Introduction to Bitcoin and Blockchain Technologies

Thomas Sermpinis

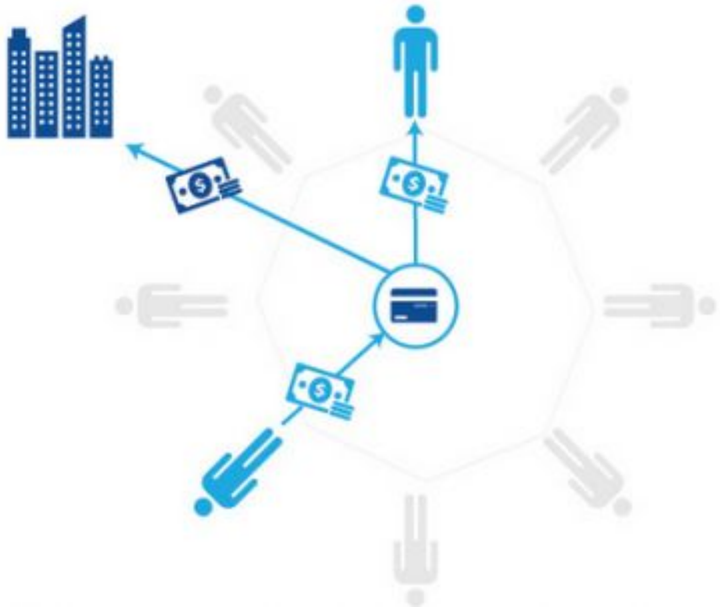
What is Bitcoin?

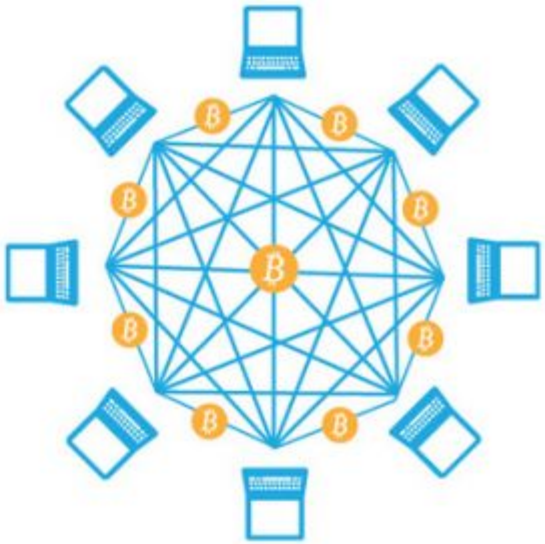
- Collection of concepts and technologies
- Platform of trust
- Basis of a digital money ecosystem
- Distributed, peer-to-peer system
- No “central” server of point of control
- Bitcoin consists of:
    - A decentralized peer-to-peer network (the bitcoin protocol)
    - A public transaction ledger (the blockchain)
    - A set of rules for independent transaction validation and currency issuance (consensus rules)
    - A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)
- “Bitcoin: A Peer-to-Peer Electronic Cash System” - Satoshi Nakamoto, 2008

Why decentralized?

- Transfers have to pass through the bank
- High fees
- Bank controls and creates currency

- No indermediateries
- Direct transfers
- Standard and distributed way of currency

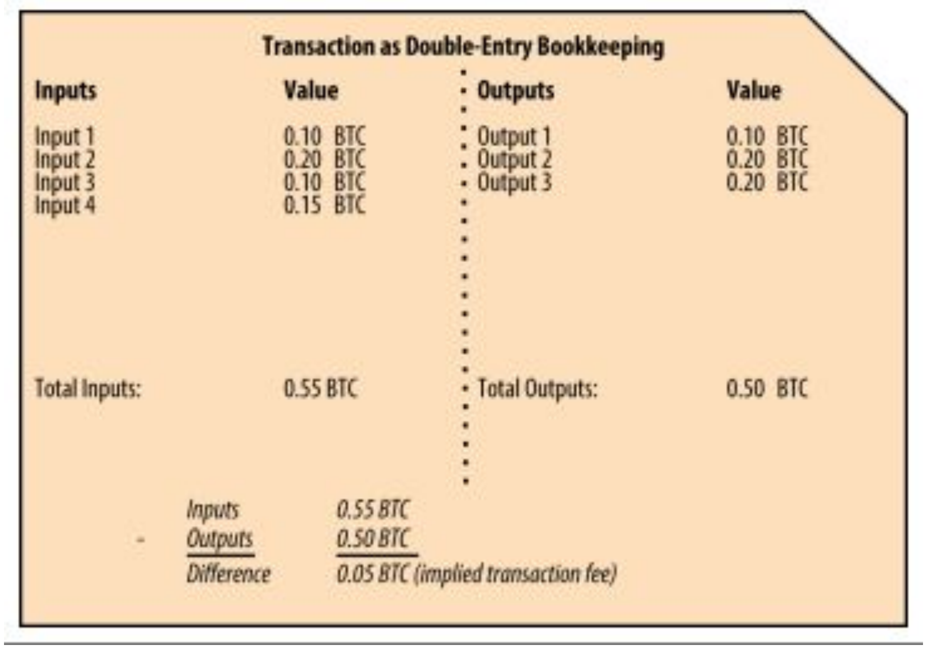




Bitcoin Transactions

- Ownership change
- Lines in a double entry ledger
- One or more “Inputs”
- One or more “Outputs”
- Inputs and outputs do not add up to the same amount
    - Transaction Fees

Bitcoin Transactions

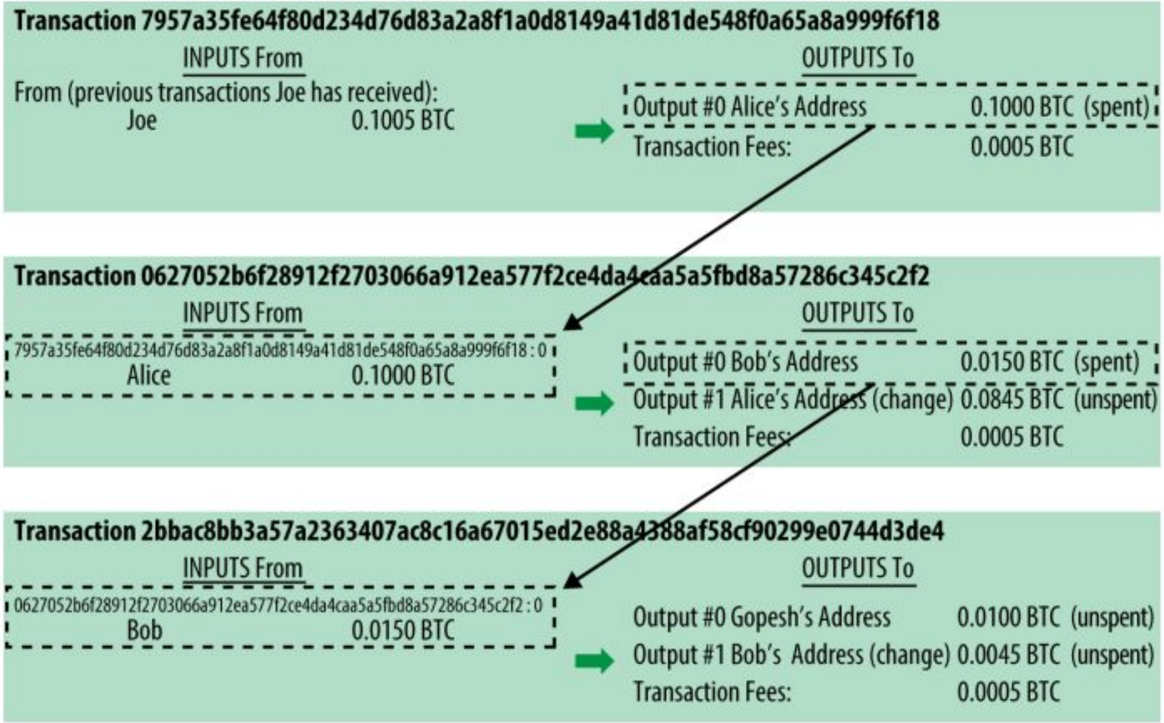


Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Transaction Chain and Change



Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From

From (previous transactions Joe has received):
Joe 0.1005 BTC

OUTPUTS To

Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

INPUTS From

7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC

OUTPUTS To

Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC

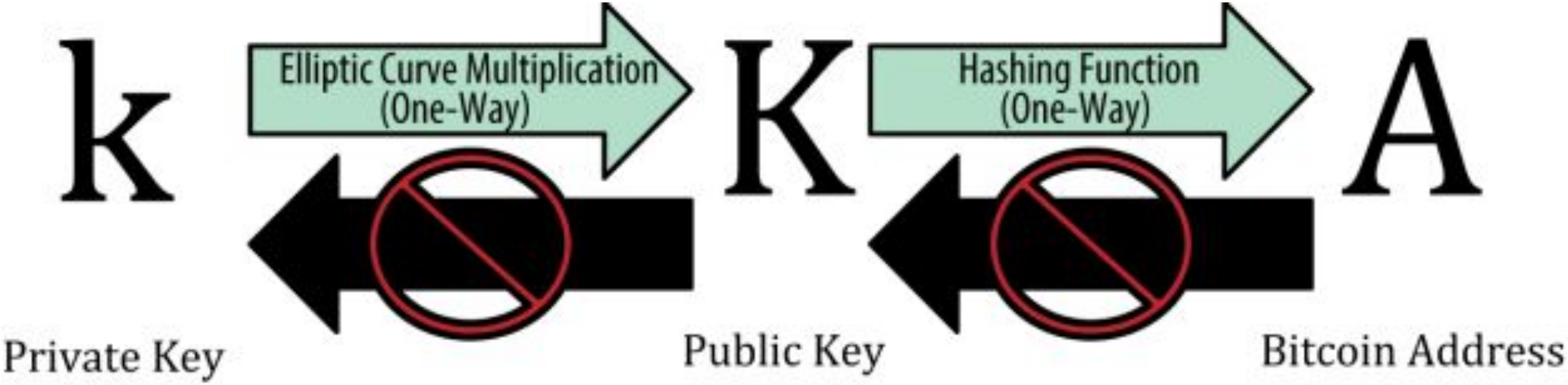
OUTPUTS To

Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0045 BTC (unspent)
Transaction Fees: 0.0005 BTC

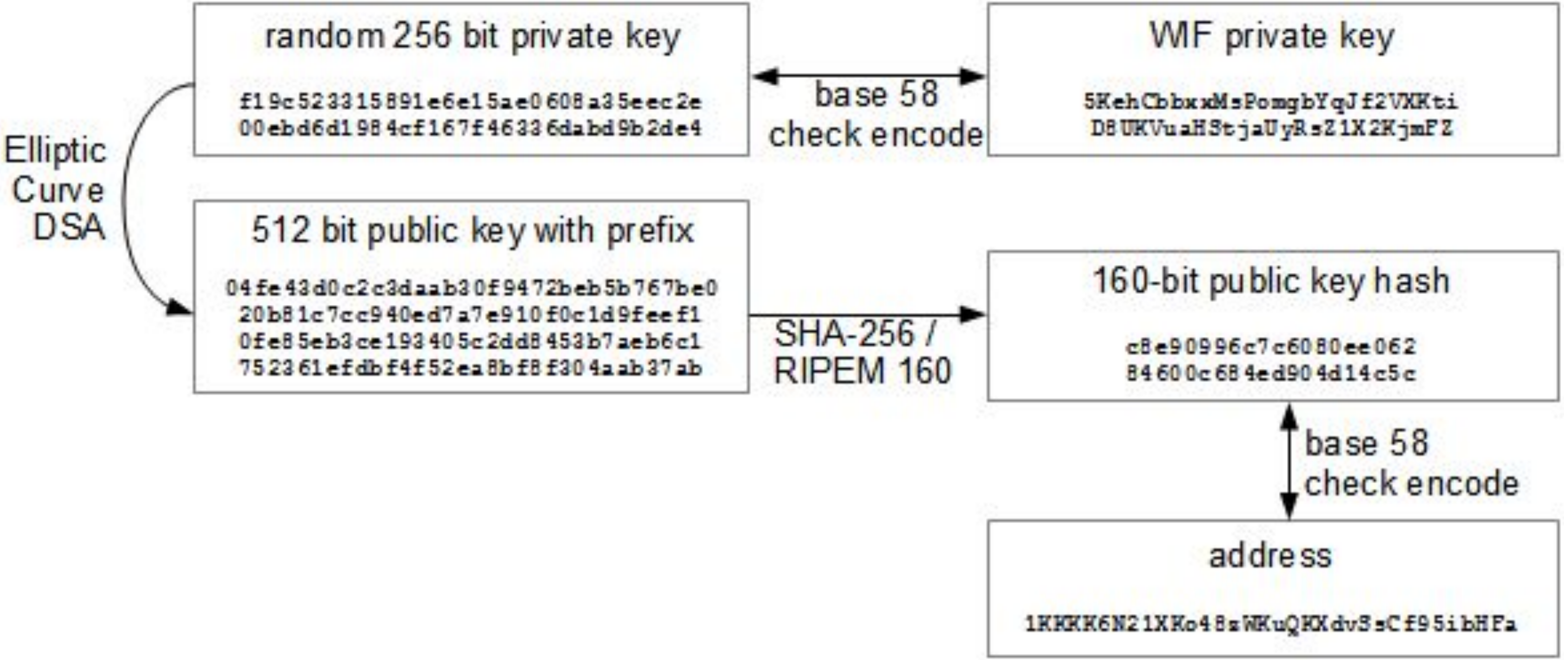
Keys and Addresses

- Private / Public key and address relationship
- Private key: Random 256-bit number
- Public Key: Calculated from private key using Elliptic Curve Multiplication
- "Trap Door" function.
  - secp256k1 standard
- Different key formats
- Bitcoin Address: "Recipient of the funds"
  - Derived from the Public Key
  - SHA256 and RIPEMD160 hash algorithms
  - **A = RIPEMD160(SHA256(K))**
  - Always encoded as "Base58Check"

Keys and Addresses



Keys and Addresses



random 256 bit private key

f19c523315891e6e15ae0608a35eec2e
00ebd6d1984cf167f46336dabd9b2de4

base 58
check encode

WIF private key

5KehCbbxxMsPomgbYqJf2VXKti
D8UKVuaHStjaUyRsZ1X2KjmFZ

Elliptic
Curve
DSA

512 bit public key with prefix

04fe43d0c2c3daab30f9472beb5b767be0
20b81c7cc940ed7a7e910f0c1d9feef1
0fe85eb3ce193405c2dd8453b7aeb6c1
752361efdbf4f52ea8bf8f304aab37ab

SHA-256 /
RIPEM 160

160-bit public key hash

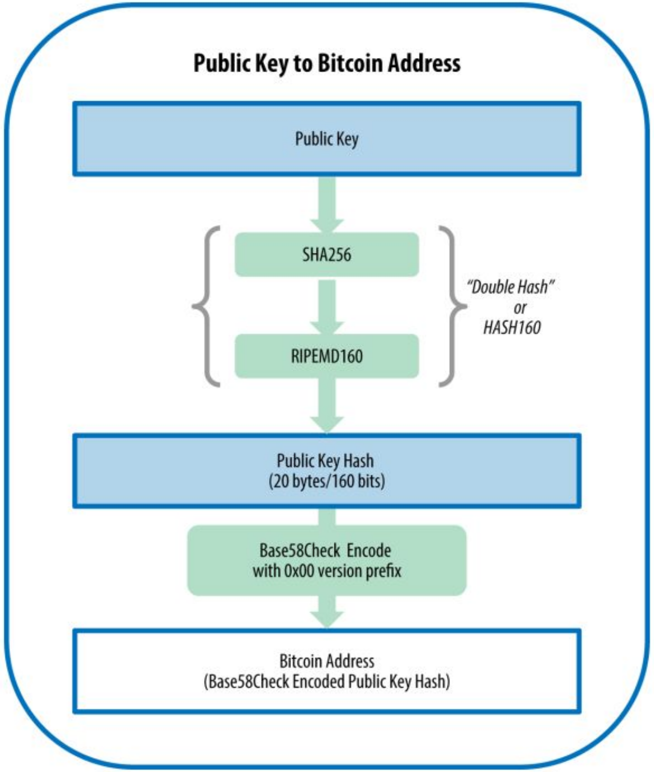
c8e90996c7c6080ee062
84600c684ed904d14c5c

base 58
check encode

address

1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa

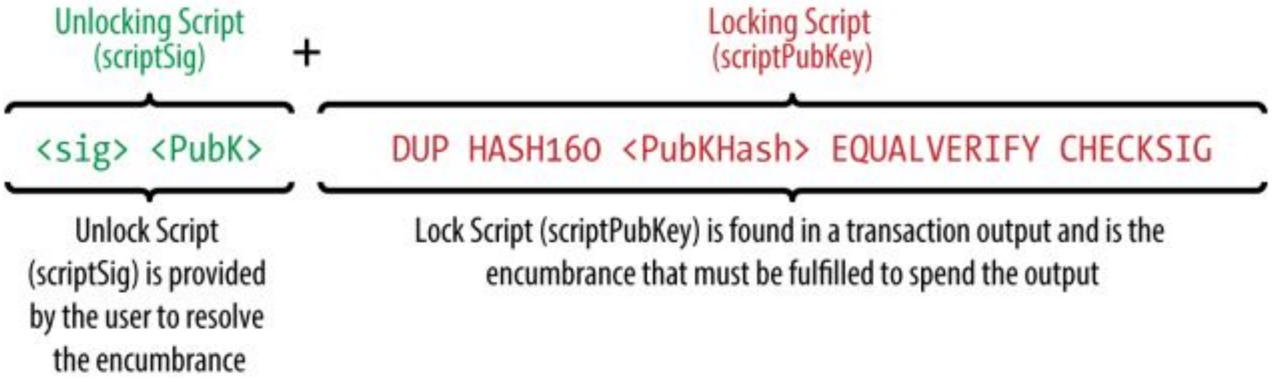
Keys and Addresses



Bitcoin Transactions

- Common Transaction Forms
  - From one address to another
  - Several inputs into a single output
  - One input to several outputs
- Wallet applications manage Inputs and Outputs
  - Offline management capabilities
- UTXO - Unspent Transaction Output
  - An amount of bitcoin, denominated in satoshis
  - A locking script
- Unlocking script is mandatory in order to spent the UTXO

Bitcoin Transactions



```
<sig> <PubK>
```

```
DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
```

Unlock Script (scriptSig) is provided by the user to resolve the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output

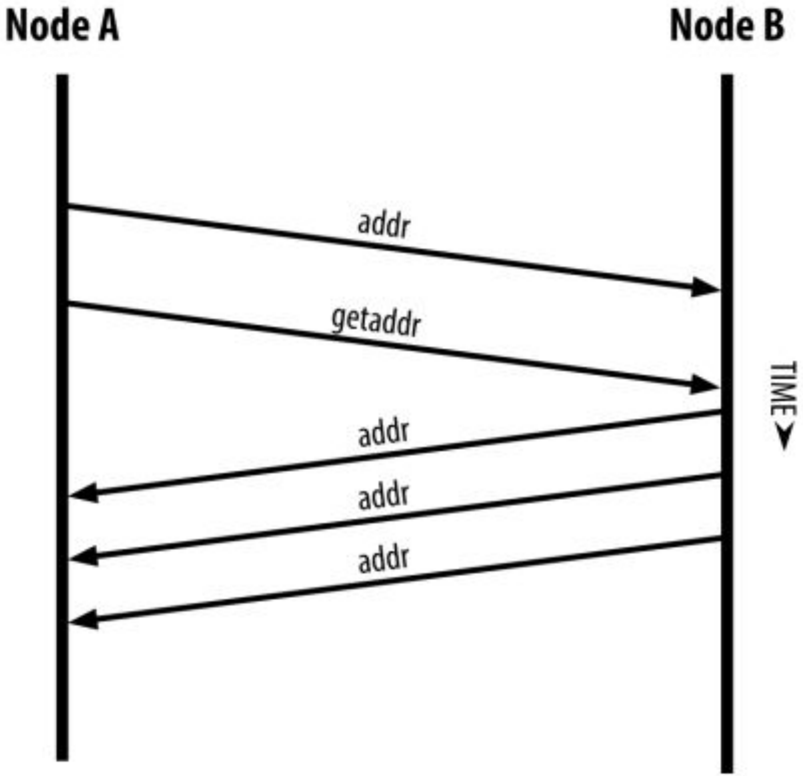
Bitcoin Network and Nodes

- Peer -to-peer architecture on top of Internet
- Collection of nodes that run the Bitcoin P2P protocol
- Bitcoin Node - collection of functions
  - Routing
  - Blockchain database
  - Mining
  - Wallet
- Full nodes have all four functions and keep a complete copy of the blockchain
- Lightweight nodes keel only a subset of the blockchain
  - Transaction verification through the *Simplified Payment Verification* or SPV

Bitcoin Network

- Discovery of other Bitcoin nodes in the network
    - Connect with at least one node in order to start the process
    - Geographic location is irrelevant
    - Random node selection
- DNS query using a number of “DNS Seeds”
    - List of IP addresses of Bitcoin nodes
- Some DNS seeds provide static lists of stable Bitcoin listening nodes
- Alternatively, the new node must be given the IP address of at least one Bitcoin node
- The new node will sent an addr message containing its IP to its neighbors
- The neighbors will forward the addr message

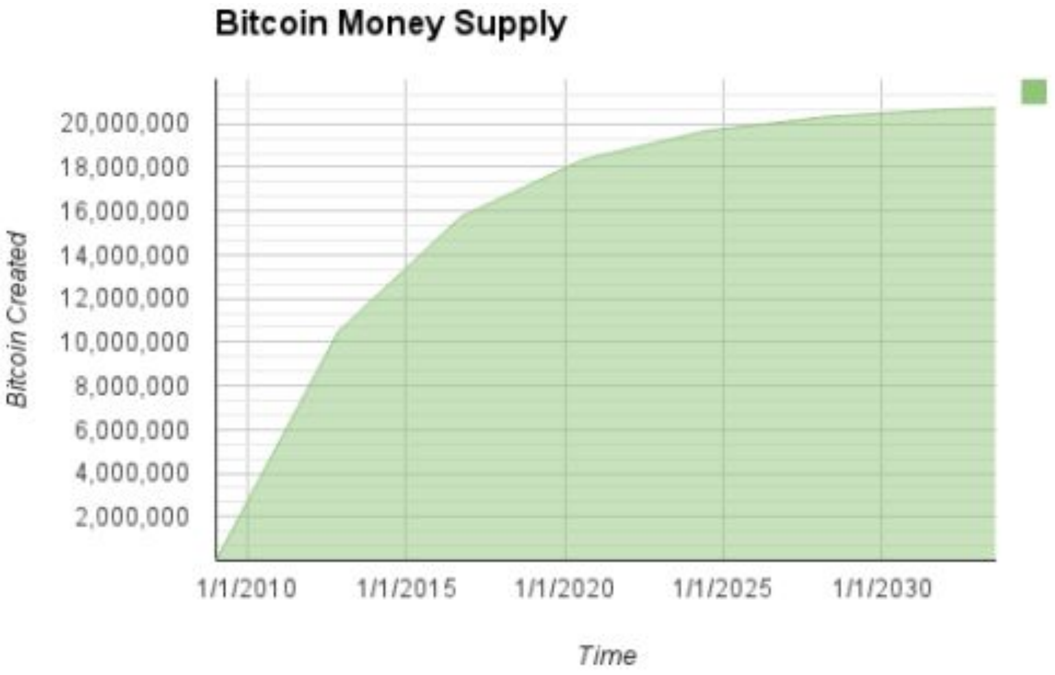
Bitcoin Network



Bitcoin Mining

- Mining nodes secure the bitcoin system
- Decentralized, network-wide consensus
- New transaction validation and record on the blockchain
- New block every 10 minutes
- Mined transactions are considered “confirmed”
- Two types of rewards for miners:
    - New coins created with each new block
    - Transaction fees that result from each block
- Mathematical problem based on a cryptographic hash algorithm solving competition
- The solution is called Proof-of-Work

Bitcoin Mining

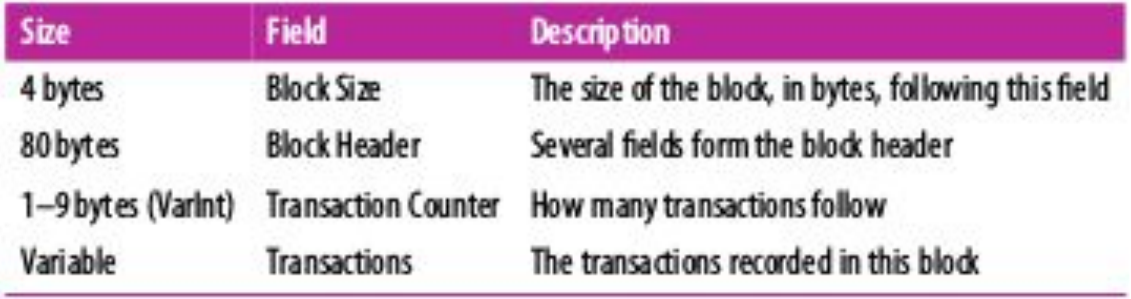


How to get Bitcoins

- Mine Bitcoins
- Buy Bitcoins from an online exchange website
- Buy from other users offline or online
- Sell services for Bitcoins
- Bitcoin ATM

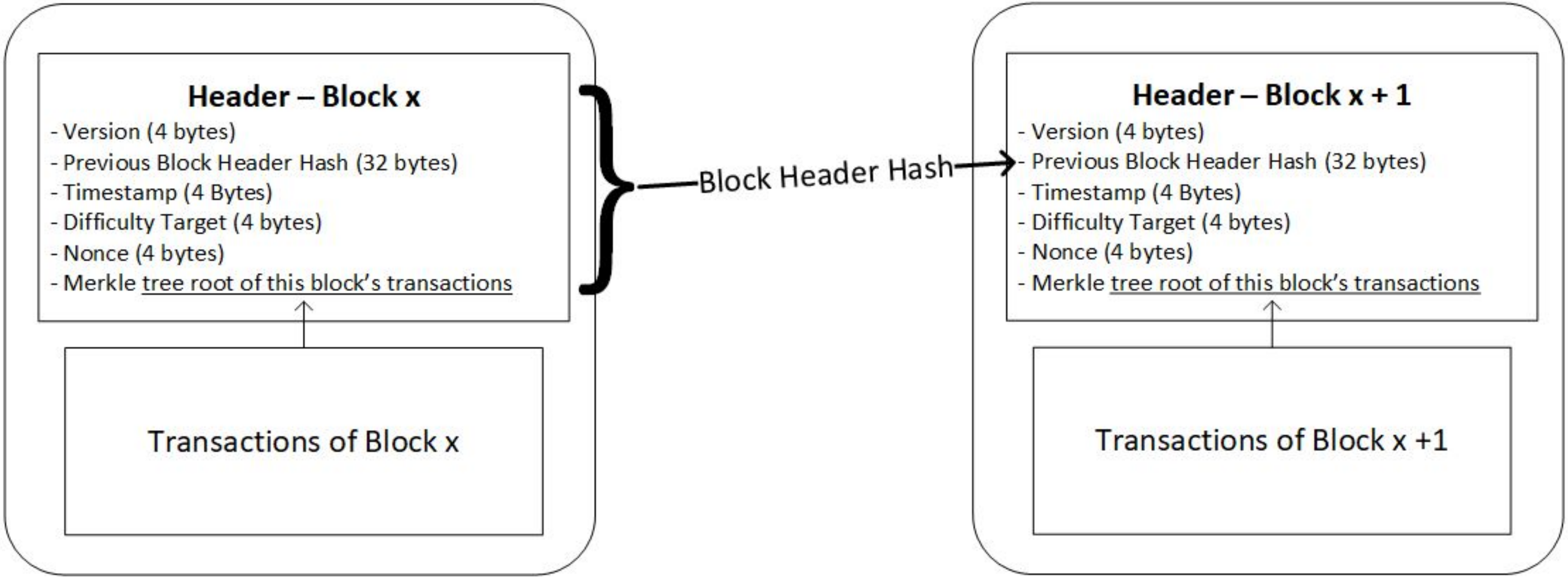
What is Blockchain?

- List of blocks of transactions
- The hash of each block is the way to identify it and it is contained in the header of each block (SHA256)
- Reference to the previous block (parent block)
  - “Previous block hash” also contained in the header
- This sequence creates a chain all the way to the first block (genesis block)



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

What is Blockchain?



Header – Block x

- Version (4 bytes)
- Previous Block Header Hash (32 bytes)
- Timestamp (4 Bytes)
- Difficulty Target (4 bytes)
- Nonce (4 bytes)
- Merkle tree root of this block's transactions

Transactions of Block x

Block Header Hash

Header – Block x + 1

- Version (4 bytes)
- Previous Block Header Hash (32 bytes)
- Timestamp (4 Bytes)
- Difficulty Target (4 bytes)
- Nonce (4 bytes)
- Merkle tree root of this block's transactions

Transactions of Block x +1

Blockchain Characteristics

- Transaction Immutability
- Transaction Transparency
- Pseudo-anonymity
- Consensus based
- Transparent rules on Blockchain and Bitcoin operations

Blockchain Use Cases

- Namecoin - Decentralized DNS
- Ethereum - Smart Contracts
- IPFS, Swarm - Distributed Storage
- uPort - Decentralized Identification
- ICOs - Digital Assets

Questions?

Email:	sermpinis@csd.auth.gr
Web:	http://cr0wsplace.wordpress.com
LinkedIn:	https://www.linkedin.com/in/thomas-sermpinis-0473a4b0/
Twitter:	@serbinhio
YouTube:	https://www.youtube.com/user/Cr0wsPlace