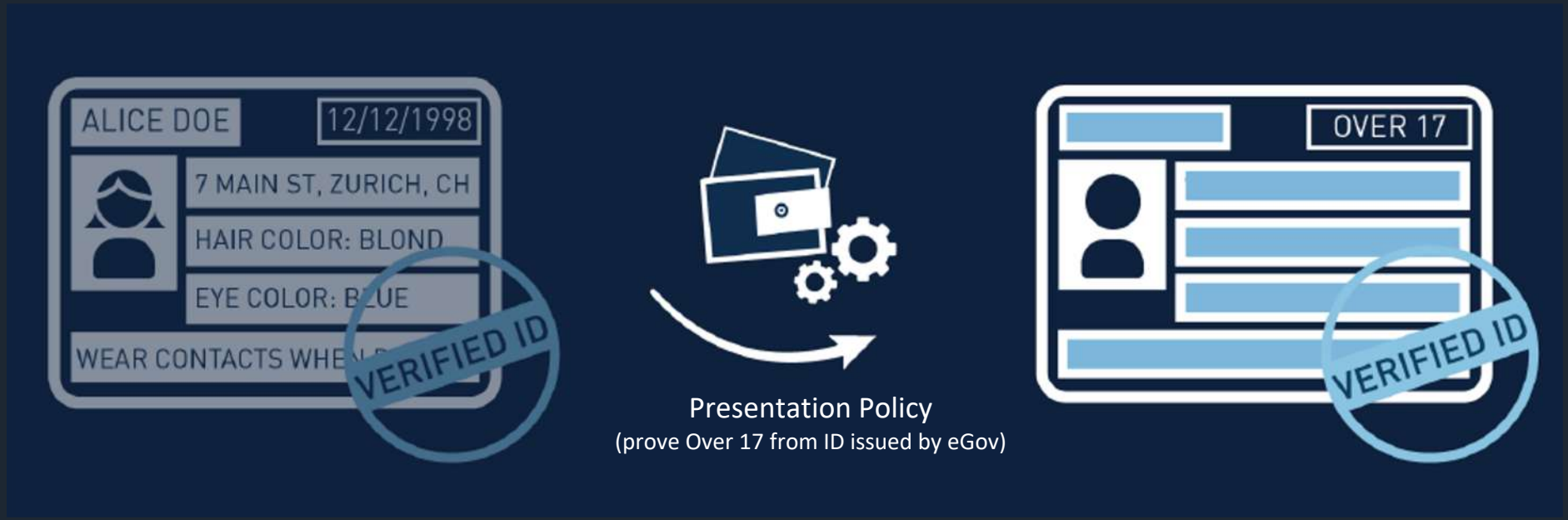
Encryption key using transient data field

- Chaincode can decrypt data but data stored is encrypted

Identity Mixer

- Attribute-based credentials
- Strong authentication (signatures)
- Privacy-preserving Access Control
  - Selective disclosure of attributes, predicates over attributes, full unlinkability
- Auditability
- Revocation
  - Preserving privacy and unlinkability

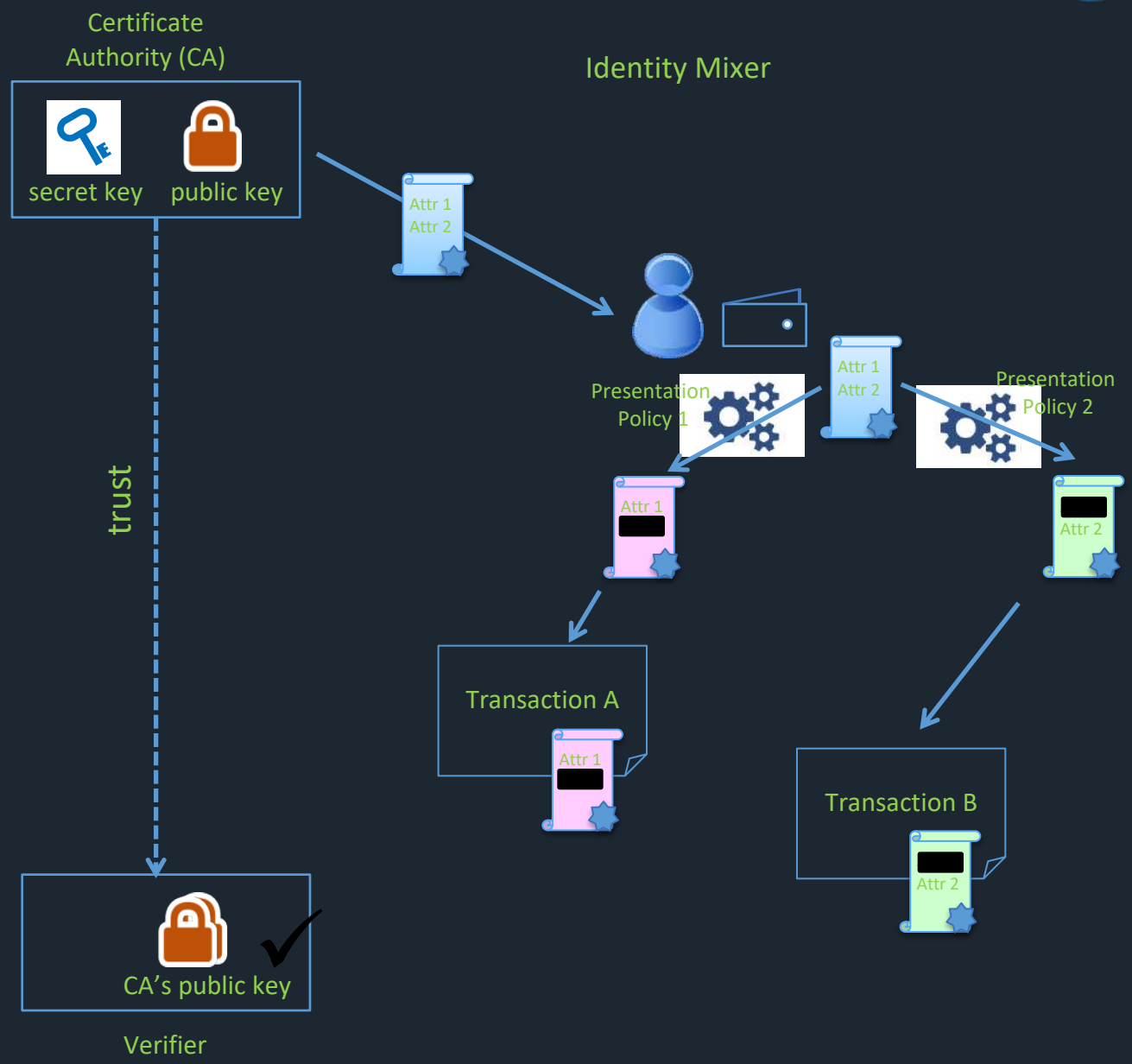




- Verification is done with the public key of the issuer only

How Identity Mixer works

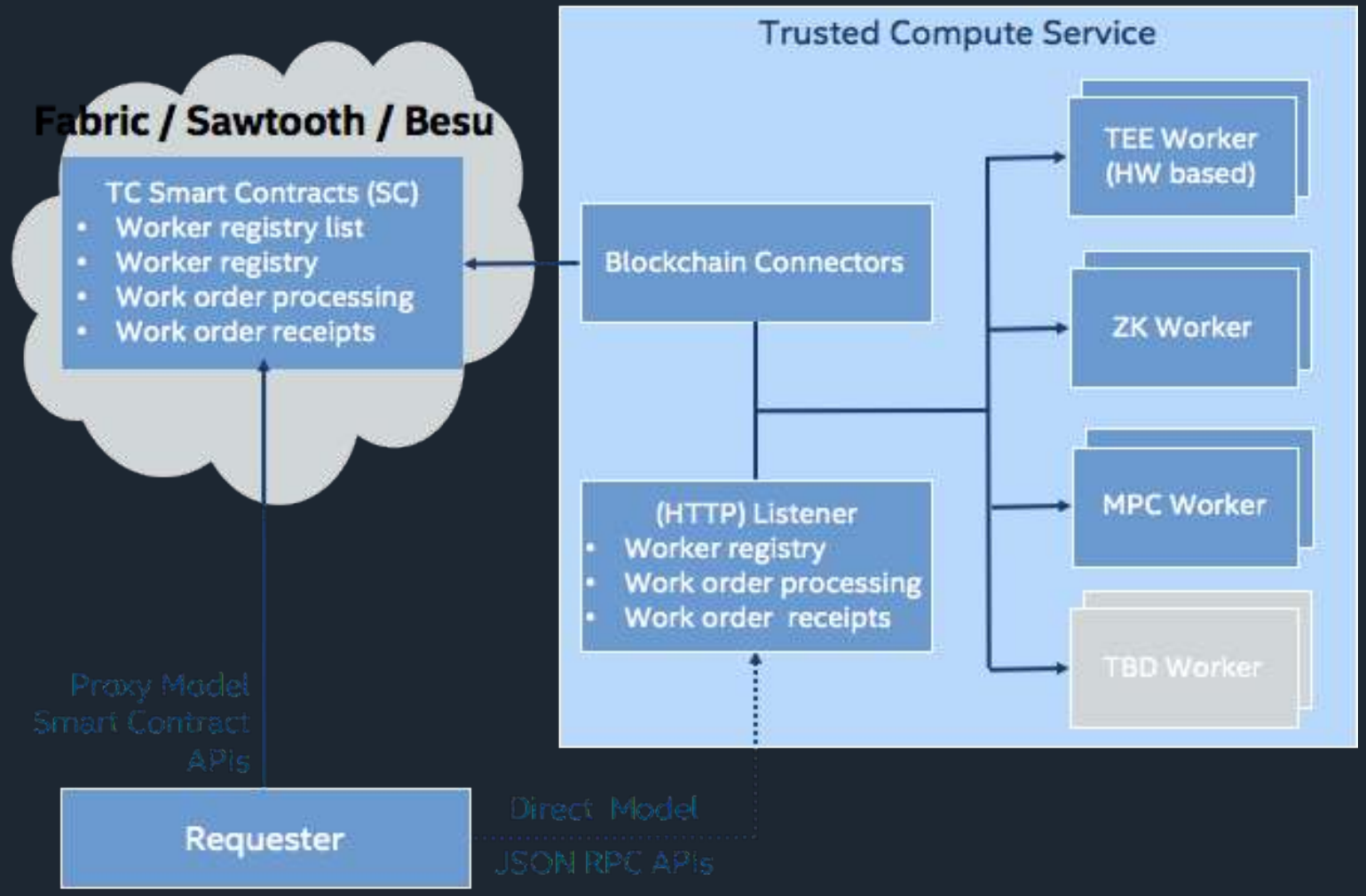
- Strong authentication (signatures)
- No linkability
- Minimal Attribute based disclosure
- Audit control



Hyperledger Avalon

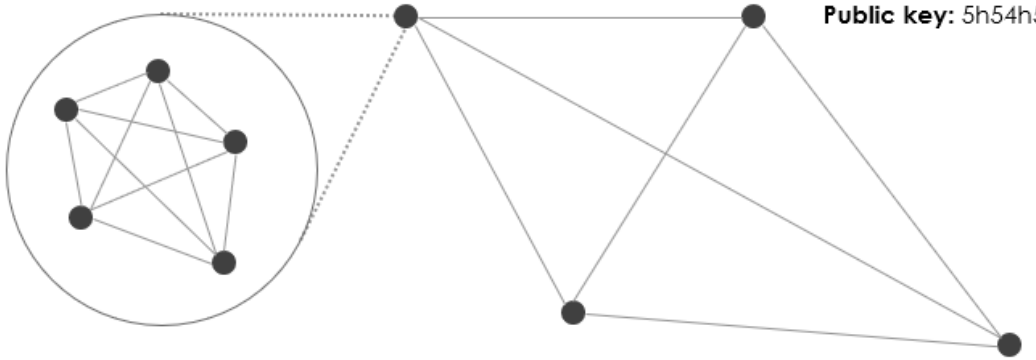
- Hyperledger Avalon is a ledger independent implementation of the Trusted Compute Specifications published by the Enterprise Ethereum Alliance.

- Enables the secure movement of blockchain processing off the main chain to dedicated computing resources. This enables
  - Improved blockchain throughput and scalability
  - Improved transaction privacy
  - Attested Oracles, trusted reporters of data generated outside of the blockchain.



Corda

Corda is for permissioned nodes to communicate on a need-to-know basis about updating shared facts



Notary Pool

Colorado River Authority
Address: 17.149.112.236:10005
Public key: 5h54h5wv632vhy55

Titan Technology Partners
Address: 115.187.28.40:10005
Public key: 5hw03nnk43jknkj4n

Bays Transcorp Inc.
Address: 120.65.158.170:10005
Public key: t453wv84bvt3cj5w3h

Corda – Consensus Mechanism

State validity
A state is valid when a transaction has correct input and output and the transaction has all required signatures

State uniqueness
Each state has only been approved once by a notary

Data Visibility

Transaction components	Validating Notary	Non-validating Notary
Input states	Fully visible	References only
Output states	Fully visible	Hidden
Commands (with signer identities)	Fully visible	Hidden
Attachments	Fully visible	Hidden
Time window	Fully visible	Fully visible
Notary identity	Fully visible	Fully visible
Signatures	Fully visible	Hidden
Network parameters	Fully visible	Fully visible

Corda – Security and Privacy Trade-off

Validating notaries

- The content of every transaction is revealed to a validating notary to be able to achieve consensus.
- Being able to observe the content of transactions may raise privacy concerns.

Non-validating notaries

- Can agree on the new state of a ledger without having to reveal to these notaries the entire transaction content.
- Opens the possibility for a denial-of-state (DoSt) attack.

Corda – Security and Privacy Trade-off

Validating notaries

- The content of every transaction is revealed to a validating notary to be able to achieve consensus.
- Being able to observe the content of transactions may raise privacy concerns.

Non-validating notaries

- Can agree on the new state of a ledger without having to reveal to these notaries the entire transaction content.
- Opens the possibility for a denial-of-state (DoSt) attack.

Solutions to address Security and Privacy concern

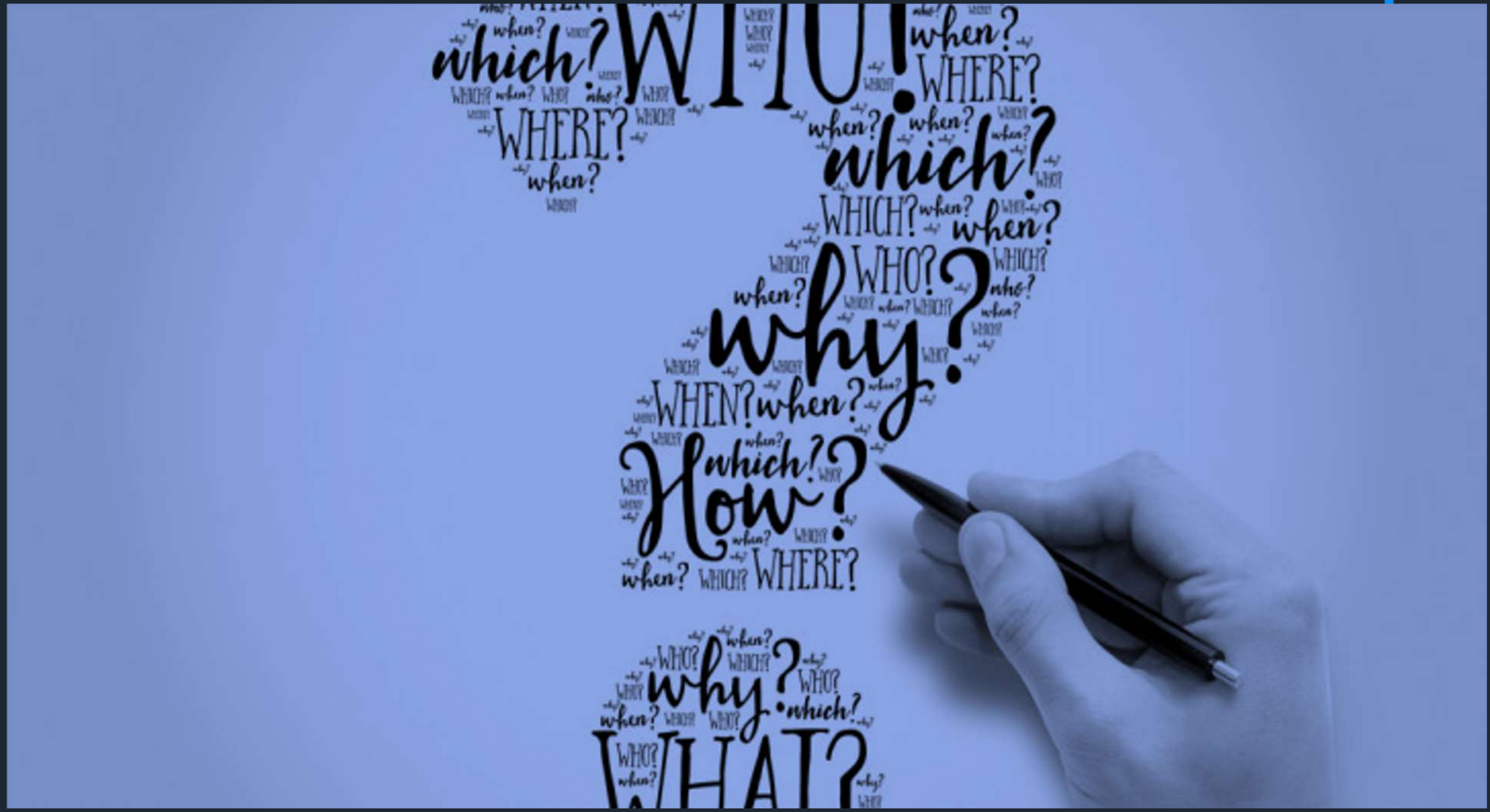
- Wet-signatures contracts
- Trusted Execution Environment (TEE)
- Zero-Knowledge Proofs (ZKP)

Supported by

nagarro

GOVERNMENT OF TELANGANA

bradsol
SIMPLIFYING BUSINESS


WHERE?
when?
which?
WHICH?
WHO?
why?
WHEN?
How?
WHERE?
WHO?
why?
WHAT?