KBA

Introduction to Blockchain

Agenda

- History of Blockchain
- Cryptographic techniques
- Blockchain
- Bitcoin Blockchain
- Consensus algorithms
- Types of Blockchains
- Application areas
- Programmable Blockchain
- Web3

History of Money

Barter System-
where one type of commodity is traded for another. The exchange seemed fast, straight and simple between two people.
The drawback was no central authority to fix a standard price.

Cowry shells-
The initial coins. Farther the place was cowry shell's source, higher the price cowry carried.
This turbulence called for much-standardized execution of the trade.

Metals-
Hard to mine and difficult to trade. Traders found it something to be counted as money.
Metals were formed into shapes to resemble cowry shells.

Banks-
Banks became the trusted authority of people to store their gold and other precious metals.
Banks introduced paper currency for putting away gold and other ware in their private vault.

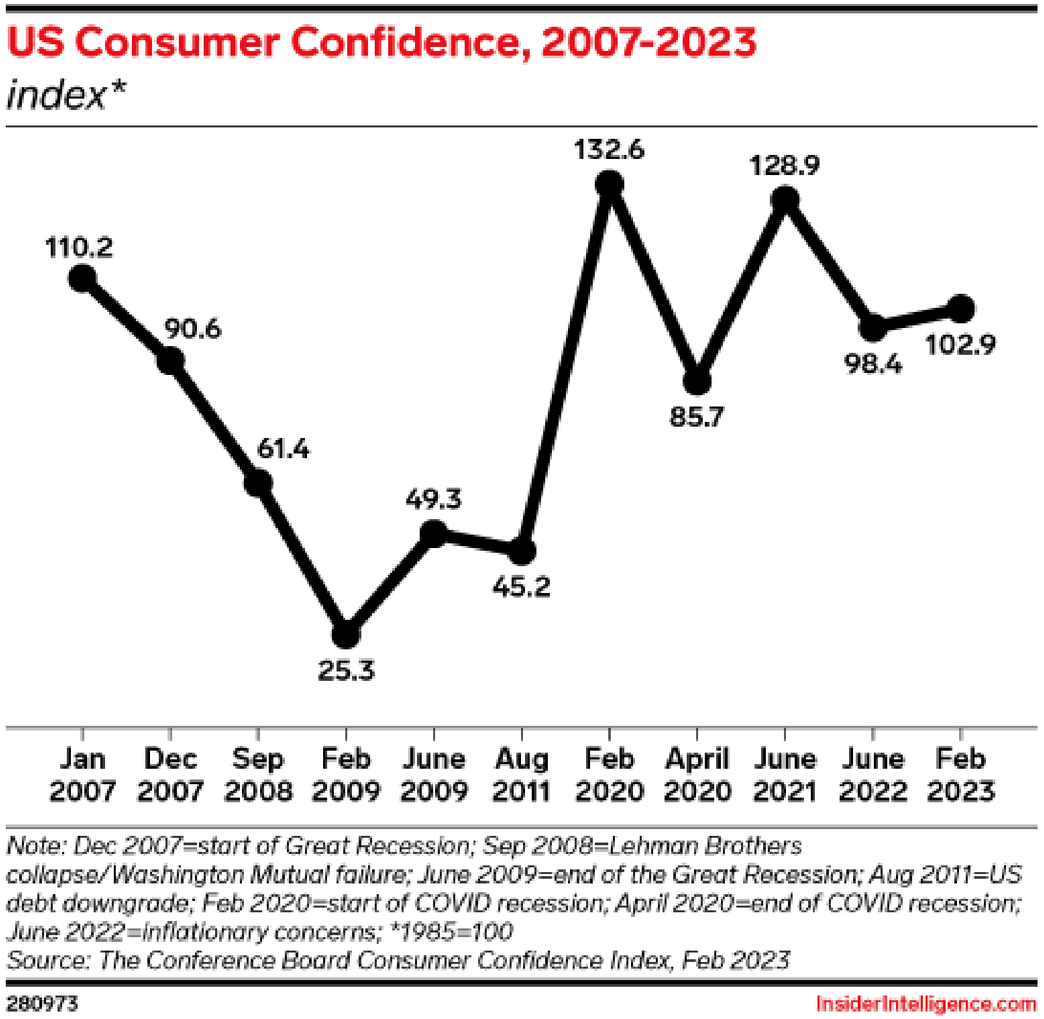
Gold-
Precious and hard to counterfeit.
The inherent rarity of gold and its ability to be melted into coins of various denominations gave traders new dimensions of exchange.

Financial Crisis 2008

The US Govt printed $ 700 billion to get out of the great recession

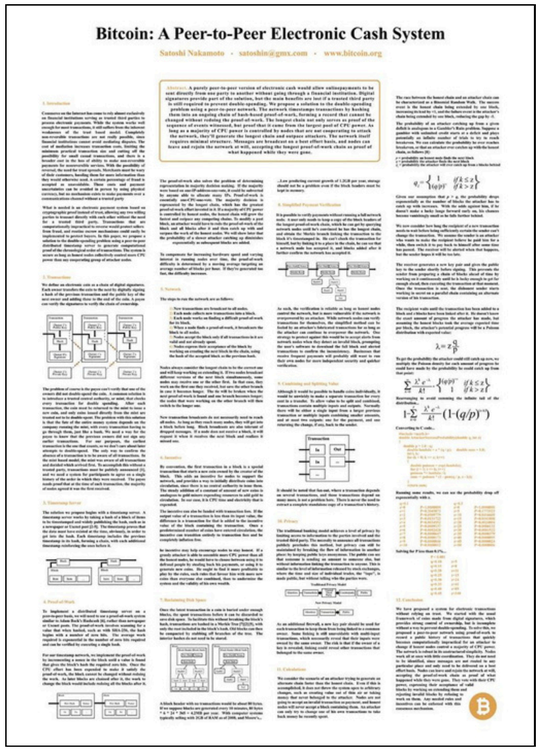
Source: https://www.nytimes.com/2008/10/03/business/worldbusiness/03iht-bailout.4.16679355.html

Financial Crisis 2008



Birth of Bitcoin

KBA



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto · satoshin@gmx.com · www.bitcoin.org

Satoshi Nakamoto published a whitepaper

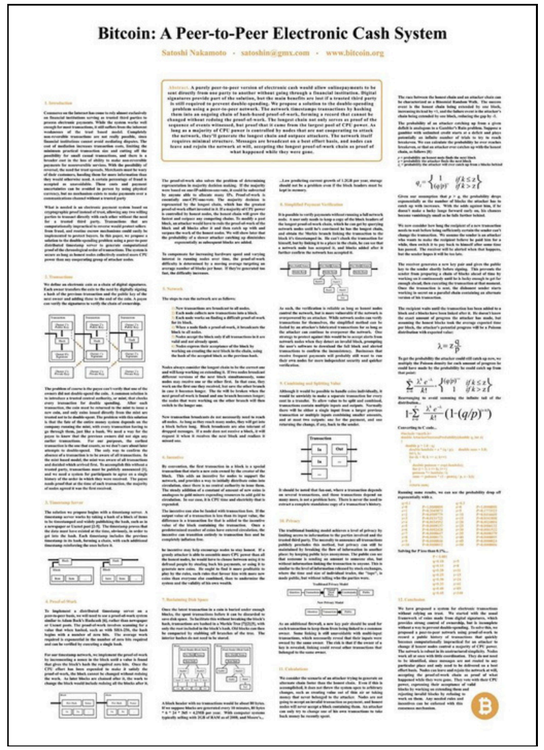
Bitcoin: A peer to peer electronic cash system

Bitcoin Whitepaper

KBA

Bitcoin Goals:

- To create a **trustless system**, using cryptography
- Solve **double-spending** problem of previous digital currencies
- Create **digital assets** that can be owned, with proof of ownership



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto · satoshin@gmx.com · www.bitcoin.org

BITCOIN ₿

KBA

Cryptocurrencies > Bitcoin Price

Bitcoin BTC Price #1

$90,084.85 ▲ 4.2%

1.0000 BTC ▲ 0.0%

$86,353.40 — 24h Range — $93,477.11

☆ Add to Portfolio • 1,733,158 added

Market Cap	$1,782,054,888,349
Fully Diluted Valuation	$1,891,781,934,000
24 Hour Trading Vol	$129,938,462,344
Circulating Supply	19,781,959
Total Supply	21,000,000
Max Supply	21,000,000

Info

Website — bitcoin.org — Whitepaper

Overview | Markets | News | Similar Coins | Historical Data | Bitcoin Halving Countdown

Price | Market Cap | TradingView | 24h | 7d | 1m | 3m | 1y | Max | LOG

KBA

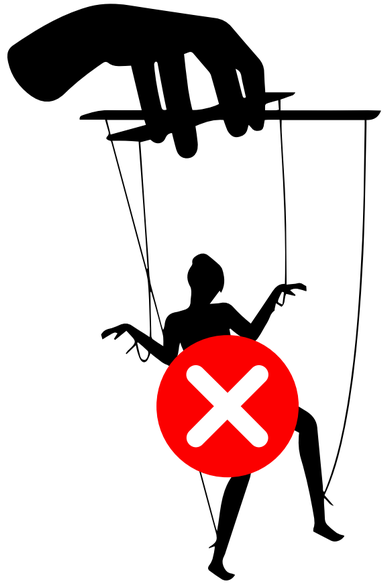
BITCOIN ₿

WHAT IS SO SPECIAL ABOUT IT ?

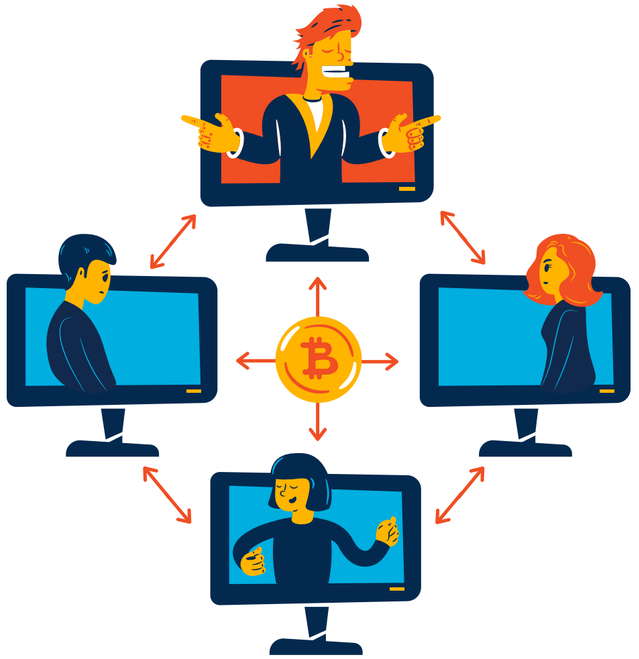
BITCOIN

KBA

Only 21 Million Bitcoins can be minted



Not controlled by anyone



Decentralized P2P network

WHAT LIES UNDER THE HOOD ?

K B A

DEFINING A CHAIN

WHAT ?

BLOCKCHAIN TECHNOLOGY IS A DECENTRALIZED , DISTRIBUTED ,IMMUTABLE ,LEDGER TECHNOLOGY

WHY ?

A REAL-TIME OPEN LEDGER FOR RECORDING ANY TYPE OF TRANSACTION(DATA) WITH NO SINGLE OWNER

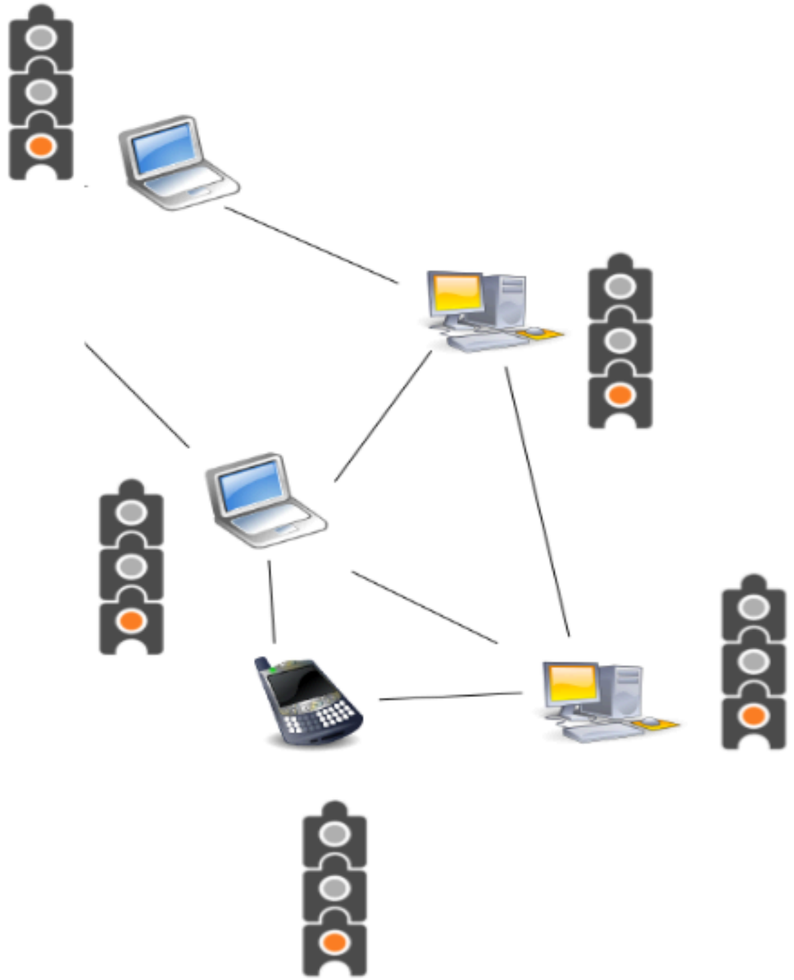
WHEN ?

CAME IN A DOCUMENT, OR WHITEPAPER PUBLISHED IN 2008 BY SATHOSHI NAKAMOTO

WHAT IS BLOCKCHAIN?

KBA

Blockchain technology is a **Distributed Ledger Technology (DLT)**

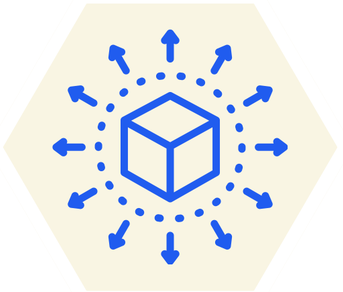


WHAT IS BLOCKCHAIN?

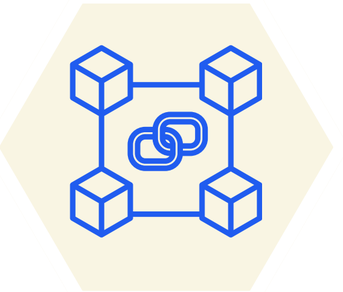
KBA

Ledger

Decentralised

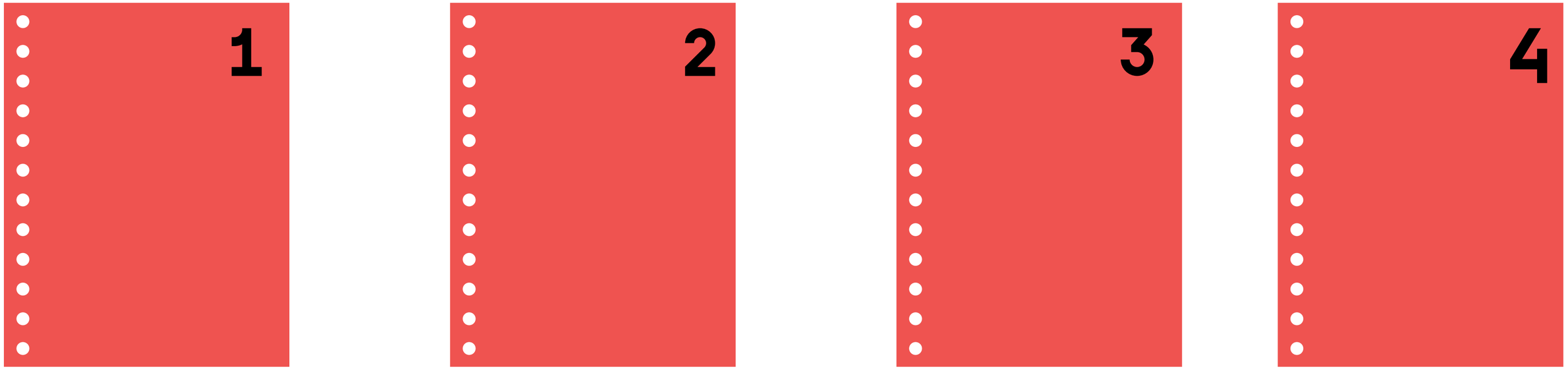


Distributed



Immutable

KBA



Each page is connected with each other

Just like how each block is connected with each other

KBA

Book consists of all the pages

Just like how blockchain consists of all the blocks





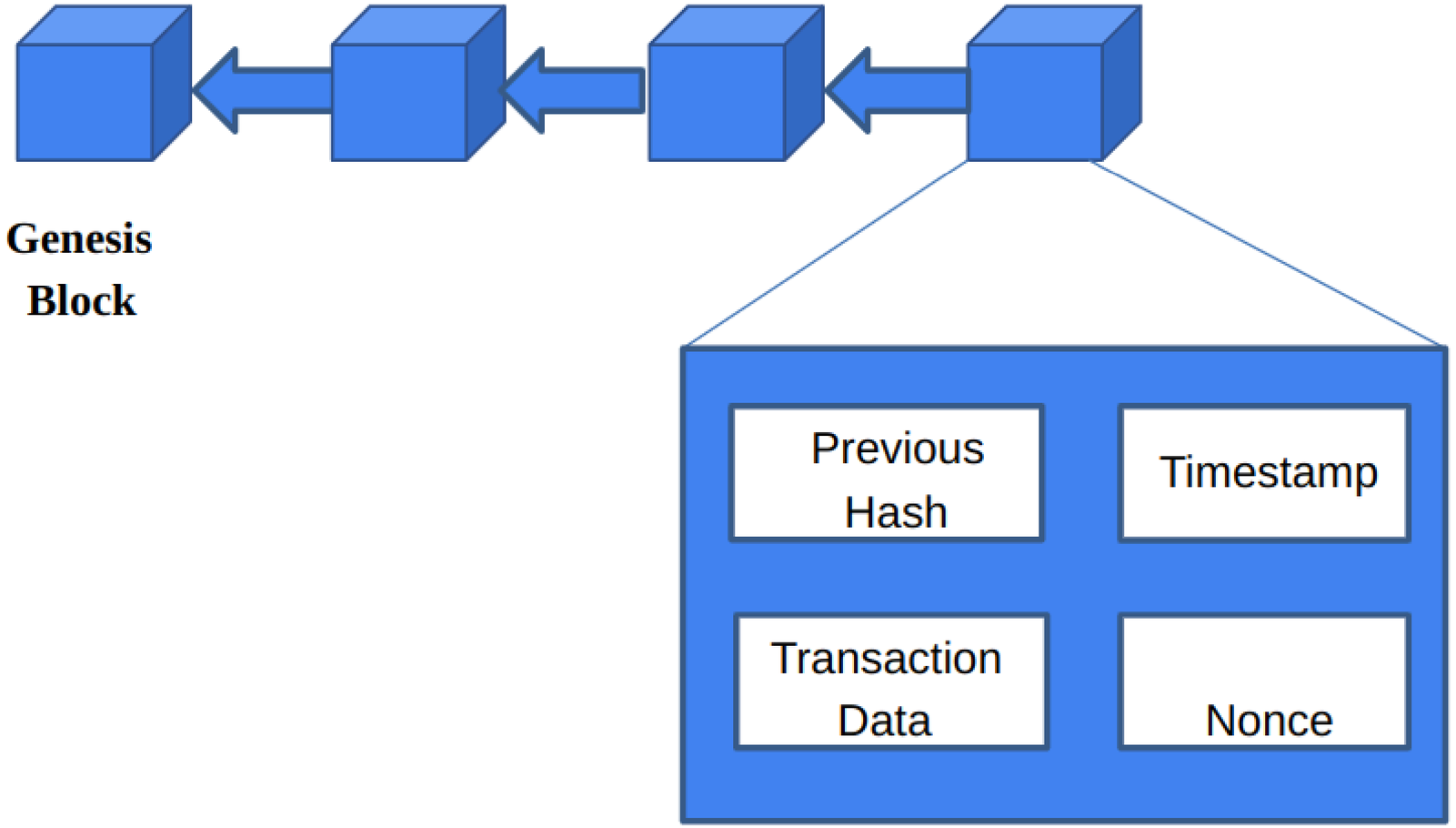



A copy of the book is given to its readers

A copy of the blockchain is given to all the network participants

BLOCKCHAIN

KBA

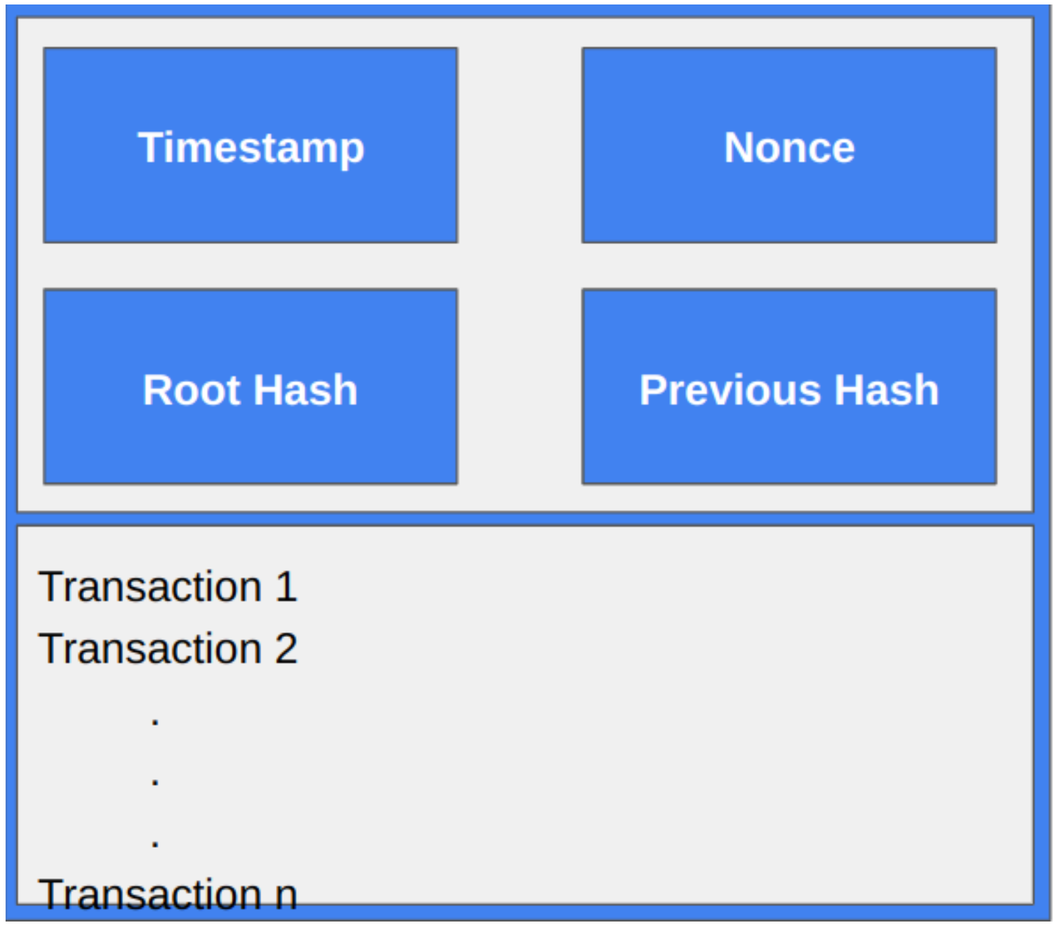


BLOCKCHAIN

KBA

HEADER

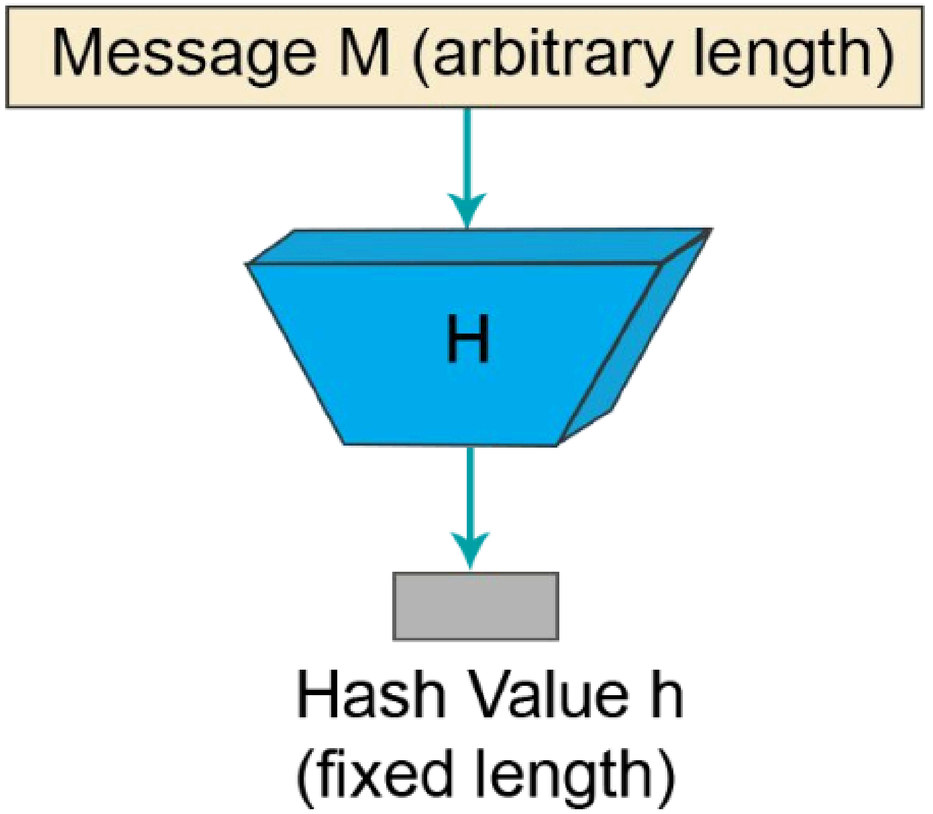
BODY



HASH

- Mathematical Function
- One-way function
- Collision resistance
- Avalanche effect

  Eg:- SHA256



Hash demo

HASH Example

KBA

SHA 256

Input

from: person1

to: person2

amount: 5000

Hash

A1BA93299F5836B8A58543CAD52B8818F0C95F12991635609B0F7CAAF6388A58

HASH Example

KBA

SHA 256

Input

from: person1

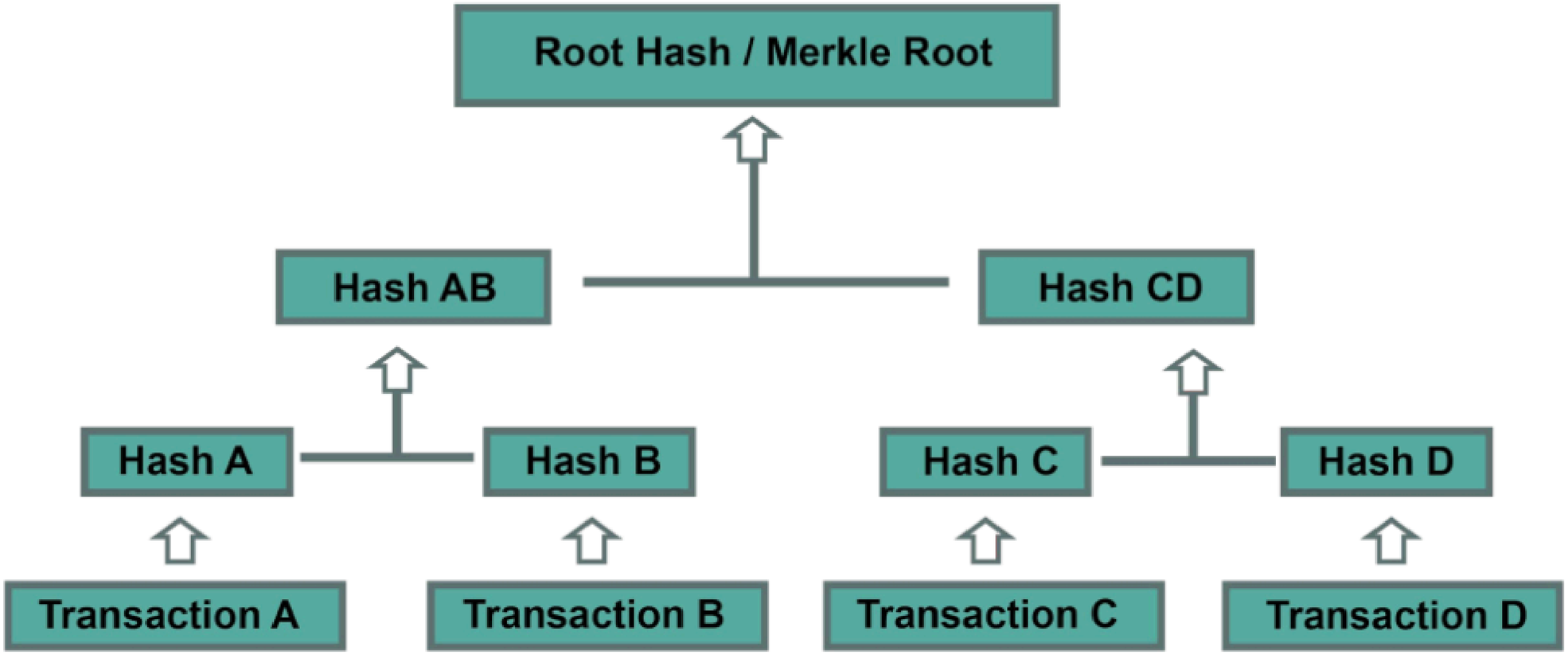
to: person2

amount: 5001

Hash

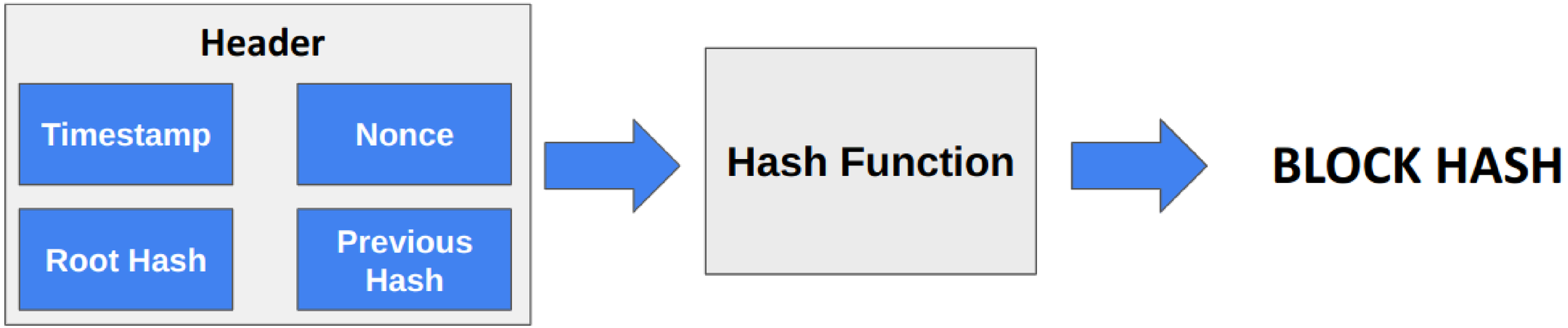
C677256A3CD1F73CD4476204BCA19050E0A11AB11FAEBF14CD7B37FB696F73C5

MERKLE TREE

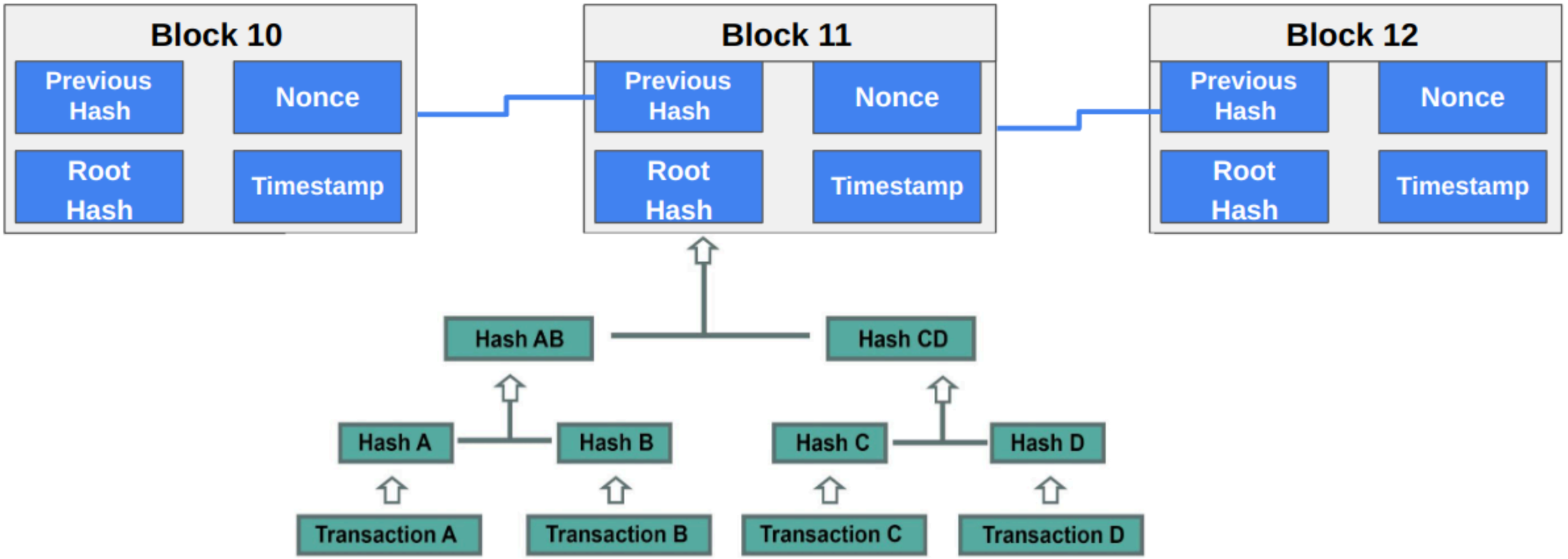


Read more about **Merkle tree**

BLOCK HASH


Header
Timestamp
Nonce
Root Hash
Previous Hash
Hash Function
BLOCK HASH

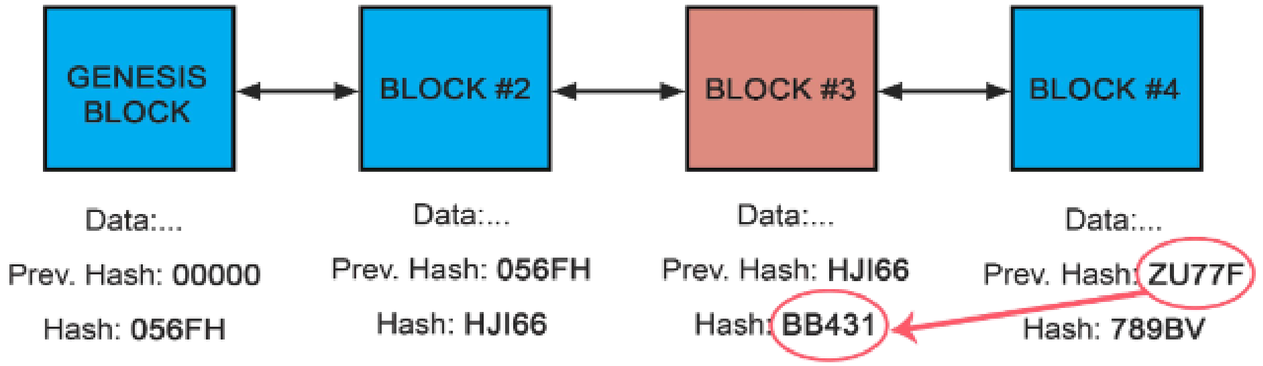
BLOCKCHAIN


Block 10
Previous Hash
Nonce
Root Hash
Timestamp
Block 11
Previous Hash
Nonce
Root Hash
Timestamp
Block 12
Previous Hash
Nonce
Root Hash
Timestamp
Hash AB
Hash CD
Hash A
Hash B
Hash C
Hash D
Transaction A
Transaction B
Transaction C
Transaction D

TAMPER PROOF

K B A

- Each block in the chain contains transaction data.
- Is cryptographically hashed.
- The blocks of hashed data draw upon the previous block in the chain
- This ensures all data in the overall "blockchain" has not been tampered with and remains unchanged.



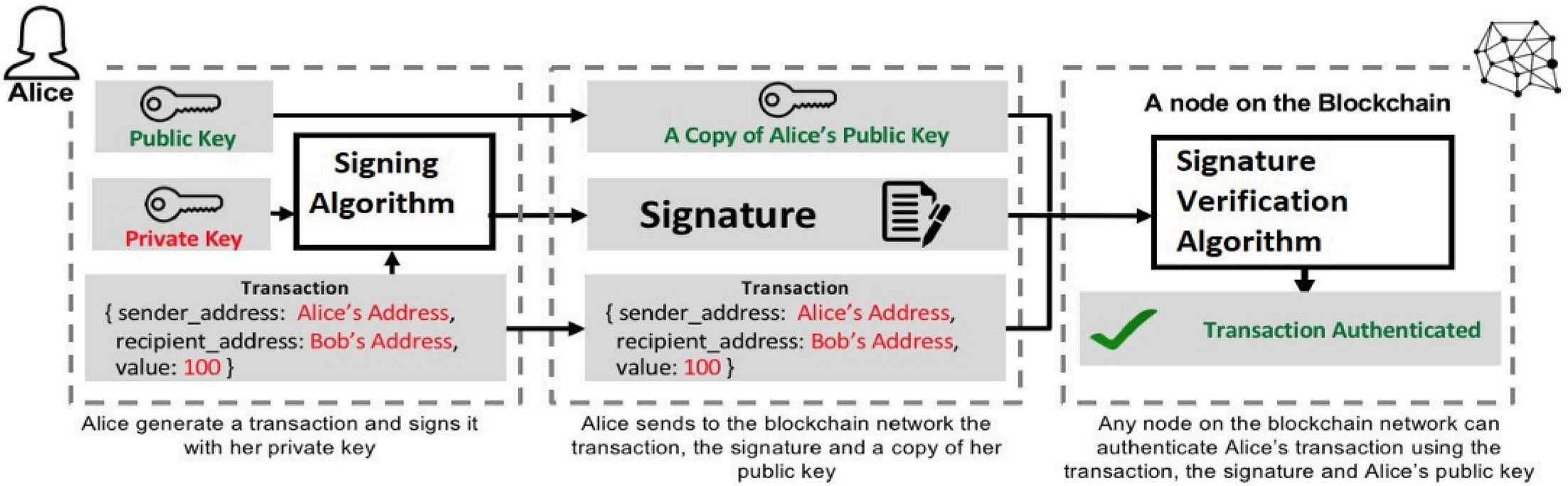
ENTERING THE BLOCKCHAIN NETWORK

BITCOIN ADDRESS

KBA

Satoshi Nakamoto Bitcoin Address

AUTHENTICATION OF A TRANSACTION



Authentication Process for Transactions on the Blockchain

source:http://adilmoujahid.com/posts/2018/03/intro-blockchain-bitcoin-python/

KBA

UTXO

UNSPENT TRANSACTION OUTPUT

UTXO

KBA

Different denomination of rupee

UTXO

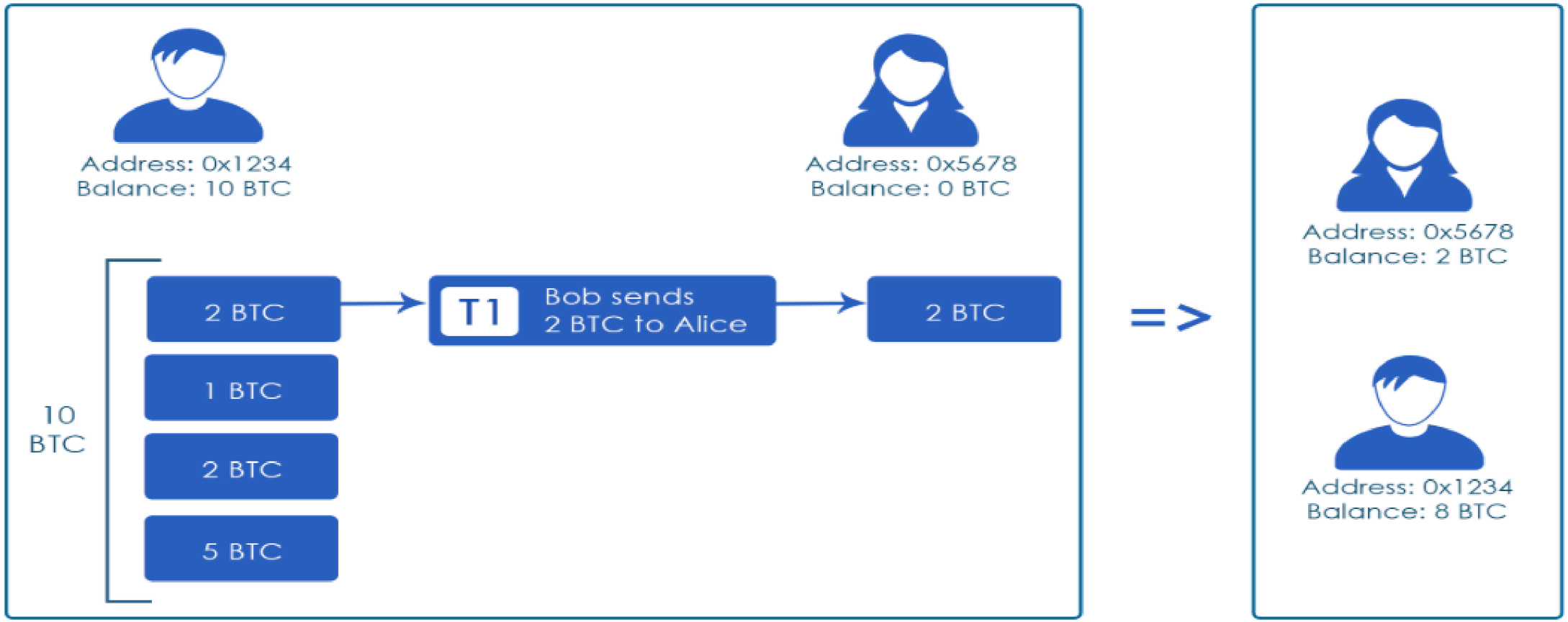
KBA

2 ₿ 2 ₿ 1 ₿ 5 ₿ 3 ₿

Inside the Bitcoin Wallet

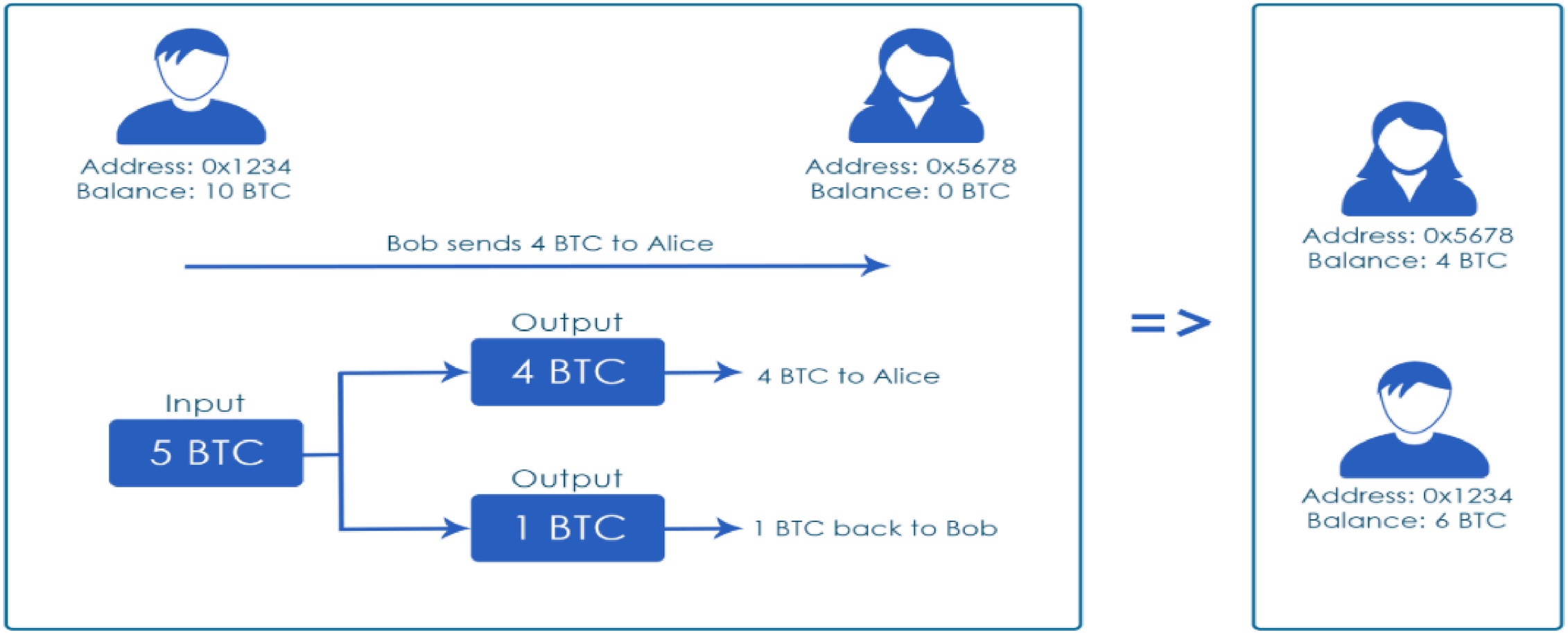
UTXO

KBA


Address: 0x1234
Balance: 10 BTC
Address: 0x5678
Balance: 0 BTC
10 BTC
2 BTC
1 BTC
2 BTC
5 BTC
T1
Bob sends
2 BTC to Alice
2 BTC
=>
Address: 0x5678
Balance: 2 BTC
Address: 0x1234
Balance: 8 BTC

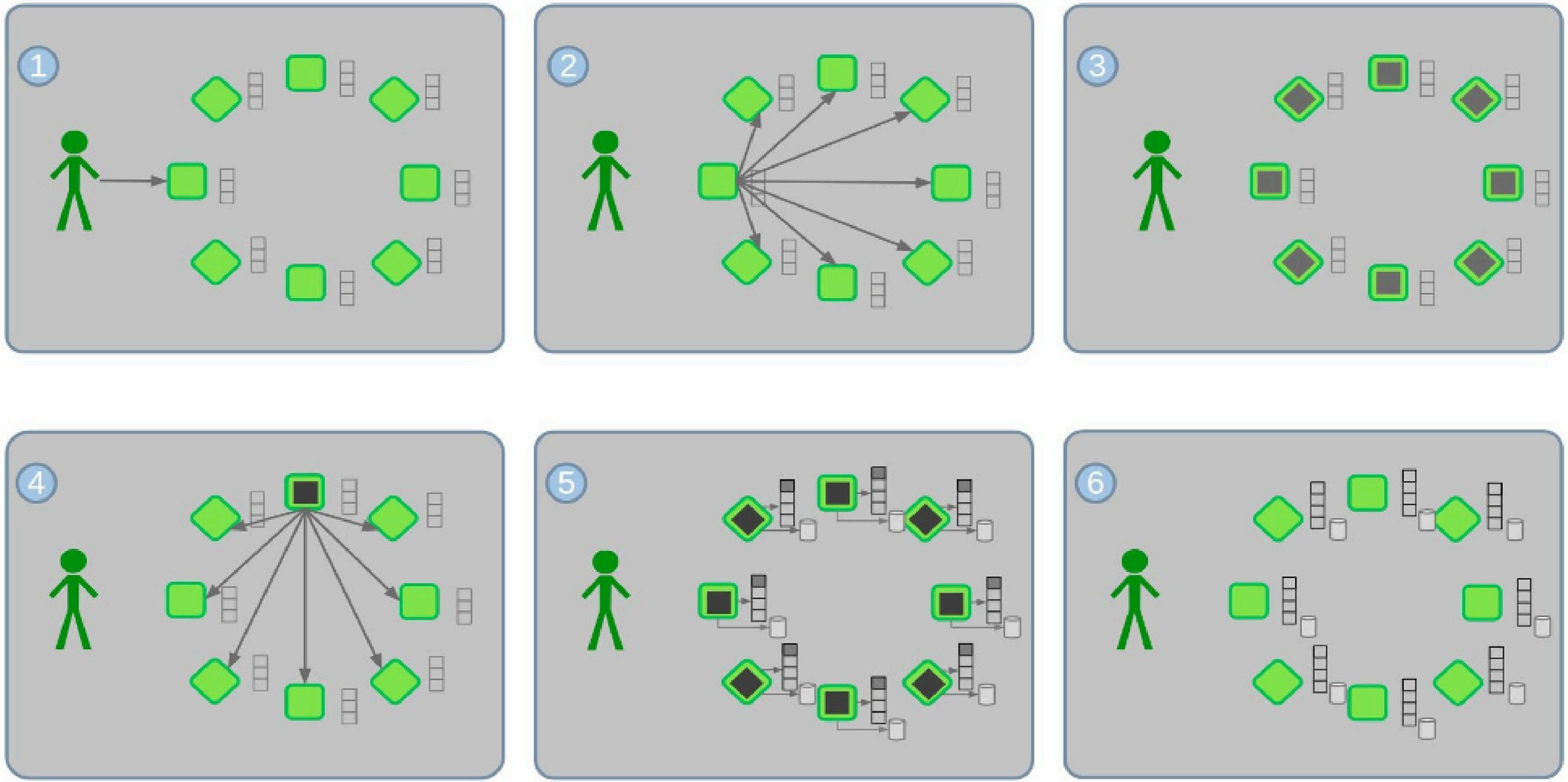
UTXO

KBA


Address: 0x1234
Balance: 10 BTC
Address: 0x5678
Balance: 0 BTC
Bob sends 4 BTC to Alice
Output
4 BTC
4 BTC to Alice
Input
5 BTC
Output
1 BTC
1 BTC back to Bob
=>
Address: 0x5678
Balance: 4 BTC
Address: 0x1234
Balance: 6 BTC

TRANSACTION FLOW

KBA



CONSENSUS

Dictionary

Search for a word

consensus

/kənˈsɛnsəs/

noun

a general agreement.
"there is a growing consensus that the current regime has failed"

Similar: agreement harmony concord like-mindedness concurrence

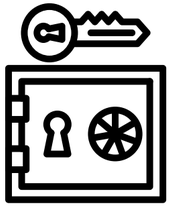
Translations, word origin and more definitions

Definitions from Oxford Languages

Feedback

Different Consensus Algorithms

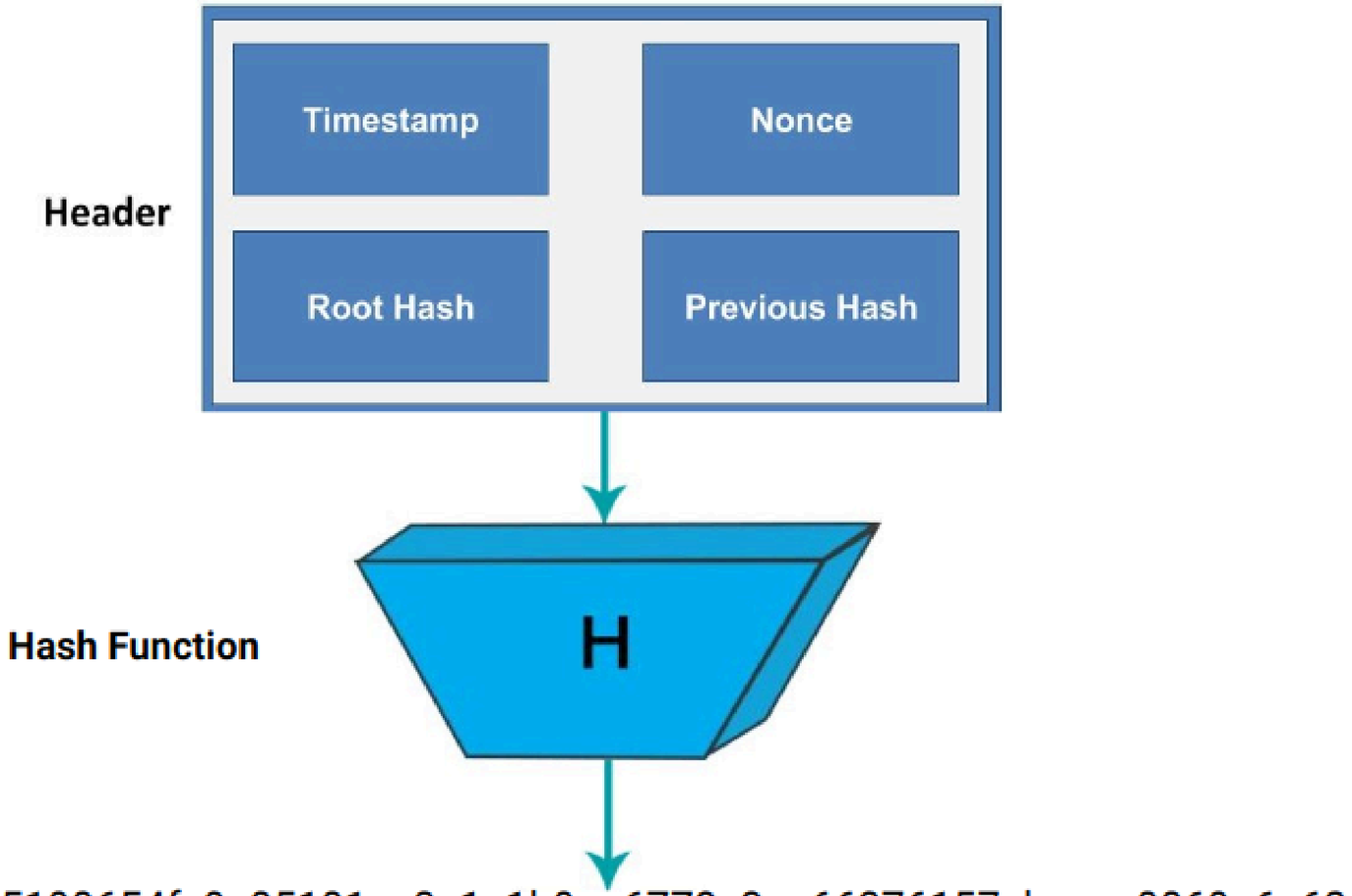
KBA

- Proof of Work (PoW) 
- Proof of Stake (PoS) 
- Proof of Authority (PoA) 
- Raft
- Practical Byzantine Fault Tolerant (pBFT)

Proof of Work

- Transactions are bundled together into a block
- Miners verify that transactions within each block are legitimate
- Solves a mathematical puzzle
- A reward is given to the first miner who solves the puzzle
- Verified transactions are stored in the public blockchain

PUZZLE


Header
Timestamp
Nonce
Root Hash
Previous Hash
Hash Function
H
9740a25190654fc9e85181ec3e1c1b9aa6778e3aa66376157ebccce0869e6e62
Block Hash

Solution

Block Hash*

9740a25190654fc9e85181ec3e1c1b9aa6778e3aa66376157ebccce0869e6e62

compared to

Threshold value*

0000000000000000110119000000000000000000000000000000000000

IF Block Hash > Threshold Increment Nonce value & Repeat hashing

IF Block Hash < Threshold

Result Found

Sample result*

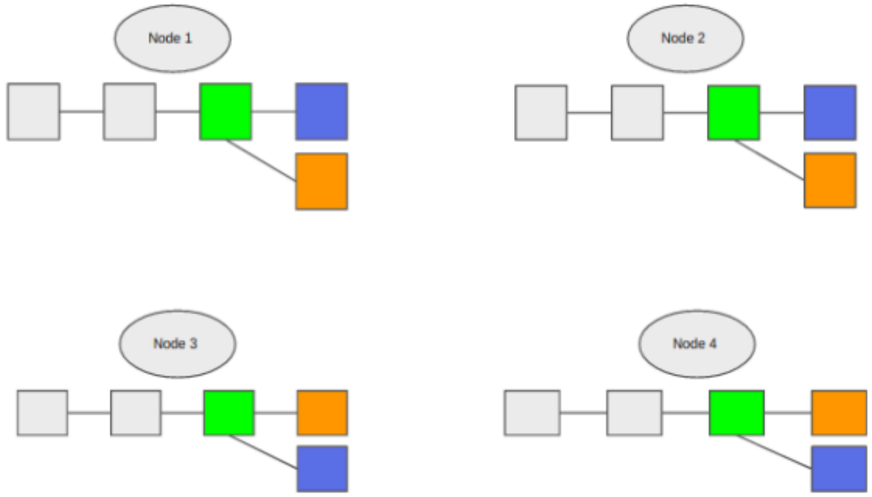
00000000000000000000000000012ae6d18c21690f7fa8faa8a8ce91c78312b6

*All values are for demonstration purpose only

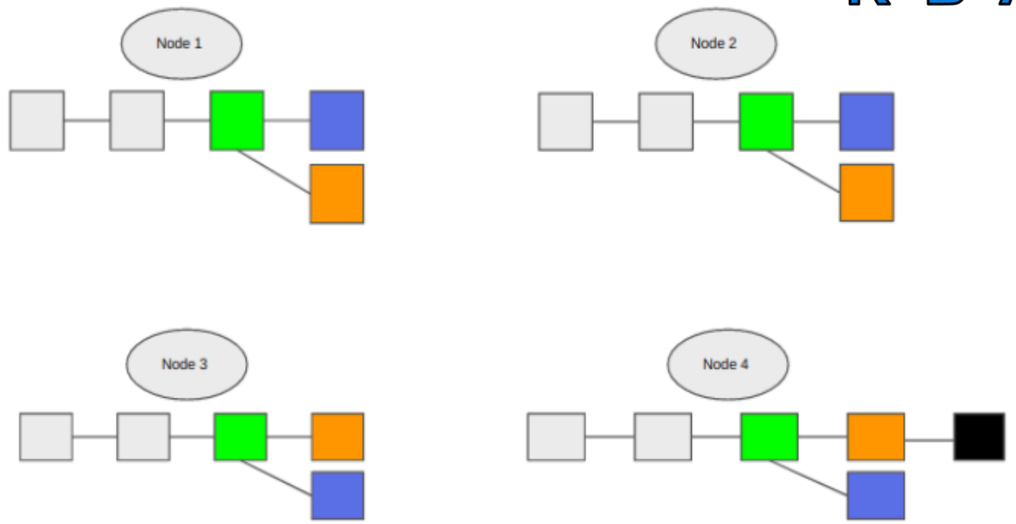
Forks

KBA

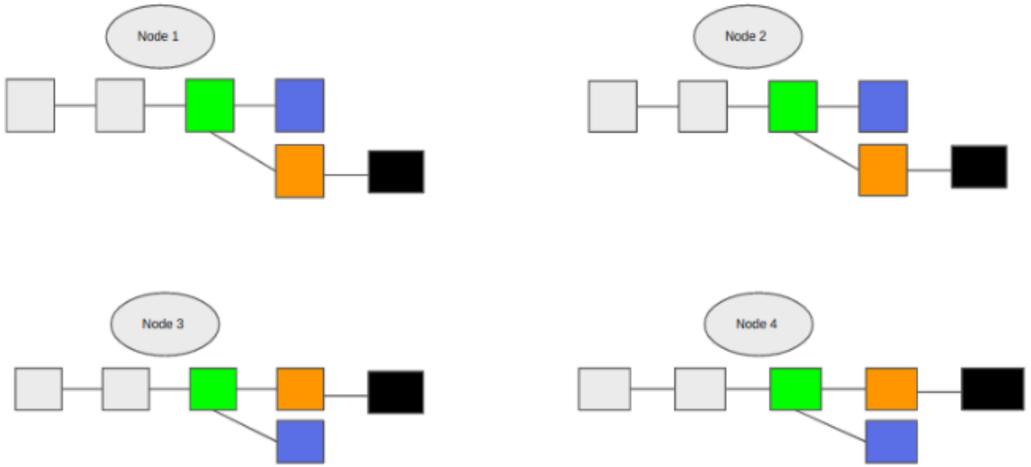
1



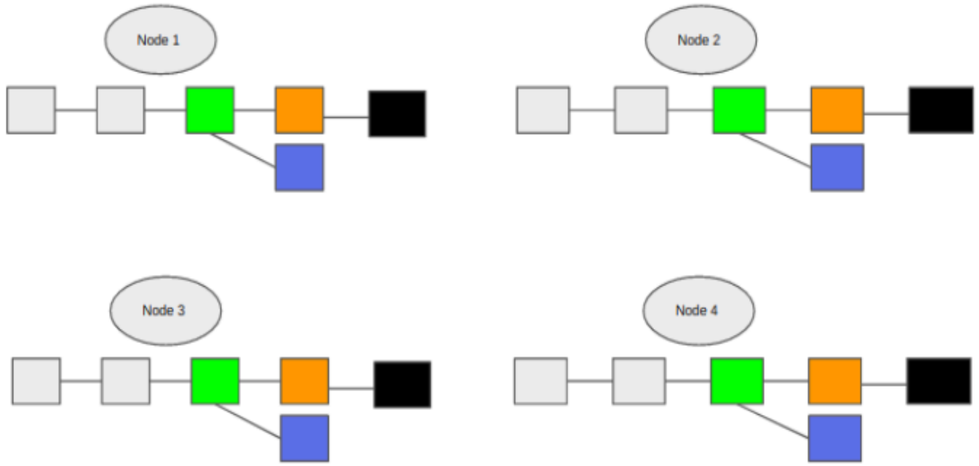
2



3



4



Mining Incentives

KBA

Miners currently receive two types of rewards in return for the security provided by mining:

- **New coins are created with each new block**
- **Transaction fees from all the transactions included in the block**

Miners get reward for mining a block

Currently 3.125 BTC per block

BITCOIN MINED

KBA

19.7 Million

21 Million

93.8 % of BITCOIN MINED

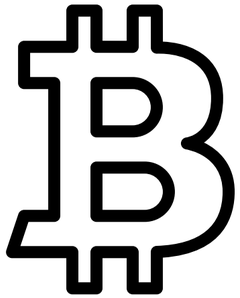
BITCOIN SUPPLY

KBA

Bitcoin Halving

- Every 21,00000 blocks. Bitcoin issuance is “halved”
- 2009-2012: 50 BTC per block
- 2012-2016: 25 BTC per block
- 2016-2020: 12.5 BTC per block
- 2020-2024: 6.25 BTC per block
- 2024-2028: 3.125 BTC per block

Where Bitcoin Fell Short ?



Only meant for bitcoin

Lack of programability

Smart Contract

KBA

" A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract. Smart contracts allow the performance of credible transactions without third parties."

Types of Blockchain

KBA

Public Blockchain

- Anyone can join the network and participate in consensus
- Lottery-based consensus mechanism is used like PoW, PoS
- Eg: Bitcoin and Ethereum

Private Blockchain

- Only a restricted set of users can participate in the network
- Raft, PBFT consensus : Only approved actors participate in consensus
- Eg: Hyperledger Fabric

Hyperledger FABRIC

corda

Why Industry loves Blockchain ?

KBA

TRACEABILITY

ENHANCED SECURITY & AVAILABILITY

AUDITABILITY

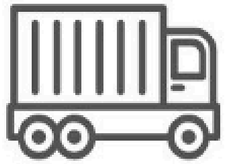
THIRD PARTY ELIMINATION

UNIVERSAL RECORD

Blockchain use cases

DIGITAL IDENTITY

A SELF SOVEREIGN ID CAN BE USED TO VERIFY IDENTITY WITHOUT NEEDING AN INDIVIDUAL TO PRODUCE NUMEROUS DOCUMENTS



SUPPLY CHAIN MANAGEMENT

BLOCKCHAINS ALLOW MULTIPLE PARTIES TO ACCESS A DATABASE TO ACT AS THE SINGLE SOURCE OF TRUTH. RECORDED TRANSACTIONS ARE IMMUTABLE, ARE APPEND ONLY AND PROVIDE A TIME STAMPED AUDIT TRAIL .

HEALTHCARE

USING BLOCKCHAIN TECHNOLOGY TO RECORD PATIENT INFORMATION ON A DISTRIBUTED LEDGER CAN ALLOW DIFFERENT STAKEHOLDERS CONDITIONAL ACCESS TO A SINGLE SOURCE OF TRUTH

REAL ESTATE

BLOCKCHAIN ALLOWS PEOPLE TO TRANSFER FUNDS, PROPERTY TITLES AND DATA IN A MORE PEER-TO-PEER MANNER THAT IS DIGITAL AND OPEN SOURCE

Value/Advantages of Blockchain

KBA

Distributed environment.

Trust-free consensus based transactions

Auditable public ledger system

Trace intruders and attackers.

Any Questions ?