BITCOIN AND BLOCKCHAIN

Robin Ye:

"At this moment, just like in 2000, software development into the Internet age, programmers either continue learning or be weeded out. Now the Internet age is over, welcome to the age of AI and blockchain."

WHAT WE ARE GOING TO TALK ABOUT?

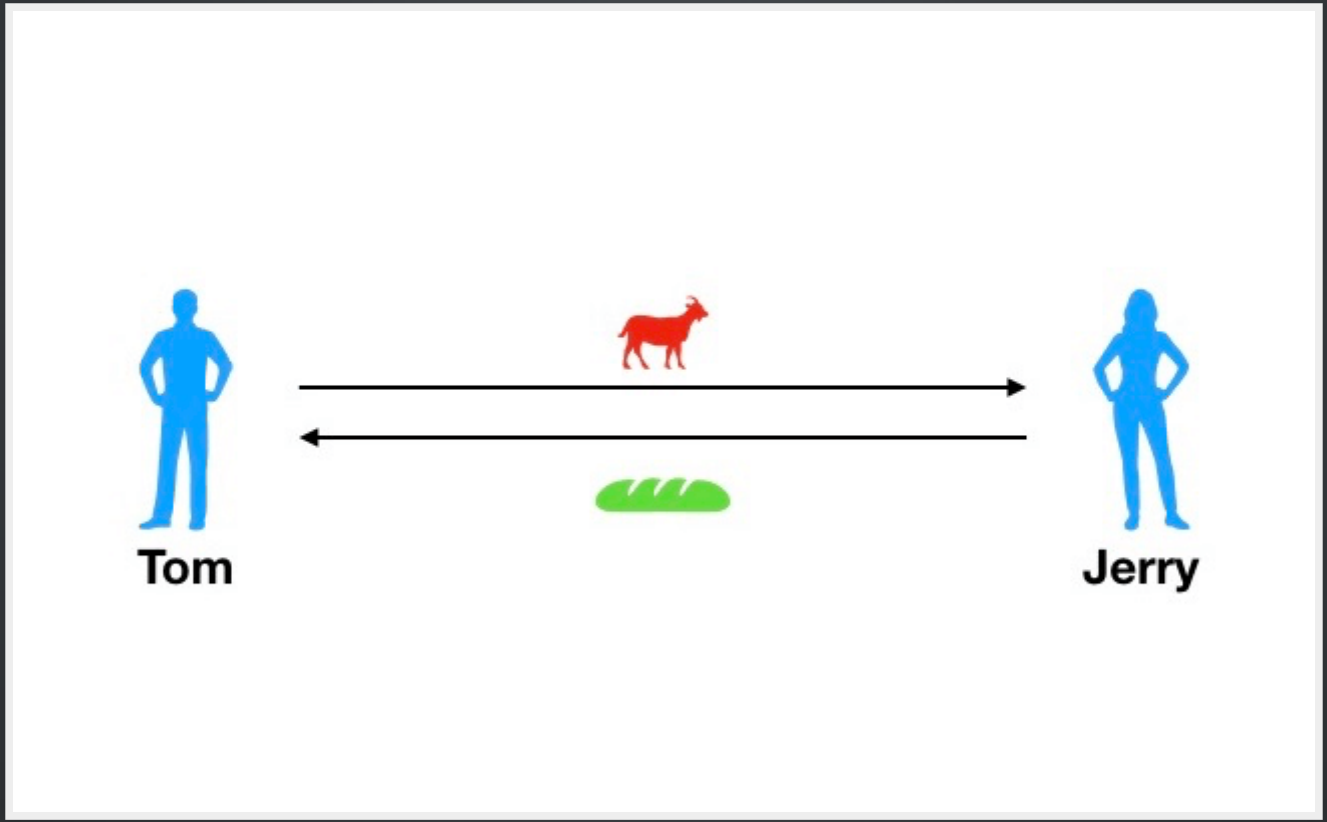
- Evolution of Currency
- What is Bitcoin
- History of Bitcoin
- Transactions
- Blockchain
- Mining and Consensus
- User Security Best Practices
- Blockchain Applications

WHAT WE ARE NOT GOING TO TALK ABOUT?

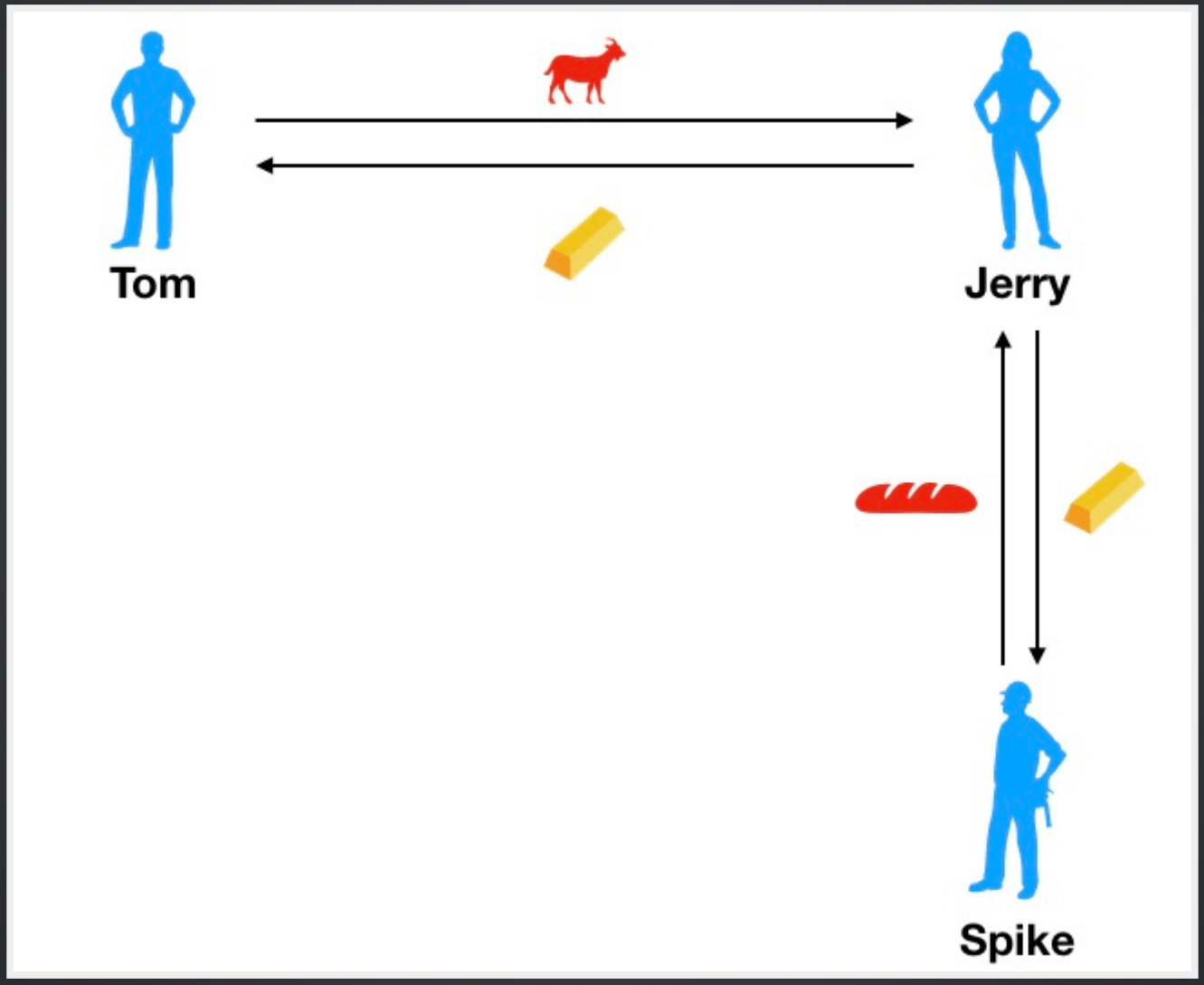
- Alternative Coins
- Ethereum
- Elliptic Curves Cryptography
- Digital Signatures (ECDSA)

EVOLUTION OF CURRENCY

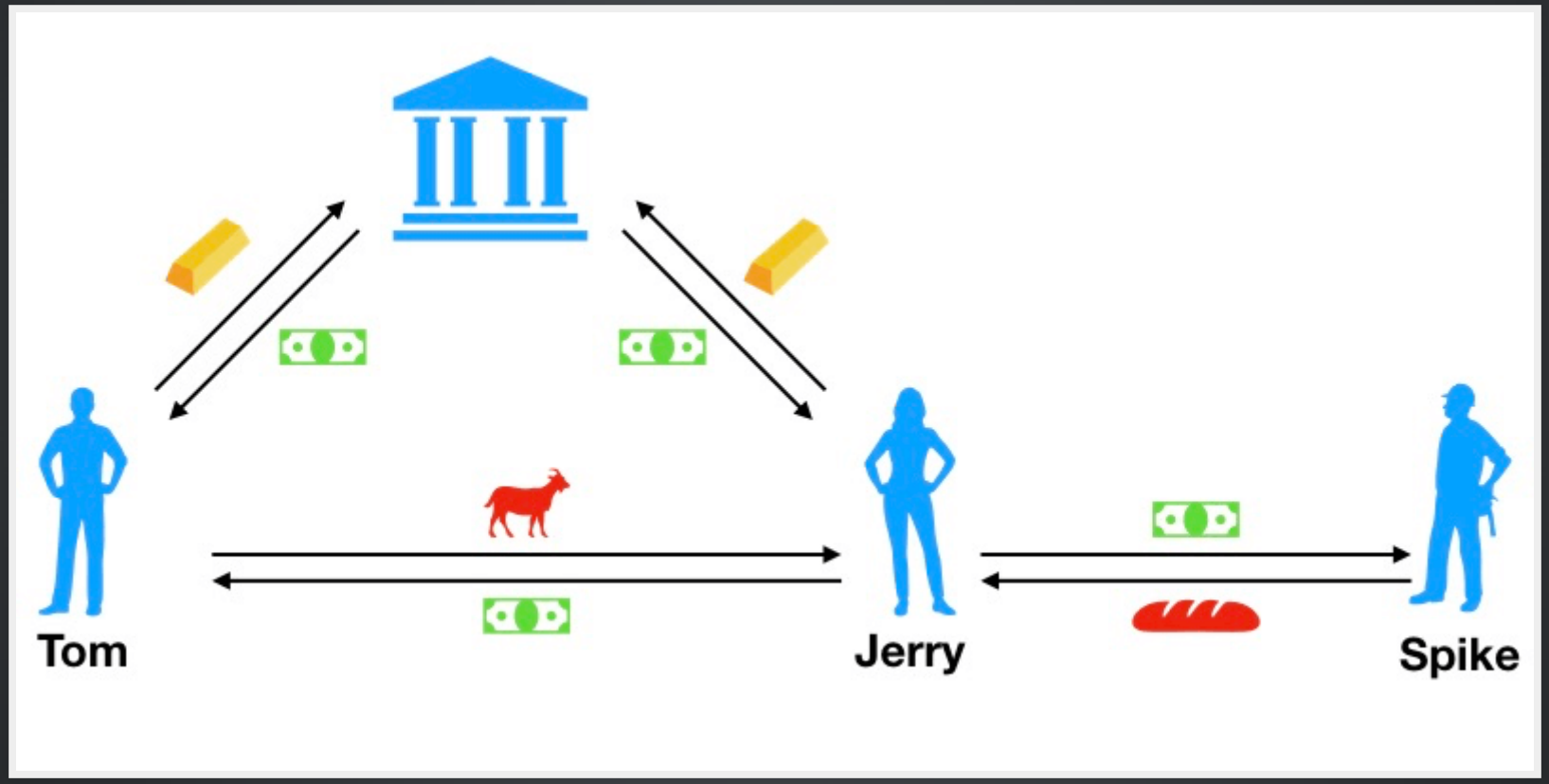
BARTER ECONOMY



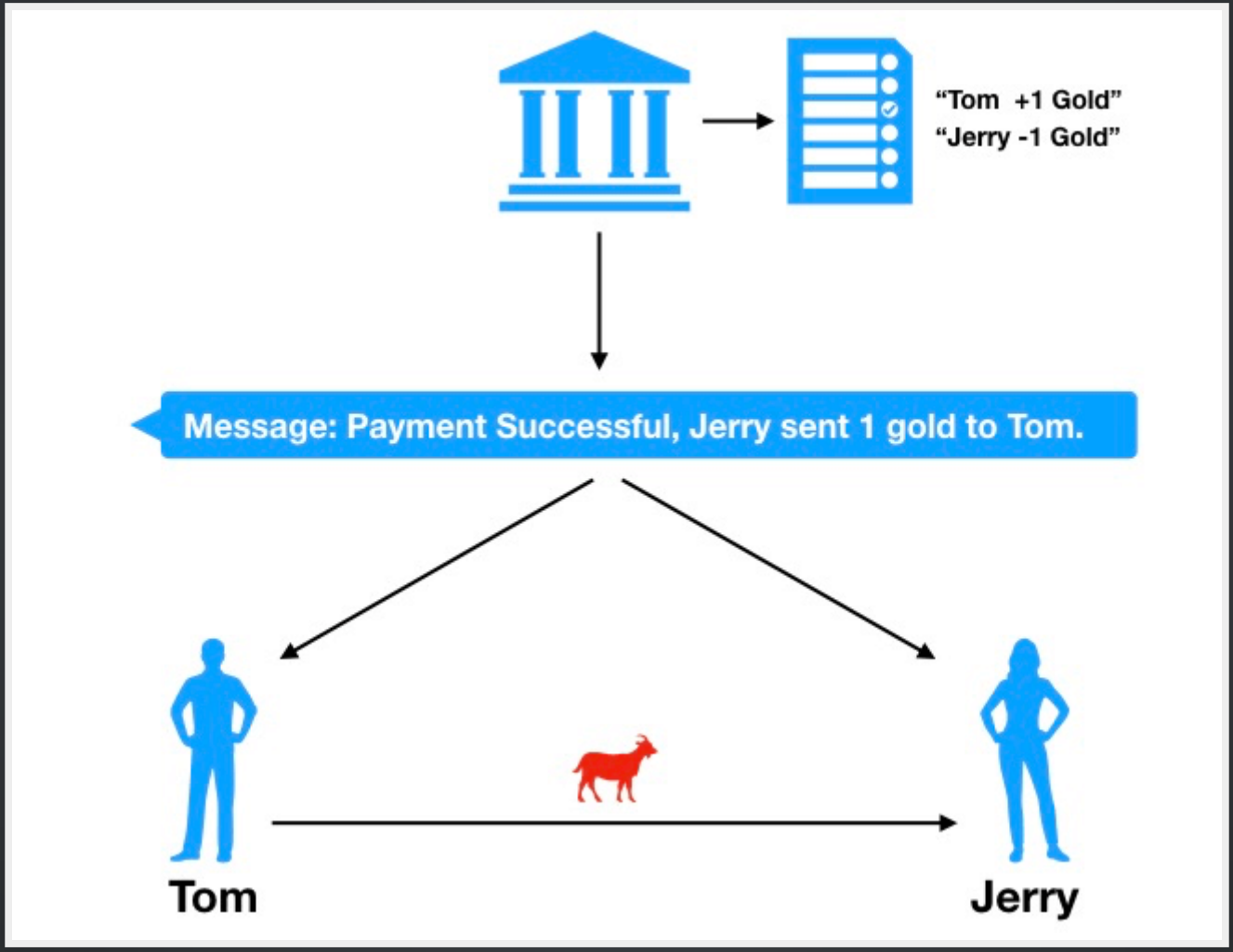
MATERIAL CURRENCY



TOKEN MONEY



CASHLESS SOCIETY



WHAT IS BITCOIN?

Bitcoin consists of:

- A decentralized P2P 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)

HISTORY OF BITCOIN

- Bitcoin was invented in 2008 with the publication of a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" written under the alias of Satoshi Nakamoto

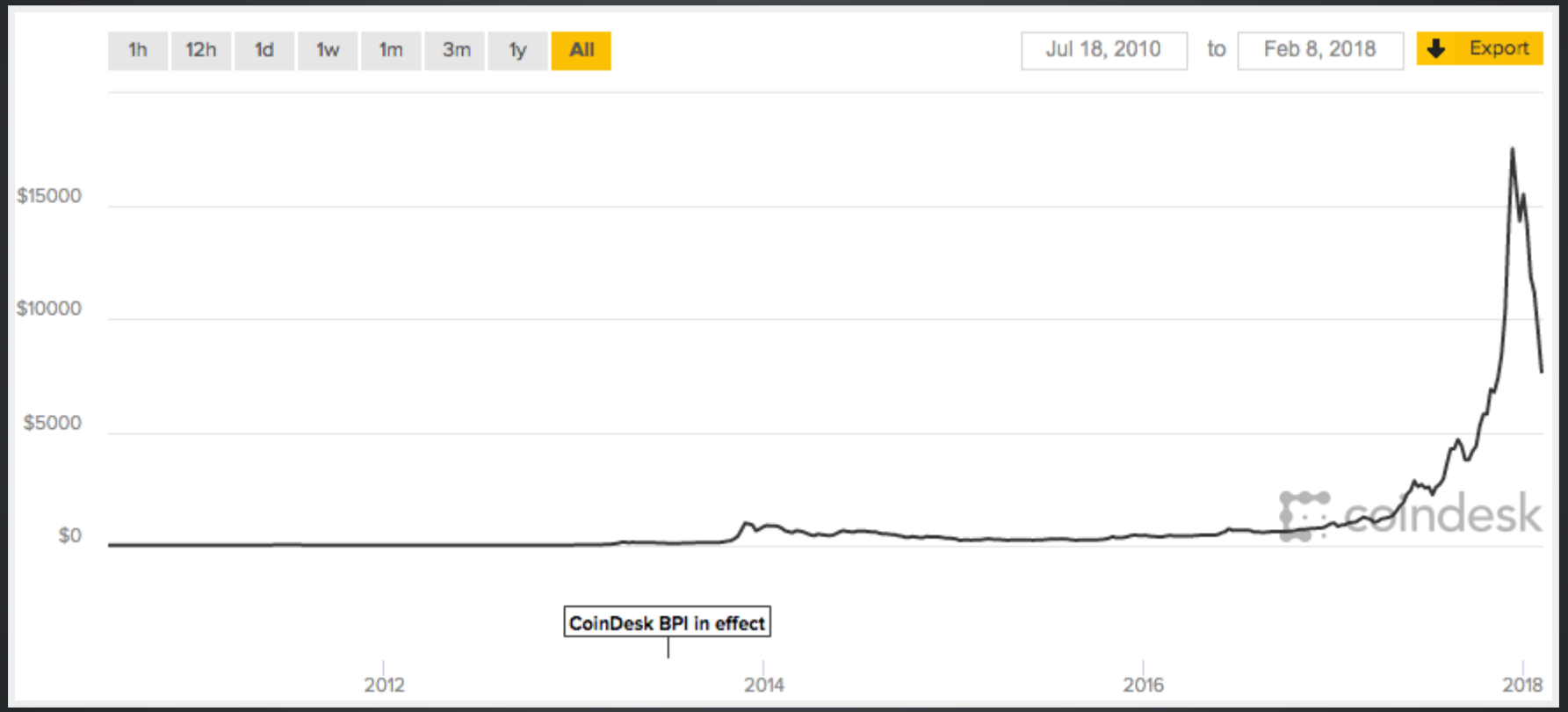
HISTORY OF BITCOIN

- The bitcoin network started in 2009, based on a reference implementation published by Nakamoto and since revised by many other programmers

HISTORY OF BITCOIN

- Satoshi Nakamoto withdrew from the public in April 2011, leaving the responsibility of developing the code and network to a thriving group of volunteers

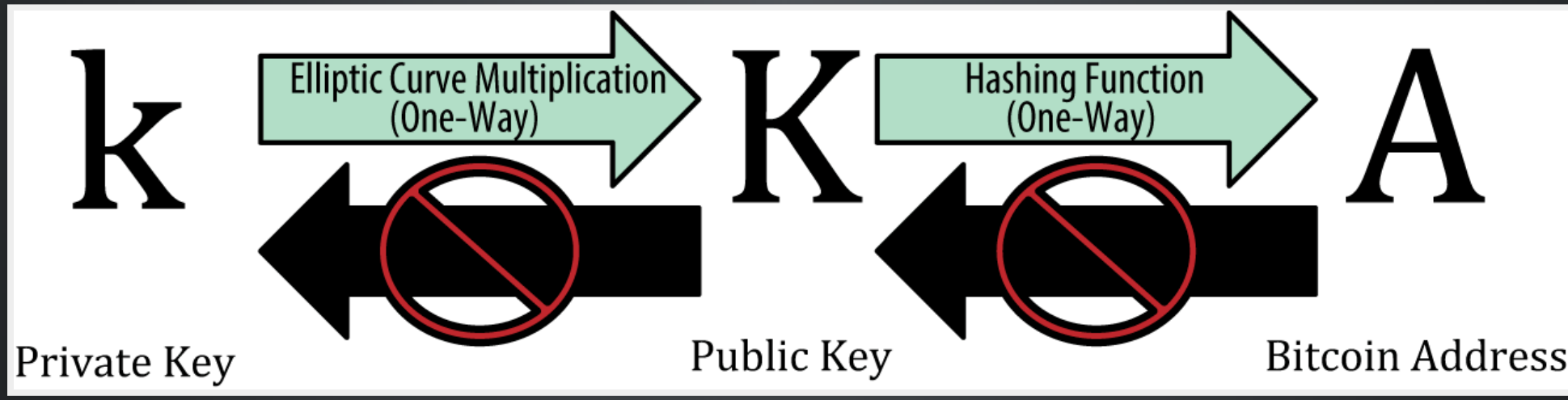
BITCOIN PRICE 2013 - 2018



BITCOIN TRANSACTION

KEYS, ADDRESSES, AND WALLETS

- Ownership of bitcoin is established through digital keys, bitcoin addresses, and digital signatures
- The digital keys created and stored by users in a file, or simple database, called a wallet



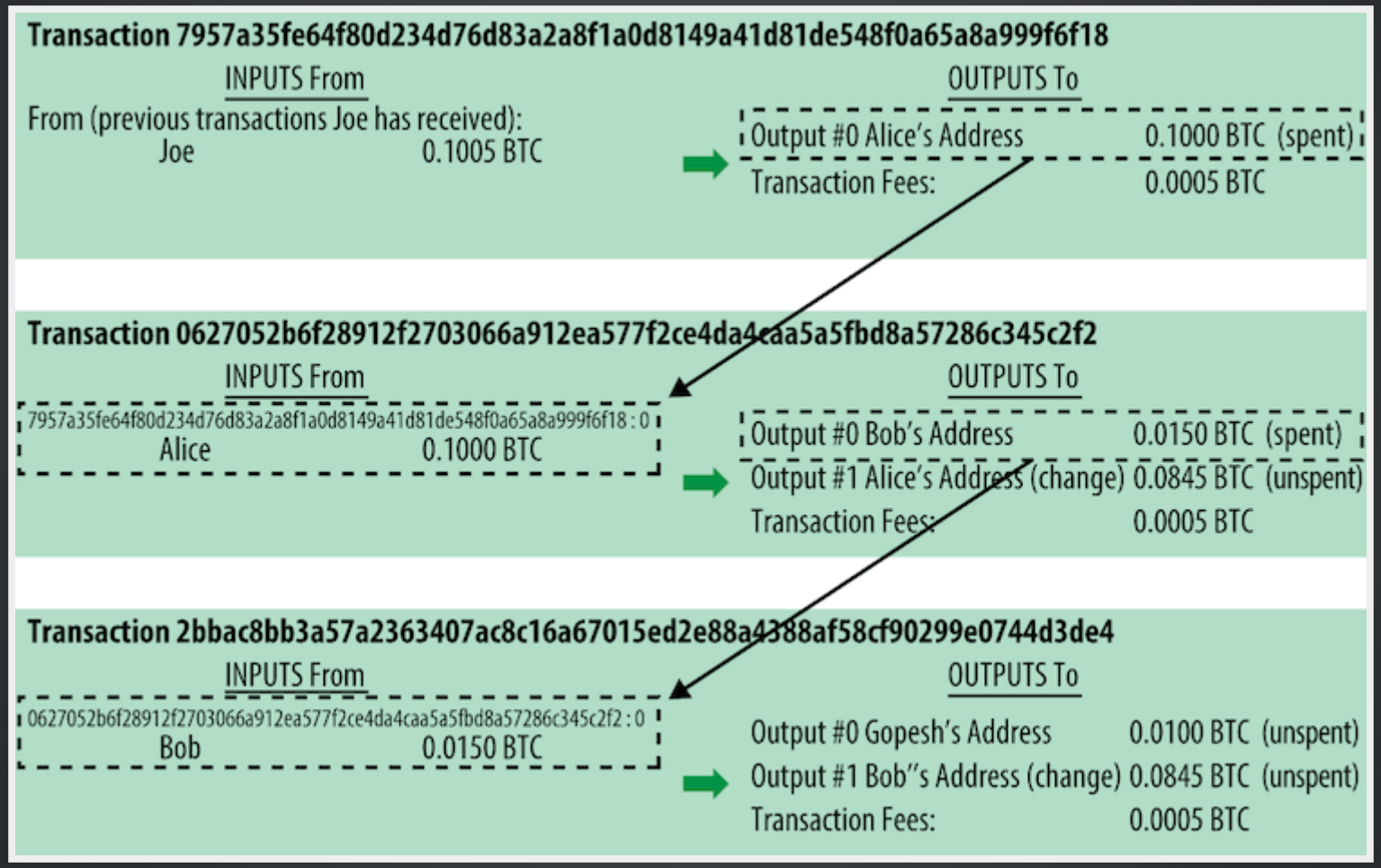
TRANSACTION INPUTS AND OUTPUTS

Transaction as Double-Entry Bookkeeping

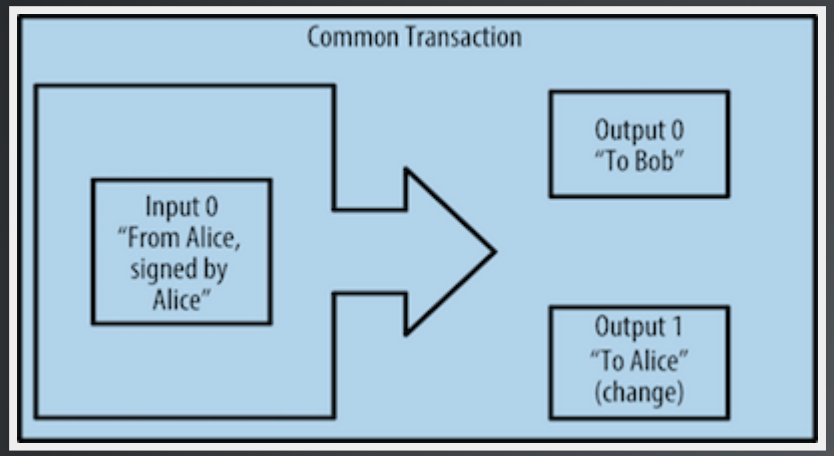
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

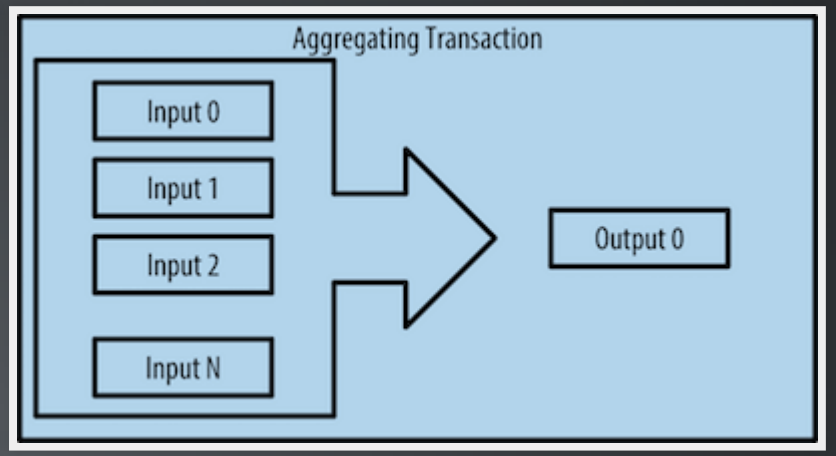
	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

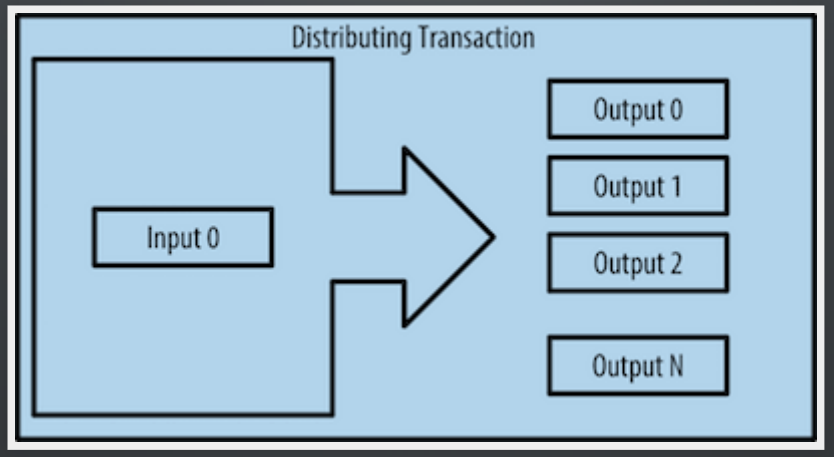
A CHAIN OF TRANSACTIONS



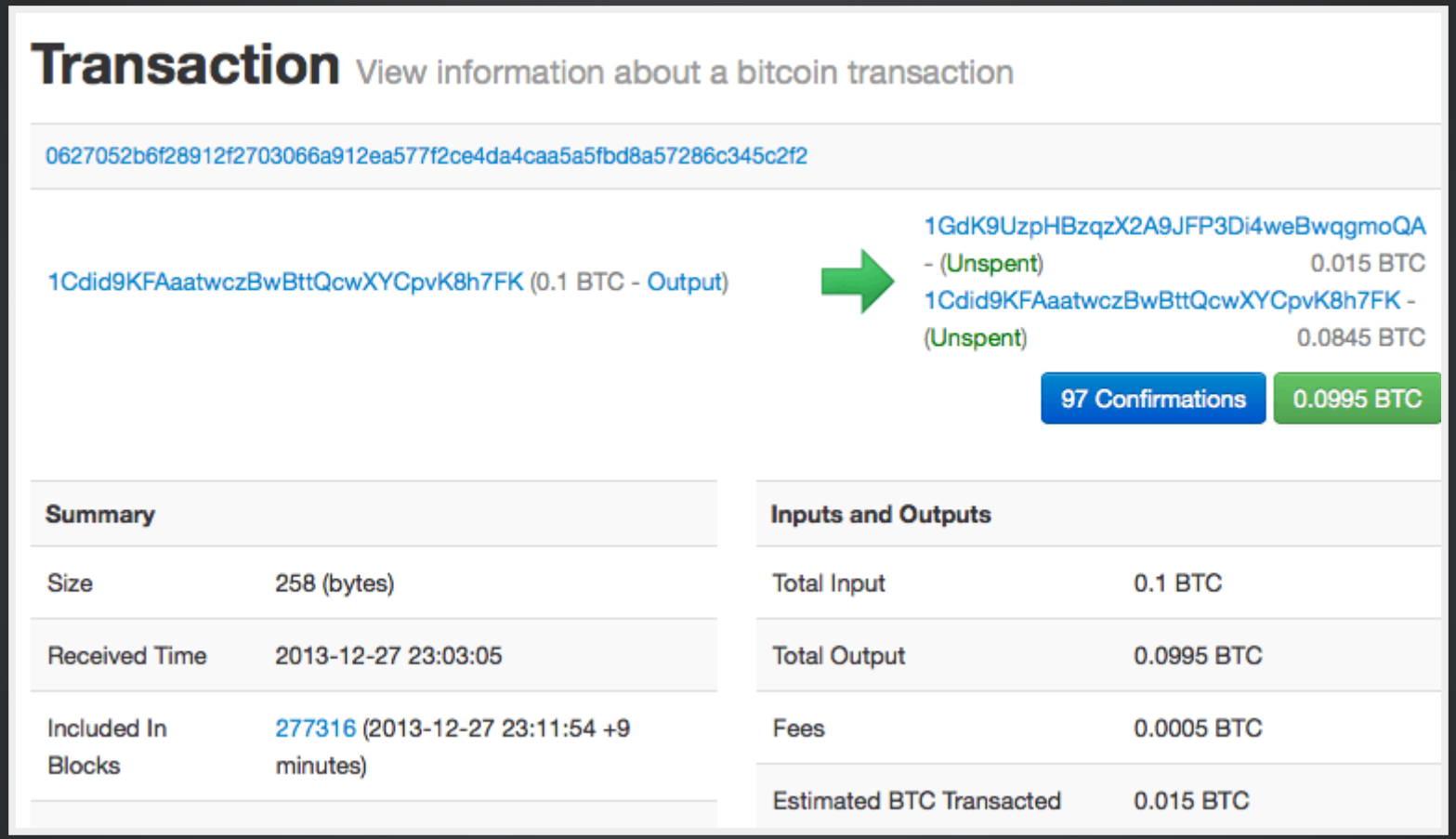
COMMON TRANSACTION FORMS







THE BLOCK EXPLORER APPLICATION



Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

blockchain.info

UTXO

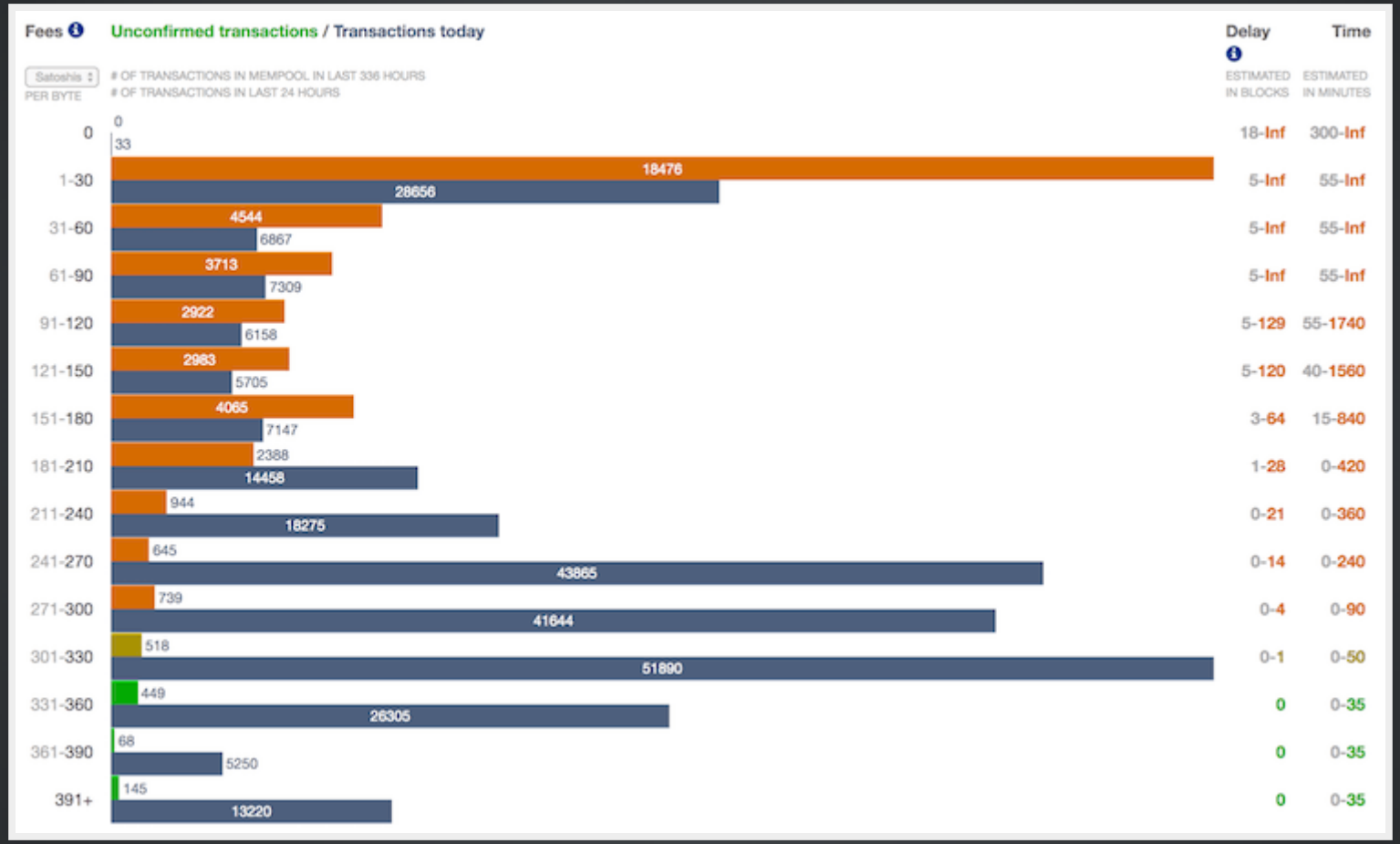
- UTXO means "Unspent Transaction Outputs"
- UTXO can be spent as an Input in a transaction
- Every transaction represents a change in the UTXO set
- Bitcoin "balance" is the sum of all UTXO that user’s wallet can spend and which may be scattered among hundreds of transactions and hundreds of blocks

TRANSACTION FEES

```
Fees = Sum(Inputs) – Sum(Outputs)
```

- Calculated based on the size of the transaction in Kbytes, not the value of the transaction in bitcoin
- Transaction fees affect the processing priority
- Most wallets calculate and include transaction fees automatically

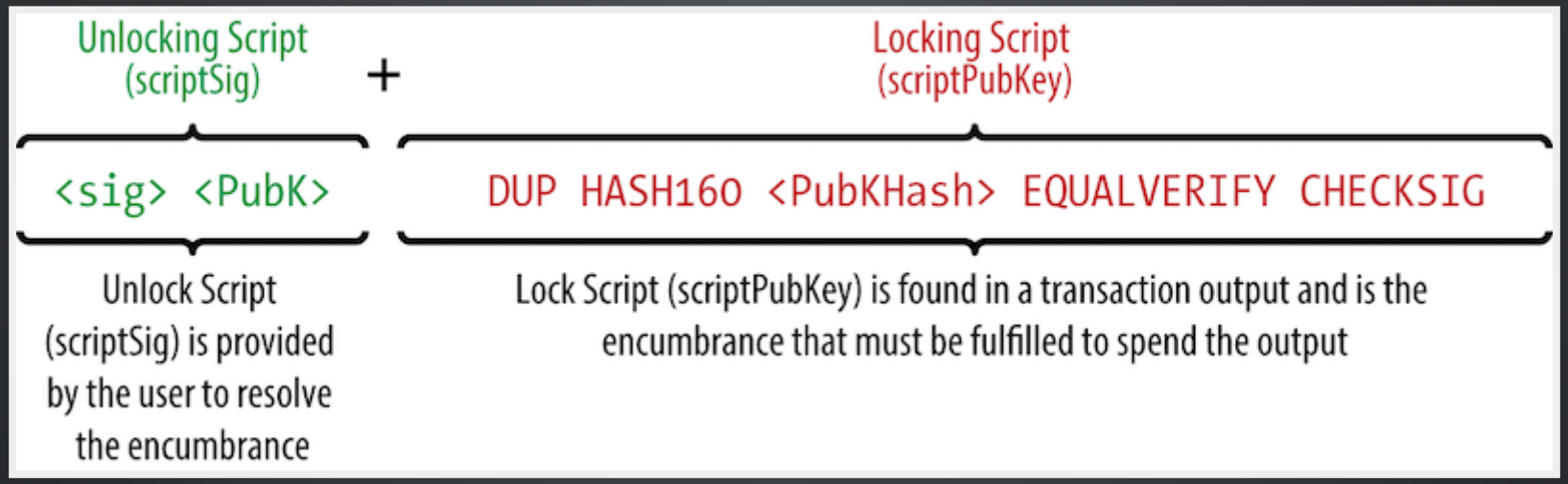
FEE ESTIMATION



https://bitcoinfees.21.co/

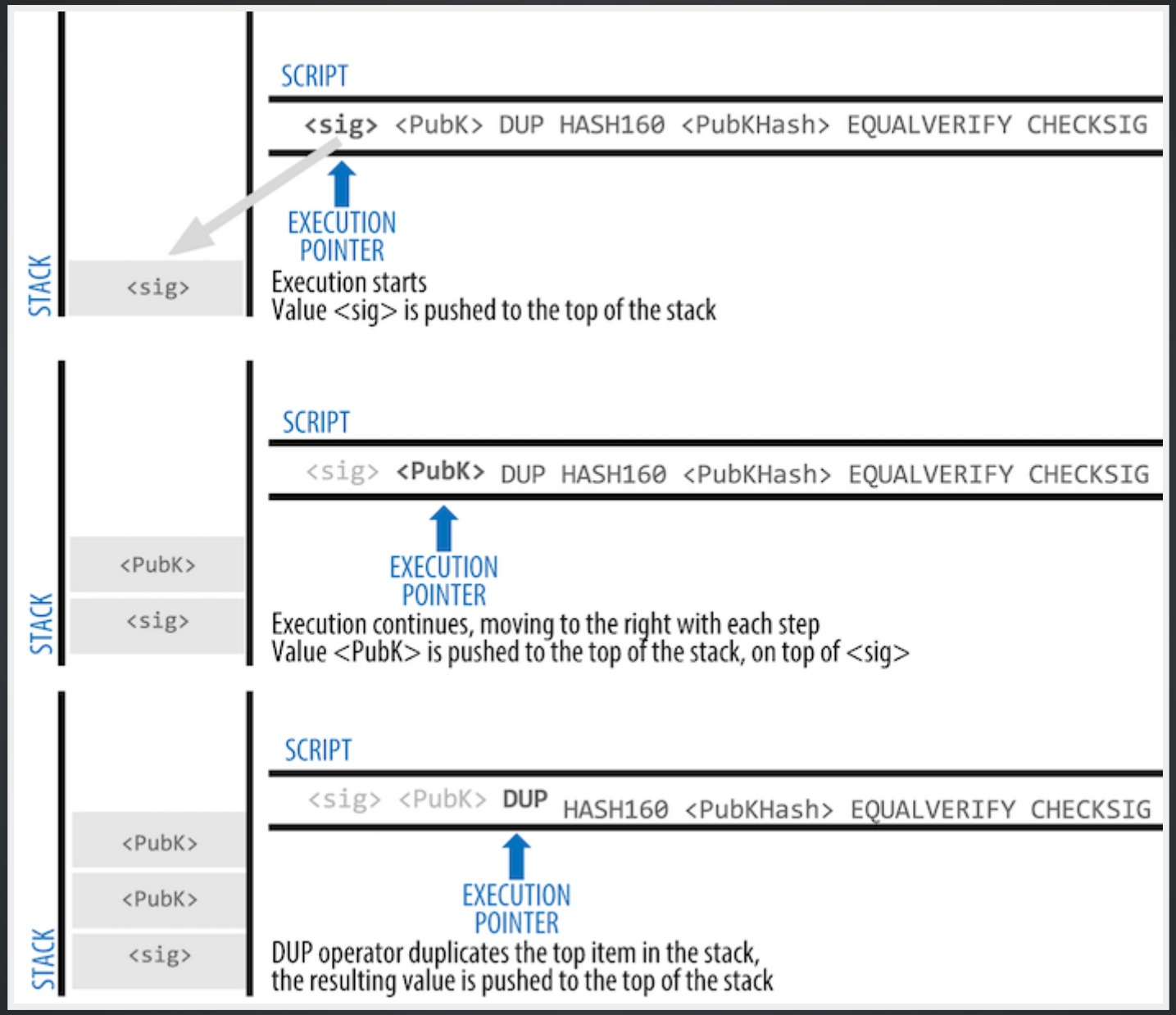
TRANSACTION SCRIPTS

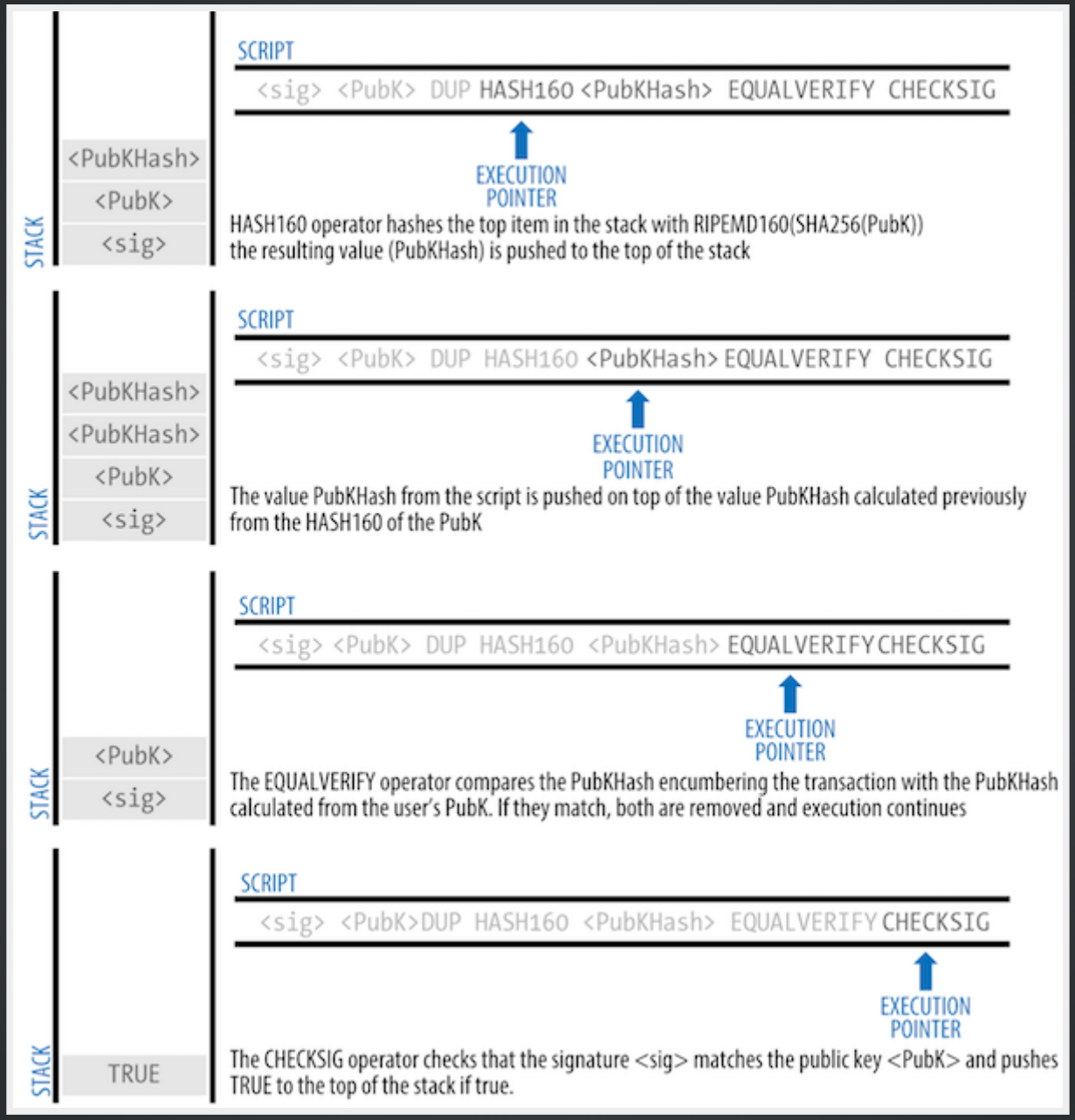
- Bitcoin's scripting language is a stack-based, turing completeness, and stateless verification language
- Bitcoin's transaction validation relies on two types of scripts: a locking script and an unlocking script



EVALUATING A SCRIPT FOR A P2PKH TRANSACTION

The vast majority of transactions processed on the bitcoin network spend outputs locked with a Pay-to-Public-Key-Hash or "P2PKH" script


SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<sig>
Execution starts
Value <sig> is pushed to the top of the stack
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<sig>
Execution continues, moving to the right with each step
Value <PubK> is pushed to the top of the stack, on top of <sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<PubK>
<sig>
DUP operator duplicates the top item in the stack,
the resulting value is pushed to the top of the stack


STACK
<PubKHash>
<PubK>
<sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
HASH160 operator hashes the top item in the stack with RIPEMD160(SHA256(PubK)) the resulting value (PubKHash) is pushed to the top of the stack
STACK
<PubKHash>
<PubKHash>
<PubK>
<sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
The value PubKHash from the script is pushed on top of the value PubKHash calculated previously from the HASH160 of the PubK
STACK
<PubK>
<sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
The EQUALVERIFY operator compares the PubKHash encumbering the transaction with the PubKHash calculated from the user's PubK. If they match, both are removed and execution continues
STACK
TRUE
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
The CHECKSIG operator checks that the signature <sig> matches the public key <PubK> and pushes TRUE to the top of the stack if true.

BLOCKCHAIN

BLOCK AND BLOCKCHAIN

- Block is a container data structure that aggregates transactions
- The blockchain data structure is an ordered, back-linked list of blocks, serves as the public ledger for all transactions

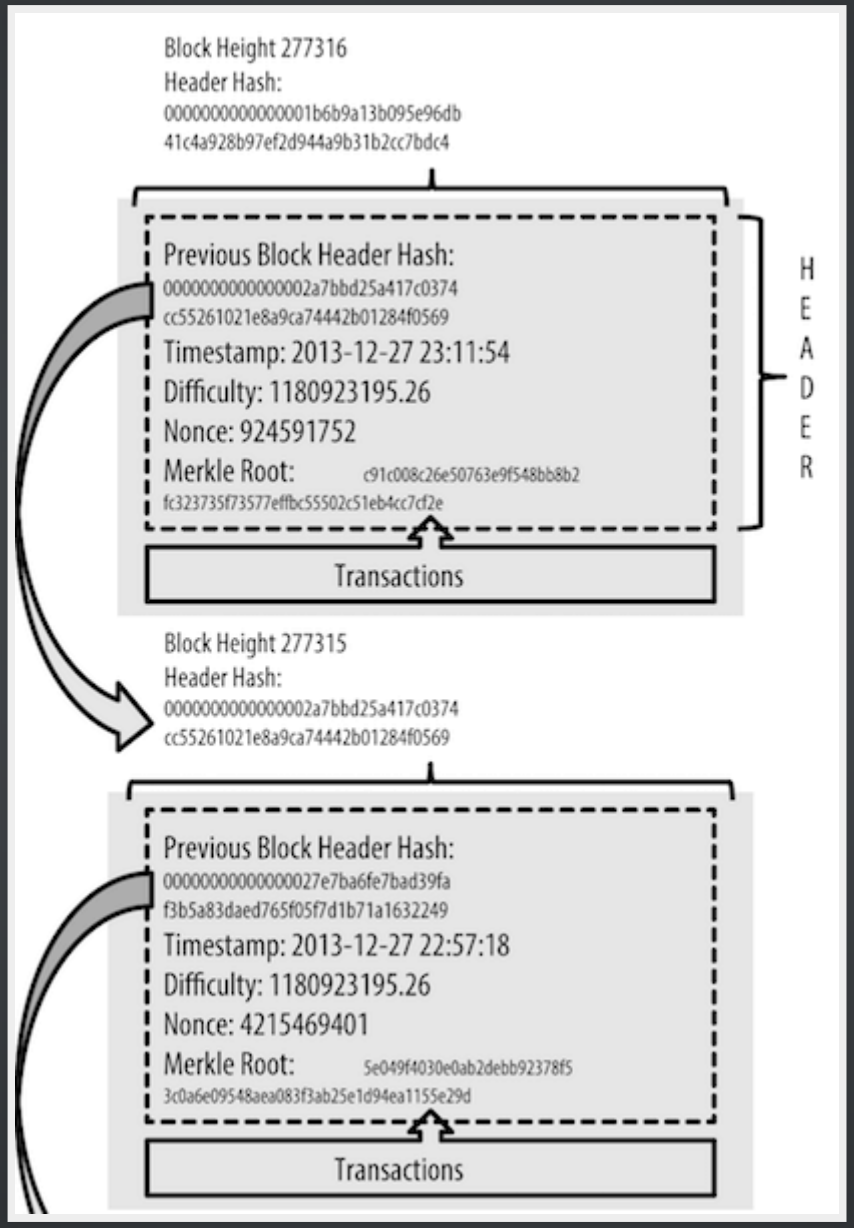
STRUCTURE OF A BLOCK

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
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 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
4 bytes	Difficulty	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

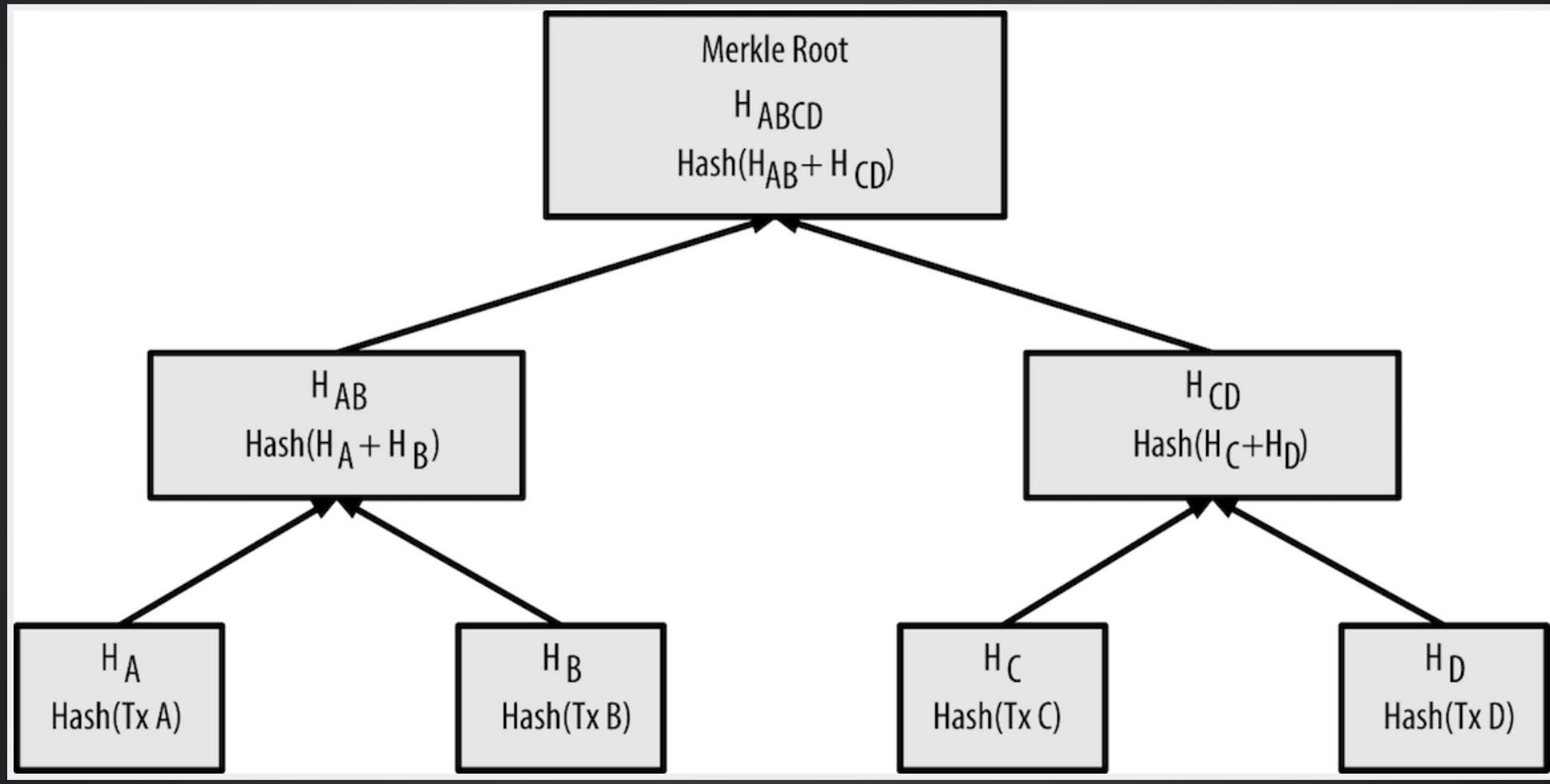
LINKING BLOCKS



THE GENESIS BLOCK

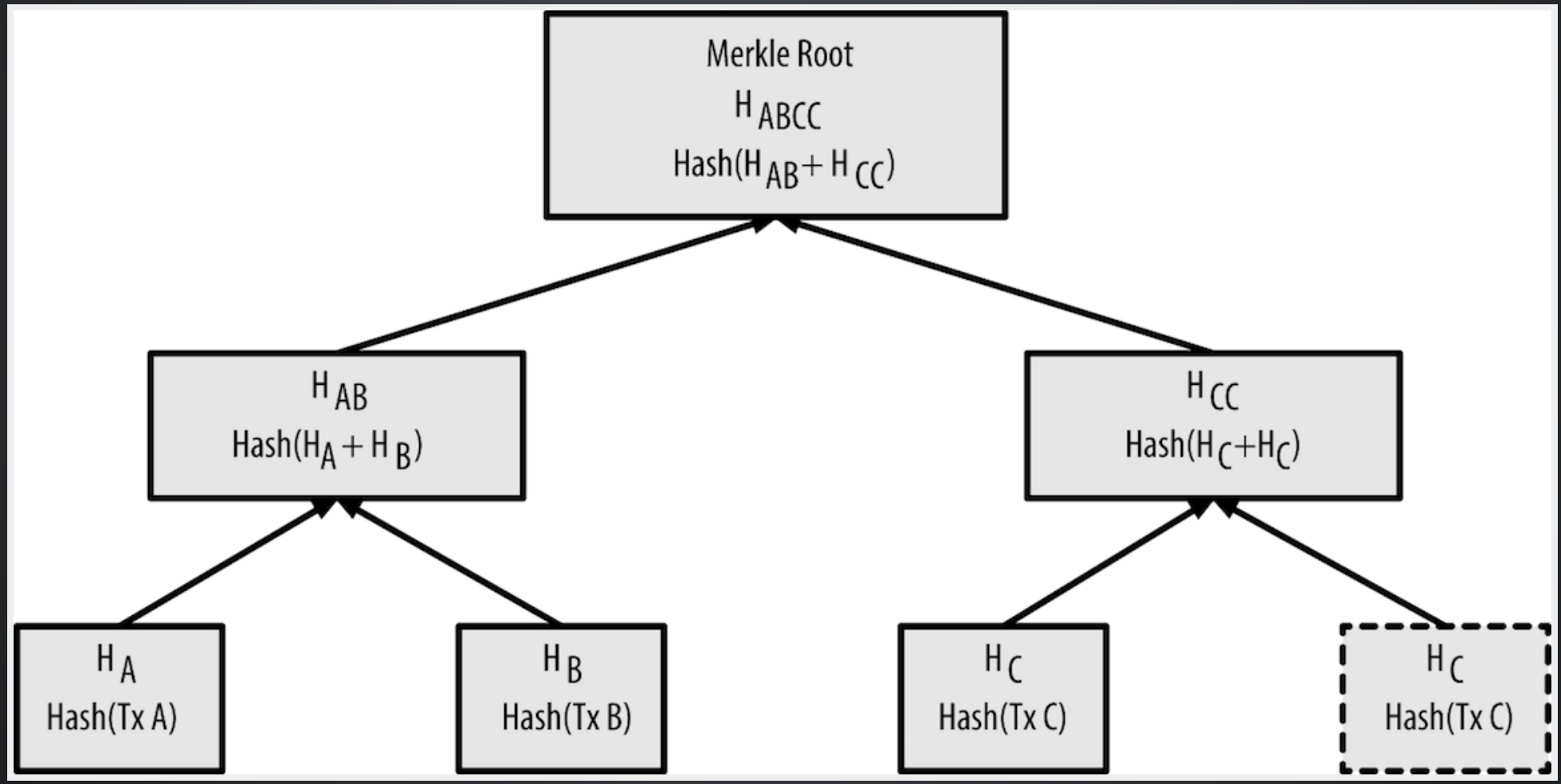
The first block in the blockchain is called the genesis block and was created in 2009. The genesis block contains a hidden message within it. The coinbase transaction input contains the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks," by referencing the headline of the British newspaper The Times.

MERKLE TREE

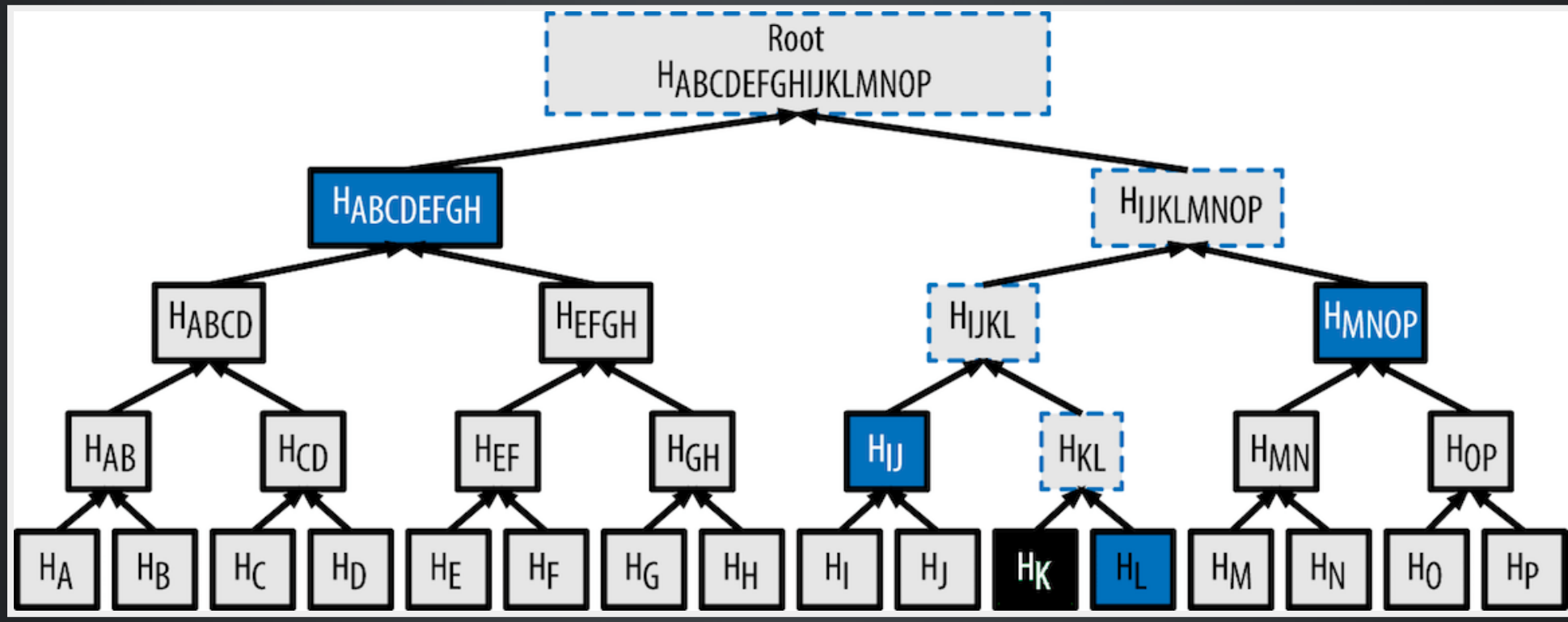

Merkle Root
H_{ABCD}
$Hash(H_{AB} + H_{CD})$
H_{AB}
$Hash(H_A + H_B)$
H_{CD}
$Hash(H_C + H_D)$
H_A
Hash(Tx A)
H_B
Hash(Tx B)
H_C
Hash(Tx C)
H_D
Hash(Tx D)

MERKLE TREE

Even number of nodes



MERKLE PATH


Root
HABCDEFGHIJKLMNOP
HABCDEFGH
HIJKLMNOP
HABCD
HEFGH
HIJKL
HMNOP
HAB
HCD
HEF
HGH
HIJ
HKL
HMN
HOP
HA
HB
HC
HD
HE
HF
HG
HH
HI
HJ
HK
HL
HM
HN
HO
HP

MERKLE TREE EFFICIENCY

Number of Txs	Approx. size of block	Path size (hashes)	Path size (bytes)
16 txs	4 KB	4 hashes	128 bytes
512 txs	128 KB	9 hashes	288 bytes
2048 txs	512 KB	11 hashes	352 bytes
65535 txs	16 MB	16 hashes	512 bytes

MINING AND CONSENSUS

MINER

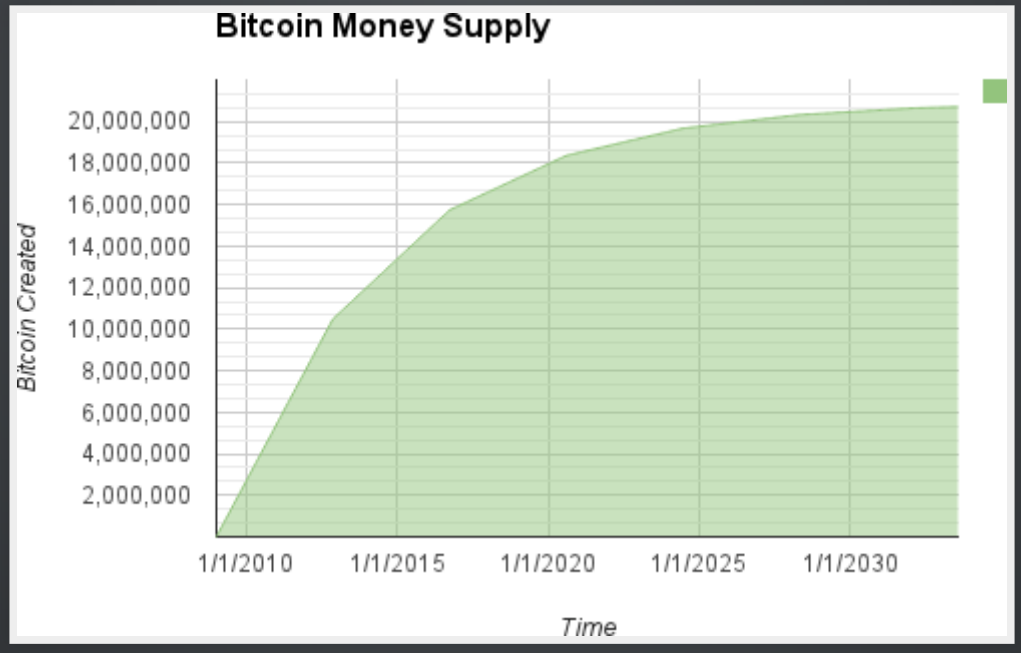
- Miners validate new transactions and record them on the global ledger
- Miners receive two types of rewards by mining: new coins created with each new block, and transaction fees from all the transactions included in the block

BITCOIN ECONOMICS AND CURRENCY CREATION

Each block, generated on average every 10 minutes, contains entirely new bitcoin, created from nothing

BITCOIN MONEY SUPPLY

- Every 210,000 blocks, or approximately every 4 years, the currency issuance rate is decreased by 50%
- Finally, in approximately 2140, almost 21 million bitcoin will be issued. Thereafter, blocks will contain no new bitcoin, and miners will be rewarded solely through the transaction fees



THE COINBASE TRANSACTION

- The first transaction in any block is a special transaction, called a coinbase transaction
- Coinbase transaction does not consume UTXO as inputs. Instead, it has only one input, called the "coinbase", which creates bitcoin from nothing

PROOF OF WORK

The Difficulty target and Nonce in block header

Size	Field	Description
4 bytes	Difficulty	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

PROOF OF WORK

The Proof-of-Work must produce a hash (Nonce) that is less than the difficulty target

```
# example of proof-of-work algorithm
max_nonce = 2 ** 32 # 4 billion

def proof_of_work(header, difficulty_bits):

    difficulty_target = 2 ** (256-difficulty_bits)

    for nonce in xrange(max_nonce):
        block_hash = hashlib.sha256(str(header)+str(nonce)).hexdigest()

        if long(block_hash, 16) < difficulty_target:
            print "Success with nonce %d" % nonce
            return (block_hash, nonce)
```

RETARGETING TO ADJUST DIFFICULTY

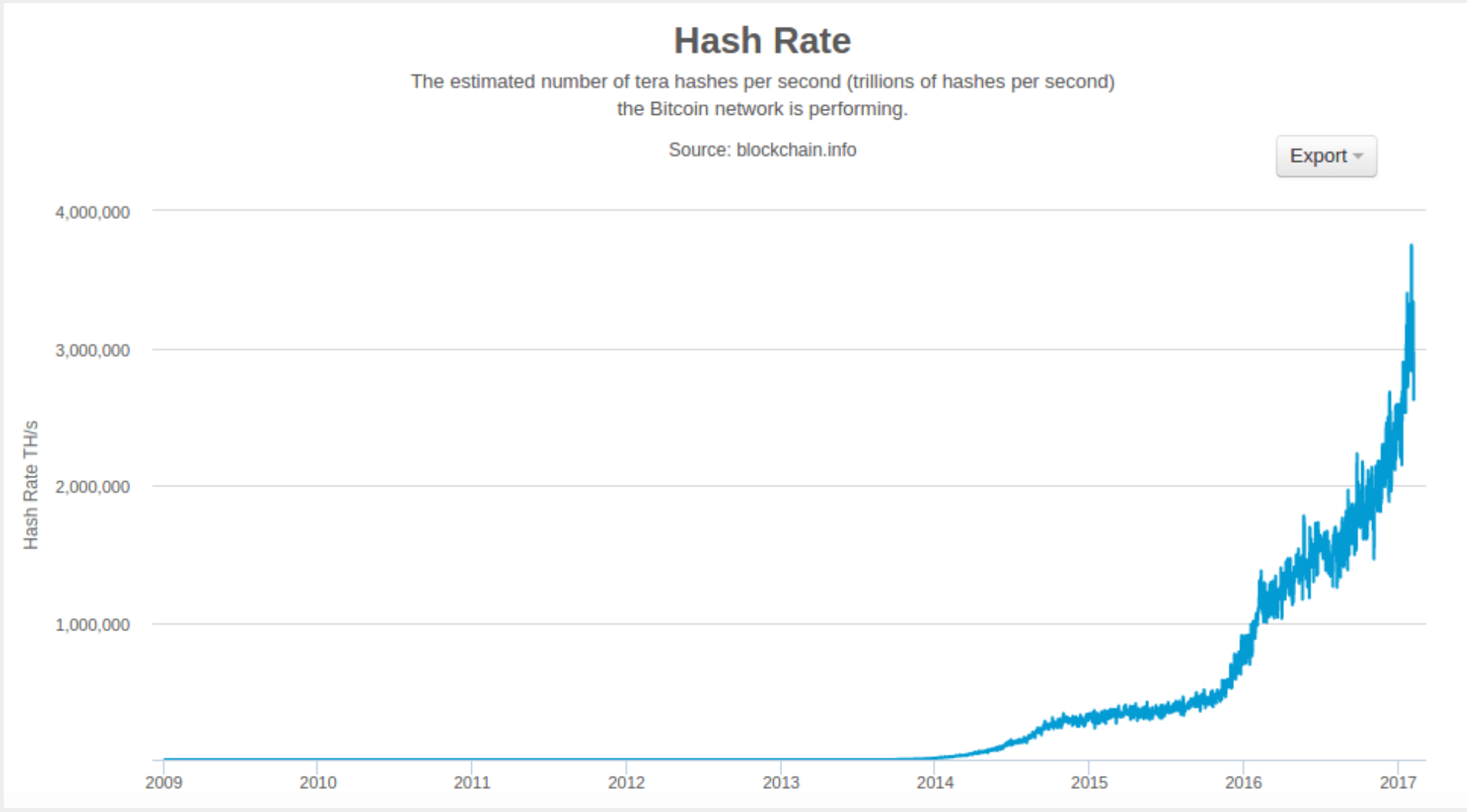
- Blocks are generated every 10 minutes, on average. This is bitcoin's heartbeat and underpins the frequency of currency issuance and the speed of transaction settlement
- Retargeting occurs automatically and on every node independently

```
New Difficulty = Old Difficulty *
            (Actual Time of Last 2016 Blocks / 20160 minutes)
```

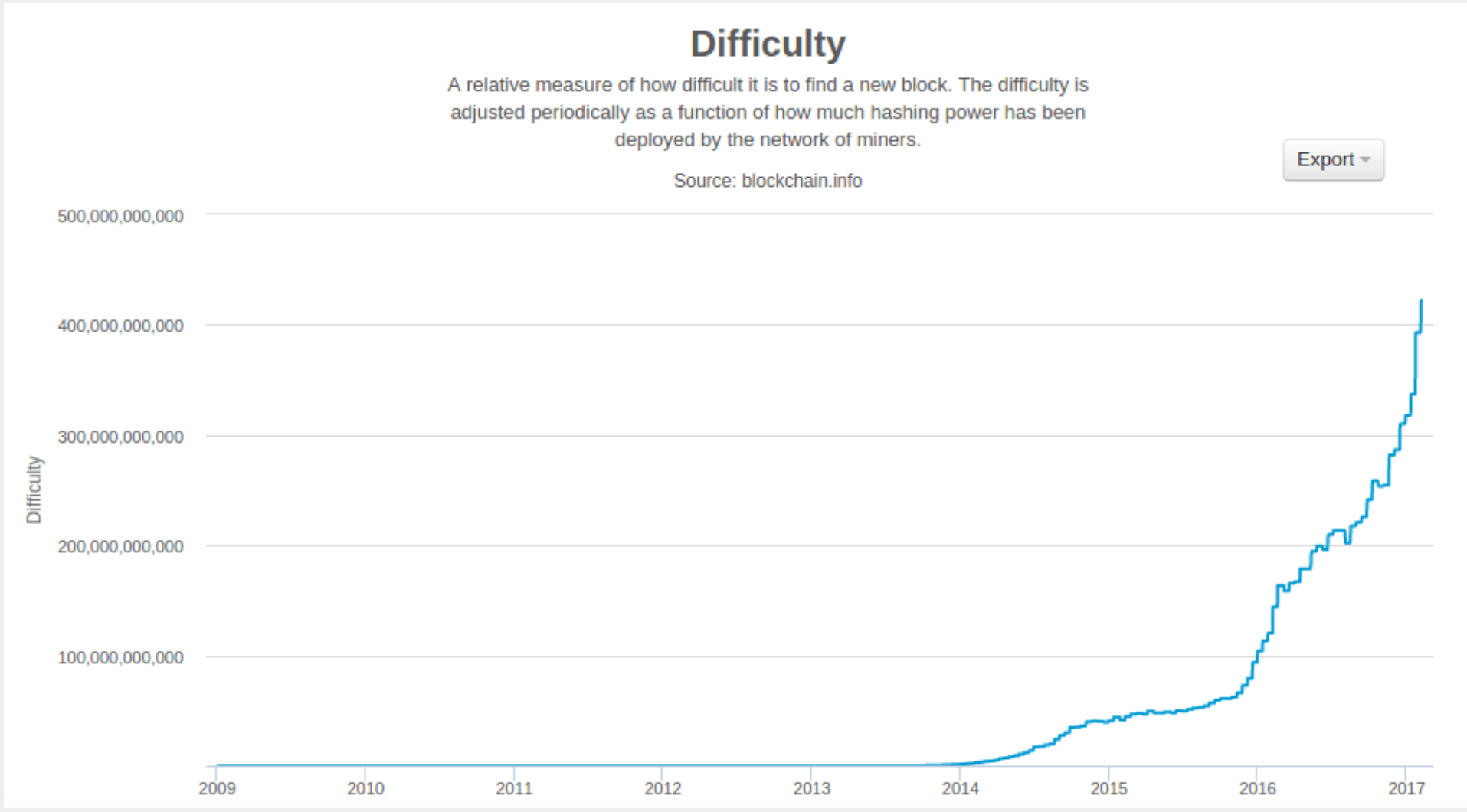
MINER COMPETITION

When one miner solves and transmits a block, other miners receive, validate, and then propagate the new block, they abandon their efforts to find a block at the same height and immediately start computing the next block in the chain

TOTAL HASHING POWER



MINING DIFFICULTY

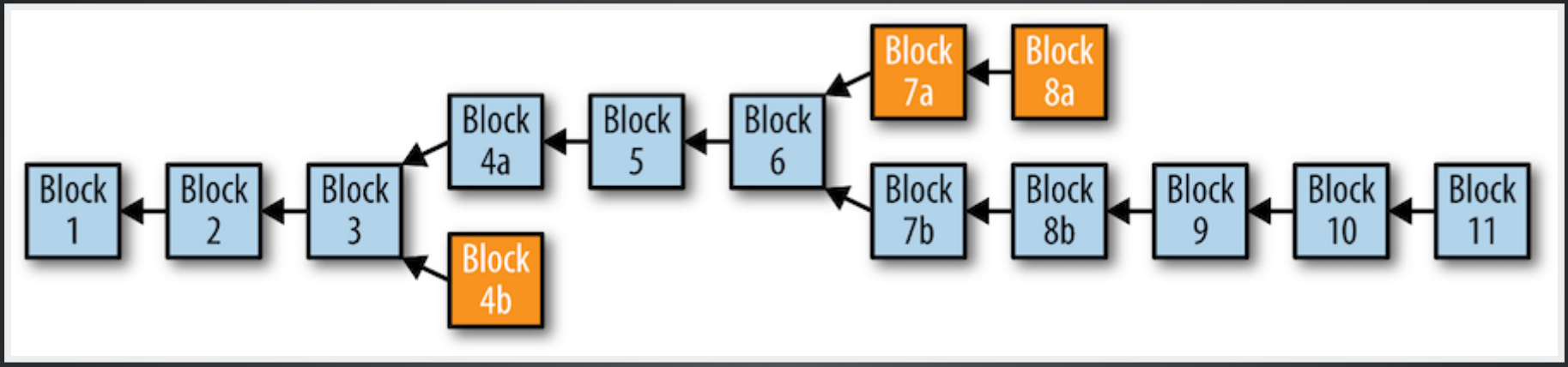


DECENTRALIZED CONSENSUS

Bitcoin's decentralized consensus emerges from the interplay of four processes that occur independently on nodes across the network:

- Independent verification of each transaction, by every full node, based on a comprehensive list of criteria
- Independent aggregation of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a Proof-of-Work algorithm
- Independent verification of the new blocks by every node and assembly into a chain
- Independent selection, by every node, of the chain with the most cumulative computation demonstrated through Proof-of-Work

BLOCKCHAIN FORKS



- Because the blockchain is a decentralized data structure, different copies of it are not always consistent
- As long as all nodes select the greatest-cumulative-work chain, the global bitcoin network eventually converges to a consistent state

HARD FORK

A permanent divergence in the blockchain, commonly occurs when non-upgraded nodes can’t validate blocks created by upgraded nodes that follow newer consensus rules

51% CONSENSUS ATTACKS

If we controlled a majority (51%) of the total network's hashing power, we can:

- Cause deliberate "forks" in the blockchain and double-spend transactions
- Execute DoS attacks against specific transactions or addresses

IS IT TOO LATE TO START MINING?

GPU MINER

Nvidia GTX1080 GPU = 2.83GH/s for 200w

ASIC: Application-Specific Integrated Circuit

AntMiner S2 ASIC = 1000GH/s for 120w

RETURN ON INVESTMENT

```
ROI = Miner costs / (Income per day - Power costs)
```

YOUR COMPETITORS: INSIDE A SECRET CHINESE BITCOIN MINE

In this highly competitive environment, miners collaborate to form mining pools

USER SECURITY BEST PRACTICES

- Physical Bitcoin Storage
- Hardware Wallets
- Balancing Risk
- Diversifying Risk
- Multisig and Governance
- Survivability

BLOCKCHAIN APPLICATIONS

- Digital Identity
- Proof-of-Existence (Digital Notary)
- Kickstarter
- Smart Contracts
- Distributed Cloud Storage

REFERENCES

- Mastering Bitcoin
- CoinDesk

THE END

Q&A