VIETNAM MINISTRY OF SCIENCE AND TECHNOLOGY

XVIII^th RENCONTRES DU VIETNAM | UNESCO'S PARTNER

PEOPLE'S COMMITTEE OF BINH DINH PROVINCE

ĐƠN VỊ TỔ CHỨC CHÍNH

icise QUY NHON VIETNAM

VIASM VIETNAM INSTITUTE FOR ADVANCED STUDY IN MATHEMATICS

VSS

ĐƠN VỊ TÀI TRỢ & ĐỒNG TỔ CHỨC

VINIF

DEPOCEN better informed, better decisions

HỌC VIỆN SÁNG TẠO S³

9th Vietnam Summer School of Science 2022

Stories of life

Quy Nhon, 2 - 5 August 2022

Security & Privacy on Blockchains

Le Duc Phong

Fintech Research, Bank of Canada

TRƯỜNG KHOA HỌC VIỆT NAM
VSS

Content

- Basics of Blockchain
- Classification of Security Threats
- Reported cyber-attacks

What is Blockchain?

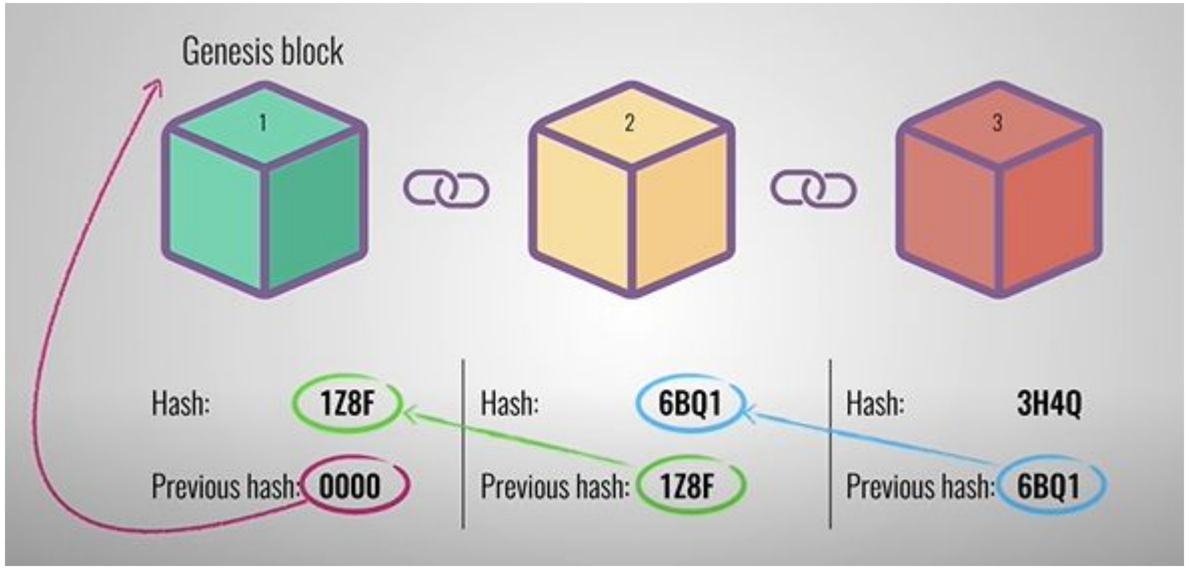
A technology or type of database

permits transactions to be gathered into blocks and recorded;

cryptographically chain blocks in chronological order; and

allows the resulting ledger to be accessed by different servers

Blockchain or Distributed Ledger

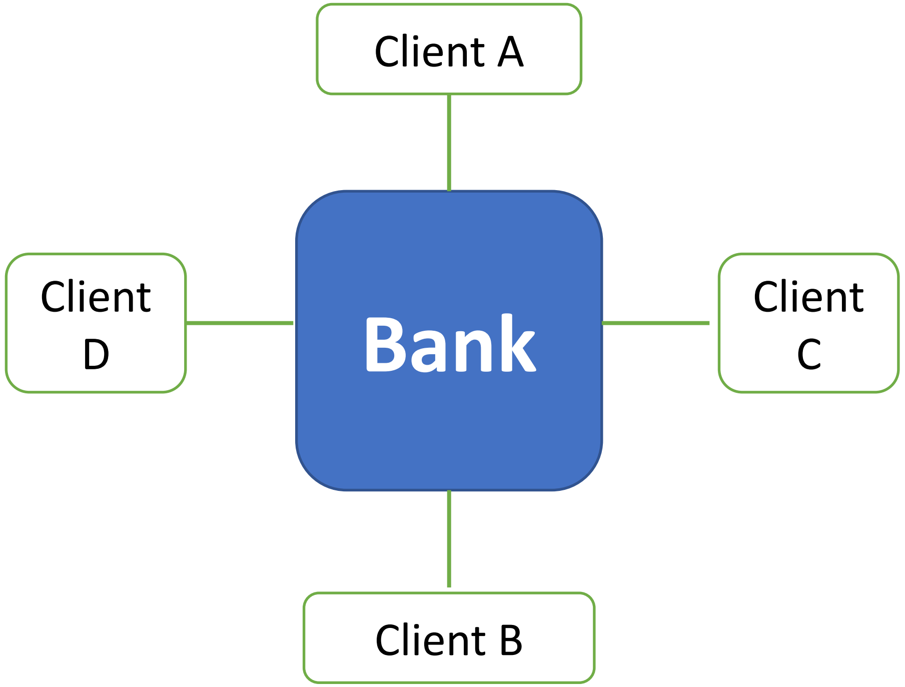


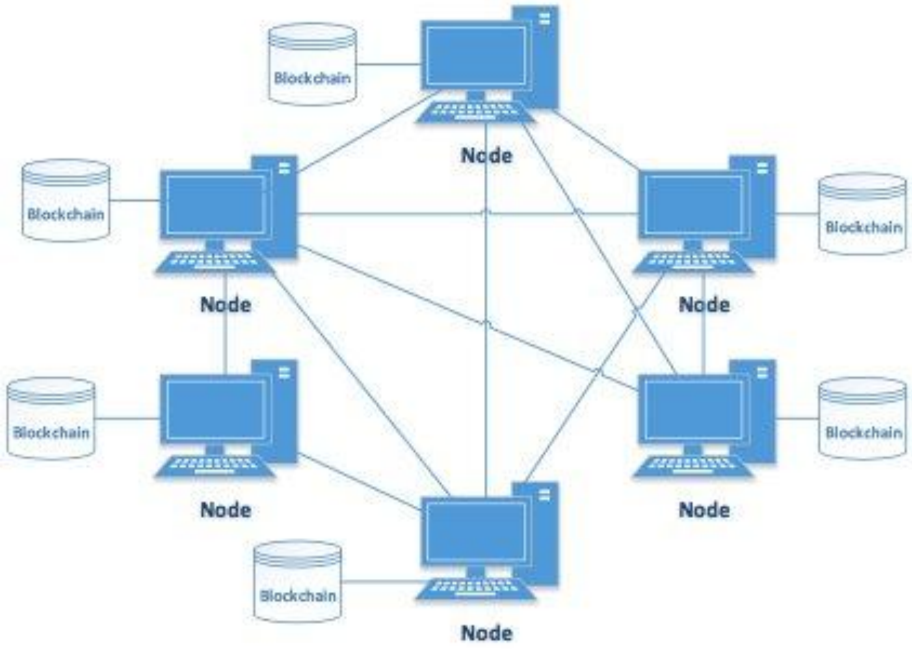
Each block contains transactions data, hash of block, and hash of previous block

Hashes link blocks, forming a chain

Timestamps, Hashes make more difficult for an adversary to manipulate the blockchain

Centralized vs. Distributed Ledger

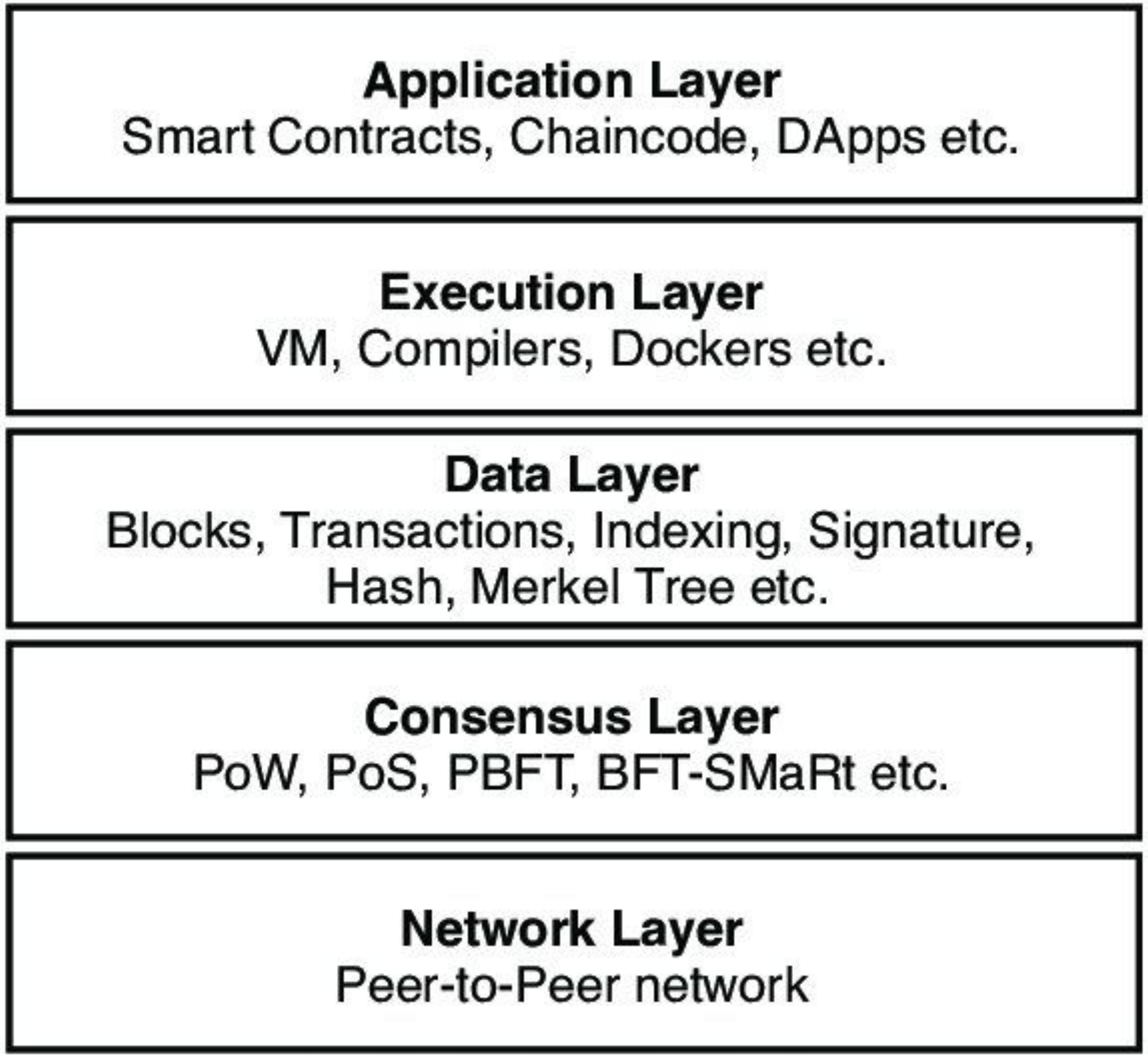




- Multiple ledgers, but Bank holds the "golden record"
- Client A must reconcile her own ledger against that of Bank, and must convince Bank of the "true state" of the ledger if discrepancies arise

- One ledger. All Nodes has access to that ledger
- All Nodes agree to a consensus protocol that determines the "true state" of the ledger

Abstraction layer model for DLT



Application Layer
Smart Contracts, Chaincode, DApps etc.

Execution Layer
VM, Compilers, Dockers etc.

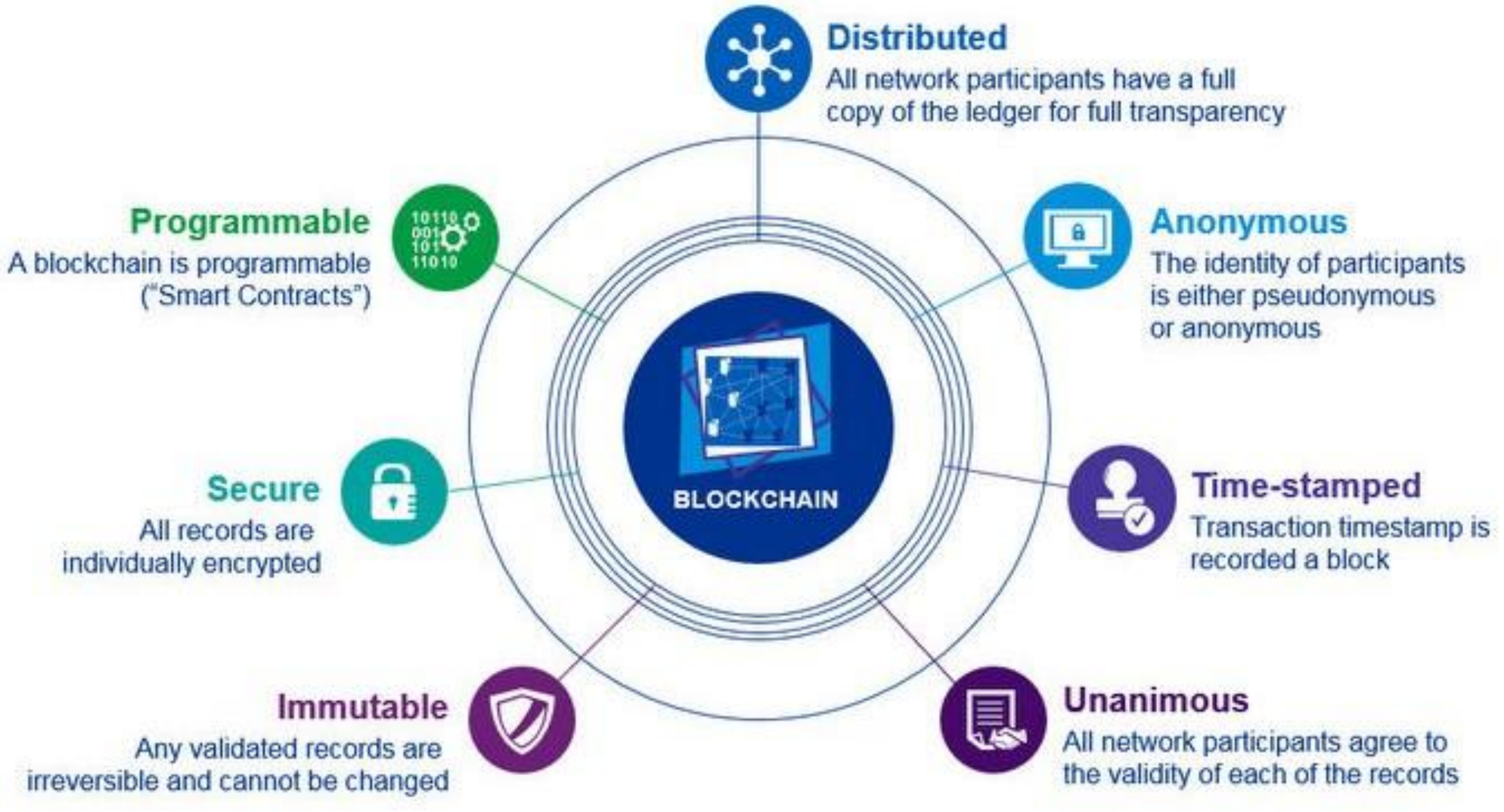
Data Layer
Blocks, Transactions, Indexing, Signature, Hash, Merkel Tree etc.

Consensus Layer
PoW, PoS, PBFT, BFT-SMaRt etc.

Network Layer
Peer-to-Peer network

Ref: Performance Evaluation of Blockchain Systems: A Systematic Survey, https://ieeexplore.ieee.org/document/9129732

Properties of Distributed Ledger Technology



Distributed
All network participants have a full copy of the ledger for full transparency

Anonymous
The identity of participants is either pseudonymous or anonymous

Time-stamped
Transaction timestamp is recorded a block

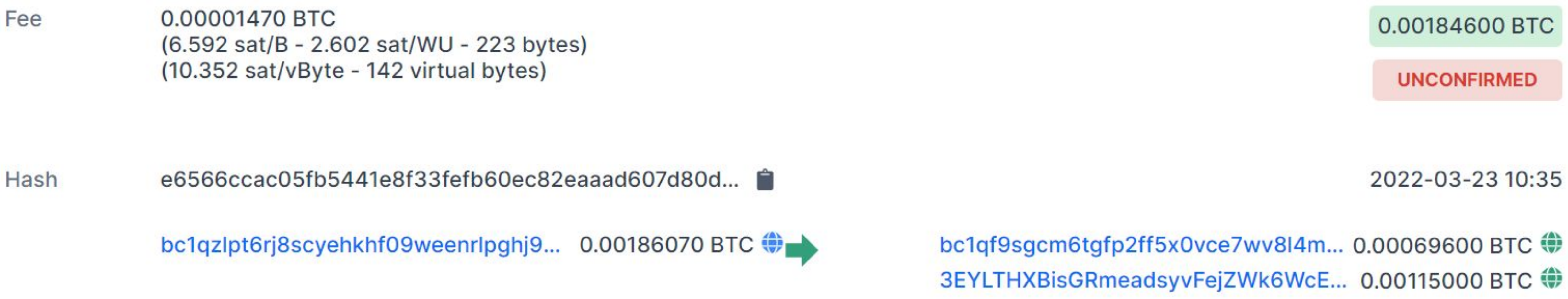
Unanimous
All network participants agree to the validity of each of the records

Immutable
Any validated records are irreversible and cannot be changed

Secure
All records are individually encrypted

Programmable
A blockchain is programmable ("Smart Contracts")

Transaction



Fee

0.00001470 BTC
(6.592 sat/B - 2.602 sat/WU - 223 bytes)
(10.352 sat/vByte - 142 virtual bytes)

0.00184600 BTC

UNCONFIRMED

Hash

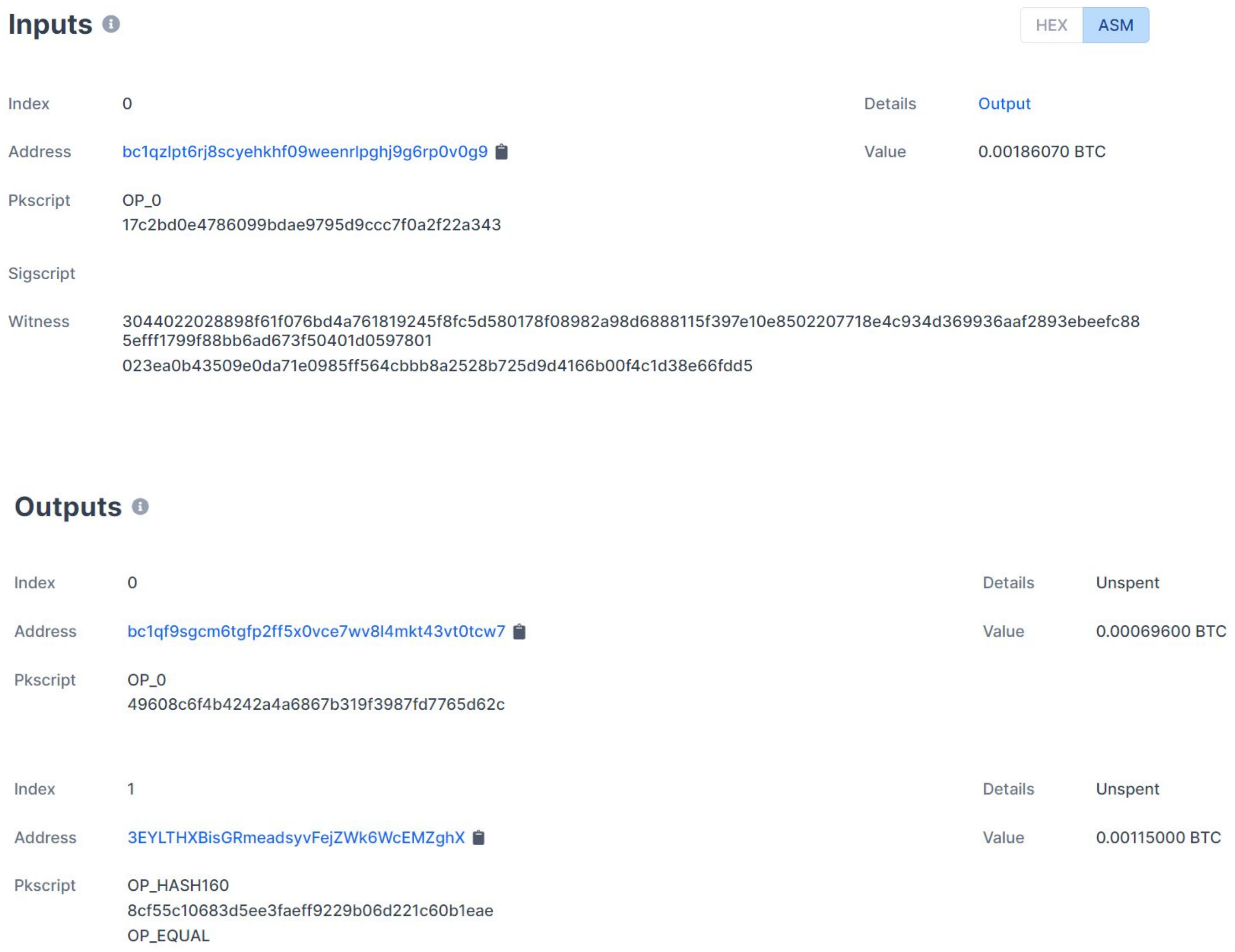
e6566ccac05fb5441e8f33fefb60ec82eaaad607d80d...

2022-03-23 10:35

bc1qzlpt6rj8scyehkhf09weenrlpghj9... 0.00186070 BTC

bc1qf9sgcm6tgfp2ff5x0vce7wv8l4m... 0.00069600 BTC
3EYLTHXBisGRmeadsyvFejZWk6WcE... 0.00115000 BTC

Transaction – A closer look



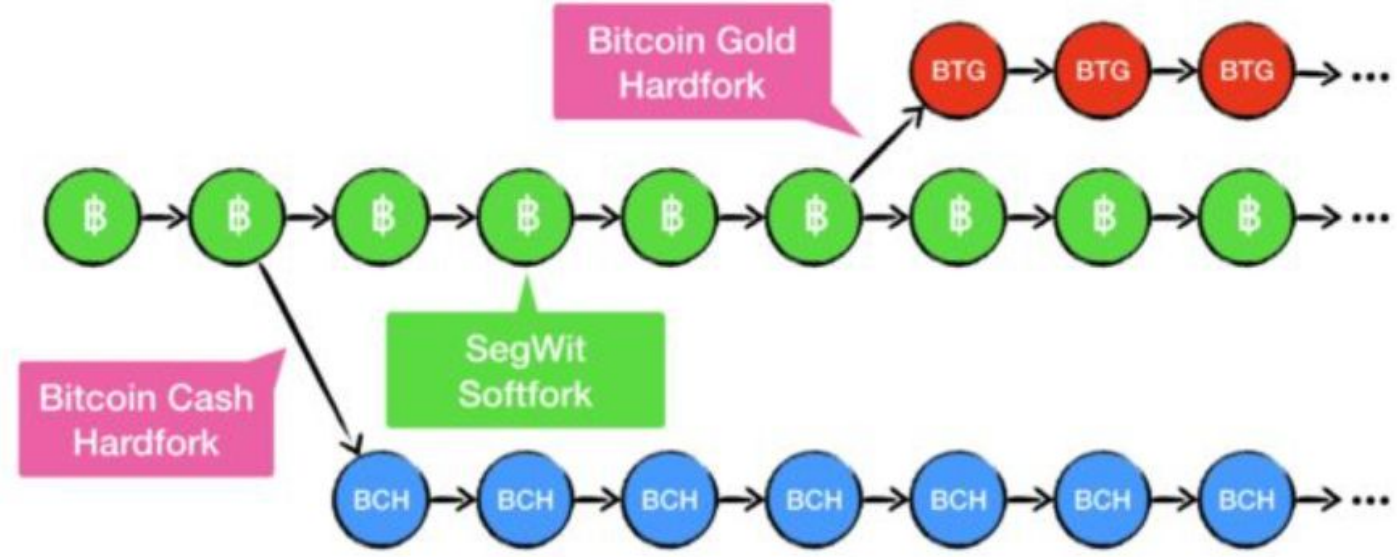
Inputs

Index	0	Details	Output
Address	bc1qzlpt6rj8scyehkhf09weenrlpghj9g6rp0v0g9	Value	0.00186070 BTC
Pkscript	OP_0 17c2bd0e4786099bdae9795d9ccc7f0a2f22a343		
Sigscript			
Witness	3044022028898f61f076bd4a761819245f8fc5d580178f08982a98d6888115f397e10e8502207718e4c934d369936aaf2893ebeefc885efff1799f88bb6ad673f50401d0597801 023ea0b43509e0da71e0985ff564cbbb8a2528b725d9d4166b00f4c1d38e66fdd5		

Outputs

Index	0	Details	Unspent
Address	bc1qf9sgcm6tgfp2ff5x0vce7wv8l4mkt43vt0tcw7	Value	0.00069600 BTC
Pkscript	OP_0 49608c6f4b4242a4a6867b319f3987fd7765d62c		
Index	1	Details	Unspent
Address	3EYLTHXBisGRmeadsyvFejZWk6WcEMZghX	Value	0.00115000 BTC
Pkscript	OP_HASH160 8cf55c10683d5ee3faeff9229b06d221c60b1eae OP_EQUAL		

Fork



A change to protocol or data in a blockchain network

- **Hard fork**: resulting in two blockchains
- **Soft fork**: still maintaining one blockchain

Security

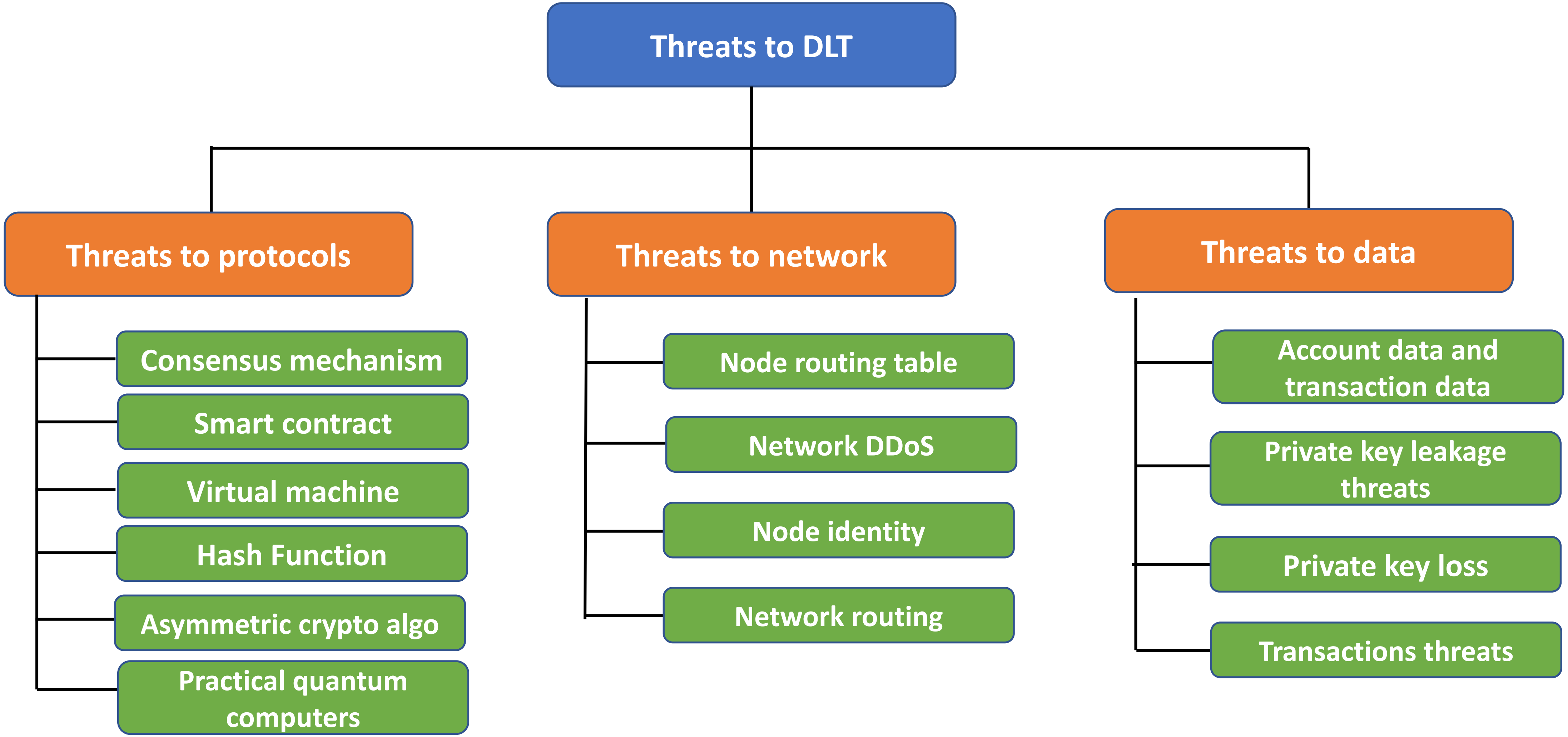
Security Requirements

Integrity & Availability of System

Consistency of The Ledger across Institutions

Confidentiality, Integrity & Availability of Transaction Data

Prevention of Double-Spending



Threats to DLT

Threats to protocols

Consensus mechanism

Smart contract

Virtual machine

Hash Function

Asymmetric crypto algo

Practical quantum computers

Threats to network

Node routing table

Network DDoS

Node identity

Network routing

Threats to data

Account data and transaction data

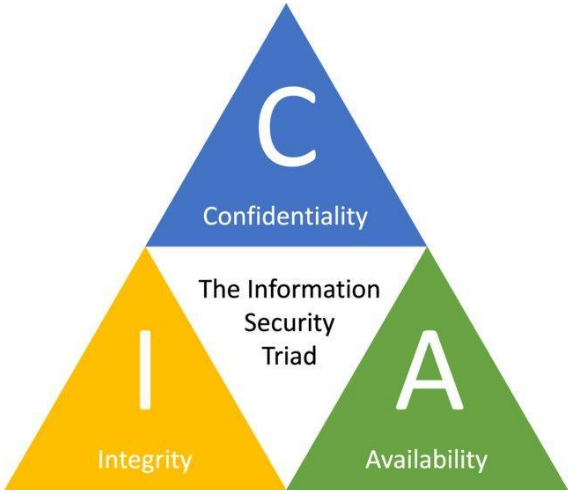
Private key leakage threats

Private key loss

Transactions threats

Security Impacts

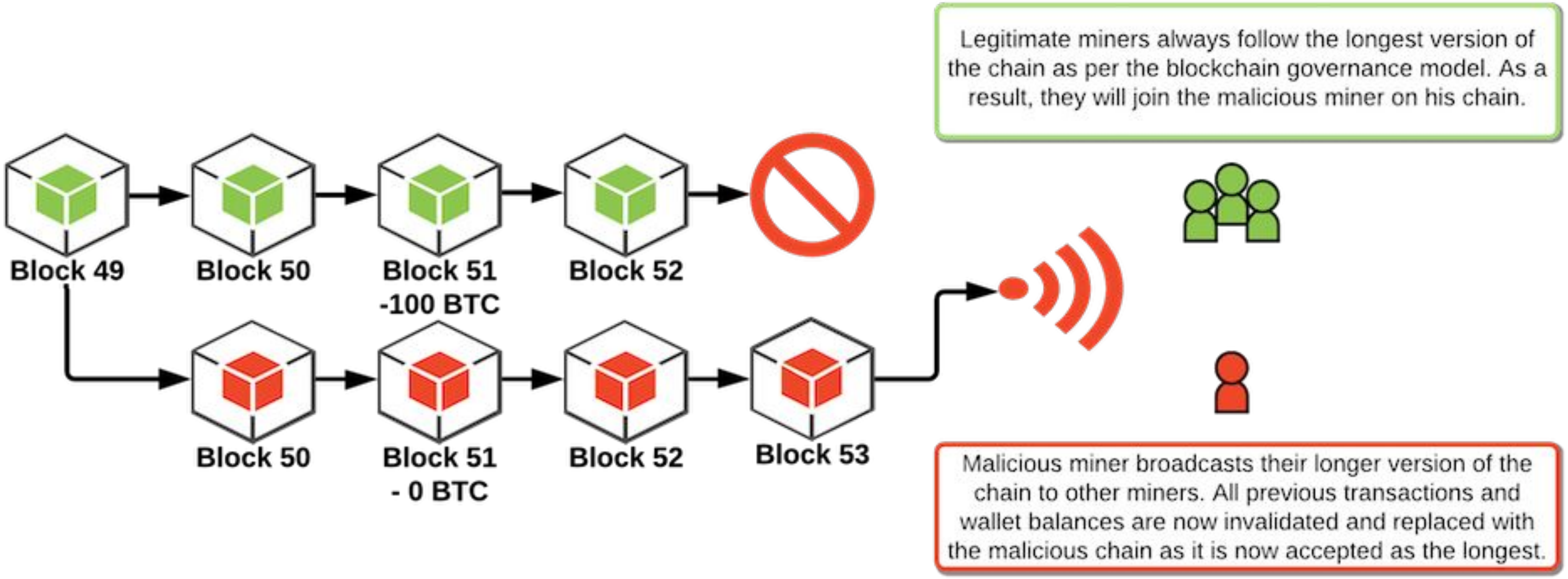
- **Protocols**: significant impact on the integrity of the blockchain system
  - For ex: a successful attack against consensus mechanism allows attacker to control the blockchain system
- **Network**: impact to the availability of the system
  - For ex:
- **Data**: impact to confidentiality and assets' ownership
  - Private key loss: no more control on digital assets
  - Private key leakage: unauthorized transactions



Security of Consensus Mechanisms

51% Attack

Consensus is the process by which a group of peers – or nodes – on a network determine which **blockchain** transactions are valid and which are not

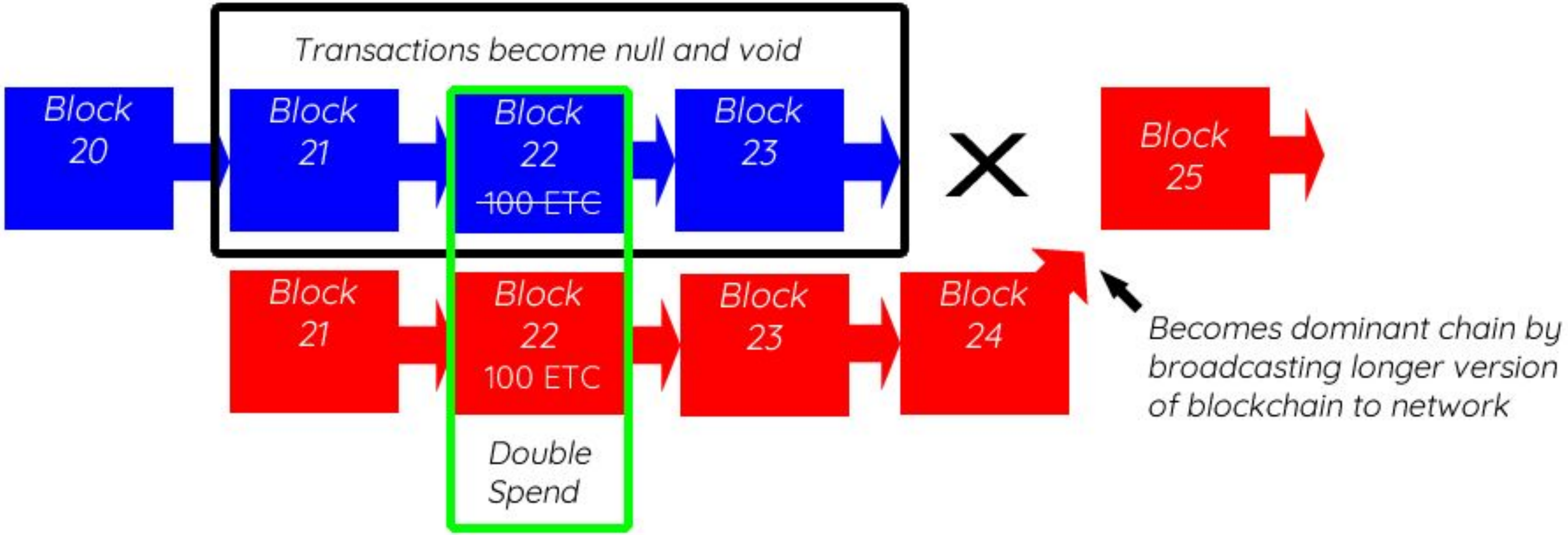


Legitimate miners always follow the longest version of the chain as per the blockchain governance model. As a result, they will join the malicious miner on his chain.

Malicious miner broadcasts their longer version of the chain to other miners. All previous transactions and wallet balances are now invalidated and replaced with the malicious chain as it is now accepted as the longest.

“If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.” -- Satoshi Nakamoto --

51% Attack (double-spend)



Transactions become null and void

Double Spend

Becomes dominant chain by broadcasting longer version of blockchain to network

🟦 Original (honest) blockchain <50% hash power

🟥 Malicious blockchain >50% hash power

© Andrew Butler

51% attack stories

- ETC, several times
  - Three attacks in August 2020: reorganized over 7,000 blocks, or two days' worth of mining
  - 88,500 ETC (roughly $450,000) were falsely deposited on the OkEX crypto exchange
  - On January 8th, 2020, Ethereum Classic had just 8.8 terrahash, compared to **over 39 million terrahash** of **Bitcoin**
- BSV, reported in August 2021
  - Nearly 100 blocks were compromised

Bitcoin SV rocked by three 51% attacks in as many months

Bitcoin SV has been under the hammer of rogue actors in a series of attempted 51% attacks against the network. Where next for BSV?

- Many other stories, including BTG, Verge, Mona, Aurum, ZenCash, etc.

Data Security

Why does it concern?

Data on Blockchain includes public/private key, wallet address, transaction data, etc.

- Losing private key results in losing funds
- Horror Stories:
  - A 35-year-old British man threw out a hard drive containing 7,500 BTC (~ $350m)
  - A German engineer who forgot the password to his encrypted device containing 7,002 BTC
  - Canada exchange QuadrigaCX's CEO went and allegedly died in India in 2018, resulting > 115,000 users' coins being lost, including 26,500 BTC; 11k BCH; 200k LTC and 430k ETH
  - And many more other stories, … just google "bitcoin private key lost stories"

Security of Smart Contracts

The Decentralized Autonomous Organization (DAO) hack

A **smart contract** is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code

- DAO is an organization represented by rules encoded as a computer program (smart contract)
- The DAO is built on Ethereum, designed for building dApps
- When launching in 2016, the DAO raised $150m worth of ETH through a token sale
- On 20 July 2016, hackers exploited a flaw in the DAO project’s smart contract
- Hackers stole 3.6 million ETH (~$50m that time, and ~$6b currently), showing that the DAO was All Too Human
- Ethereum made a hard fork to restore the money

Interoperability & Security

Poly Network Hack

An interoperability protocol allowing users swap tokens between different blockchains, for example, trading BTC to ETH

- August 2021, hackers stole $610m in digital crypto assets from Poly Network
- Hackers exploited vulnerabilities between smart contract calls
- Hackers then returned the whole funds to multi-signature wallets
- Poly Network offered $500,000 bug bounty and launched a global bug bounty program to audit Poly Network's core functions

Interoperability & Security

Layer 2 Security

- Recently (March 23, 2022): >173,000 ETH and around >25 million USDC were hacked from Axie Infinity’s Ronin Network
  - Axie Infinity is a Web3 game. Players use NFT digital pets, Axies to interact with the game’s community
  - Ronin Network is an independent, layer 2 and Ethereum-compatible blockchain (like Lightning Network vs. Bitcoin), developed to convert currency between Ethereum and Ronin blockchains
  - Ronin consists of 9 validator nodes. Using threshold signature (5 out of 9) to validate TXs in & out
  - Hackers compromised private keys (4 Ronin Validators & a 3rd party run by Axie DAO) and performed withdrawal transactions

Privacy

Privacy Issues in Blockchain

Can we have private transactions on a public blockchain?

- Blockchain data is public and transparent
    - Cannot store confidential data
        - E.g., sender & receiver info, amount transferred
    - Any interaction with the smart contract is also public

Can data on blockchain comply privacy acts?

- Blockchain data is immutable
    - Once data is written into blockchain, it cannot be removed
    - Cannot fulfill the right to be forgotten
    - Incompatible with GDPR

Limit the application of blockchain technology

Privacy in Digital Payments

Payments publicly visible and linkable

- Bitcoin
- Ethereum

Payments only visible to bank

- VISA
- Mastercard
- Internet banking

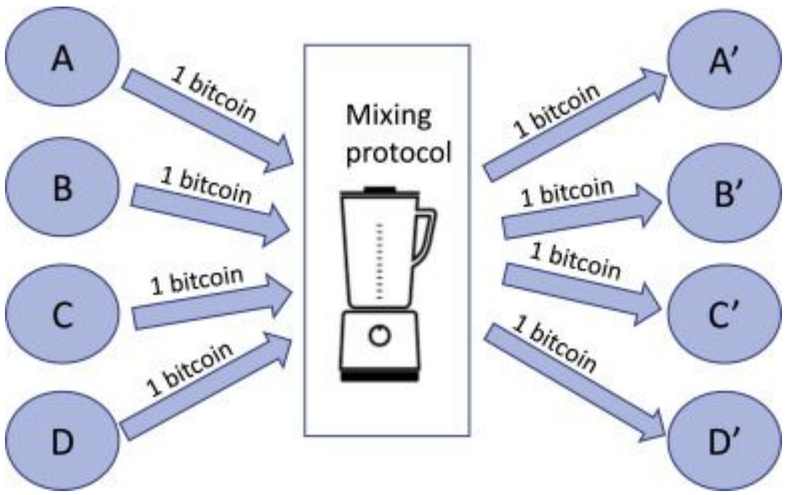
Private payments

- Monero
- ZCash
- Tonardo

Obfuscation Techniques

Mixing Services

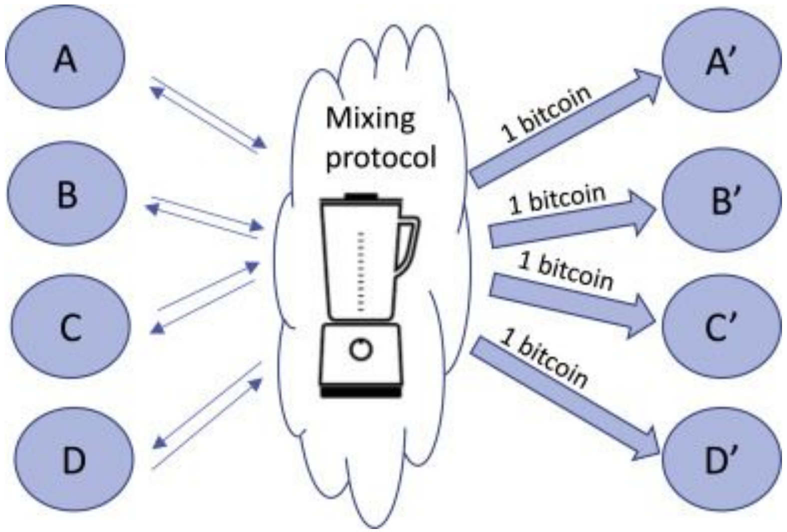
Centralized



Based on a trusted or semi-trusted third party, so-called mix server

- Mixcoin, Blindcoin (combining with blind signatures), DASH (set of mixer nodes), etc.

Decentralized



A group of payers negociates to form a jointly payment

- CoinJoin, CoinShuffle, CoinParty (using SMPC), etc.

Cryptographic Techniques

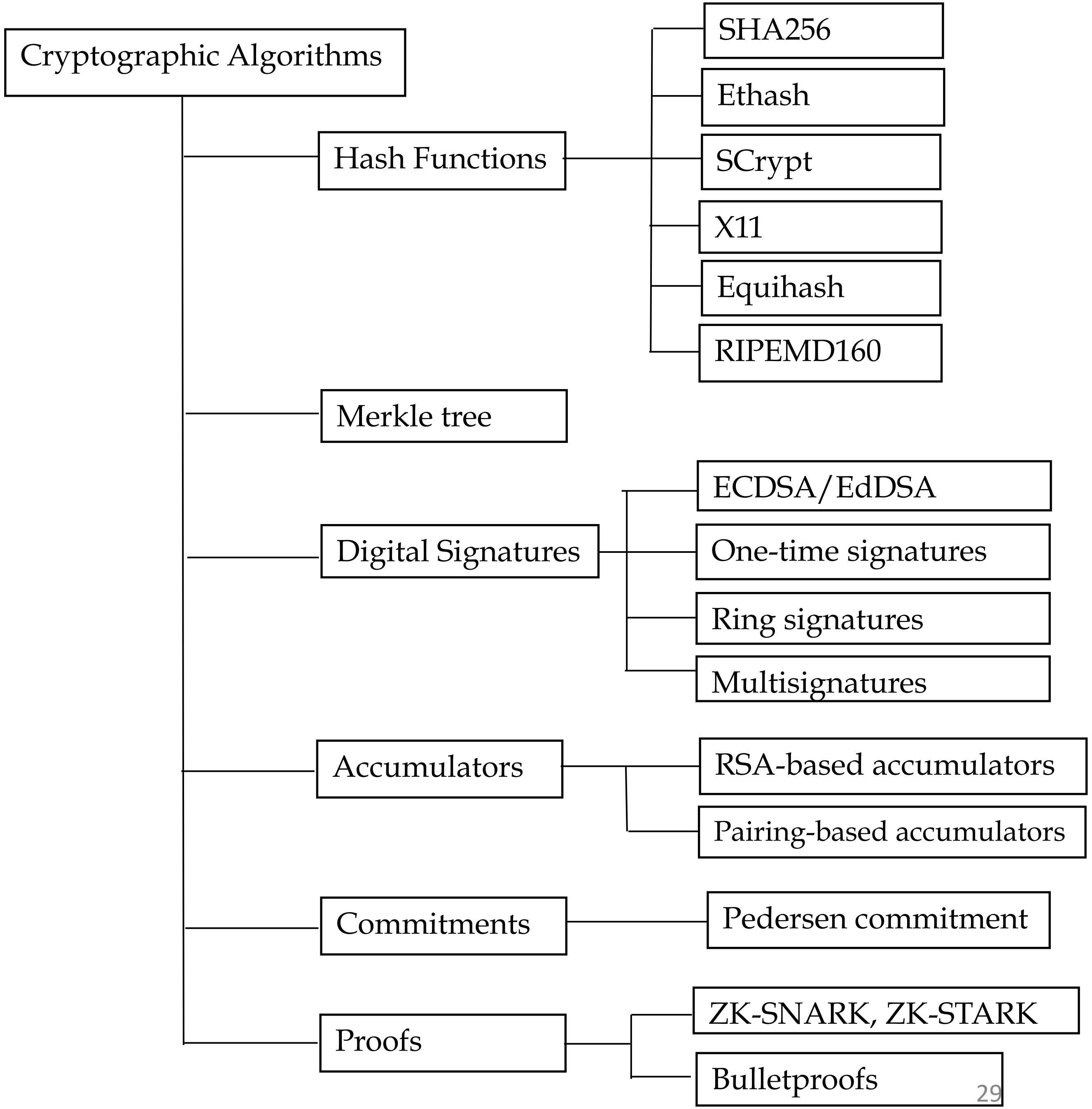
- Strawman approach
  - Encrypt data before writing into blockchain
  - Limitations:
    - Smart contract can not process ciphertext
    - Encrypted data can not be publicly verified
- Cryptographic Commitments
  - Allow committing to a chosen value while keeping it hidden to others, with the ability to reveal the committed value later
  - Monero implements Pedersen commitment to hide transaction amount
- Zero-Knowledge Proofs
  - Prover can prove a knowledge to a verifier without revealing any useful thing
  - Used in ZCash to provide privacy for sender and confidentiality of transaction amount

Cryptographic Techniques (cont.)

- Ring Signatures
  - A group of user jointly sign a message
  - Used in CryptoNote and Monero to protect sender privacy
- One-Time (Ring) Signatures
  - One -time signature signs each message with a different pair of public/private keys
  - Combine with ring signatures to provide the privacy of sender
- Stealth Address
  - Generate new address for each transaction
  - Used in Monero and ZCash to provide the receiver privacy

Cryptography in Blockchain

A brief summary



Open Research Questions

- Security and Privacy of on-chain transactions
    - The current cryptographic primitives being used to ensure privacy such as Zero-Knowledge Proofs or special signatures are not suitable for use in a tap-pay user experience. Can we design efficient cryptographic algorithms for low resource devices?
- Security and Privacy of off-chain channel
- Security and privacy of interoperability between blockchain platforms
- Blockchain Trilemma: Decentralized, scalable, secure
    - How to increase the scalability without losing the decentralization and security?
    - Can we provide the same level of security in a private blockchain compared to the public blockchain networks with a higher level of decentralization?
-

Open Research Questions

- Security and Privacy of Smart Contracts
  - Many contracts performed in a business context is done in confidence. How can we implement private smart contracts?
- Privacy Compliance
  - How can we perform an KYC/AML compliance in blockchain-based applications whilst offering users and transactions privacy?
  - How can blockchain-based applications comply with privacy requirements such as the right to be forgotten, or other data rights under the GDPR framework?

Thank You!