Chapter 2

CRYPTOGRAPHY AND CRYPTOCURRENCY

TP. HCM 2022

OVERVIEW

- Blockchain definition
- Bitcoin Design Features
- Cryptographic Hash Functions
- Timestamped Append-only logs
- Block Headers & Merkle Trees
- Asymmetric Cryptography & Digital Signatures
- Bitcoin Addresses

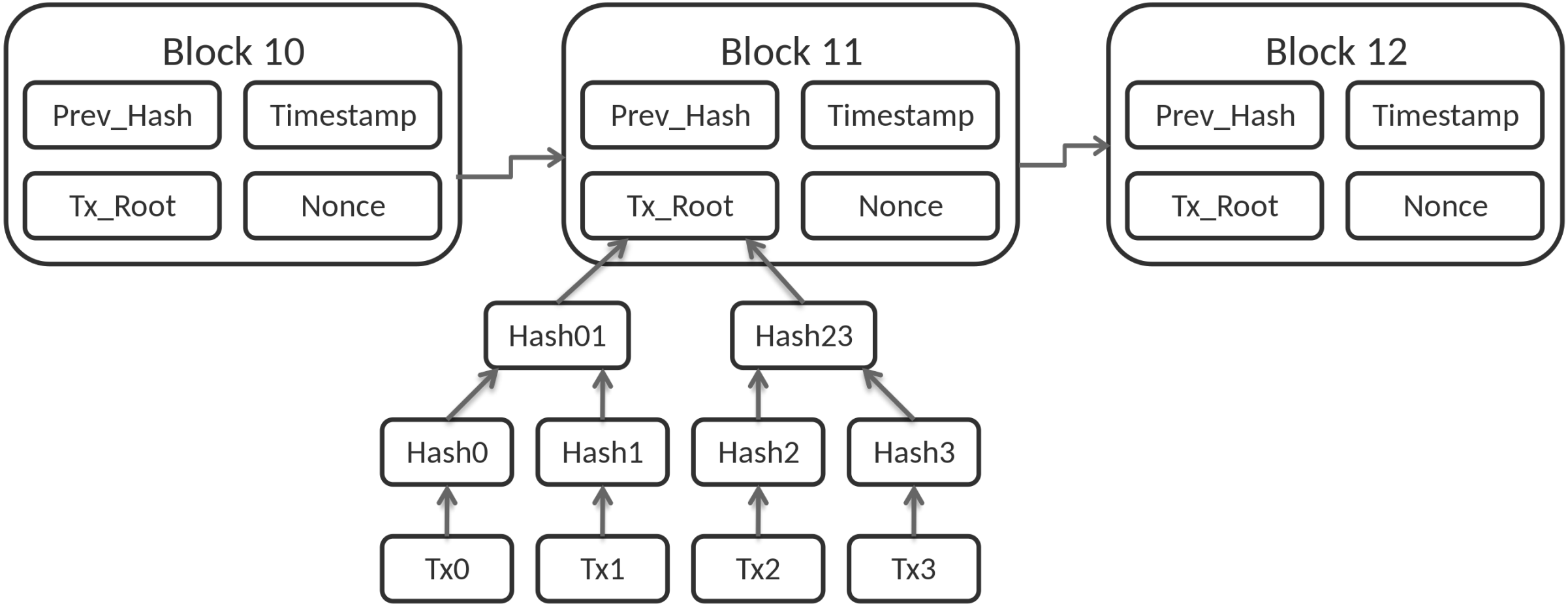
Study Questions

- What is distributed ledger technology (DLT)?
- The relationships between blockchain and DLT?
- What is a block, transactions?
- Types of blockchains?
- Advantages & Disadvantages of Blockchains?
- Potential applications of blockchain in practice?
- Group of 3 or 4 students:
  - self-study and take notes: 25 minutes
  - discussion: 25 minutes

Blockchain - Definition

- A blockchain is a type of **distributed ledger technology (DLT)** that consists of growing list of records, called ***blocks***, that are securely ***linked*** together using cryptography [wikipedia].
- Each block contains:
  - a timestamp
  - a cryptographic hash of the previous block,
  - transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves)
- Types of blockchains:
  - Public Blockchains
  - Private Blockchains
  - Hydrid blockchains (consortiums)
  - Sidechains

Blockchain - An Instance



Structure of Bitcoin blockchain (image: wikipedia)

Blockchain - Types

- Public blockchains:
  - open, decentralized networks of computers accessible to anyone who want to **request** or **validate** a transaction (check for accuracy)
  - Those (miners) who validate transactions receive rewards.
  - Proof-of-work or proof-of-stake consensus mechanisms are used.
  - Examples: the Bitcoin and Ethereum (ETH) blockchains.

Blockchain - Types

- Private blockchains:
  - NOT open, they have access restrictions
  - Require a permission from the system administrator to join
  - They are typically governed by one entity, meaning they're centralized
  - Example: Hyperledger is a private, permissioned blockchain

Blockchain - Types

- Hybrid blockchains (consortiums):
  - a combination of public and private blockchains
  - contain centralized and decentralized features.
  - Example: Dragonchain, Energy Web Foundation, and R3.

Blockchain - Types

- Sidechains:
  - a blockchain running parallel to the main chain.
  - allows users to move digital assets between two different blockchains
  - improves scalability and efficiency.
  - Example: the Liquid Network.

Blockchain - How it works

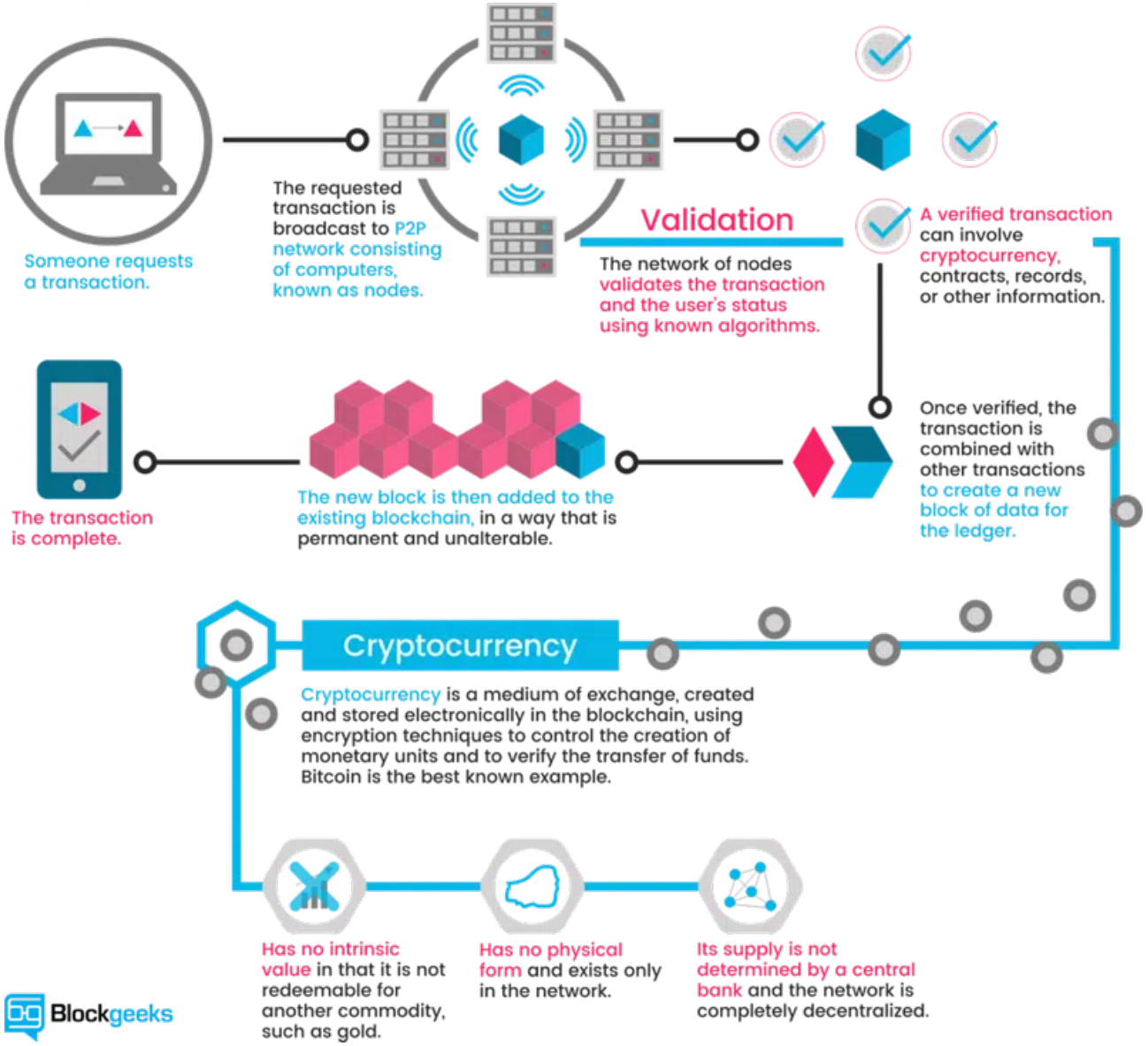


Image by http://www.blockgeeks.com

Benefits of Blockchain Over Traditional Finance

- Trustless
- Unstoppable
- Immutable
- Decentralized
- Lower Cost
- Peer-to-Peer
- Transparent
- Universal Banking

Disadvantages of Blockchain

- Environmental Impact
- Personal Responsibility
- Growing Pains
- False Narratives

Applications of Blockchain

- Cryptocurrencies: Bitcoin, Ethereum, etc.
- Smart Contracts
- Decentralized Banking
- Video Games/Art
- Peer-to-peer Energy Trading
- Supply chain and logistics tracking
- Healthcare process optimization

Applications of Blockchain

- Real estate processing platform
- NFT marketplaces: These are marketplaces that allow you to buy nonfungible tokens (NFTs) ➔ “FTX sập rồi”
- Music royalties tracking
- Personal identity security
- Automated Advertising Campaigns

BITCOIN DESIGN FEATURES

Cryptography & Timestamped Logs

- Cryptographic Hash Functions
- Timestamped Append-only Logs (Blocks)
- Block Headers & Merkle Trees
- Asymmetric Cryptography & Digital Signatures
- Addresses

Decentralized Network Consensus

- Consensus through Proof of Work
- Network of Nodes
- Native Currency

Transaction Script & UTXO

- Transaction Inputs & Outputs
- Unspent Transaction Output (UTXO)
- Scripting language

CRYPTOGRAPHIC HASH FUNCTIONS

Hash = Digital Fingerprints for Data

General Properties

- Maps Input x of any size to an Output of fixed size – called a ‘Hash’
- Deterministic: Always the same Hash for the same x
- Efficiently computed

Cryptographic Properties

- Preimage resistant (One way): infeasible to determine x from Hash(x)
- Collision resistant: infeasible to find and x and y where Hash(x) = Hash(y)
- Avalanche effect: Change x slightly and Hash(x) changes significantly
- Puzzle friendliness: knowing Hash(x) and part of x it is still very hard to find rest of x 1

CRYPTOGRAPHIC HASH FUNCTIONS

Hash = Digital Fingerprints for Data

Use cases

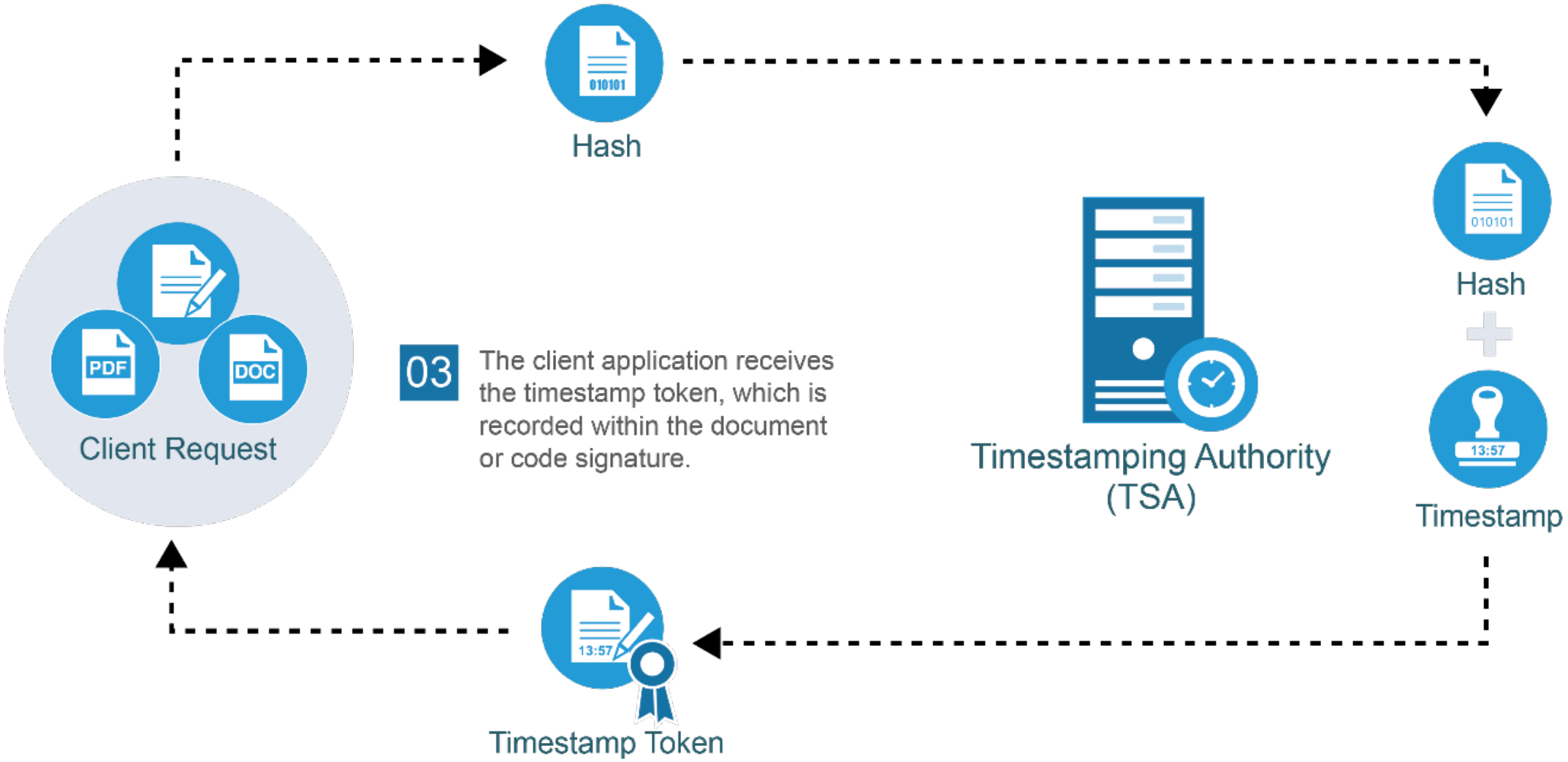
- Hash password before storing in database
- Verify data integrity when receiving
- Using as reference
- Using in digital signature

Bitcoin hash functions

- Headers & Merkle Trees – SHA 256
- Bitcoin Addresses – SHA 256 and RIPEMD160

Hash calculator online

TIME-STAMP DIGITAL DOCUMENT



TIME-STAMP DIGITAL DOCUMENT

WHY TIME-STAMP?

- Bind a signed document to a particular date and time
- Prove in the future that the signed document existed at this particular date and time.
- Ensure the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound

USE CASE

- Digital signature for contract

TIME-STAMP DIGITAL DOCUMENT

WHY TIME-STAMP?

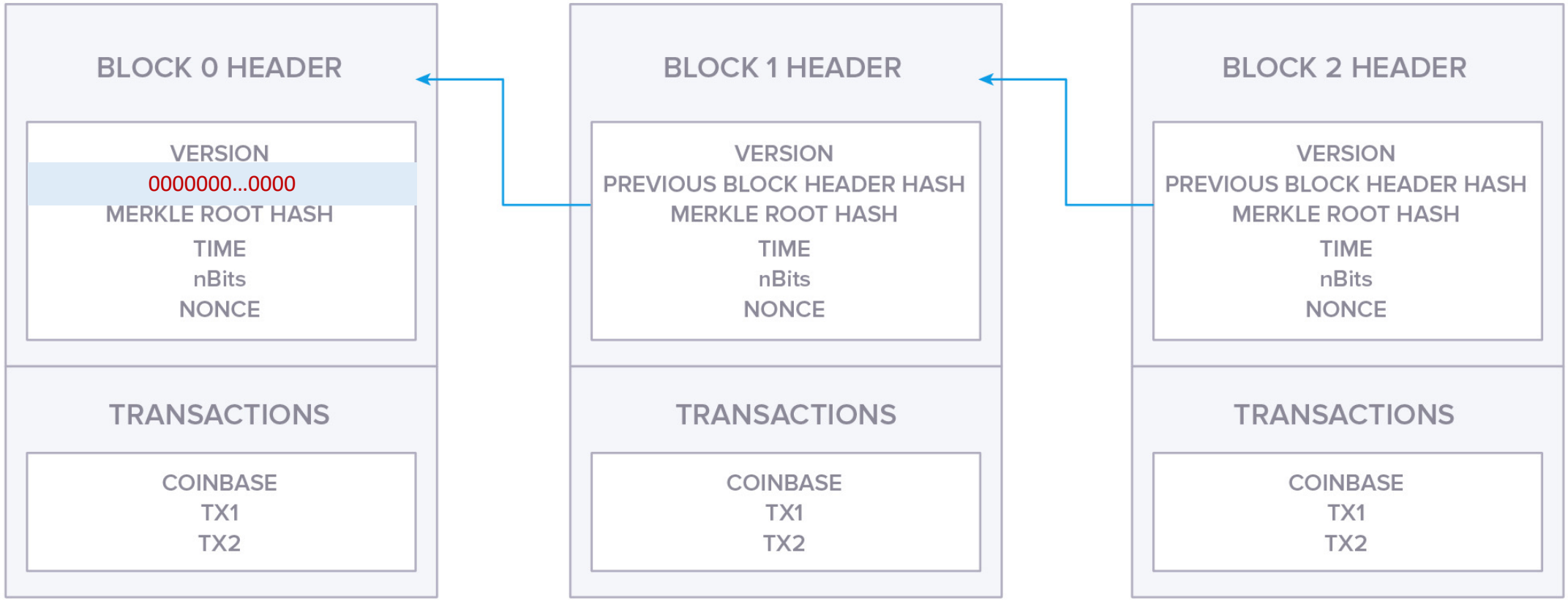
- Bind a signed document to a particular date and time
- Prove in the future that the signed document existed at this particular date and time.
- Ensure the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound

USE CASE

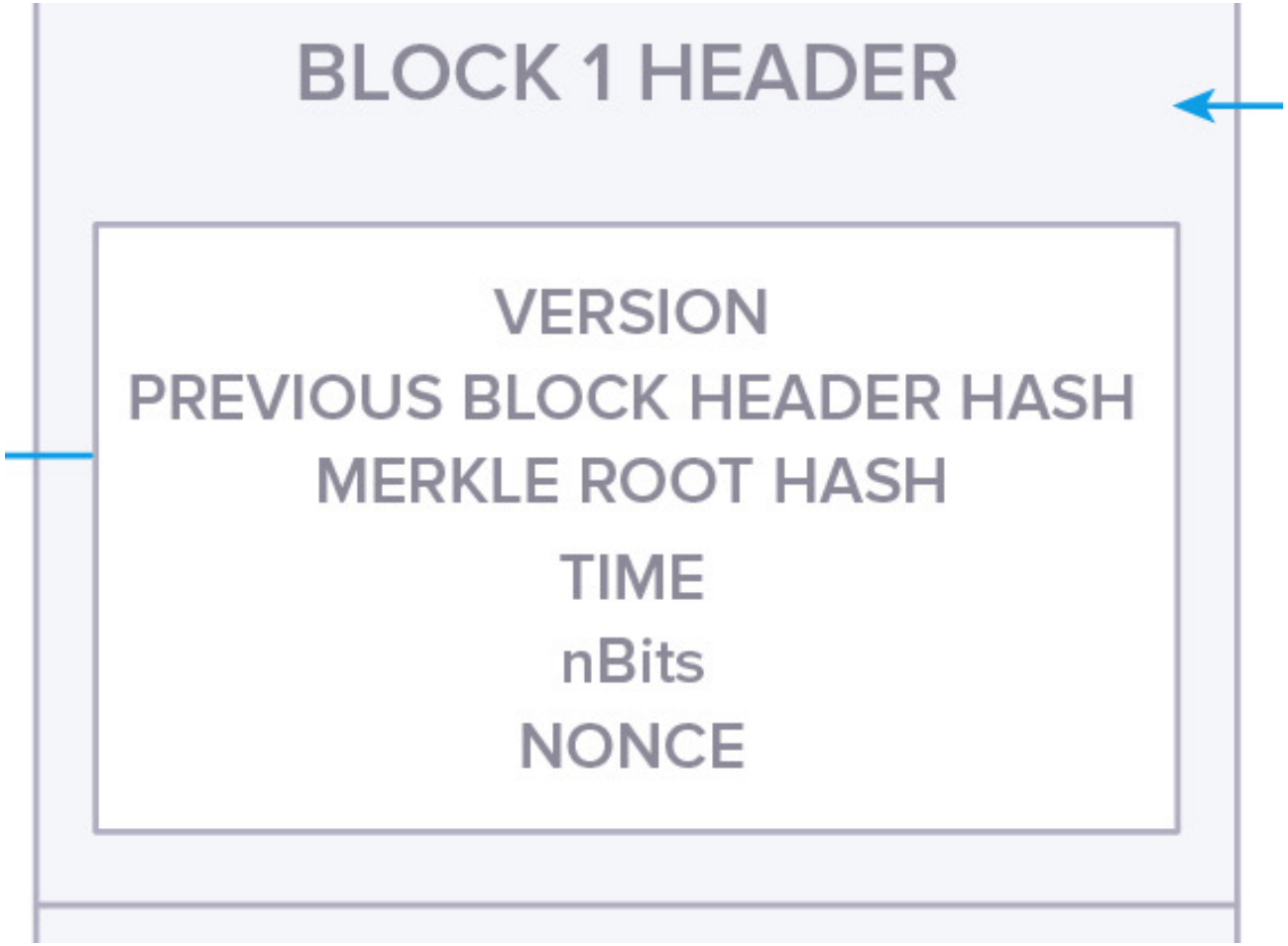
- Digital signature for contract

TIMESTAMPED APPEND-ONLY - BLOCKCHAIN

GENESIS BLOCK



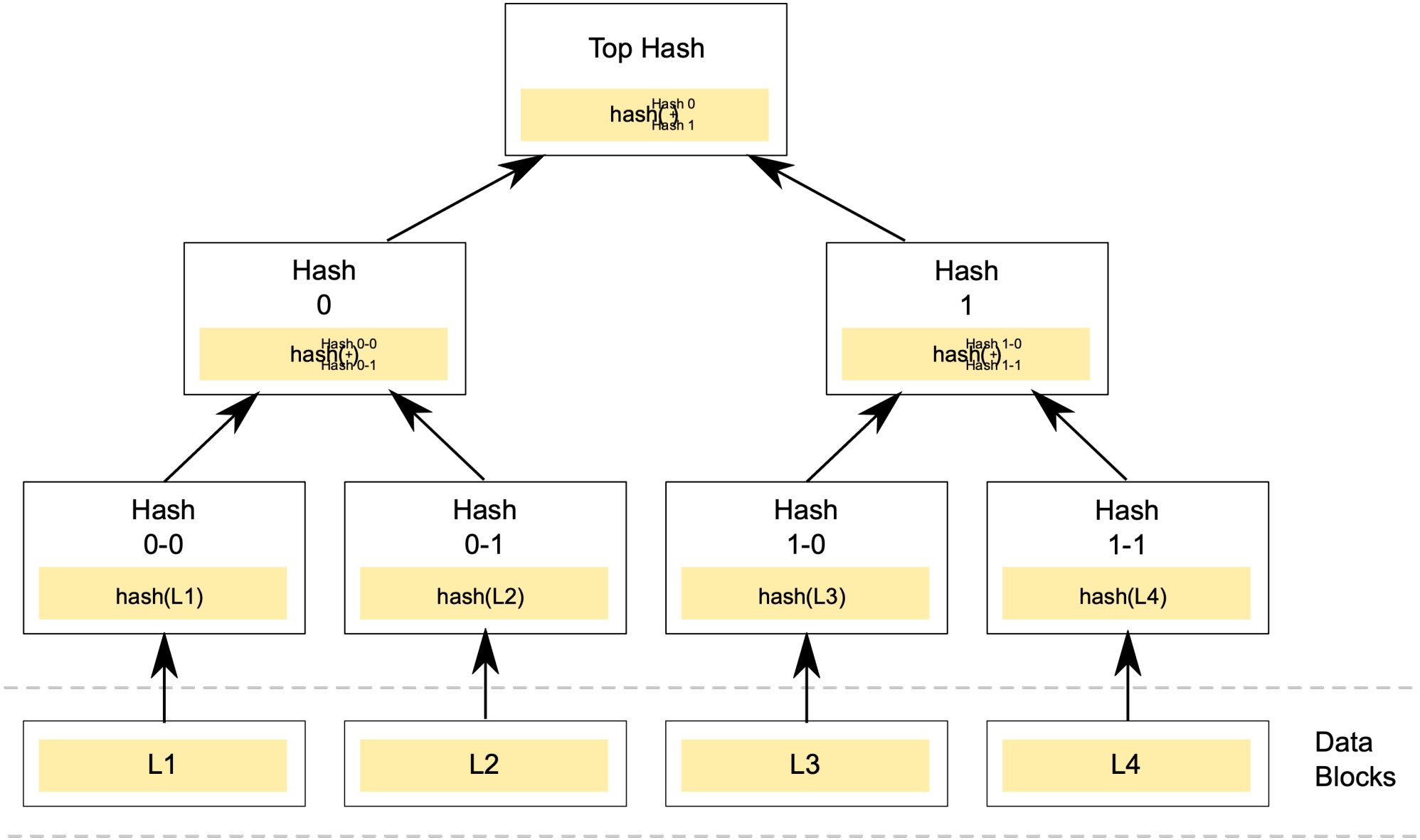
BLOCK HEADER



- Version
- Previous Block hash
- Merkle Root hash
- Timestamp
- Difficulty target
- Nonce

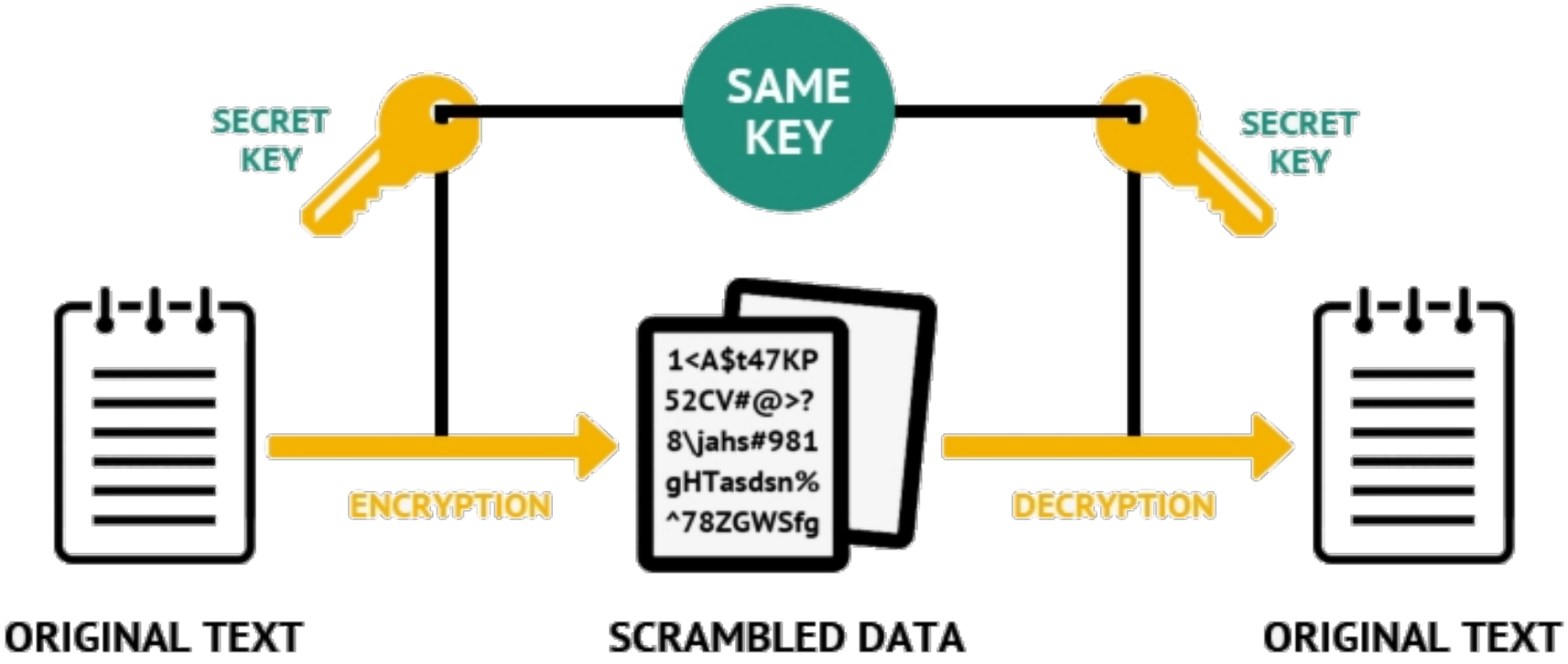
MERKLE TREE

Binary Data Tree with Hashes

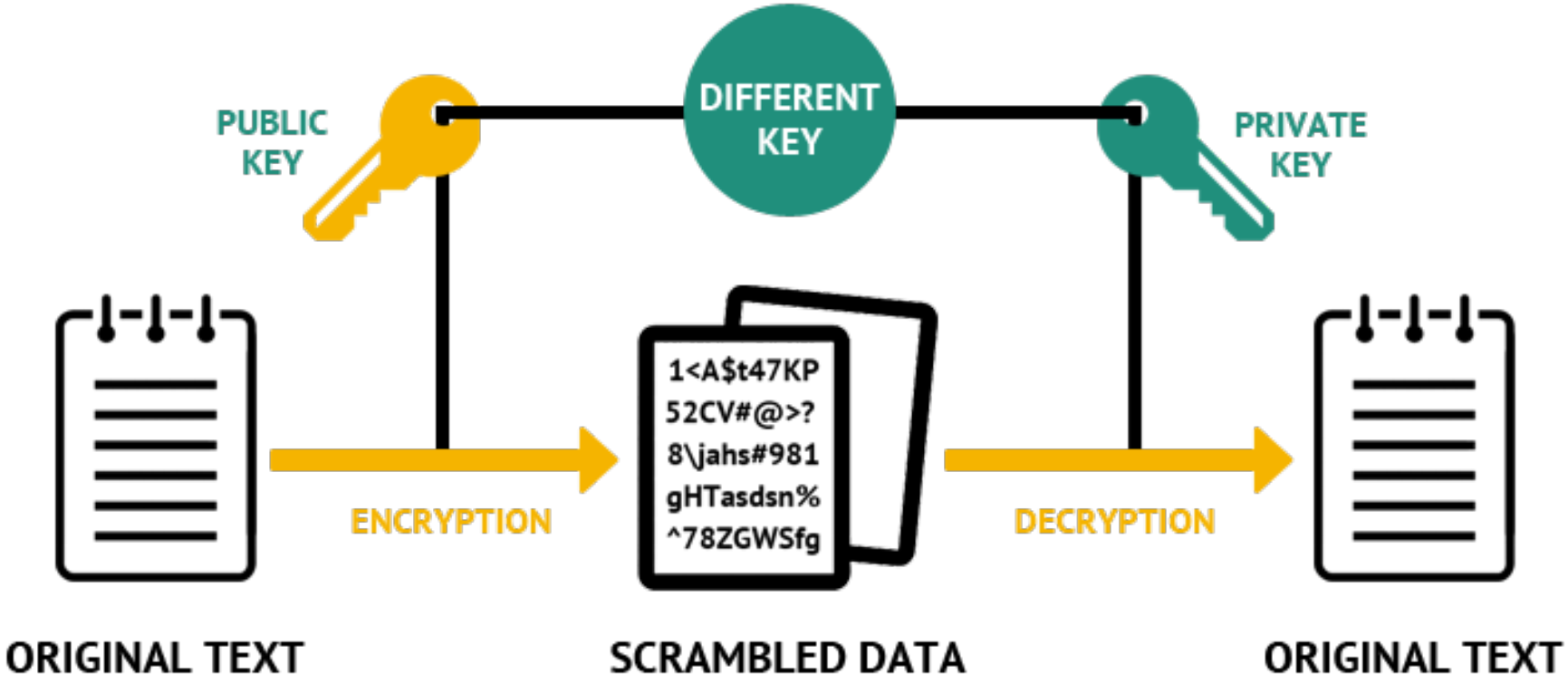


SYMMETRIC & ASYMMETRIC CRYPTOGRAPHY

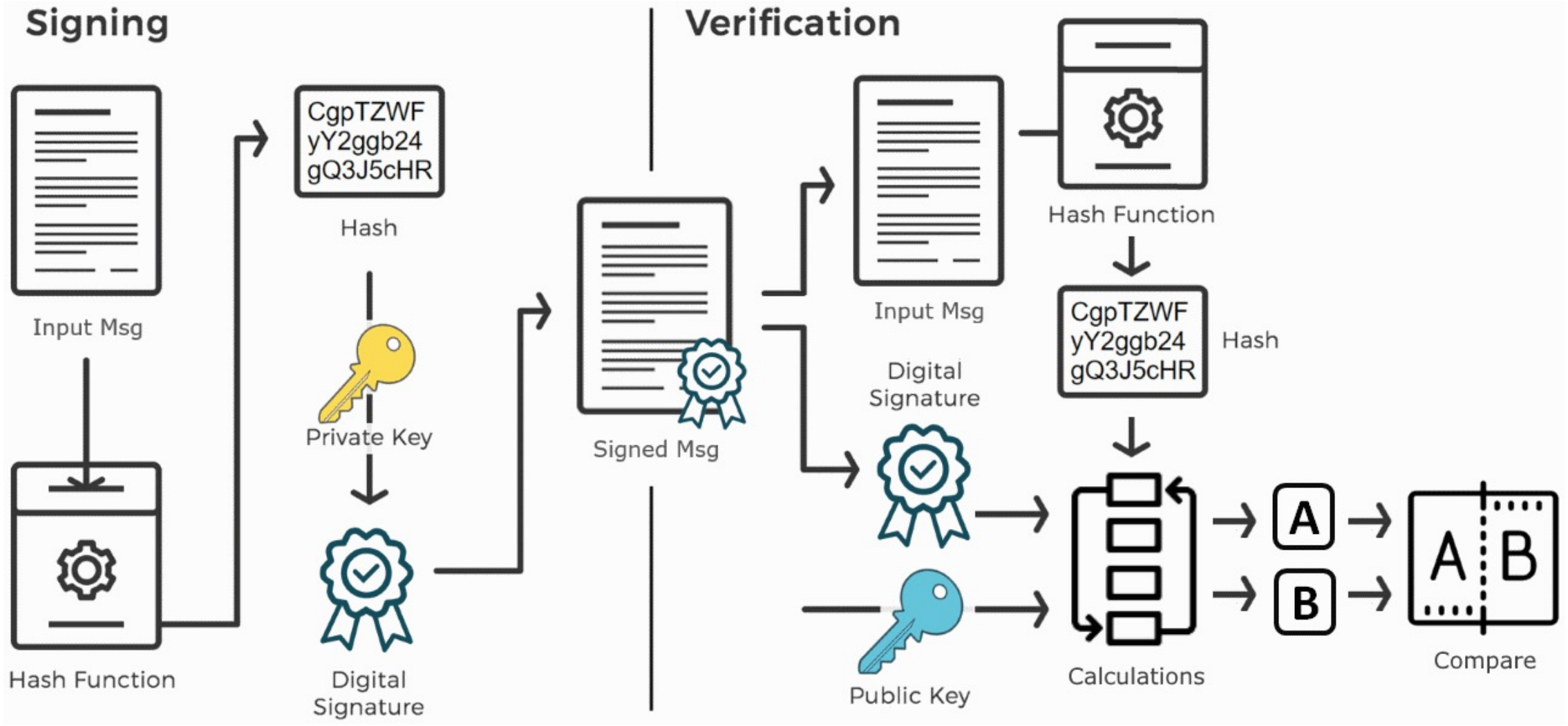
SYMMETRIC ENCRYPTION



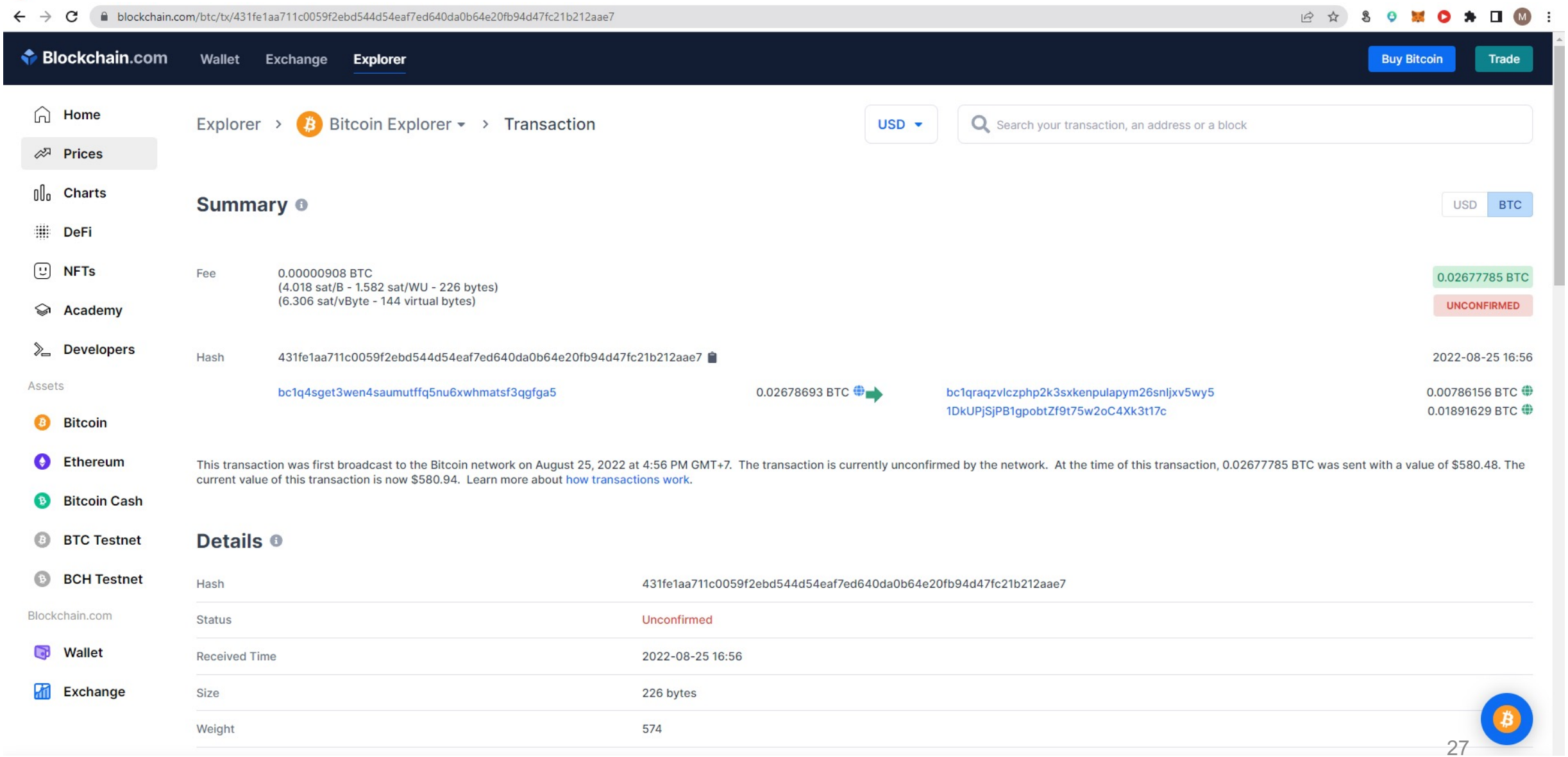
SYMMETRIC & ASYMMETRIC CRYPTOGRAPHY



ASYMMETRIC CRYPTOGRAPHY & DIGITAL SIGNATURES



BITCOIN ADDRESSES



[Bitcoin explorer]

BITCOIN ADDRESSES

Hash 431fe1aa711c0059f2ebd544d54eaf7ed640da0b64e20fb94d47fc21b212aae7

bc1q4sget3wen4saumutffq5nu6xwhmatsf3qgfga5 0.02678693 BTC bc1qraqzvlczphp2k3sxkenpulapym26snljxv5wy5
1DkUPjSjPB1gpobtZf9t75w2oC4Xk3t17c

Sign transaction with private key

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOgIBAAJBAKj34GkxFhD90vcNLYLInFEX6Ppy1tPf9Cnzj4p4WGeKLs1Pt8Qu
KUpRKfFLfRYC9AIKjbJTWit+CqvjWYzvQwECAwEAAQJAIJLixBy2qpFoS4DSmoEm
o3qGy0t6z09AIJtH+5OeRV1be+N4cDYJKffGzDa88vQENZiRm0GRq6a+HPGQMd2k
TQIhAKMSvzIBnni7ot/OSie2TmJLY4SwTQAevXysE2RbFDYdAiEBCUEaRQnMnbp7
9mxDXDf6AU0cN/RPBjb9qSHDcWZHGzUCIG2Es59z8ugGrDY+pxLQnwfotadxd+Uy
v/Ow5T0q5gIJAiEAyS4RaI9YG8EWx/2w0T67ZUVAw8eOMB6BIUg0Xcu+3okCIBOs
/5OiPgoTdSy7bcF9IGpSE8ZgGKzgYQVZeN97YE00
-----END RSA PRIVATE KEY-----
```

Verify transaction with public key

```
-----BEGIN RSA PUBLIC KEY-----
MEgCQQCo9+BpMRYQ/dL3DS2CyJxRF+j6ctbT3/Qp84+KeFhnii7NT7fELilKUSnx
S30WAvQCCo2yU1orfgqr41mM70MBAgMBAAE=
-----END RSA PUBLIC KEY-----
```

HASH SHA 256

61087f7e8804c5361dd0291c2dd4083a6d28014a999b43c981a42435cf0fce00

HASH RIPEMD 160

First 4 bytes (8 hex digits) 09bcbf6b

2x SHA 256

21799c282798d07dc5cf385d5fe2fcb7c5e91a53

Bitcoin address

3xVUrcYNkxtrpgeD6Lez2QbfZGW7g3MDWTV34mZy

base58

21799c282798d07dc5cf385d5fe2fcb7c5e91a5309bcbf6b

Bitcoin explorer

QUESTIONS

- Why bitcoin need time-stamp and hash?
- Why we need seed phrase instead of password to initiate blockchain transaction?

DISCUSSION