Bitcoin: A Peer-to-Peer Electronic Cash

Dr. Subba Rao Y.V.

School of Computer and Information Sciences

Agenda

- Crypto Preliminaries
- What is Bitcoin?
- Decentralization Challenges
- Double Spending
- The Blockchain
- Block Structure
- Bitcoin Mining
- Transaction Output and Input
- Bitcoin’s script validation
- Top 20 Cryptocurrencies
- Applications

Crypto Preliminaries

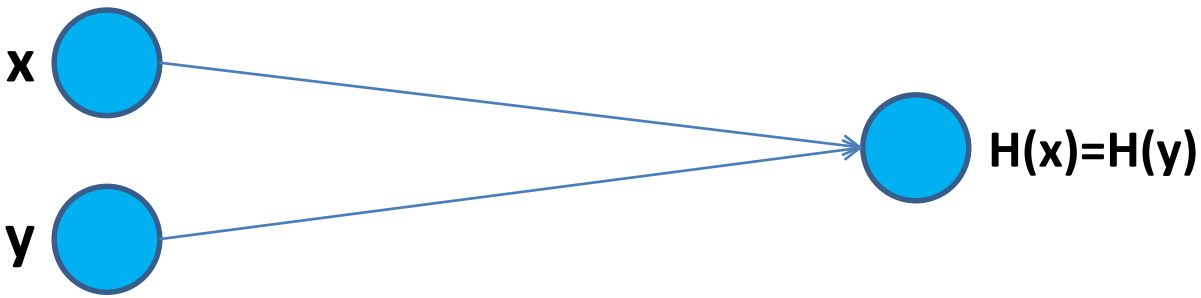
- Cryptographic hash function
- Hash pointers and Data Structures
- Digital Signatures

Cryptographic hash function

- Its input can be any string of any size.
- It produces a fixed-sized output.

$$H: \{0, 1\}^* \dashrightarrow \{0, 1\}^n$$

- **<u>Property 1</u>: Collision Resistance**



- **<u>Property 2</u>: Hiding**

A hash function H is said to be hiding if when a secret value r is chosen using “a probability distribution” that has high min-entropy, then, given

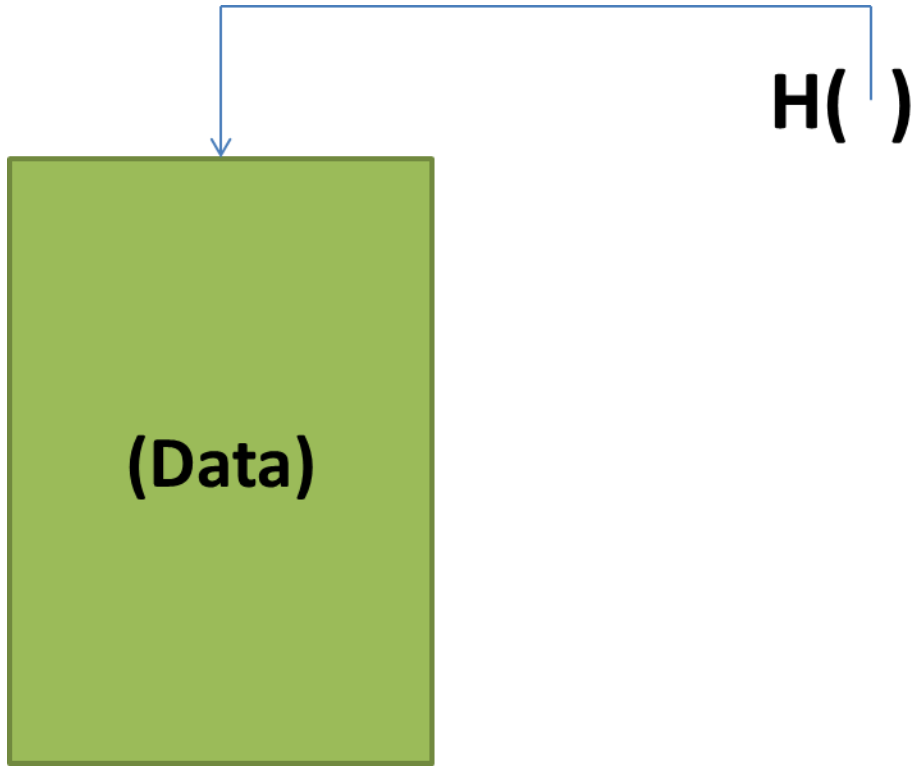
H(r ‖ x), it is infeasible to find x.

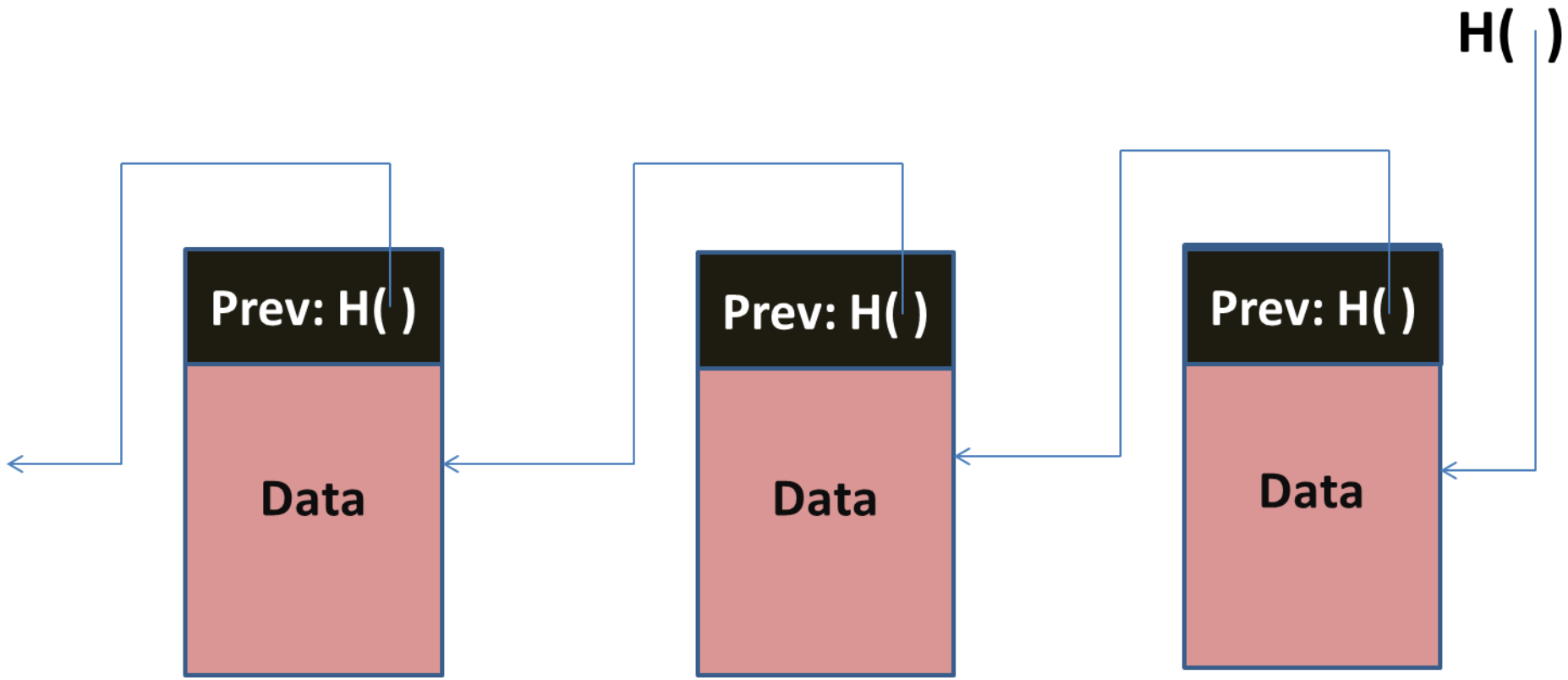
- **<u>Property 3</u>: Puzzle Friendliness**

A hash function H is said to be puzzle friendly if for every possible n-bit output value y, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that,

H(k ‖ x) = y in time significantly less than 2^n.

Hash pointers and Data Structures




H( )
Prev: H( )
Data
Prev: H( )
Data
Prev: H( )
Data

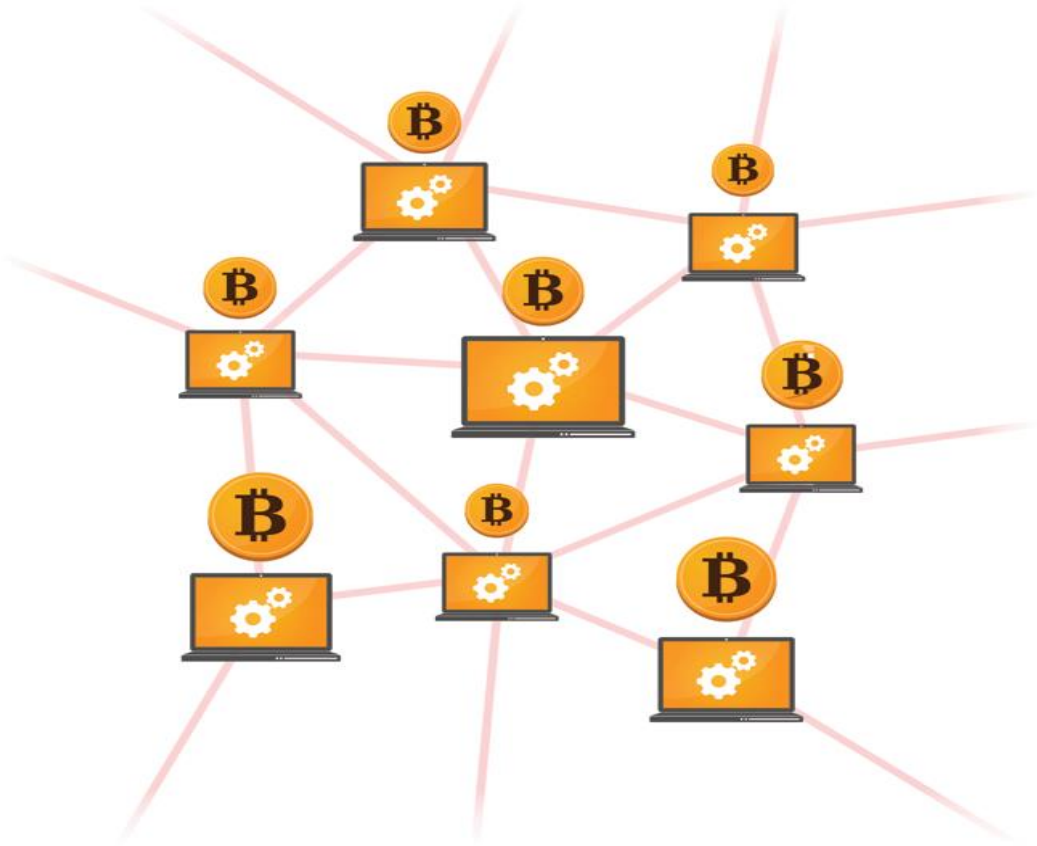
Digital Signatures

- A digital signature scheme consists of the following three algorithms:
  - **(sk, pk) := generateKeys(keysize)**
  - **sig := sign(sk, message)**
  - **isValid := verify(pk, message, sig)**
- We require that the following two properties hold:
  - Valid signatures must verify:

    verify(pk, message, sign(sk, message)) == true.
  - Signatures are existentially unforgeable.

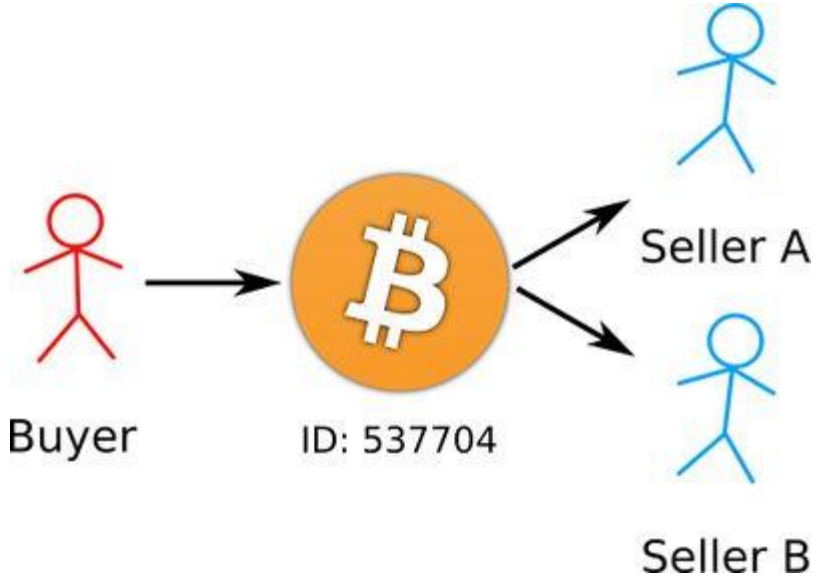
What is Bitcoin?

- Cryptocurrency
- Open source
- Decentralized network



Decentralization Challenges

- Counterfeiting
- Currency creation rules
- Double spending
  - Alice pays Bob n digicoins for a cake
  - Alice uses the **same** n digicoins to pay Charlie for a book



Solution without a central coordinator?

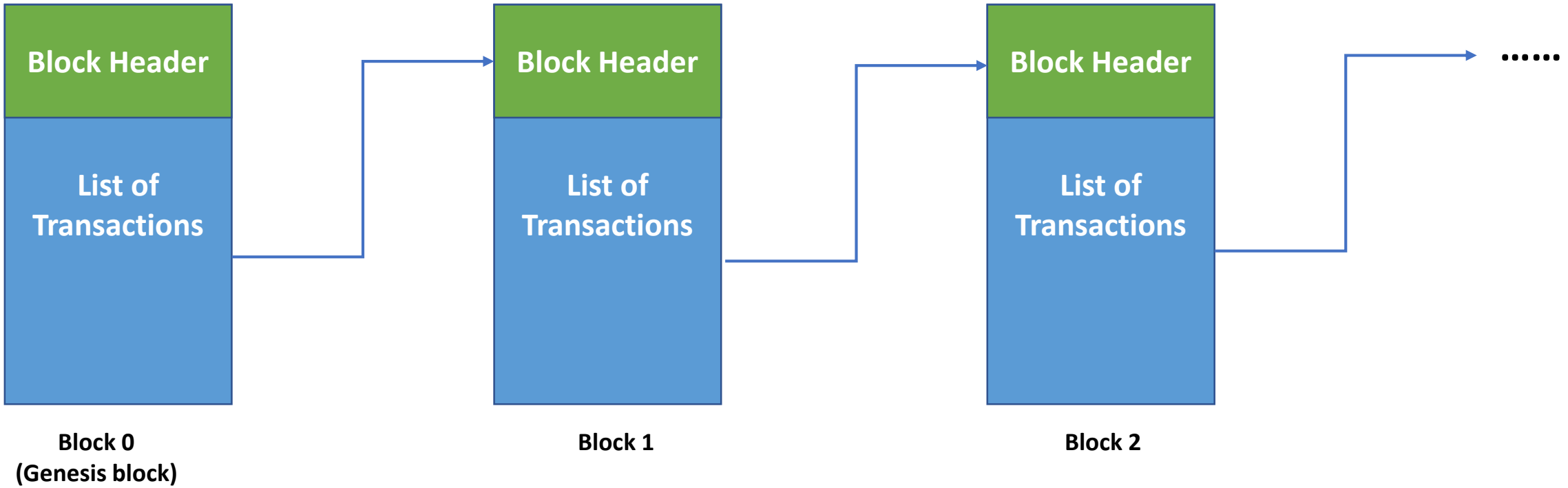
Double Spending

- Familiar to academics
  - Submitting same paper to two conferences
- **Possible solution**
  - Reviewers google paper contents to find duplicates
- Solution fails if
  - Conferences accepting papers at same time
  - Conference proceedings not published/indexed
- **Better solution**

  A single public database to store all submissions to all conferences

The Blockchain

- **Blockchain**: A public database to store all transactions which is replicated by many network nodes



How are the blocks linked?

Block Structure

- The Block contains two parts – **the header** and **the data (the transactions)**
- The header of a block connects the transactions – any change in any transaction will result in a change at the block header
- The headers of subsequent blocks are connected in a **chain – the entire blockchain needs to be updated if you want to make any change anywhere**

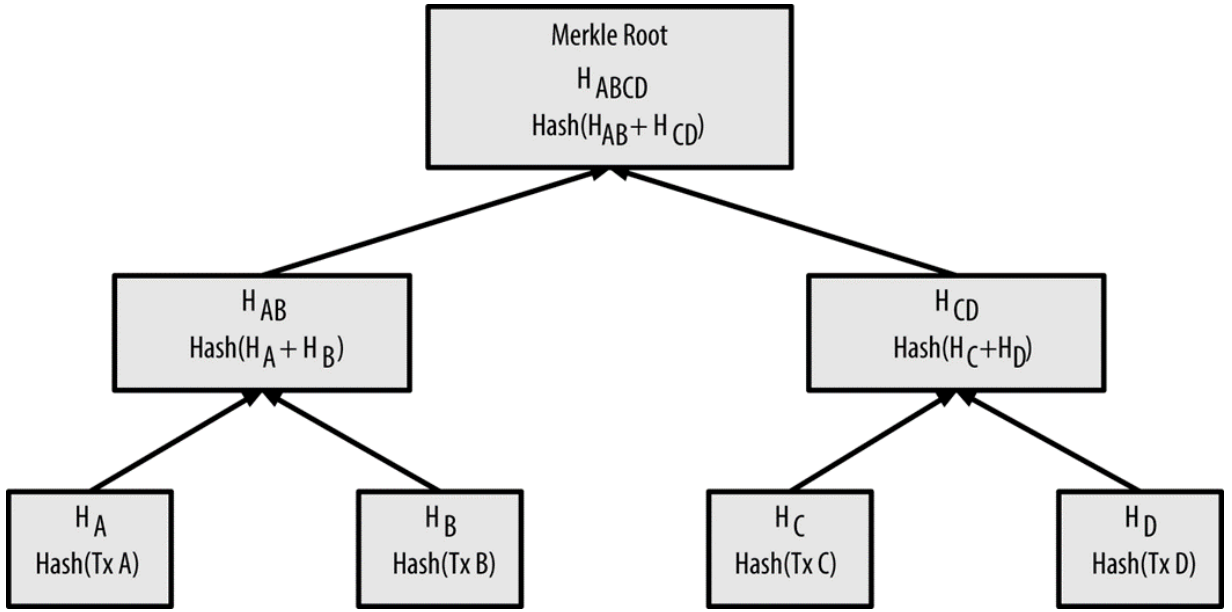
Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following this field
80 bytes	Block Header	Several fields form the block header
1–9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Block Header

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades
32 bytes	Previous Block Hash	A reference to the hash of the previous (parent) block in the chain
32 bytes	Merkle Root	A hash of the root of the merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Merkle Tree

- Transactions are organized as a Merkle Tree. The Merkle Root is used to construct the block hash
- If you change a transaction, you need to change all the subsequent block hash
- The **difficulty** of the mining algorithm determines the **toughness** of tampering with a block in a blockchain



Bitcoin Mining

- Miner who can find Nonce such that

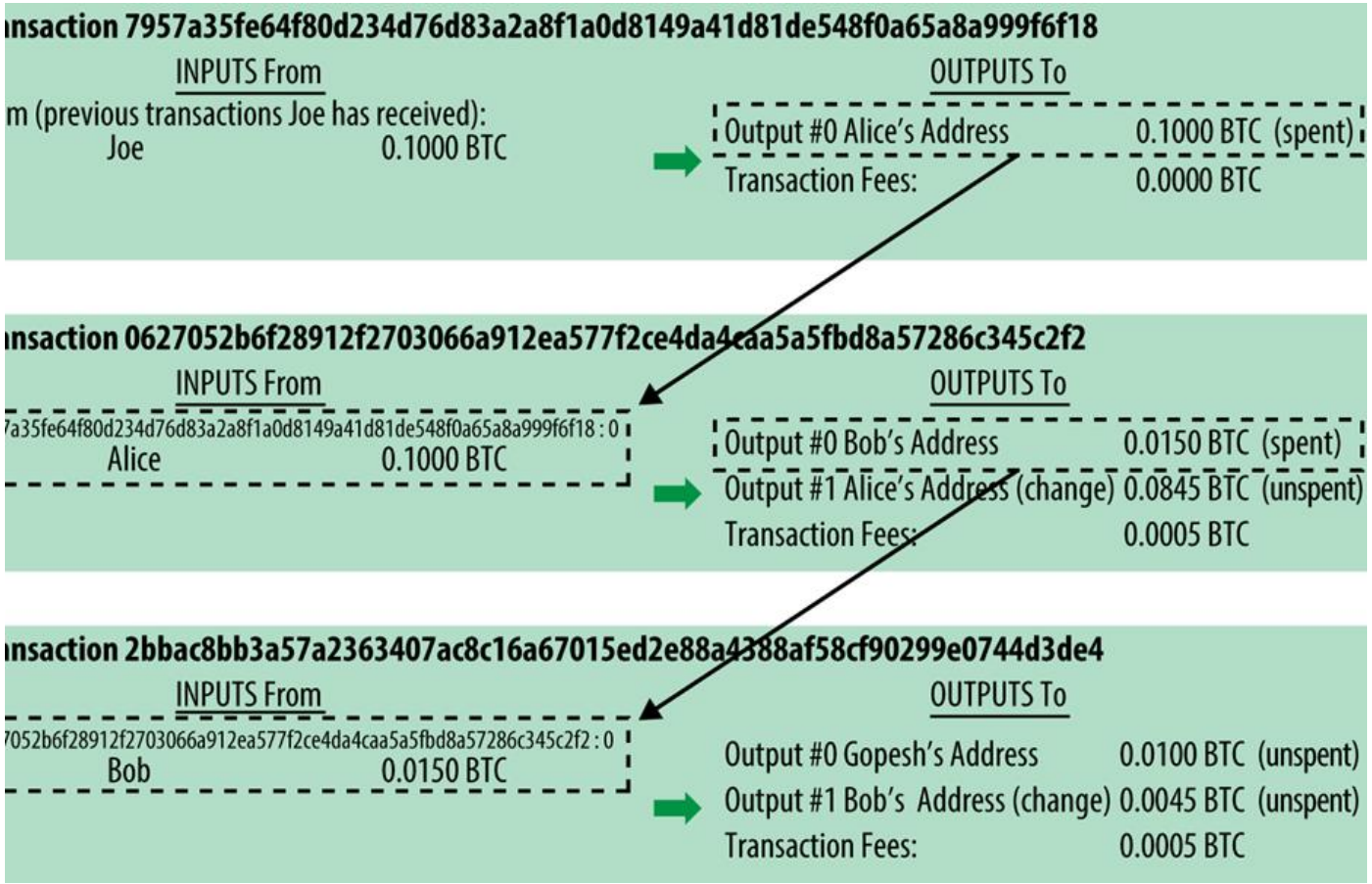
SHA256(SHA256(last_hash|| Tx || nonce))<D

  - Tx :Transactions to be approved
  - D: parameter for difficulty

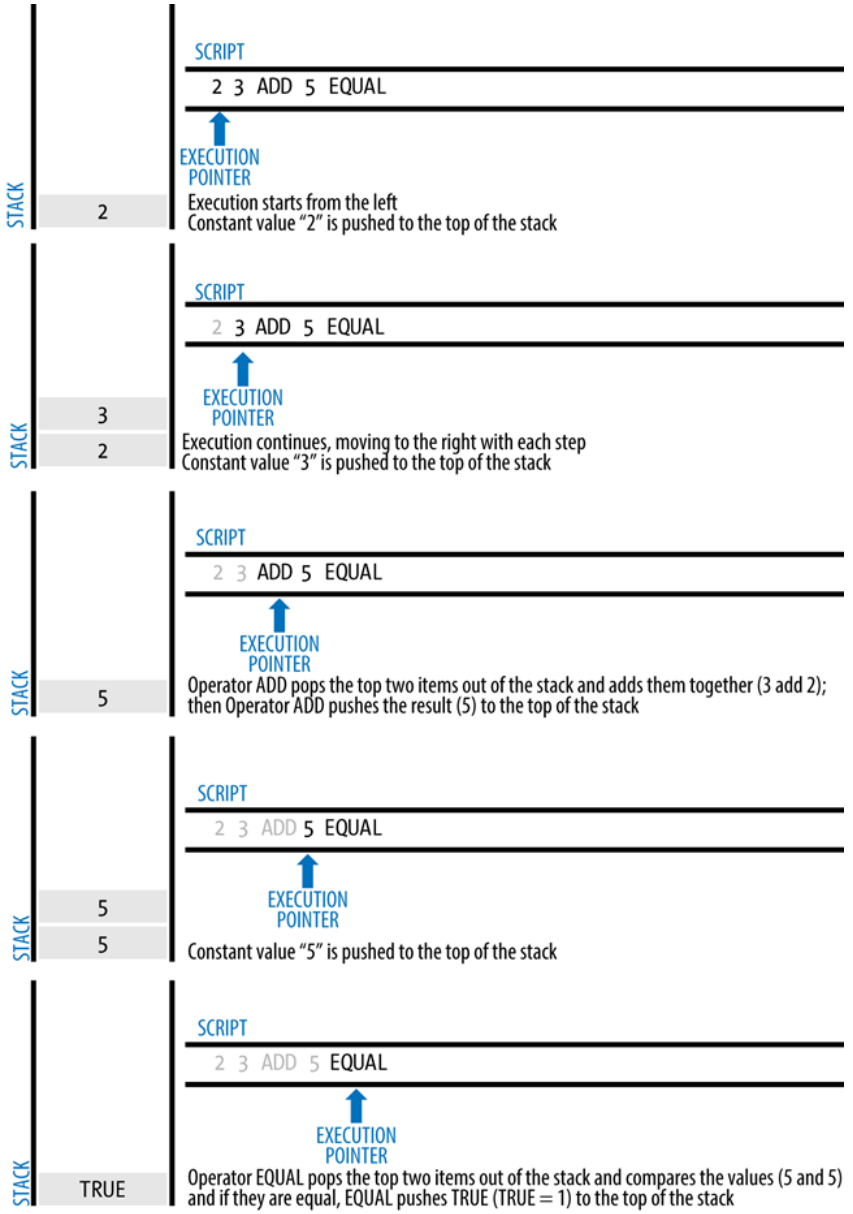
can add a new block

- Modifying any header field will require solving PoW puzzle again

Transaction Output and Input



Bitcoin’s script validation



Transaction Script

- **Locking script form:**

  OP_DUP OP_HASH160 <cafe Public Key Hash> OP_EQUALVERIFY OP_CHECKSIG

- **Unlocking script form:**

  <Cafe Signature> <Cafe Public Key>

- **Evaluating combined script:**

<sig> <Pubk> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG

Top 20 Cryptocurrencies

No.	Name	BC or DAG	Proof of 'X'	Hash Algorithm	Mining Time	ASIC resist.
1	Bitcoin	BC	PoW	SHA-256	10 min	✓
2	Ethereum	BC(DAG)	(PoW,) PoS	Ethash	12 seconds	✓
3	Bitcoin Cash	BC	PoW	SHA-256	10 min	✓
4	Ripple		PoCons	80% majority	-	
5	Litecoin	BC	PoW	Scrypt	2.5 min	✓
6	Dash	BC	PoW	X11 of SHA-3 cand.	5 seconds	✓
7	NEM	BC	PoI	SHA-256	1 min	✓
8	NEO	BC	dBFT	-	20 seconds	
9	Ethereum Classic	BC(DAG)	PoW	Ethash	12 seconds	✓
10	Monero	BC(DAG)	PoW	CryptoNight	-	✓
11	IOTA	DAG "Tangle"	PoW	SHA-3, Kerl	-	✓
12	Qtum	BC	PoS	-	-	✓
13	OmiseGO	BC	PoS	-	-	
14	BitConnect	BC	PoW, PoS	-	-	
15	Zcash	BC	PoW	Equihash	2.5 min	✓
16	ADA	BC	PoS	-	-	
17	Lisk	BC	DPoS	-	-	
18	Tether	BC	PoRes	-	-	
19	EOS	BC	DPoS	-	-	
20	Stellar	BC	PoCons	80% majority	-	

Types of Blockchains

- **Permissionless (Public)**
  - Bitcoin
  - Ethereum
  - Ripple
  - Litecoin etc.
- **Permissioned (Private)**
  - Hyperledger Fabric
  - Hyperledger Sawtooth
  - Hyperledger Composer etc.

Applications

- Internet of Things (IoT)
- Land Registry
- Voting
- Food
- Patient Data Management
- Drug Traceability
- Cross-border transactions
- Digital Identity
- Smart Contracts

References

1. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. Andreas M, Mastering Bitcoin: Programming the Open Blockchain, Second Edition, O'REILLY, 2017
3. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder "Bitcoin and Cryptocurrency Technologies – A Comprehensive Introduction", Princeton University Press, 2016
4. https://www.blockchaintechnologies.com/applications/internet-of-things-iot/

Thank You