Blockchain Technology and Its Impact on the Global Economy

Zichao Yang

Email: yang_zichao@outlook.com

Website：www.yzc.me

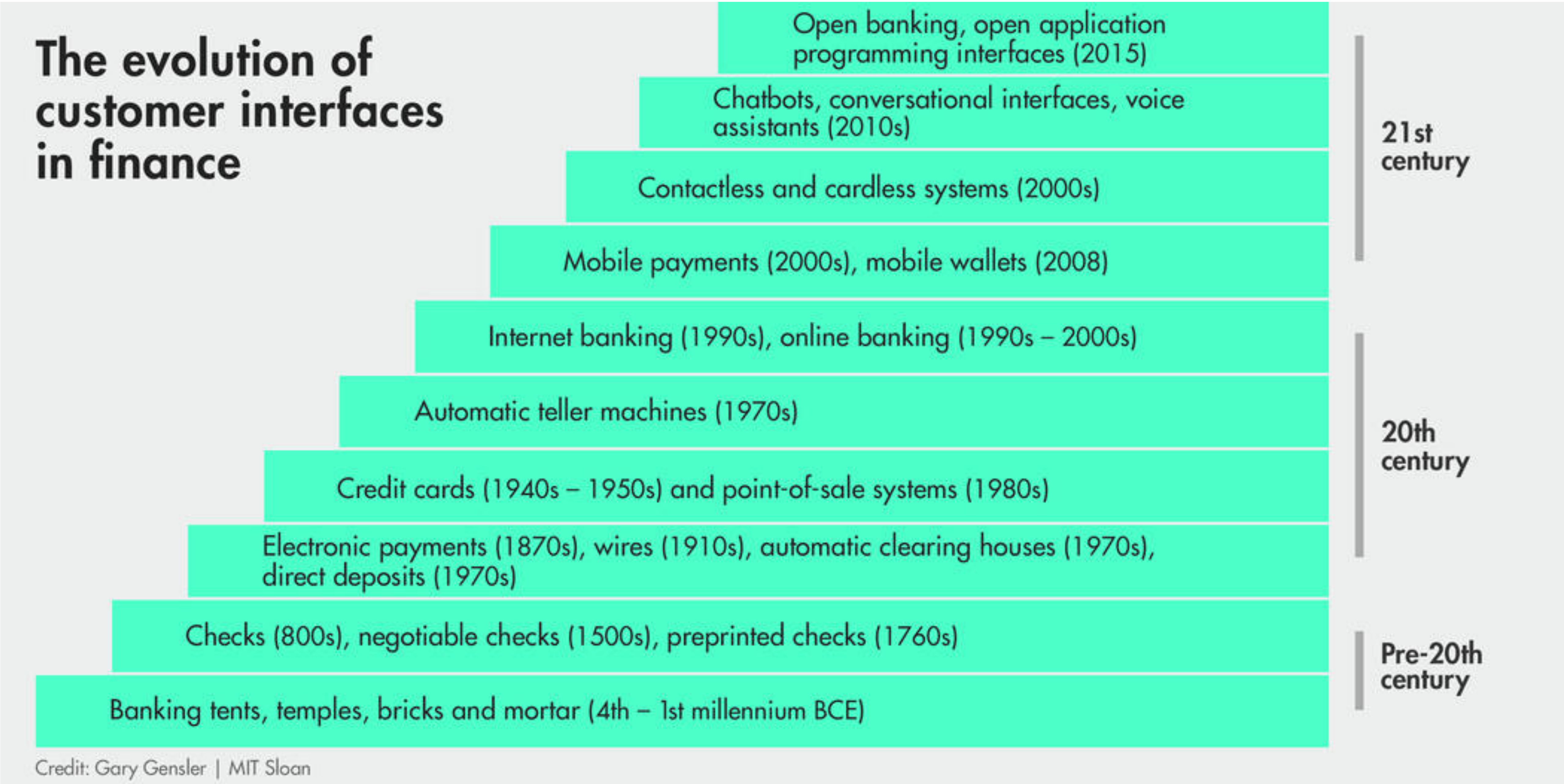
What is Fintech?

- Fintech = financial technology

- Globally, financial technology is projected to reach a market value of $305 billion by 2025. (Source: Market Data Forecast)

- Three essential components: the internet, mobile phones, and the cloud

“Fintech… goes back to the invention of money.” – Gary Gensler



The evolution of customer interfaces in finance

21st century

- Open banking, open application programming interfaces (2015)
- Chatbots, conversational interfaces, voice assistants (2010s)
- Contactless and cardless systems (2000s)
- Mobile payments (2000s), mobile wallets (2008)

20th century

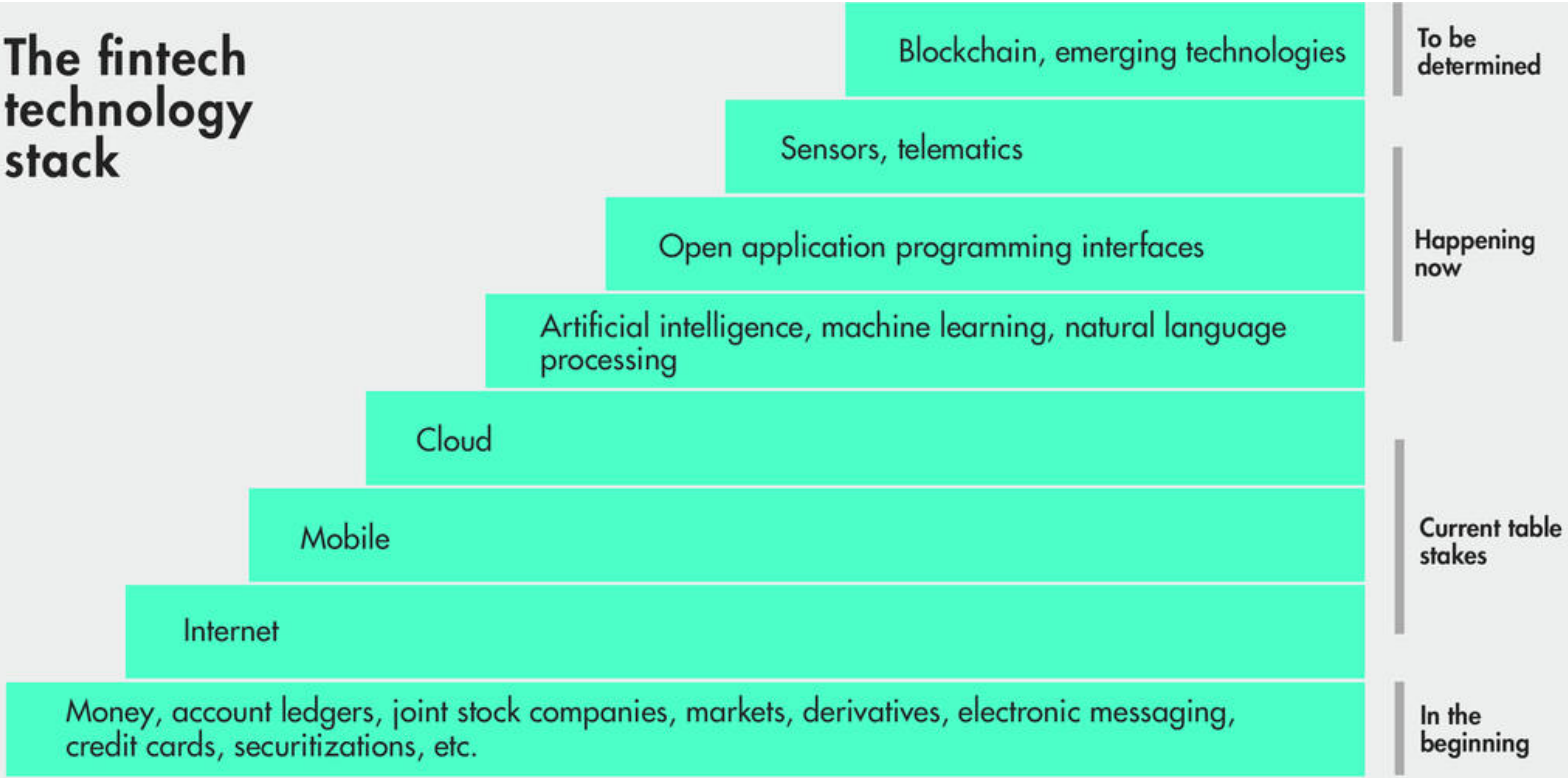
- Internet banking (1990s), online banking (1990s – 2000s)
- Automatic teller machines (1970s)
- Credit cards (1940s – 1950s) and point-of-sale systems (1980s)
- Electronic payments (1870s), wires (1910s), automatic clearing houses (1970s), direct deposits (1970s)

Pre-20th century

- Checks (800s), negotiable checks (1500s), preprinted checks (1760s)
- Banking tents, temples, bricks and mortar (4th – 1st millennium BCE)

Credit: Gary Gensler | MIT Sloan

The fintech technology stack



Blockchain, emerging technologies

Sensors, telematics

Open application programming interfaces

Artificial intelligence, machine learning, natural language processing

Cloud

Mobile

Internet

Money, account ledgers, joint stock companies, markets, derivatives, electronic messaging, credit cards, securitizations, etc.

To be determined

Happening now

Current table stakes

In the beginning

Credit: Gary Gensler | MIT Sloan

Part I: Origins of Blockchain Technology

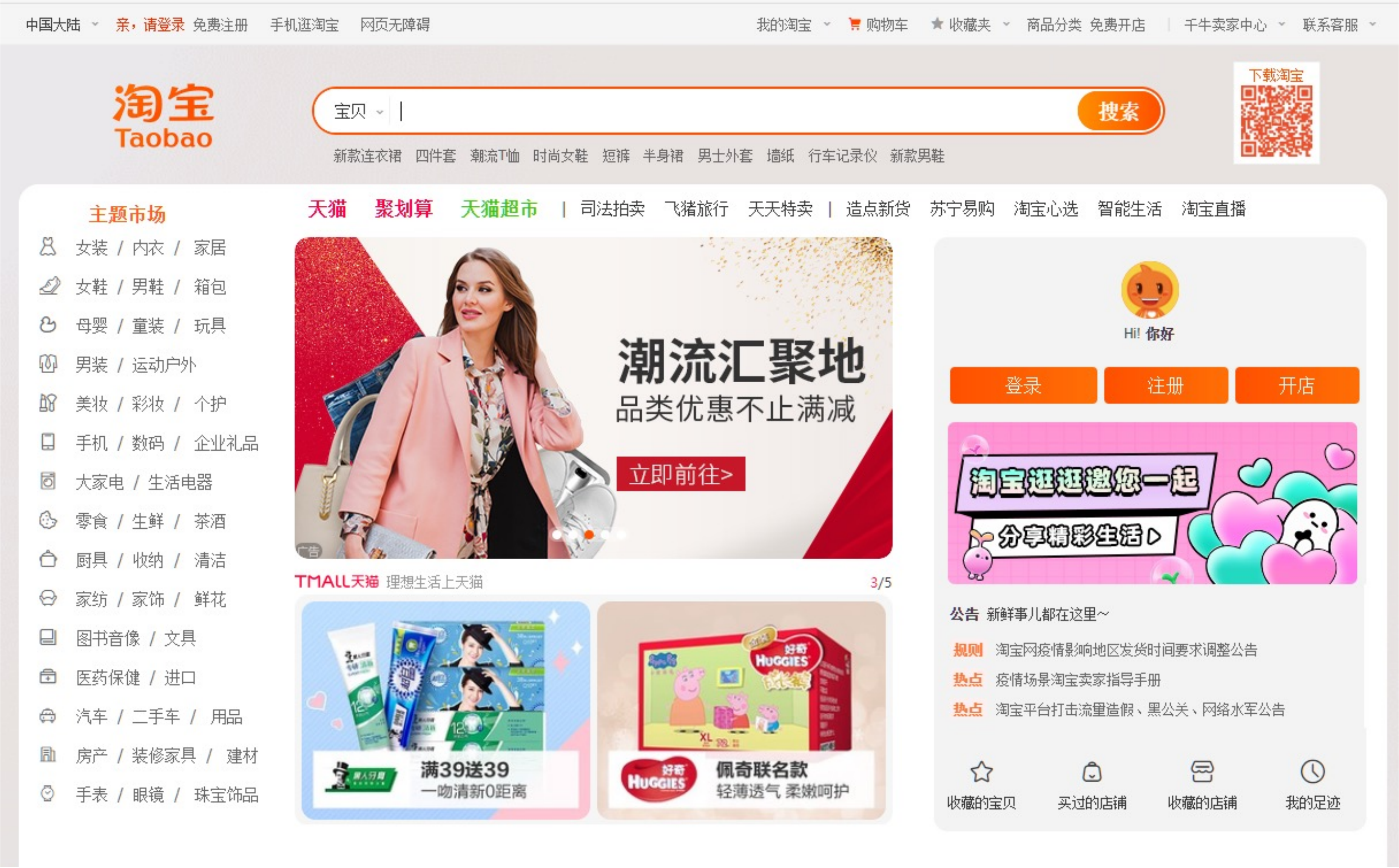
The evolution of the internet

- Created in 1960s, the internet was a simple network used by university researchers and the US government to share information digitally.

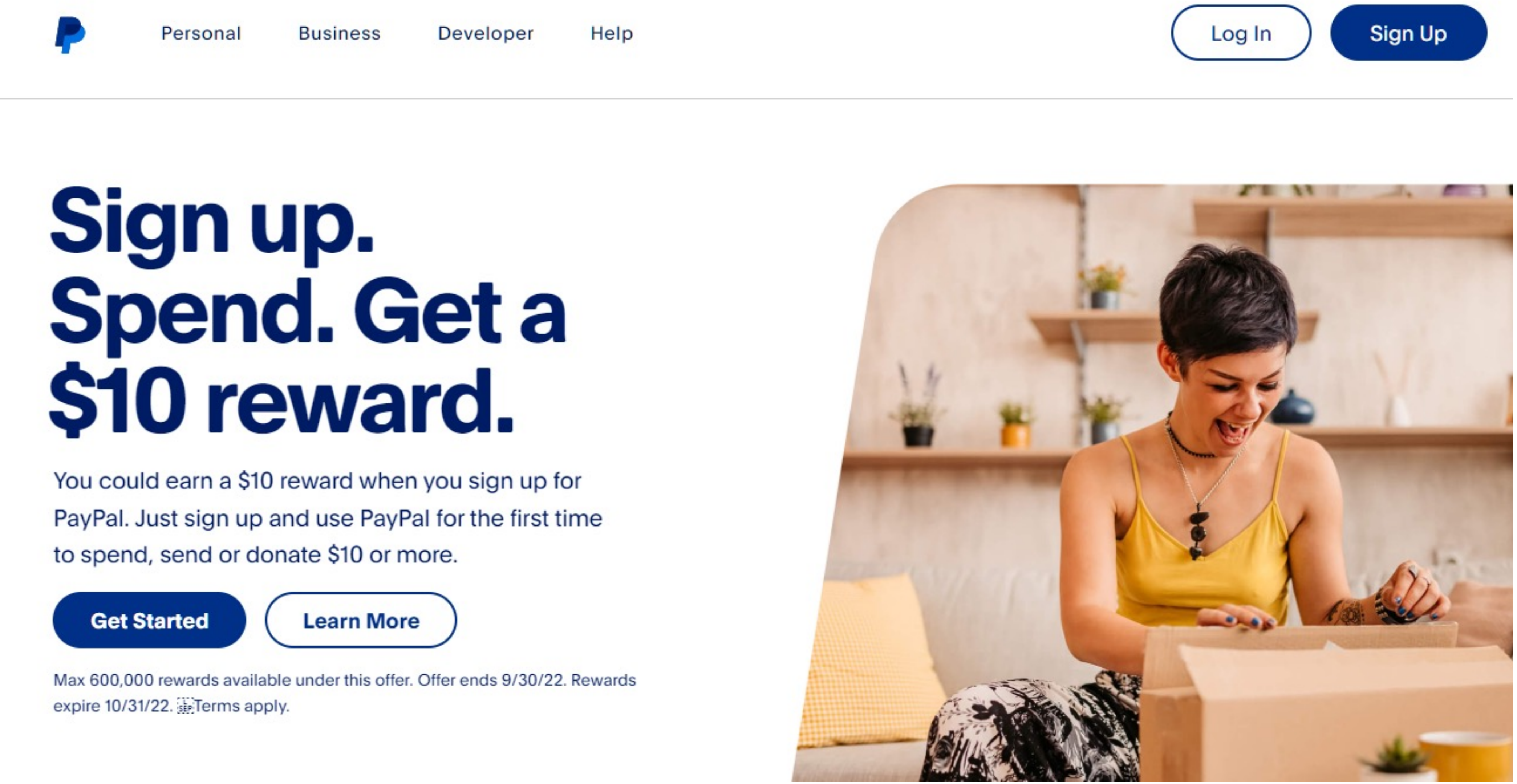
- Protocols (i.e. TCP/IP, HTTP, SMTP etc.) are introduced, and made the internet accessible to everyone in the world.

- 4G, 5G, SpaceX, smart phone, tablet…the internet has become part of our lives.

Case Study: the success of Taobao



Case study: the success of PayPal



Sign up. Spend. Get a $10 reward.

You could earn a $10 reward when you sign up for PayPal. Just sign up and use PayPal for the first time to spend, send or donate $10 or more.

Max 600,000 rewards available under this offer. Offer ends 9/30/22. Rewards expire 10/31/22. Terms apply.

Trust

- Intermediary trust

A third party is relied on to make rational and fair decisions.

- Issuance trust

A third party is relied on to ensure the safety and security of any value.

Before blockchain, several applications have tried to establish trust.

Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

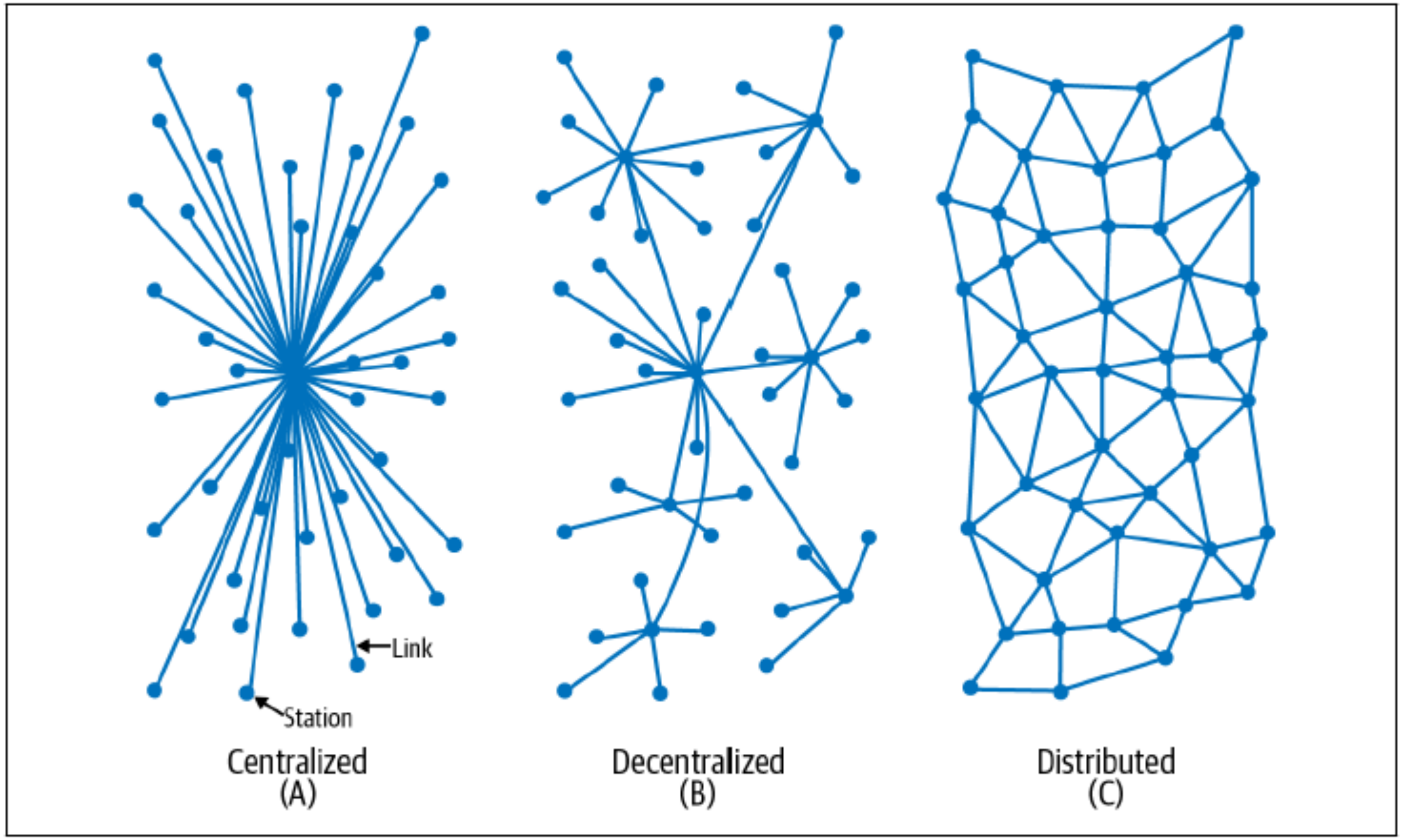
Distributed VS Centralized VS Decentralized

- In the early days, internet was designed as a distributed system to prevent single point of failure.

- Recently, big companies like Alibaba, Tencent, Google, and Amazon, etc. largely dominate the internet.

- Can we still go back?

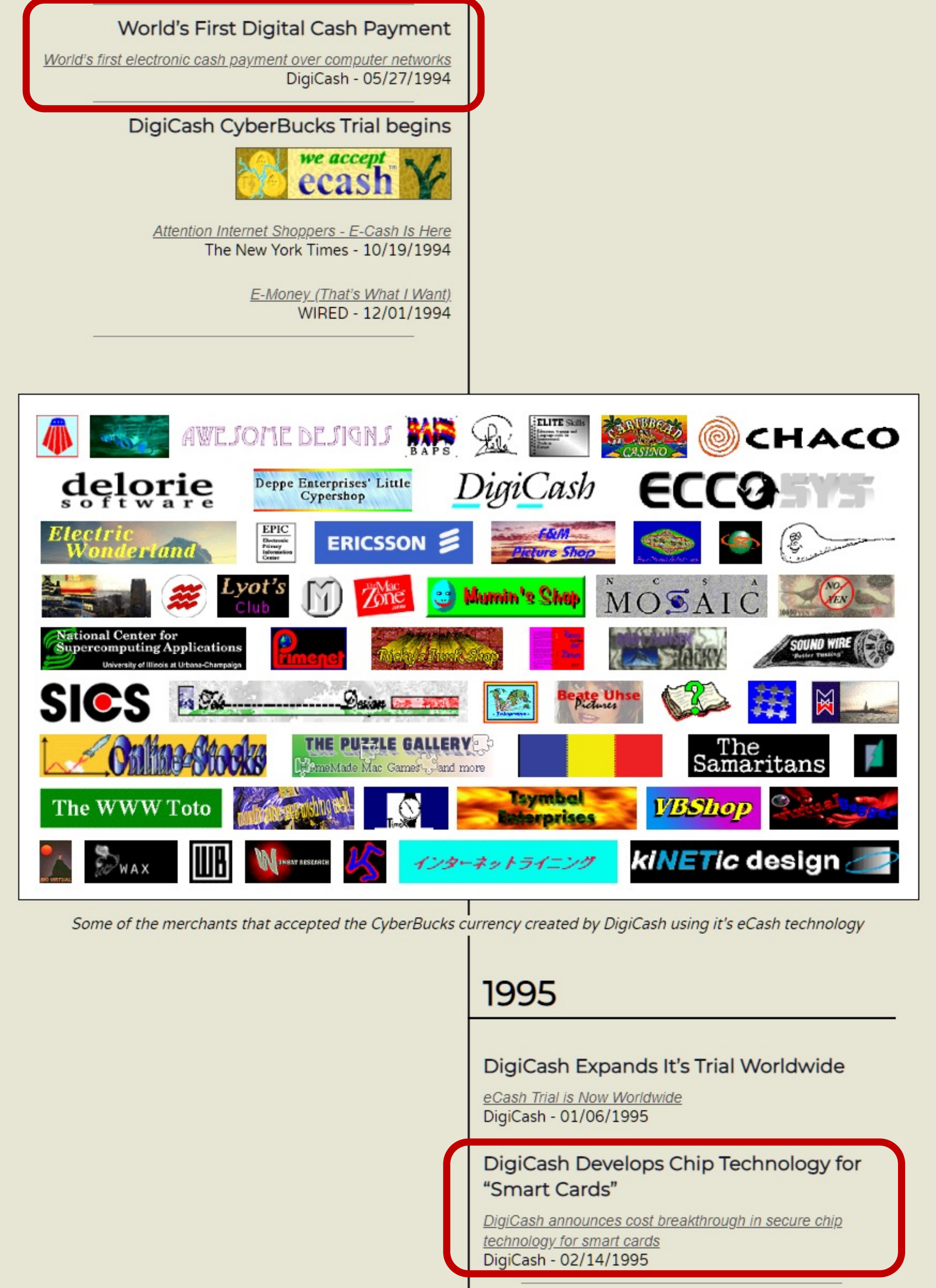
Illustration of different network types



Source: On Distributed Communications Networks, Paul Baran, 1962

DigiCash

- https://www.chaum.com/ecash
- Founded by David Chaum in 1994 based on his paper published in 1984, DigiCash facilitates anonymous digital payments online.
- Cyberbucks
- Secure microchipped smart card
- Lack of merchants, DigiCash filed for bankruptcy in 1998.



World's First Digital Cash Payment

World's first electronic cash payment over computer networks
DigiCash - 05/27/1994

DigiCash CyberBucks Trial begins

Attention Internet Shoppers - E-Cash Is Here
The New York Times - 10/19/1994

E-Money (That's What I Want)
WIRED - 12/01/1994

Some of the merchants that accepted the CyberBucks currency created by DigiCash using it's eCash technology

1995

DigiCash Expands It's Trial Worldwide

eCash Trial is Now Worldwide
DigiCash - 01/06/1995

DigiCash Develops Chip Technology for "Smart Cards"

DigiCash announces cost breakthrough in secure chip technology for smart cards
DigiCash - 02/14/1995

E-Gold

- https://en.wikipedia.org/wiki/E-gold
- Established in 1996, E-gold was backed by real units of precious metal.
- Micropayments: you can transact as small as one ten-thousandth of a gram of gold.
- E-Gold provides API to developers to build additional services on top of their platform.
- The US government shut down E-Gold.

Hashcash

- http://www.hashcash.org
- Invented by Adam Back in 1997
- Introduced the idea of using *proof-of-work* to verify the validity of digital funds
- This system is proposed to reduce email spam

B-Money

- http://www.weidai.com/bmoney.txt
- Introduced by Wei Dai in 1998
- Proposed the concept of nongovernmental money supply
- Advanced the idea of broadcasting transactions to a network
- Introduced the idea of using proof-of-work to create money
- B-Money is mainly a thought experiment

Bit Gold

- https://nakamotoinstitute.org/bit-gold/
- Proposed in 2005 by Nick Szabo
- Bit Gold wants to issue digital gold like E-gold
- A trustless version of E-gold
- Bit Gold is largely a thought experiment

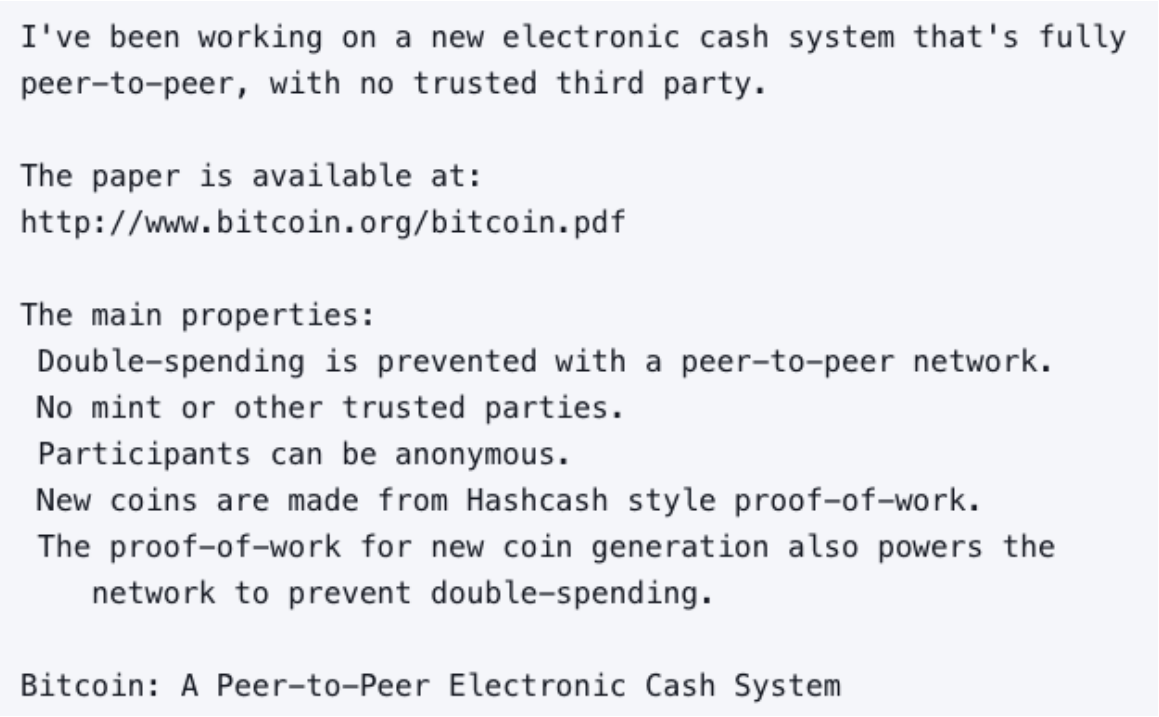
In 2008...

- Google Map, Baidu Map
- IM apps: MSN, QQ, Skype
- Amazon, Taobao
- Paypal, Alipay
- iPhone, Android Phone
- Financial Crisis

Bitcoin Intro

- In the Genesis block of bitcoin, Satoshi Nakamoto left a message,

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”



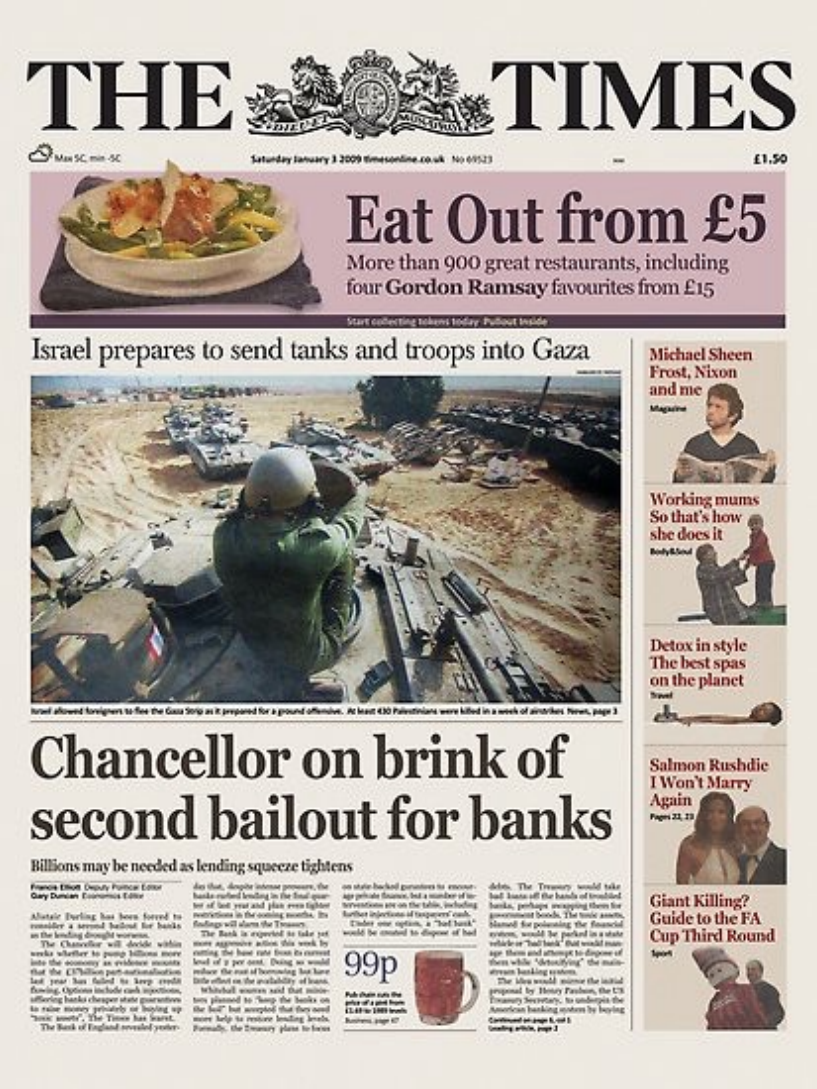
```
I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System
```

Source: https://www.bitcoin.com/satoshi-archive/emails/cryptography/1



THE TIMES

Max 5C, min -5C Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37 billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p
Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

Michael Sheen Frost, Nixon and me
Magazine

Working mums So that's how she does it
Body&Soul

Detox in style The best spas on the planet
Travel

Salmon Rushdie I Won't Marry Again
Pages 22, 23

Giant Killing? Guide to the FA Cup Third Round
Sport

Bitcoin Concepts

- **Double spending**

The risk that a unit of currency is spent more than one time.

- **Proof-of-work**

The solution to a mathematical problem. It is used as the consensus mechanism in bitcoin.

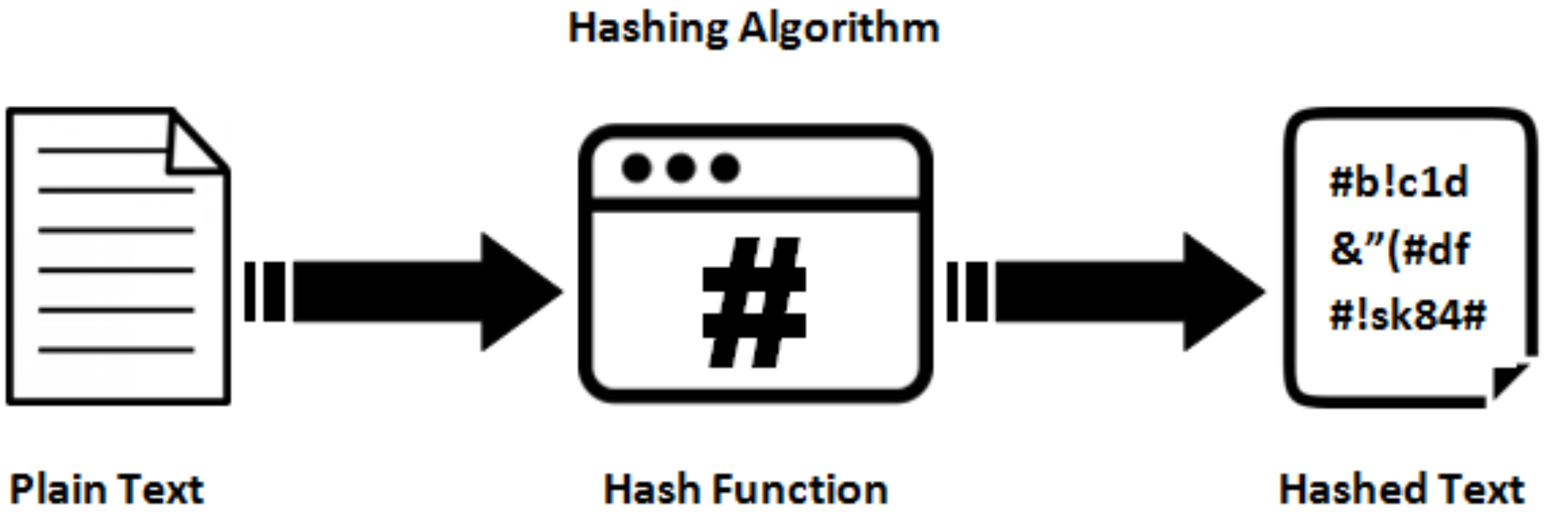
- **Nonces**

A random number used to meet the goal set by proof-of-work.

- **Hash function**

A hash function is any function that can be used to map data of arbitrary size to fixed-size values (called **hash**).

Hash Function



Plain Text: arbitrary length
Hashed Text: certain length (like 32 bytes)
SHA-256: https://www.movable-type.co.uk/scripts/sha256.html

Bitcoin Concepts

- **Block hash**

a unique identifier for a block

- **Transaction hash**

a unique identifier for a transaction

- **Coinbase transaction**

The first transaction in each block, and it is used to reward the miner who successfully minted/confirmed the block.

- **Block height number**

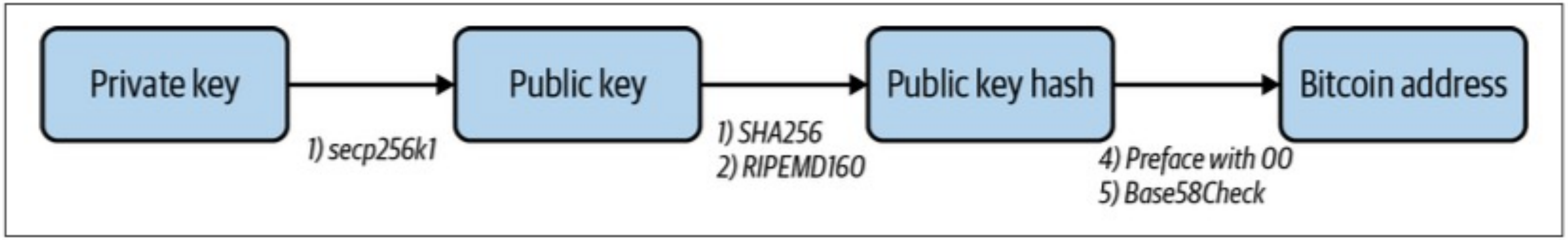
It measures the distance between the referred block and the first block.

- **UTXO**

Unspent Transaction Output

Public-key cryptography

- The system includes a pair of keys: public key and private key
- The cryptography is widely used and has been proved to be reliable, e.g. end-to-end encryption
- Private key is used to sign a transaction
- Public key is used to generate the bitcoin address



Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

Why Bitcoin took off?

- Open source

It is not proprietary, every one can check the code.

- Distribution

Use decentralized nodes to maintain the record of transactions.

- Consensus

Use Proof-of-Work to maintain the security of the bitcoin network.

- Right timing

The technology is ready, people are ready.

Part II: Cryptocurrency Fundamentals: Transactions

Bitcoin Transaction

- Transaction hash (transaction ID)

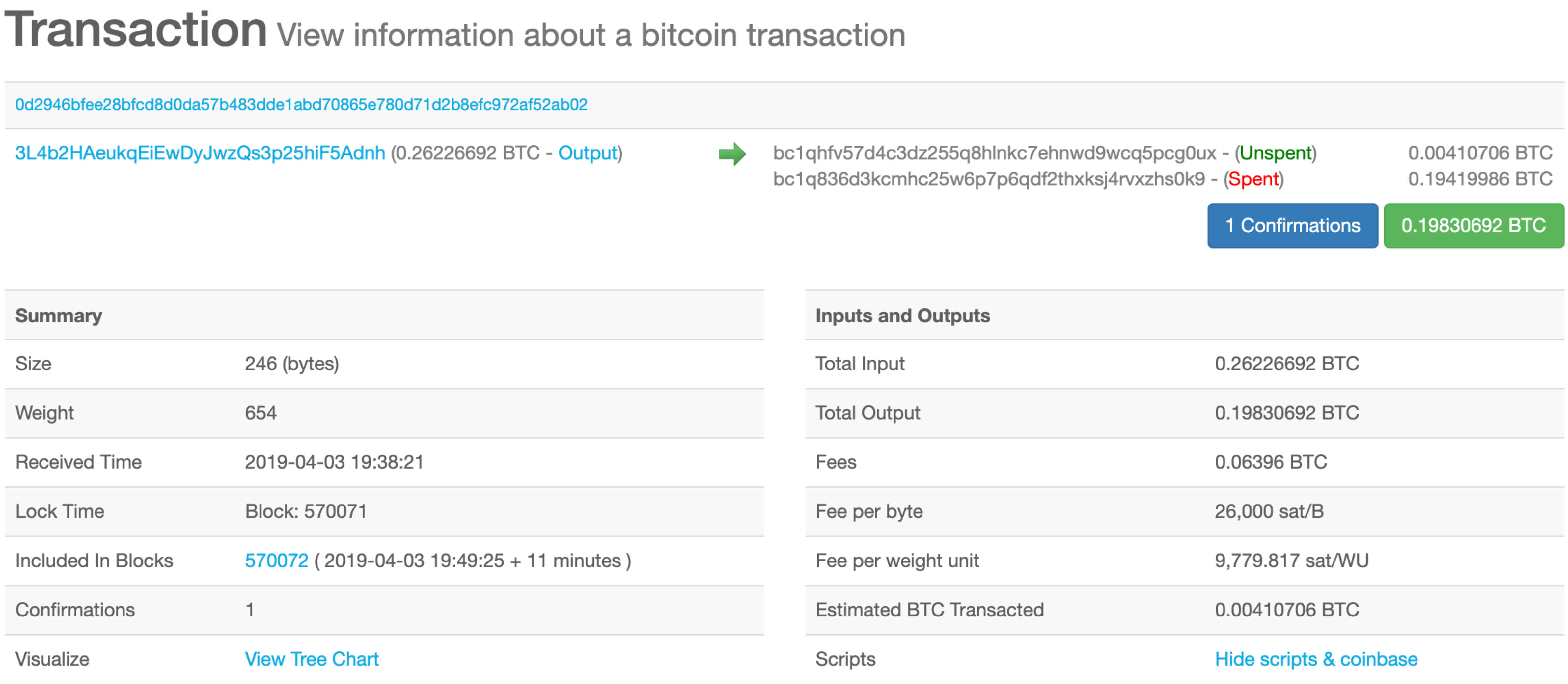
A transaction hash is a double-SHA256 hash of the serialized transaction:

```
01000000017b1eabe0209b1fe794124575ef807057c77ada213
8ae4fa8d6c4de0398a14f3f00000000494830450221008949f0
cb400094ad2b5eb399d59d01c14d73d8fe6e96df1a7150deb38
8ab8935022079656090d7f6bac4c9a94e0aad311a4268e082a7
25f8aeae0573fb12ff866a5f01ffffffff01f0ca052a0100000
01976a914cbc20a7664f2f69e5355aa427045bc15e7c6c77288
ac00000000
```

- Why double-hashing?

There are multiple double-hashing in bitcoin protocol. We don’t know why for sure, the most popular theory is to protect against length extension attacks.

Bitcoin Transaction



Transaction View information about a bitcoin transaction

0d2946bfee28bfcd8d0da57b483dde1abd70865e780d71d2b8efc972af52ab02

3L4b2HAeukqEiEwDyJwzQs3p25hiF5Adnh (0.26226692 BTC - Output) ➡

bc1qhfv57d4c3dz255q8hlnkc7ehnwd9wcq5pcg0ux - (Unspent) 0.00410706 BTC
bc1q836d3kcmhc25w6p7p6qdf2thxksj4rvxzhs0k9 - (Spent) 0.19419986 BTC

1 Confirmations | 0.19830692 BTC

Summary	
Size	246 (bytes)
Weight	654
Received Time	2019-04-03 19:38:21
Lock Time	Block: 570071
Included In Blocks	570072 (2019-04-03 19:49:25 + 11 minutes)
Confirmations	1
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.26226692 BTC
Total Output	0.19830692 BTC
Fees	0.06396 BTC
Fee per byte	26,000 sat/B
Fee per weight unit	9,779.817 sat/WU
Estimated BTC Transacted	0.00410706 BTC
Scripts	Hide scripts & coinbase

Source: www.blockchain.com

Bitcoin Transaction

- A bitcoin transaction

0d2946bfee28bfcd8d0da57b483dde1abd70865e780d71d2b8efc972af52ab02

- Blockchain explorer

https://www.blockchain.com/btc/tx/0d2946bfee28bfcd8d0da57b483dde1abd70865e780d71d2b8efc972af52ab02

Transaction Output

Transaction Output includes 3 elements:

(1) **Amount:** bitcoin value (in *satoshis*) sent to the receiver

(2) Locking-Script Size

(3) **Locking-Script:** it contains a public key or a bitcoin address (publickey hash)

1 BTC = 10^8 satoshis

UTXO

- **UTXO**: unspent transaction outputs.

- UTXO is indivisible. An UTXO can only be consumed in its entirety by a transaction.

- UTXO works like paper money.

- What will happen if I want to conduct a small transaction?

Transaction Input

Transaction Input includes 5 elements:

(1) **Transaction Hash:** pointer to the transaction that contains the UTXO

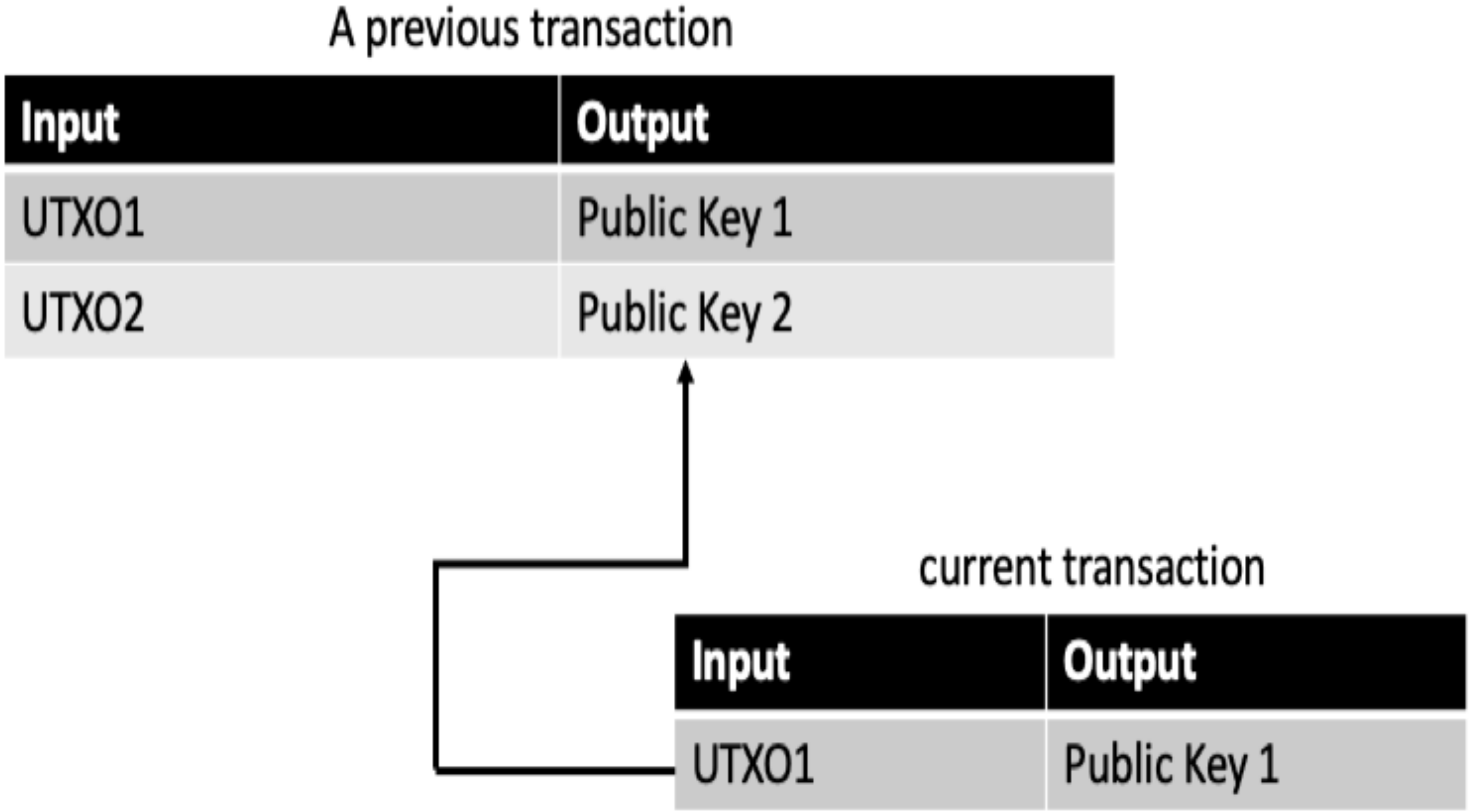
(2) **Output Index:** the index number of UTXO to be spent

(3) Unlocking-Script Size

(4) Unlocking-Script

(5) Sequence Number

Bitcoin Transactions



A previous transaction

Input	Output
UTXO1	Public Key 1
UTXO2	Public Key 2

current transaction

Input	Output
UTXO1	Public Key 1

Transaction Fees

- Transaction fees not only provide incentives to miners, but also serve as a security mechanism.

- Transaction fee is calculated based on the size of the transaction in kb, not the value of the transaction in bitcoins.

- What is the potential problem?

Transaction Fees

- Transaction fees are left by users, then collected by miners.

- When miners build their blocks, they select the transactions which have the highest reward-size ratio (RSR):

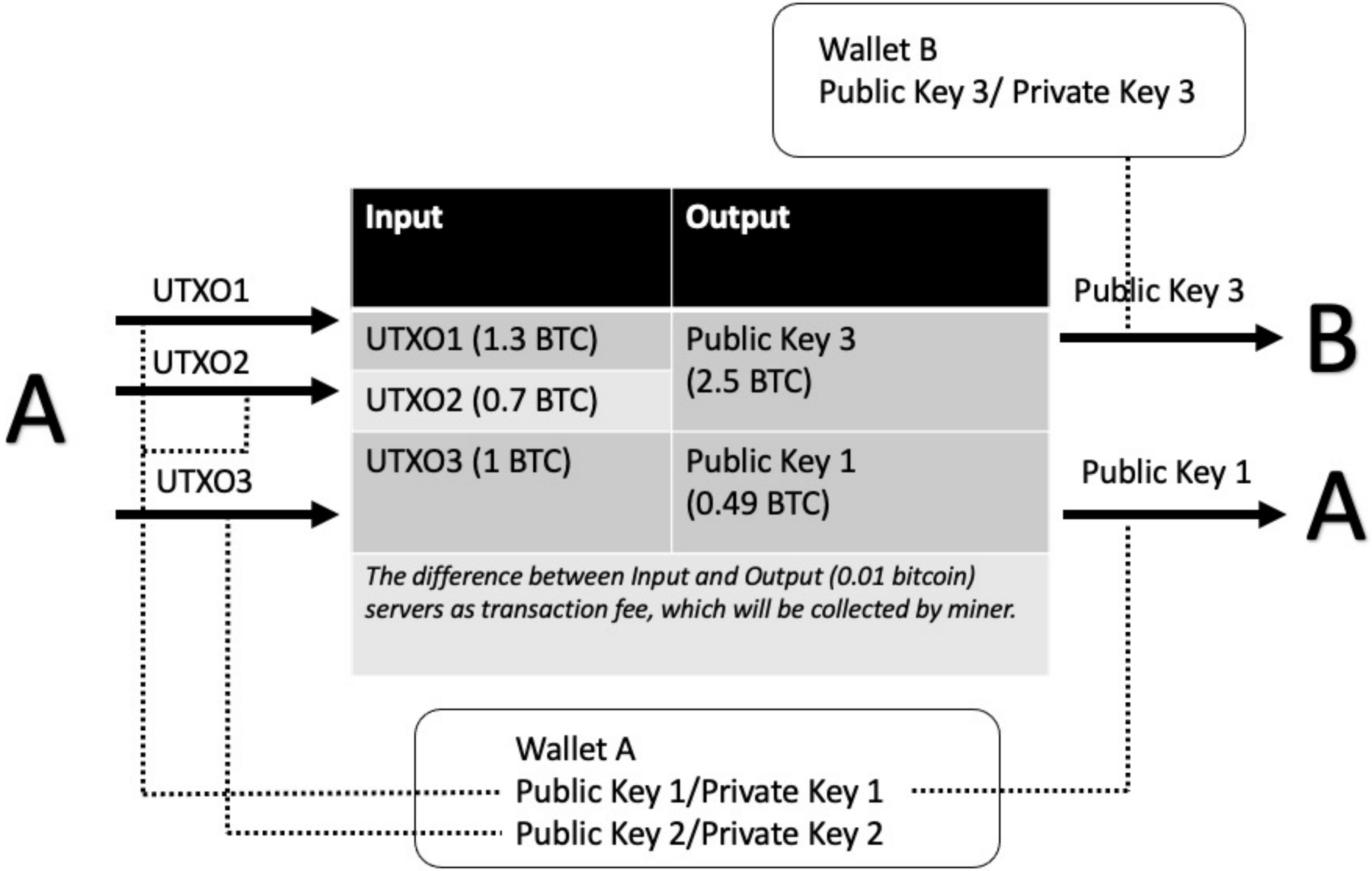
RSR = transaction fee paid in this transaction/the size of this transaction data

- Users make transaction decisions based on the ratio of transaction value to transaction fee (TFR):

TFR = transaction fee paid in this transaction/the value of this transaction

- The gap between the goals of miners and users is bridged by the bitcoin wallet.

Bitcoin Transactions



Wallet B
Public Key 3/ Private Key 3

A

UTXO1

UTXO2

UTXO3

Input	Output
UTXO1 (1.3 BTC)	Public Key 3 (2.5 BTC)
UTXO2 (0.7 BTC)	
UTXO3 (1 BTC)	Public Key 1 (0.49 BTC)

The difference between Input and Output (0.01 bitcoin) servers as transaction fee, which will be collected by miner.

Public Key 3

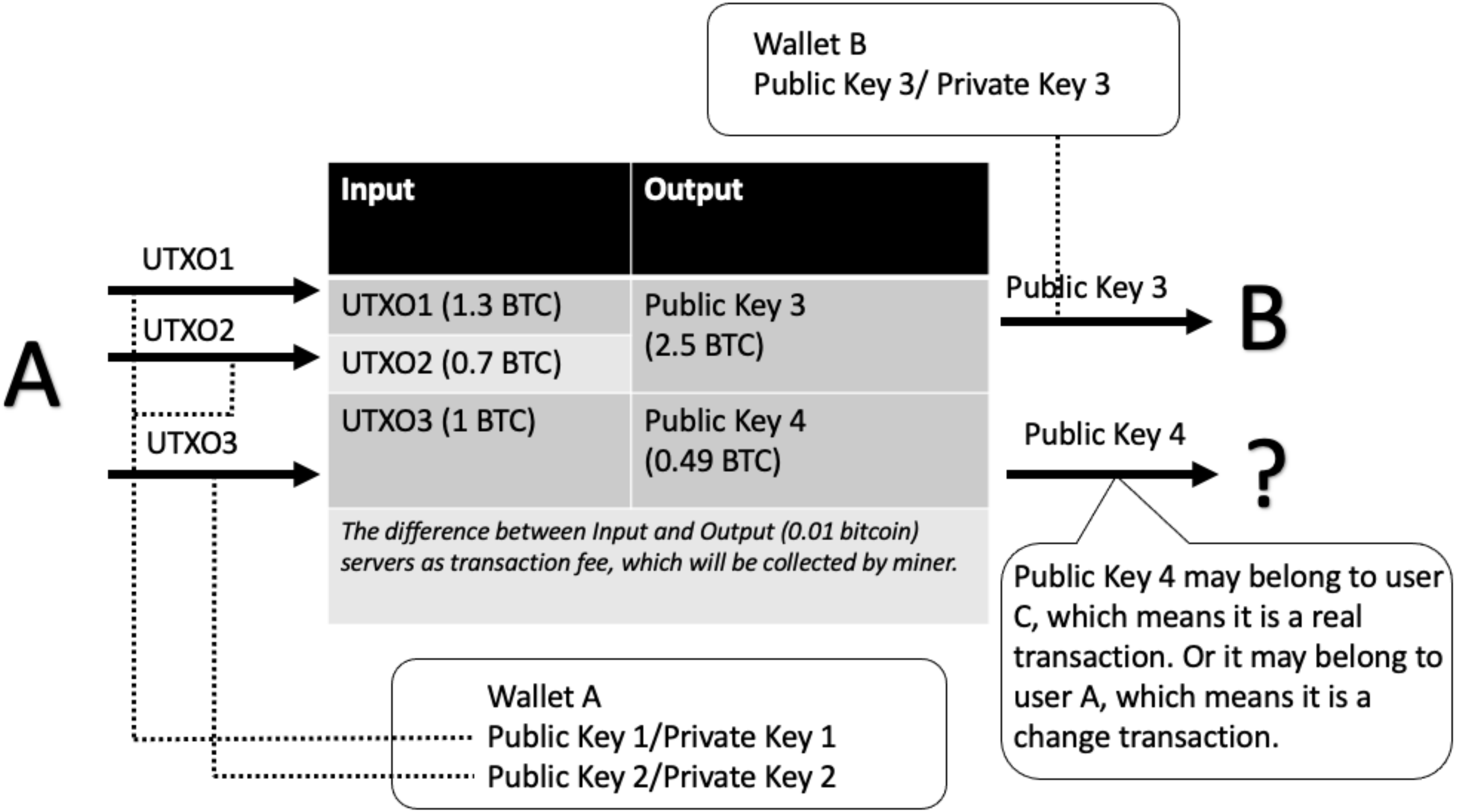
B

Public Key 1

A

Wallet A
Public Key 1/Private Key 1
Public Key 2/Private Key 2

Bitcoin Transaction



Wallet B
Public Key 3/ Private Key 3

Input	Output
UTXO1 (1.3 BTC)	Public Key 3 (2.5 BTC)
UTXO2 (0.7 BTC)	
UTXO3 (1 BTC)	Public Key 4 (0.49 BTC)

The difference between Input and Output (0.01 bitcoin) servers as transaction fee, which will be collected by miner.

Public Key 4 may belong to user C, which means it is a real transaction. Or it may belong to user A, which means it is a change transaction.

Wallet A
Public Key 1/Private Key 1
Public Key 2/Private Key 2

Transaction Scripts and Turing Incompleteness

- Turing Incompleteness

The bitcoin script language is intentionally designed to be Turing incomplete.

- Pay-to-Public-Key-Hash (P2PKH) script

An UTXO locked by P2PKH script can be unlocked (spent) by presenting the corresponding public key and a digital signature created by the corresponding private key.

- How does the digital signature work?

Elliptic Curve Digital Signature Algorithm

Transaction Scripts and Turing Incompleteness

- Pay-to-Script-Hash (P2SH) script

Companies may want to use multi-signatures to lock their bitcoin assets, and require at least two signatures to conduct a transaction.

(1) Complex script without P2SH:

Locking Script: 2 pk1 pk2 pk3 pk4 pk5 5 CHECHMULTISIG

Unlocking Script: sig1 sig2

(2) Complex script with P2SH:

Redeem Script: 2 pk1 pk2 pk3 pk4 pk5 5 CHECHMULTISIG

Locking Script: HASH160<20-byte hash of redeem script> EQUAL

Unlocking Script: sig1 sig2 <redeem script>

Source: Mastering Bitcoin, 2nd Edition, Andreas M. Antonopoulos

Part III: Cryptocurrency Fundamentals: Blockchain

Bitcoin Block

- Block

A block is defined as a storage unit which contain confirmed transaction data.

- Block header

A block header is part of a block, and it contains three sets of block metadata: (1) the location of last block, (2) metadata related to mining, (3) merkle tree root

Bitcoin Block

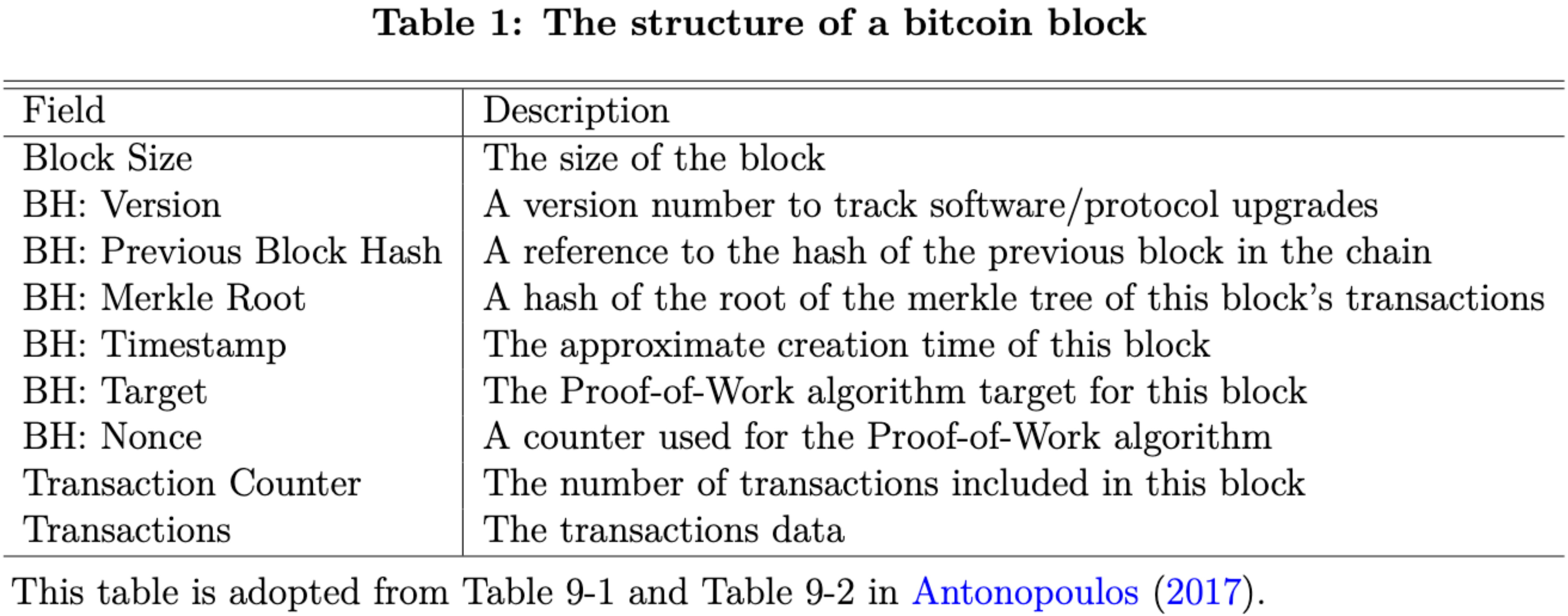


Table 1: The structure of a bitcoin block

Field	Description
Block Size	The size of the block
BH: Version	A version number to track software/protocol upgrades
BH: Previous Block Hash	A reference to the hash of the previous block in the chain
BH: Merkle Root	A hash of the root of the merkle tree of this block's transactions
BH: Timestamp	The approximate creation time of this block
BH: Target	The Proof-of-Work algorithm target for this block
BH: Nonce	A counter used for the Proof-of-Work algorithm
Transaction Counter	The number of transactions included in this block
Transactions	The transactions data

This table is adopted from Table 9-1 and Table 9-2 in Antonopoulos (2017).

Block ID: Block Hash & Block Height

- Block hash/ block header hash

Block hash is a 32-byte hash generated by hashing the **block header** twice using SHA256. More accurately, it should be called the block header hash.

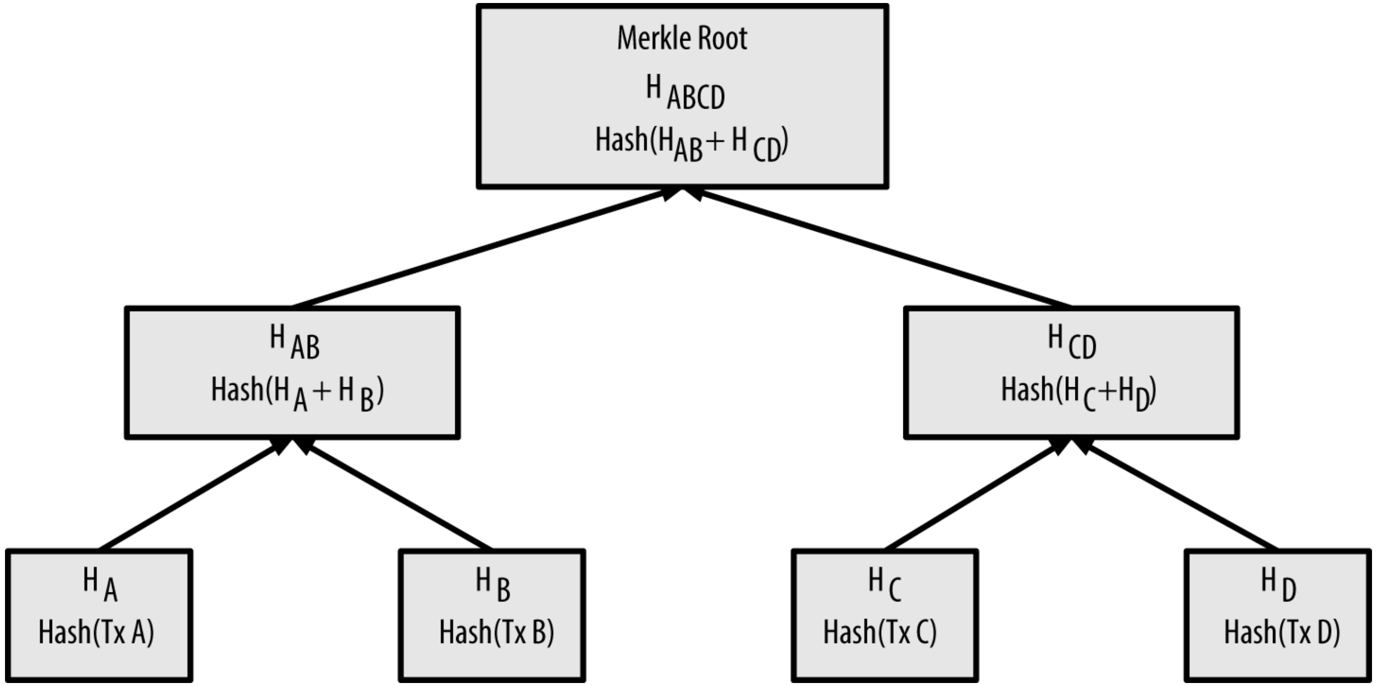
The block hash is **NOT** included in the block’s data structure. Miners calculate the block hash by themselves after receiving the block from the network.

- Block height

Block height measures the distance between the referred block and the first block.

Merkle Trees

- A merkle tree is a data structure used for efficiently summarizing and verifying the integrity of large sets of data.



Suppose we have 4 transactions: A, B, C, and D. They are the *leaves* of the merkle tree.

$$H_A = SHA256\big(SHA256(TX\ A)\big)$$
$$H_{AB} = SHA256\big(SHA256(H_A + H_B)\big)$$

Merkle Trees allow us to check if a transaction is included in the tree with at most $2 * \log_2(N)$, where N is the number of transactions.

Source: Mastering Bitcoin, 2nd Edition, Andreas M. Antonopoulos

Why Merkle Trees?

- Significantly reduce the computing power and storage requirement for nodes in the bitcoin network

- With merkle trees, a node only need:

(1) the block header (why?)

+

(2) a small merkle path downloaded from a full node

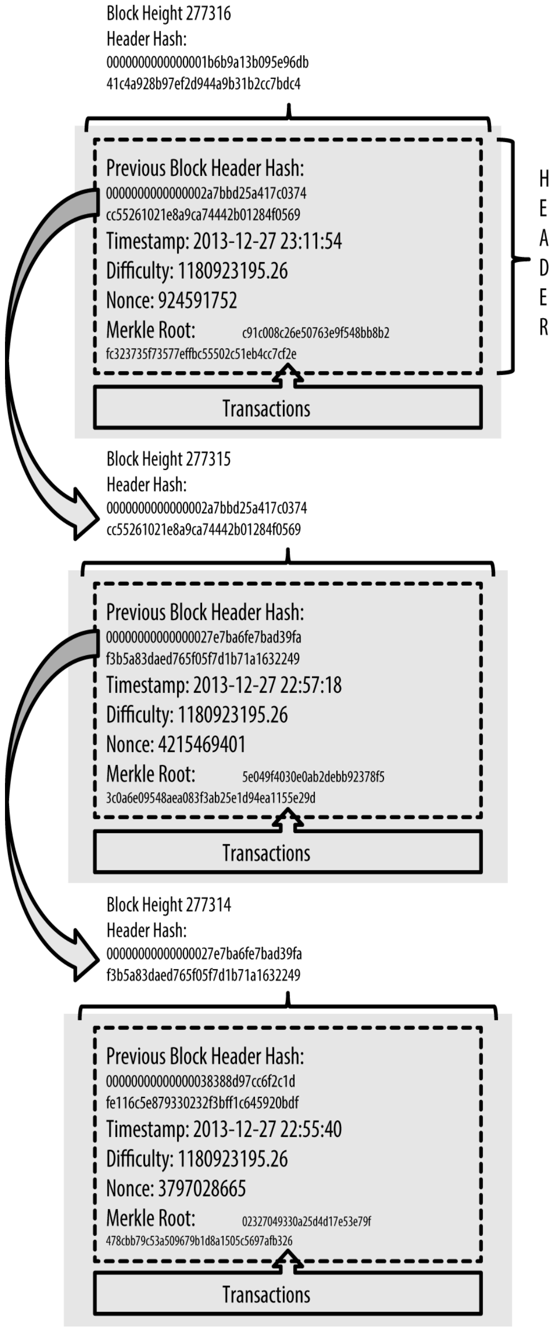
to verify if a transaction is included in a certain block.

Blockchain

- Block 277,314

```
{
   "size" : 43560,
   "version" : 2,
   "previousblockhash" :
      "000000000000000027e7ba6fe7bad39faf3b5a83daed765f05f7d1b71a1632249",
   "merkleroot" :
      "5e049f4030e0ab2debb92378f53c0a6e09548aea083f3ab25e1d94ea1155e29d",
   "time" : 1388185038,
   "difficulty" : 1180923195.25802612,
   "nonce" : 4215469401,
   "tx" : [
      "257e7497fb8bc68421eb2c7b699dbab234831600e7352f0d9e6522c7cf3f6c77",
 #[... many more transactions omitted ...]
      "05cfd38f6ae6aa83674cc99e4d75a1458c165b7ab84725eda41d018a09176634"
   ]
}
```

Blockchain



Block Height 277316
Header Hash:
00000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

HEADER

Previous Block Header Hash:
00000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e

Transactions

Block Height 277315
Header Hash:
00000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

Previous Block Header Hash:
000000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d

Transactions

Block Height 277314
Header Hash:
000000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249

Previous Block Header Hash:
0000000000000000038388d97cc6f2c1d
fe116c5e879330232f3bff1c645920bdf
Timestamp: 2013-12-27 22:55:40
Difficulty: 1180923195.26
Nonce: 3797028665
Merkle Root: 02327049330a25d4d17e53e79f
478cbb79c53a509679b1d8a1505c5697afb326

Transactions

Source: Mastering Bitcoin, 2nd Edition, Andreas M. Antonopoulos

Part IV: Cryptocurrency Fundamentals: Mining

What is mining?

- Block header hash:

00000000000000000000ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

- **Mining**

A process of hashing the block header repeatedly. In each time, the miner change the value of nonce a little bit until the block header hash satisfies the target set by the **Proof-of-Work** algorithm.

An example: https://www.blockchain.com/btc/block/570072

Coinbase Transactions

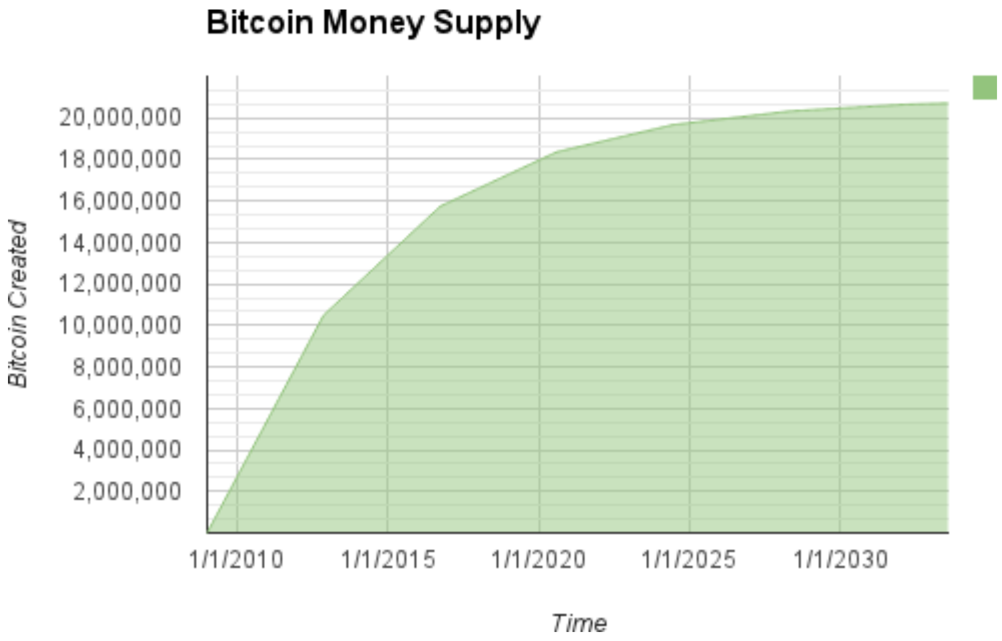
- Coinbase transactions are used to reward miners for confirming blocks.

Normal Transaction Input		Coinbase Transaction Input	
Field	Description	Field	Description
Transaction Hash	Point to the transaction that contains the UTXO	Transaction Hash	Set to zeros, not a real hash
Output Index	The index number of the UTXO	Output Index	Set to ones, not a real UTXO index
Unlocking-Script Size	Unlocking-Script length	Coinbase Data Size	Coinbase data size
Unlocking-Script	Script to unlock the UTXO	Coinbase Data	Arbitrary data used by miners*
Sequence Number	Set to 0xFFFFFFF	Sequence Number	Set to 0xFFFFFFF

*In V2 blocks, the Coinbase data must begin with block height
Source: Mastering Bitcoin, 2nd Edition, Andreas M. Antonopoulos

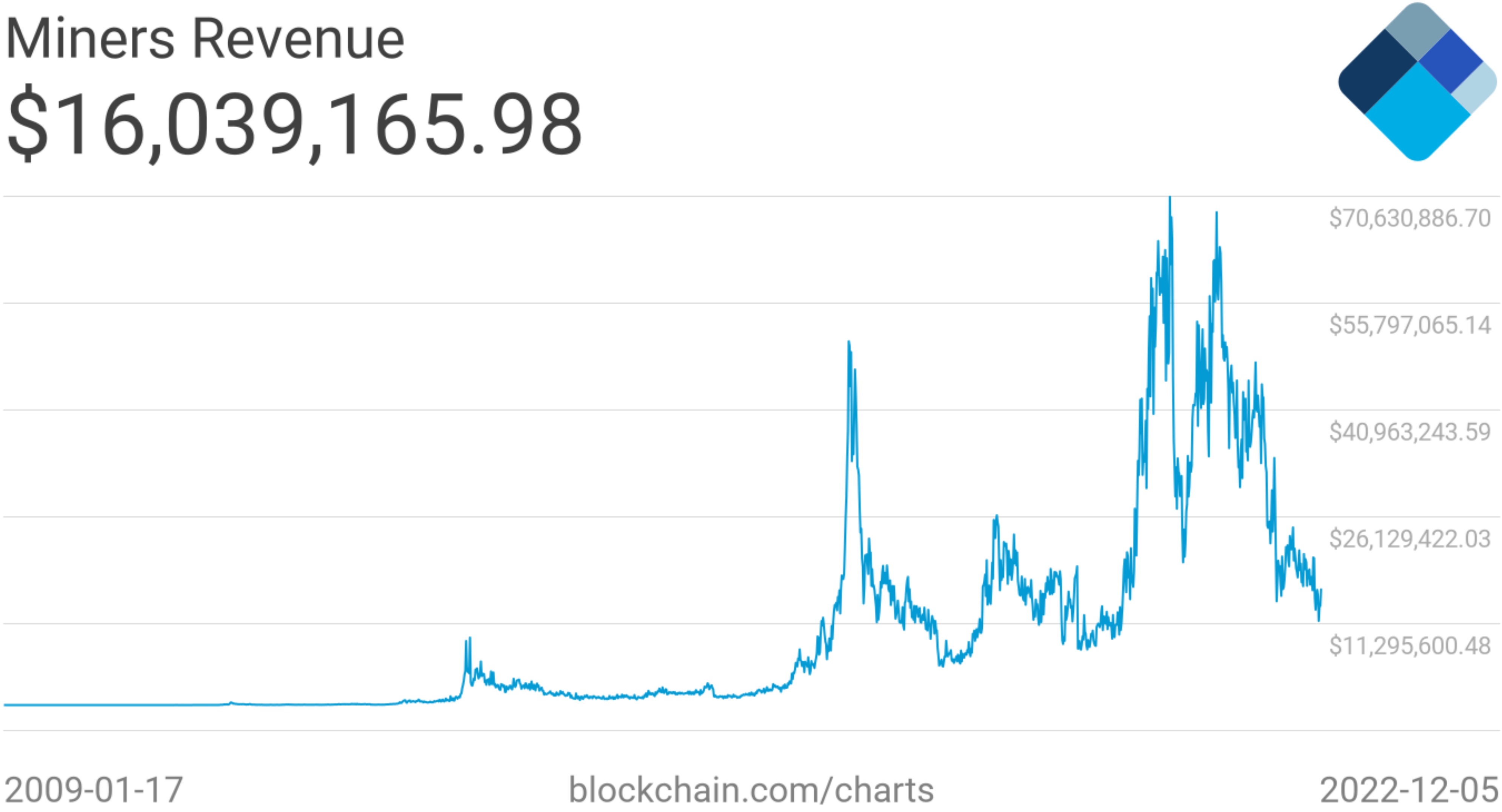
Bitcoin Mining Basics

- Bitcoin blocks are mined, on average, every 10 minutes.
- After every 210,000 blocks, coinbase reward is decreased by 50%. (initial: 50 btc, current: 6.25 btc)
- In approximately 2140, all the bitcoins will be issued.
- The total amount of bitcoin is around 21 million.



Source: Mastering Bitcoin, 2nd Edition, Andreas M. Antonopoulos

Mining is About Incentives



Miners Revenue

$16,039,165.98

Proof-of-Work

- Difficult to find the nonce, but easy to verify the finding
- Makes the blockchain almost immutable (with mining competition)
- Auto-adjustable, generates blocks, on average, every 10 minutes
- Adjustment not symmetric

Proof-of-Work: target & difficulty

- Block hash:

000000000000000000000ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

- Target

Target sets a number that must be greater or equal to the block hash in the new block. Otherwise, the new block is not valid.

- Difficulty

Intuitively speaking, difficulty equals to how many leading 0s in the target.

Bitcoin Block

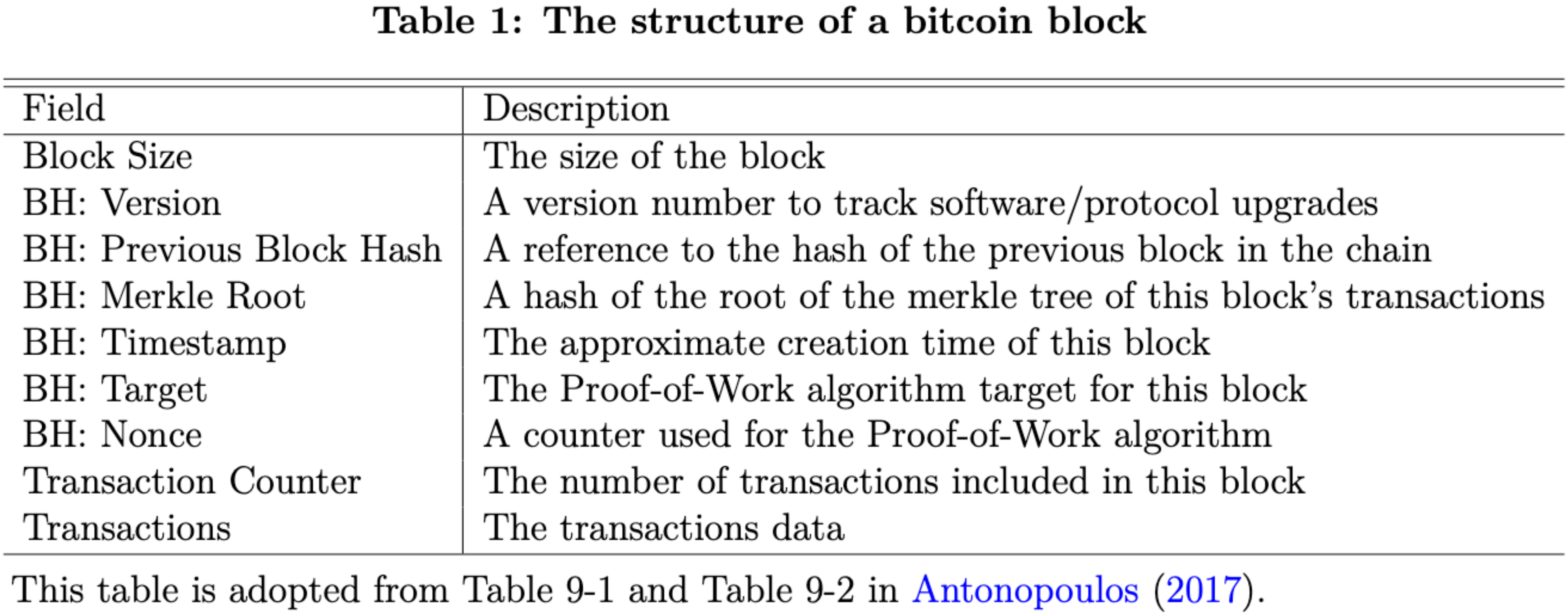


Table 1: The structure of a bitcoin block

Field	Description
Block Size	The size of the block
BH: Version	A version number to track software/protocol upgrades
BH: Previous Block Hash	A reference to the hash of the previous block in the chain
BH: Merkle Root	A hash of the root of the merkle tree of this block's transactions
BH: Timestamp	The approximate creation time of this block
BH: Target	The Proof-of-Work algorithm target for this block
BH: Nonce	A counter used for the Proof-of-Work algorithm
Transaction Counter	The number of transactions included in this block
Transactions	The transactions data

This table is adopted from Table 9-1 and Table 9-2 in Antonopoulos (2017).

Difficulty Adjustment

- Every 2016 blocks, all nodes retarget the Proof-of-Work

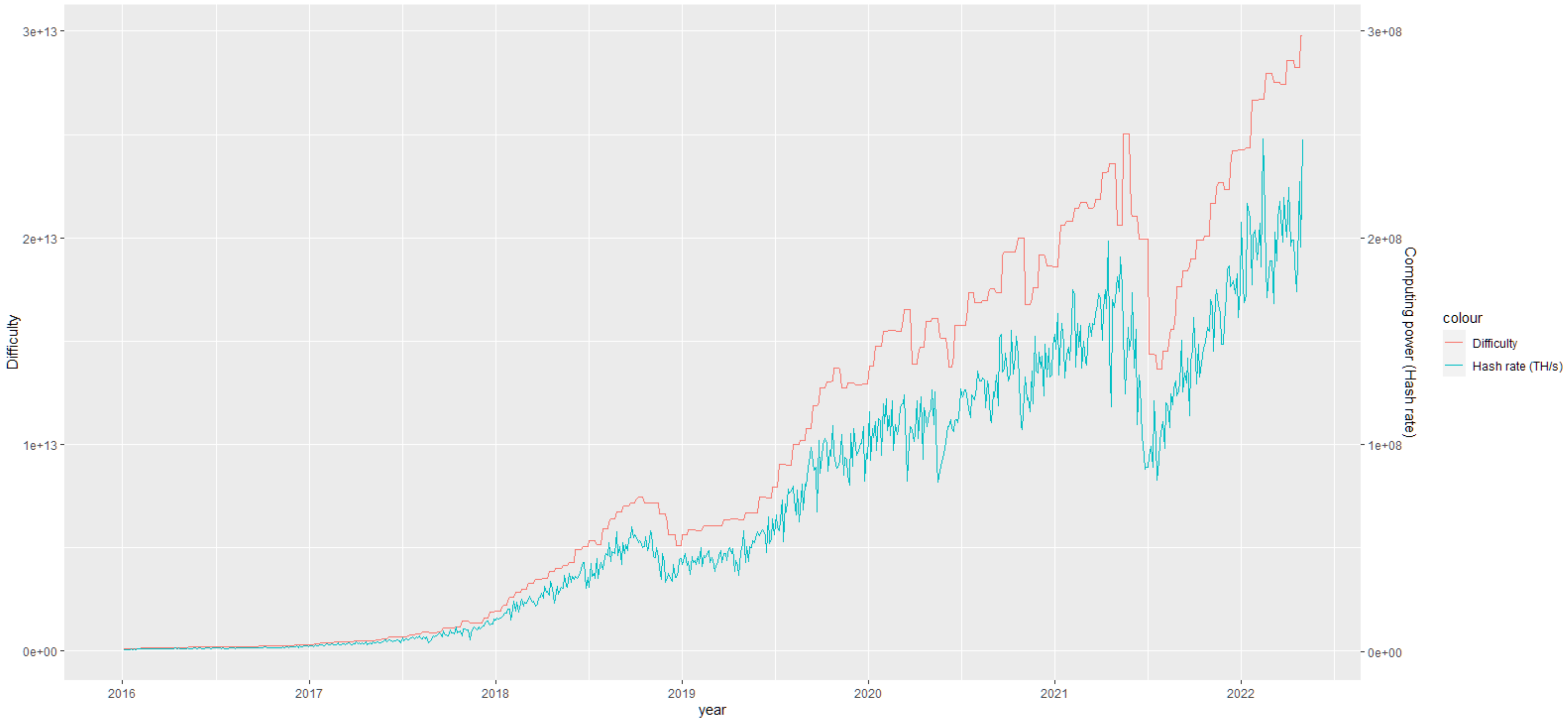
If actually time > 20160 minutes, reduce the difficulty

If actually time < 20160 minutes, increase the difficulty

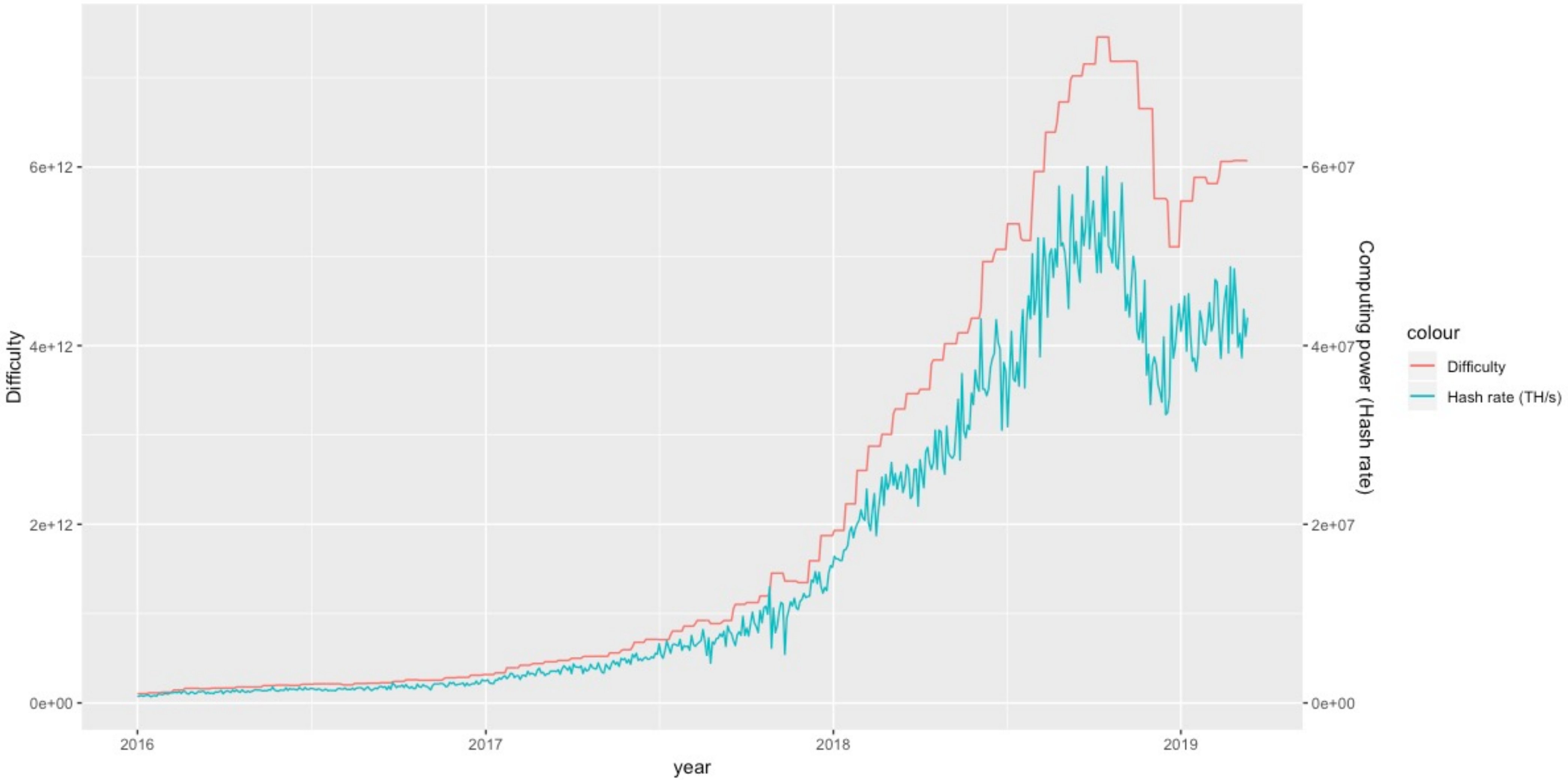
- Difficulty adjustment mechanism makes sure that block are mined, on average, every 10 minutes.

- Difficulty adjustment is asymmetrical.

Asymmetrical adjustment of difficulty



Asymmetrical adjustment of difficulty



Mining Pools & Mempools

- Mining Pools

Miners pool their hashing power together to mine a block and share the Coinbase reward.

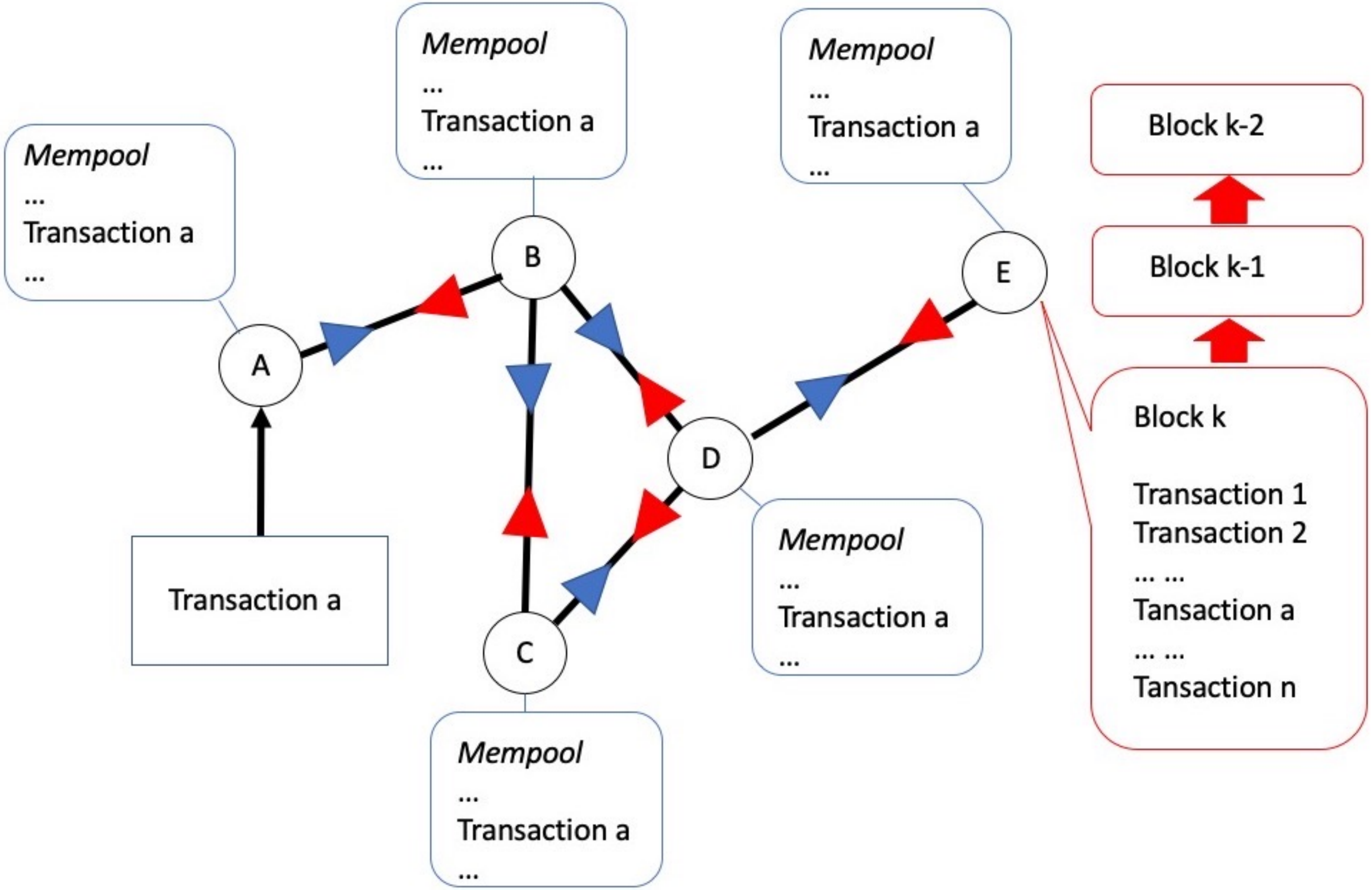
- Mempools

A mempool is where all unconfirmed transactions stay in the bitcoin network.

Mempools are maintained by miners themselves.

The Mempool size indicates how congested the bitcoin network is.

The procedure of transaction confirmation



Mempool
…
Transaction a
…

Mempool
…
Transaction a
…

Mempool
…
Transaction a
…

Block k-2

Block k-1

Block k

Transaction 1
Transaction 2
… …
Tansaction a
… …
Tansaction n

Mempool
…
Transaction a
…

Mempool
…
Transaction a
…

Transaction a

Part V: Cryptocurrency Fundamentals: Scaling Issue

Bitcoin Scaling Issue

- Bitcoin block size is restricted to 1 MB, and each block can at most contain around 2000 transactions. The transaction confirmation speed is inadequate for processing daily transactions.

- Solution 1: increase the block size
- Solution 2: remove some of the data out of blockchain and stored it in external files

- The majority of contentious hard forks are enacted because people want to choose different solutions.

Forks in Bitcoin Network

- Soft Fork

A soft fork is an upgrade to mining software that does not require all miners participate. The upgrade should be backwards compatible. How to implement a soft fork is documented in BIP9.

- Hark Fork

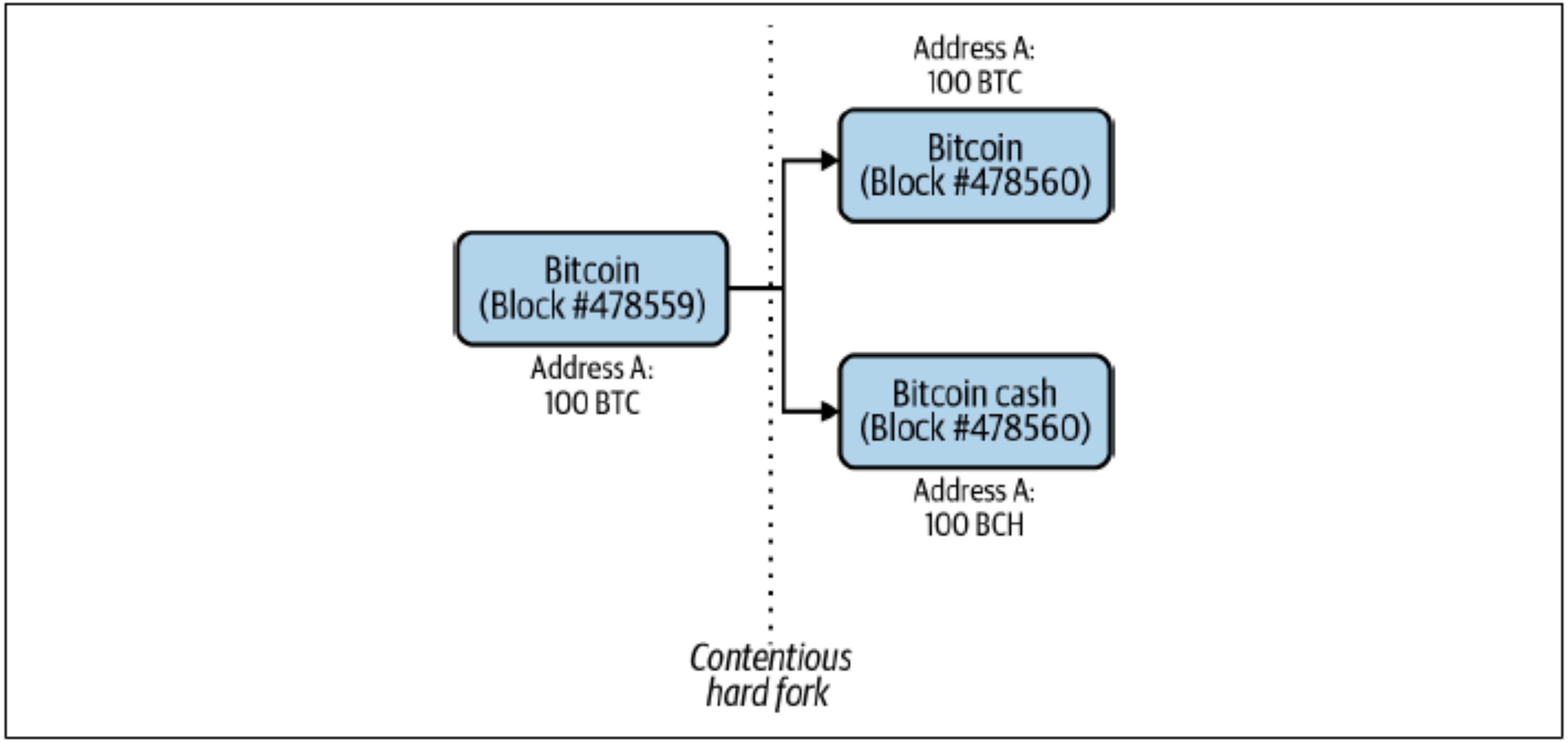
A hard fork is an upgrade to mining software that require the participation of all miners. The upgrade is not backwards compatible.

- Contentious Hard Fork

A hard fork when there is a disagreement within the bitcoin community.

Effects of Contentious Hard Forks

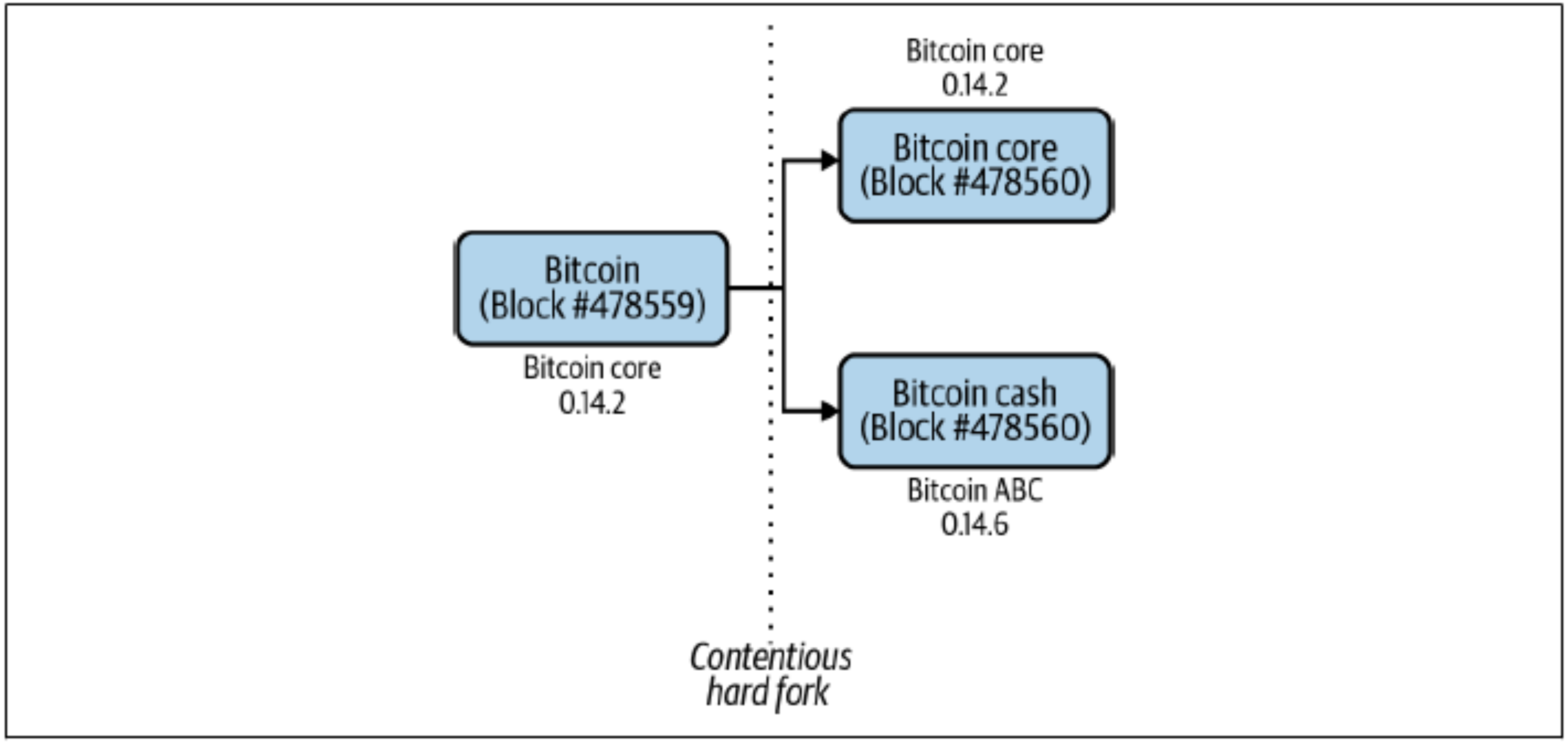
- Users



Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

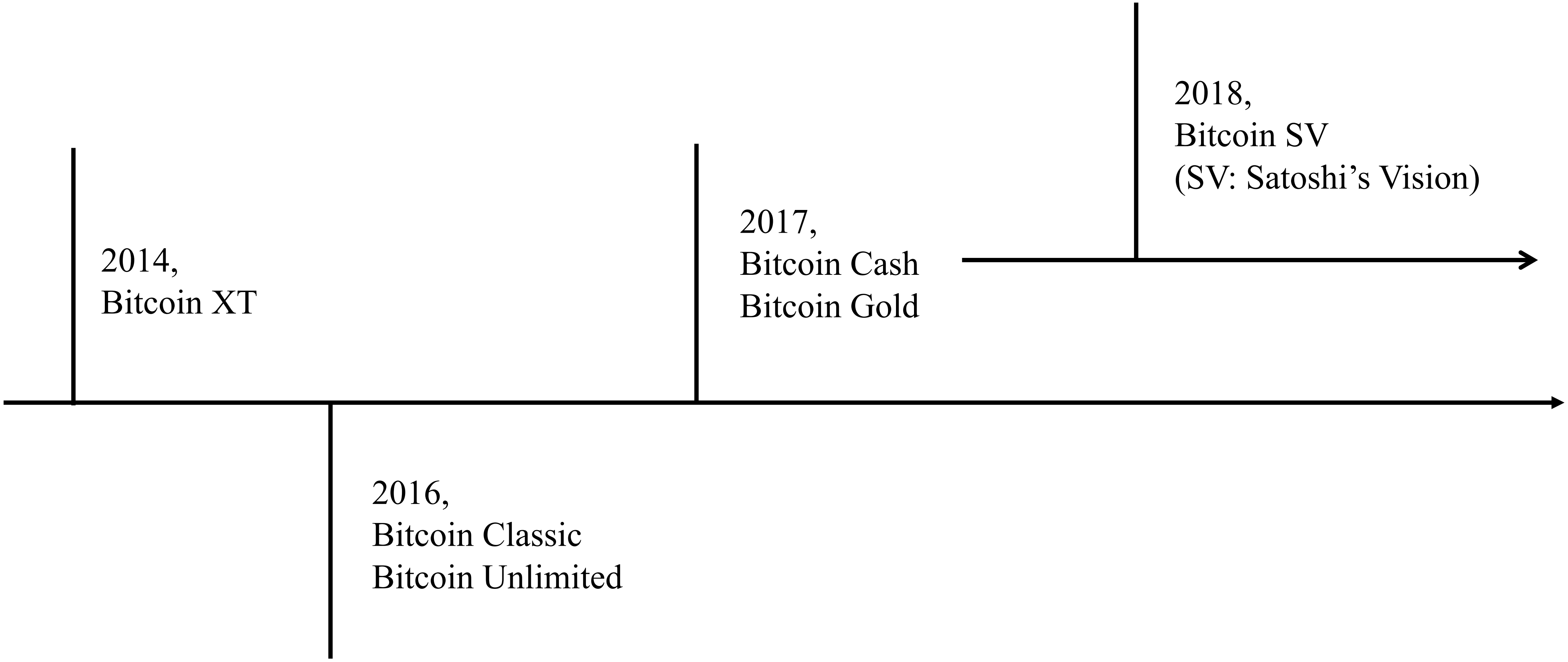
Effects of Contentious Hard Forks

- Miners



Source: Mastering Blockchain, Lorne Lantz & Daniel Cawrey

A History of Bitcoin Hard Forks



2014,
Bitcoin XT

2016,
Bitcoin Classic
Bitcoin Unlimited

2017,
Bitcoin Cash
Bitcoin Gold

2018,
Bitcoin SV
(SV: Satoshi’s Vision)

Source: Investopedia, Wikipedia

Bitcoin XT

In Jun 2014, Mike Hearn proposed BIP64, which is "*a small P2P protocol extension that performs UTXO lookups given a set of outpoints",* and created Bitcoin XT.

In Aug. 2015, BIP101 proposed by Gavin Andresen is implemented in Bitcoin XT. The main goal of BIP 101 is to increase the block size from 1 MB to 8 MB, and double the block size every two years. This is a controversial proposal and it failed eventually.

In Jan. 2016, BIP 101 was removed from Bitcoin XT and replaced with a one-time block size increase to 2 MB (BIP109). However, Bitcoin XT has lost popularity.

Bitcoin Classic

- In Jan. 2016, Gavin Andresen proposed to increase the block size to 2MB in BIP109. Then the project Bitcoin Classic is initialized.

- Bitcoin Classic has received support from some Bitcoin companies, developers, investors and miners. However, the wider bitcoin community did not think a hard fork is justified.

- The software's peak use was observed in early 2016 with a steady decline in usage from March 2016 onwards.

Bitcoin Unlimited

- https://www.bitcoinunlimited.info

- This project is not associated with a famous developer, it arose from a single thread on Bitcoin Talk known as "Gold Collapsing Bitcoin Up“.

- This project is inspired by BIP100, which suggests to *“replace the static base block size hard limit with a hard limit set by Coinbase vote, conducted on the same schedule as difficulty retargeting.”*

Bitcoin Cash

- https://bitcoincash.org

- Bitcoin Cash was launched by the Chinese mining pool ViaBTC.

- The Bitcoin Cash hard fork took place on August 1, 2017, after block 478558

- Bitcoin Cash increased the block size to 8 MB, then further increased it to 32 MB in May 2018.

Bitcoin SV

- https://bitcoinsv.com

- Bitcoin SV stands for Bitcoin Satoshi Vision, and it was created after a hard ford of the Bitcoin Cash project in November 2018.

- This project is leaded by Craig Wright, who claims to be Satoshi Nakamoto, although there's little evidence to support this assertion.

- Initially, the block size is 128 MB, then it is increased to 2 GB in July 2019, and infinity in February 2020.

- Why do we care about block size?

Bitcoin Gold

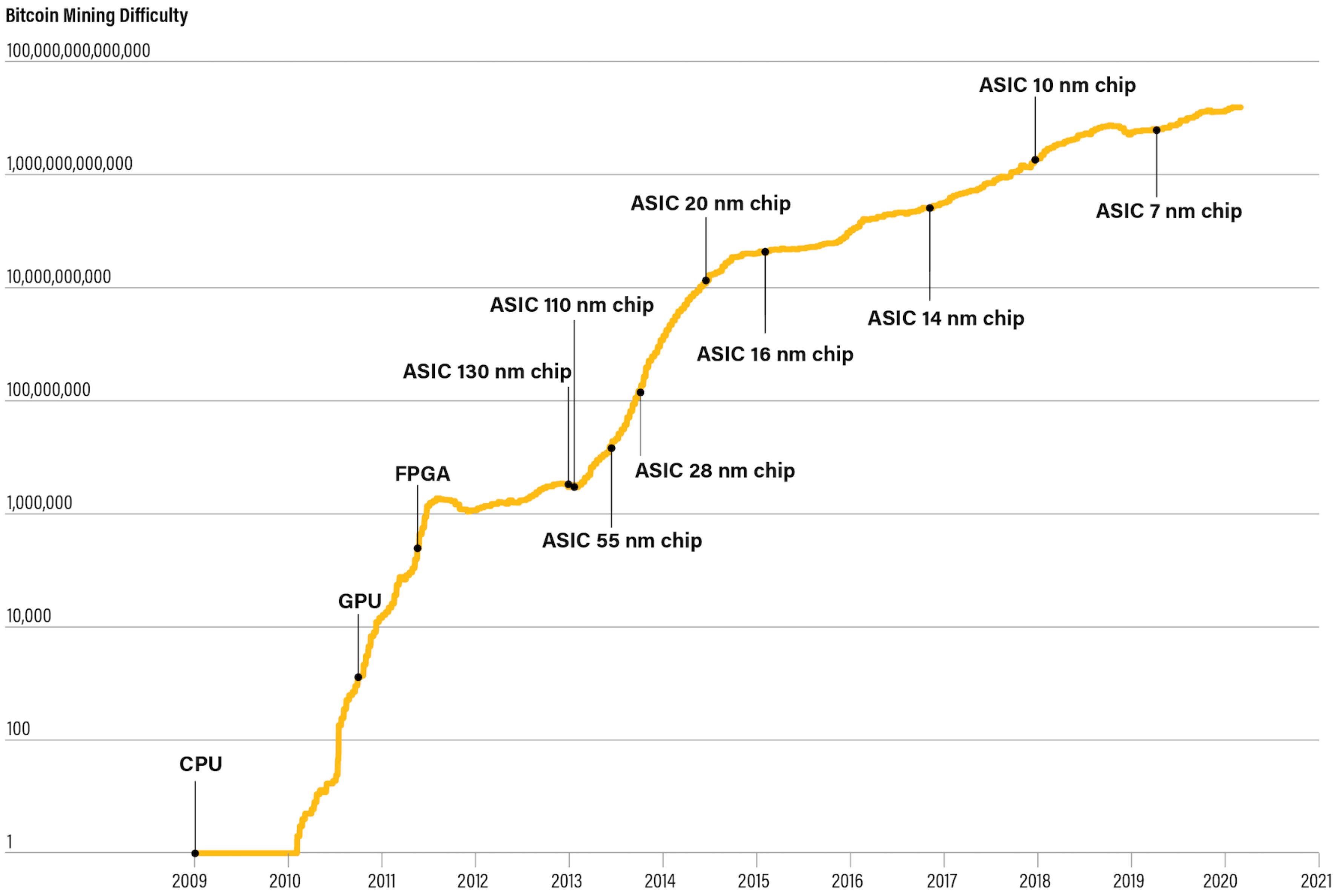
- https://bitcoingold.org

- The Bitcoin Gold fork from the original Bitcoin blockchain took place on October 24, 2017 at block height 491407.

- Bitcoin Gold modified the mining algorithm (Equihash, a memory-hard Proof-of-Work algorithm) to make it ASIC-resistant.

- Why do we care about being ASIC-resistant?

Bitcoin Mining Equipment Evolution



Source: CoinDesk

Altcoins

Altcoin is used to referee to all cryptocurrencies except bitcoin. Some famous altcoins are:

- Ether

Ether is the coin used on Ethereum platform, it the second largest cryptocurrency in the world.

- Litecoin

One of the first altcoins, released in 2011. The block time was set to be four times faster than bitcoin’s. The algorithm is ASIC-resistant.

- Dogecoin

Released in 2013, dogecoin was originally created out of a joke, and it got popularized by Elon Musk in 2021.

Part VI: Cryptocurrency Fundamentals: Consensus

Consensus Algorithm

Consensus: a voting protocol for making decisions.

- Proof-based consensus

Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), etc.

- Voting-based consensus

Practical Byzantine Fault Tolerance

Extra: Byzantine Generals Problem

Suppose a group of generals have besieged a city and they have to agree on either attaching or retreating. Generals can only communicate through messages, then they have a communication problem:

(1) Messages can get delayed, destroyed or lost

(2) One or more generals may act maliciously and send out fraudulent messages.

Think of these generals as nodes in the blockchain system, then we still need to solve this Byzantine Generals Problem in nowadays.

Extra: Byzantine Fault Tolerance

- Byzantine Fault Tolerance is a system's ability to continue operating even if some of its nodes fail or act maliciously.
- The consensus algorithm is how a permissioned blockchain achieves Byzantine Fault Tolerance.
- Byzantine Fault Tolerance Intro

Proof-of-Work

- Allocate the validation rights through the hashing power competition
- PoW takes the workload as the safeguard.
- PoW is susceptible to 51% attack.
- PoW wastes a lot of computing power and natural resources.

Consensus Attack -- Proof of Work

- 51% Attack

If one entity controls a majority (51%) of the total network's hashing power, it has the ability to invalidate confirmed blocks and double-spend its own transactions.

Solution: wait longer to confirm your transaction

- Deny Service Attack

An attacker with a majority of the mining power can simply ignore specific transactions, for example transactions that involve a certain address.

Proof-of-Stake

PoS algorithms use several methods to select who will validate the next block:

(1) The size of the stake

The more tokens staked, the higher the chance of being chosen to validate.

(2) The age of the tokens staked

The longer the tokens have been unspent, the higher the chance of being chosen to validate. Once that stake is used to verify a block, its age is reset to zero.

(3) Random Selection

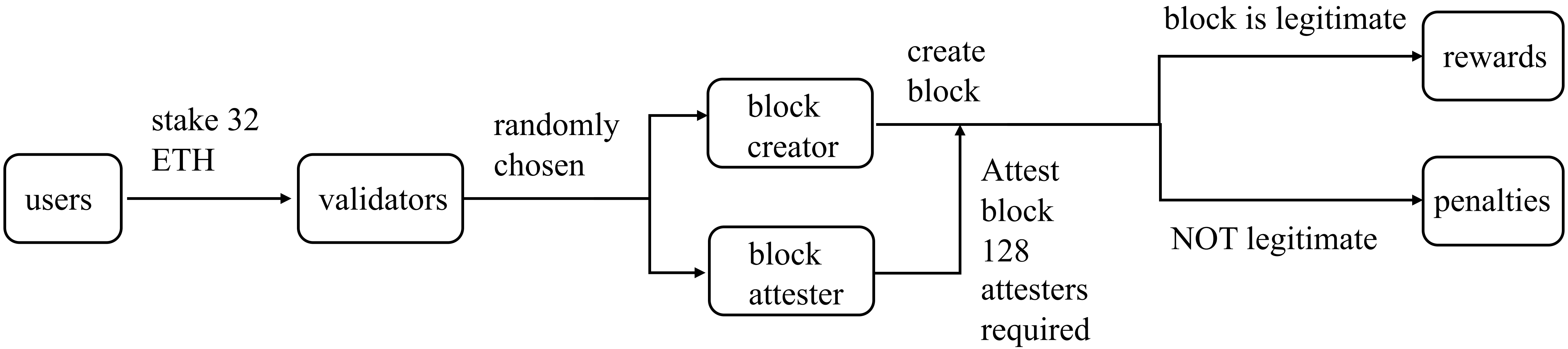
Proof-of-Stake in Ethereum 2.0

- Shard chain: mainly addresses the scalability concern. There are 64 shard chains in the Ethereum network.

- Beacon chain: coordinates the information between different shard chains and manages validators.

- Validator: the nodes in the Ethereum network who want to confirm transactions. Users need to stake 32 ETH to become validators.

Proof-of-Stake in Ethereum 2.0



Source: Ethereum Whitepaper

Proof-of-Stake in Ethereum 2.0

(1) Pros

- Better energy efficiency
- Lower barriers to entry (hardware requirement is low)
- Stronger immunity to centralization

(2) Cons

Compared with Proof-of-Work, Proof-of-Stake is less battle-tested in the real world.

Q: Does 51% attack still exist in proof-of-stake?

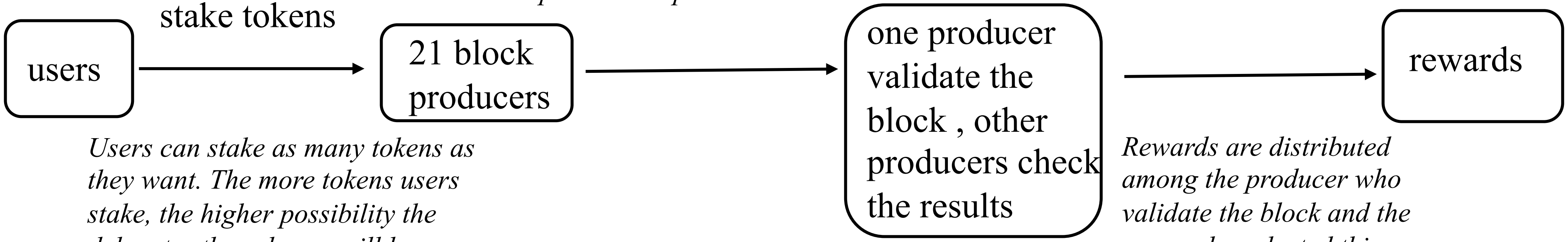
Delegated Proof of Stake

- In DPoS, users do not directly become validators, they vote for delegates to become validators.

- Users vote on delegates by pooling their tokens into a staking pool and linking those tokens to a particular delegate.

- These delegates are usually called as witnesses or block producers.

Delegated Proof of Stake in EOS



users
stake tokens
21 block producers
one producer validate the block , other producers check the results
rewards

These 21 producers produce 12 contiguous blocks per person in alphabetical order.

Users can stake as many tokens as they want. The more tokens users stake, the higher possibility the delegates they chosen will become producers. The top 21 proposed delegates will become block producers.

Rewards are distributed among the producer who validate the block and the users who selected this producer.

Resource: [EOS Whitepaper]()

Proof-based or Voting-based consensus?

- Proof-based consensuses are widely used in **permissionless** networks. There is no control on the nodes. Nodes can join or leave the network as their wish.

- Voting-based consensuses are usually used in **permissioned** networks. In a permissioned network, all the nodes are identified, and the designer knows how many validators at most can be compromised.

- Proof-based consensuses are less efficient than voting-based consensuses.