Frontier of Technology and Economics II

Zichao Yang
Wenlan School of Business
Website：www.yzc.me

Roadmap

- Lectures on different topics

  Guest speakers to talk about the development in their research fields.

- Presentation: present one of assigned papers

  Presentations are scheduled on **Jun 3rd, Jun 10th** and **17th** , 90 minutes per person, slides should be written in English.

  Please send me the name of your paper before **May 13th**.

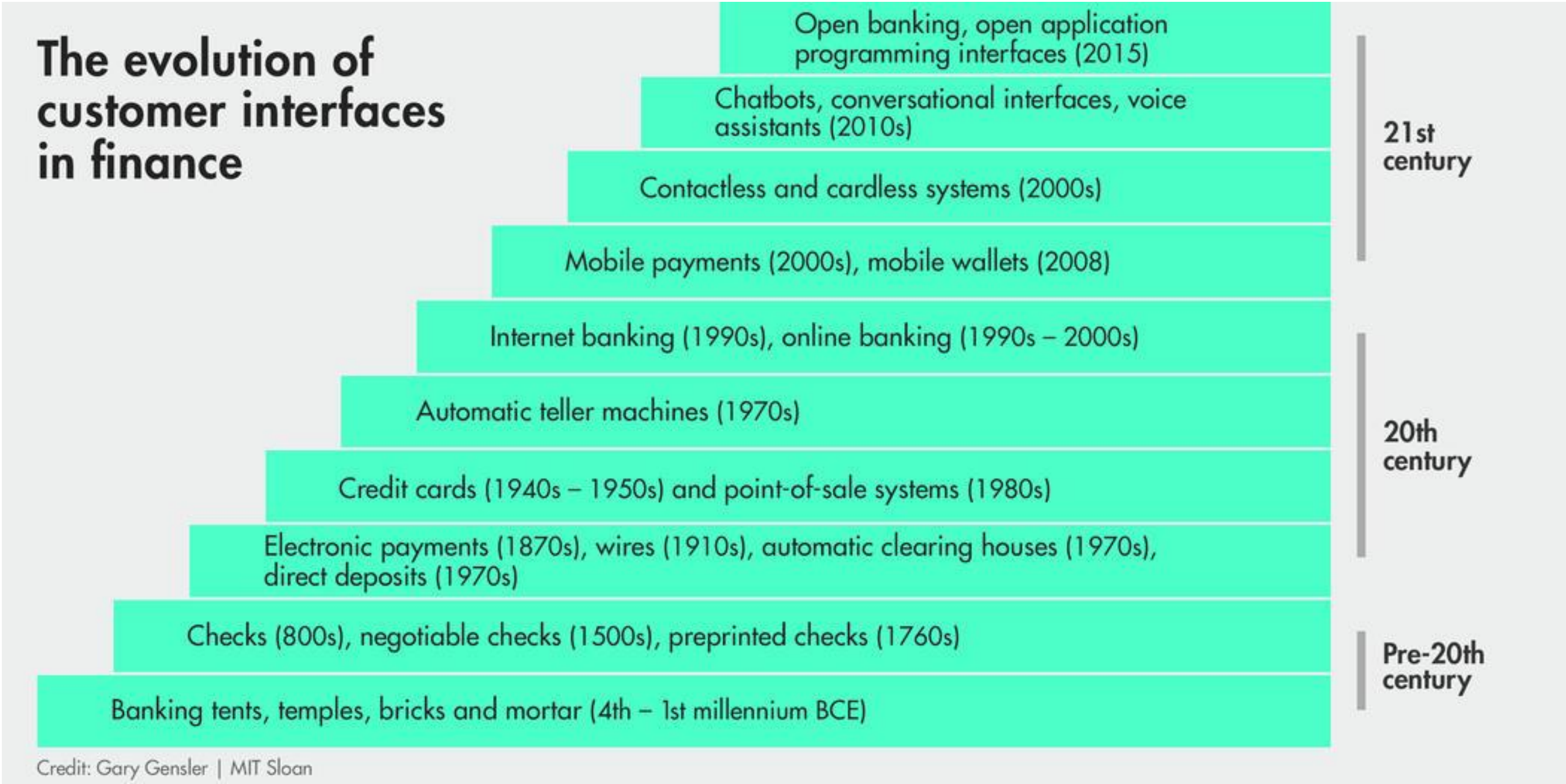
- Referee report: write a referee report for another assigned paper

  Write a referee report for one of the papers presented by your classmates. 2-4 pages, 1.5 line space, font: Times New Roman, font size: 12.

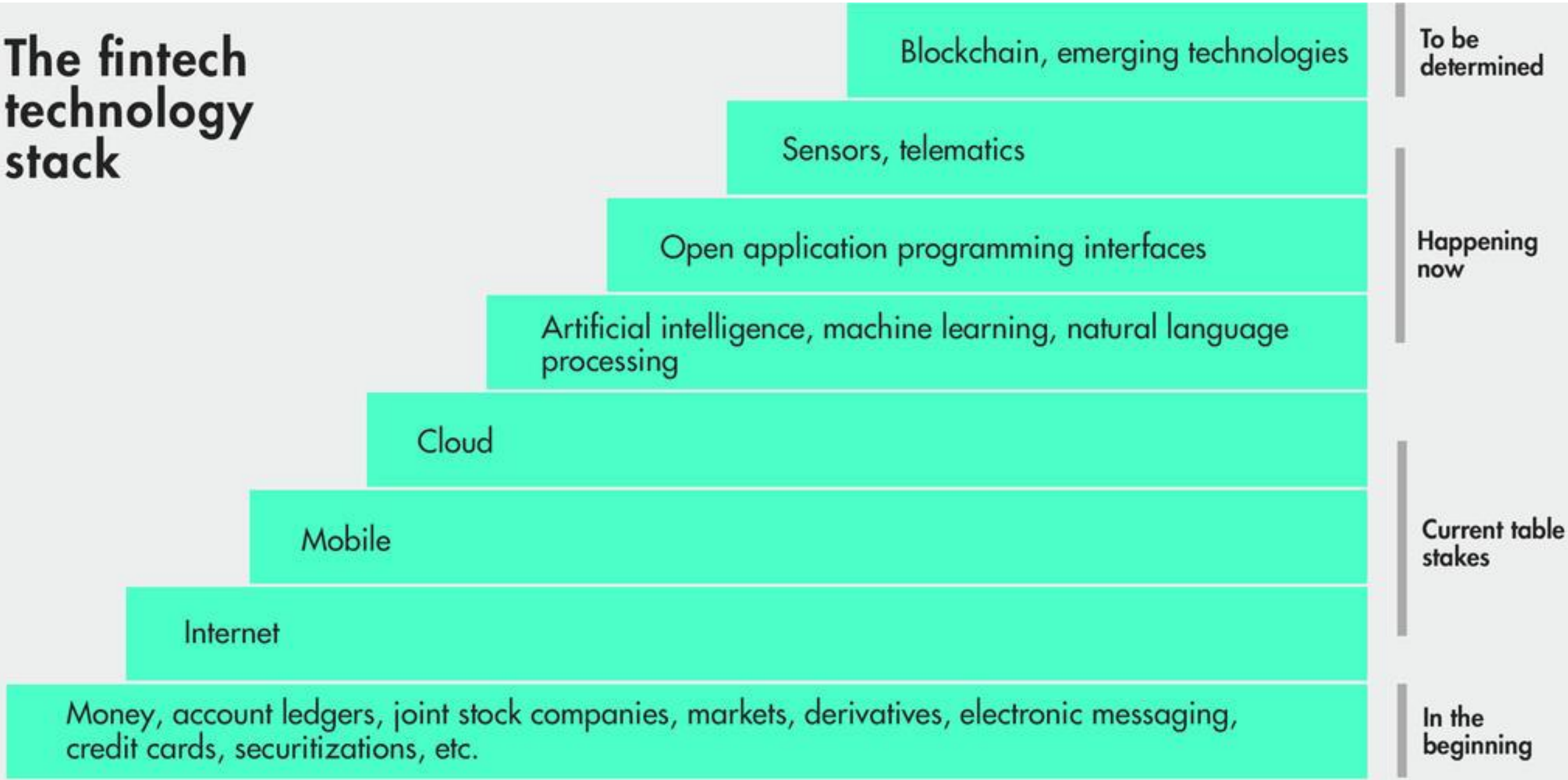
What is Fintech?

- 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 fintech technology stack



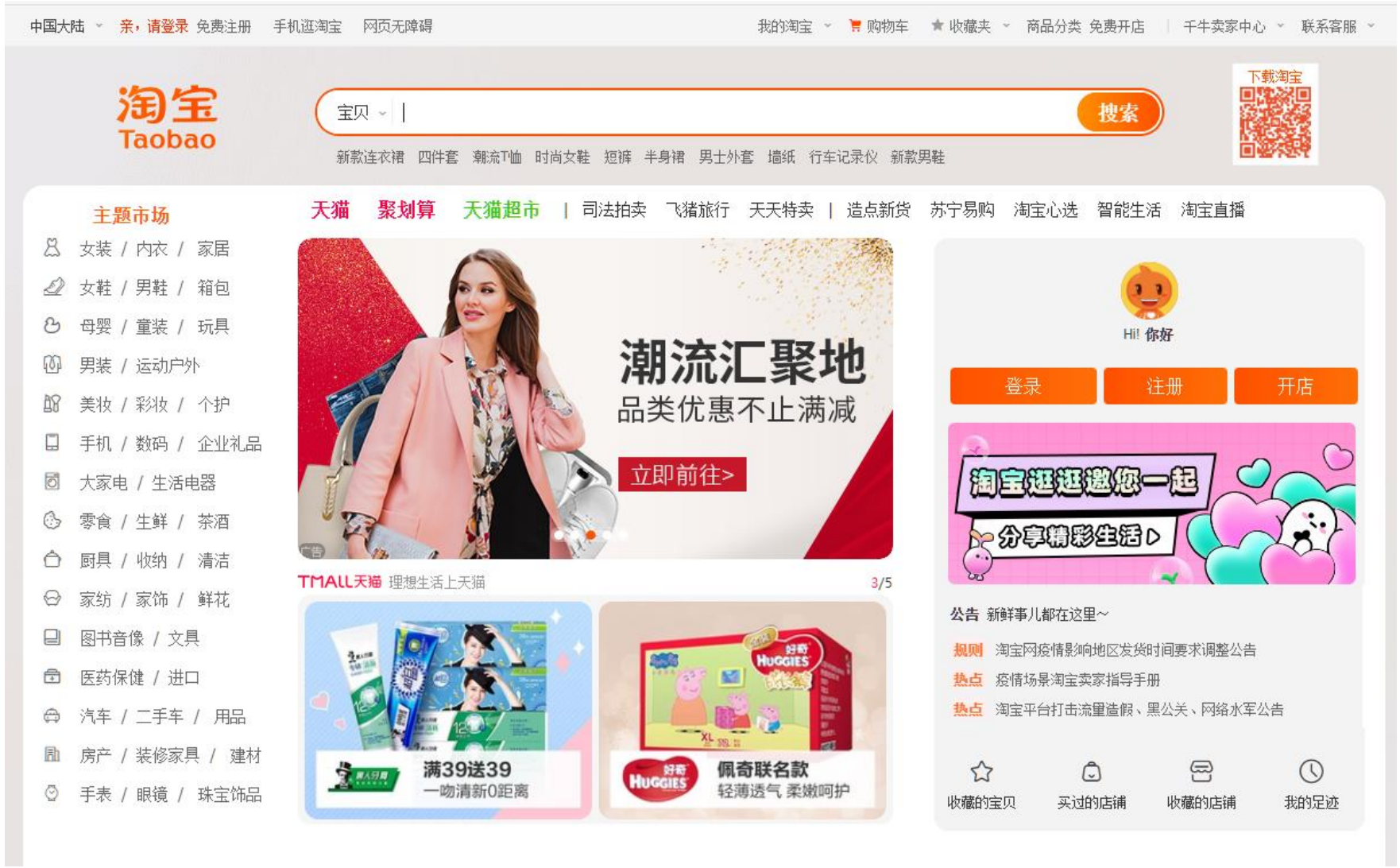
Credit: Gary Gensler | MIT Sloan

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 Alipay

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

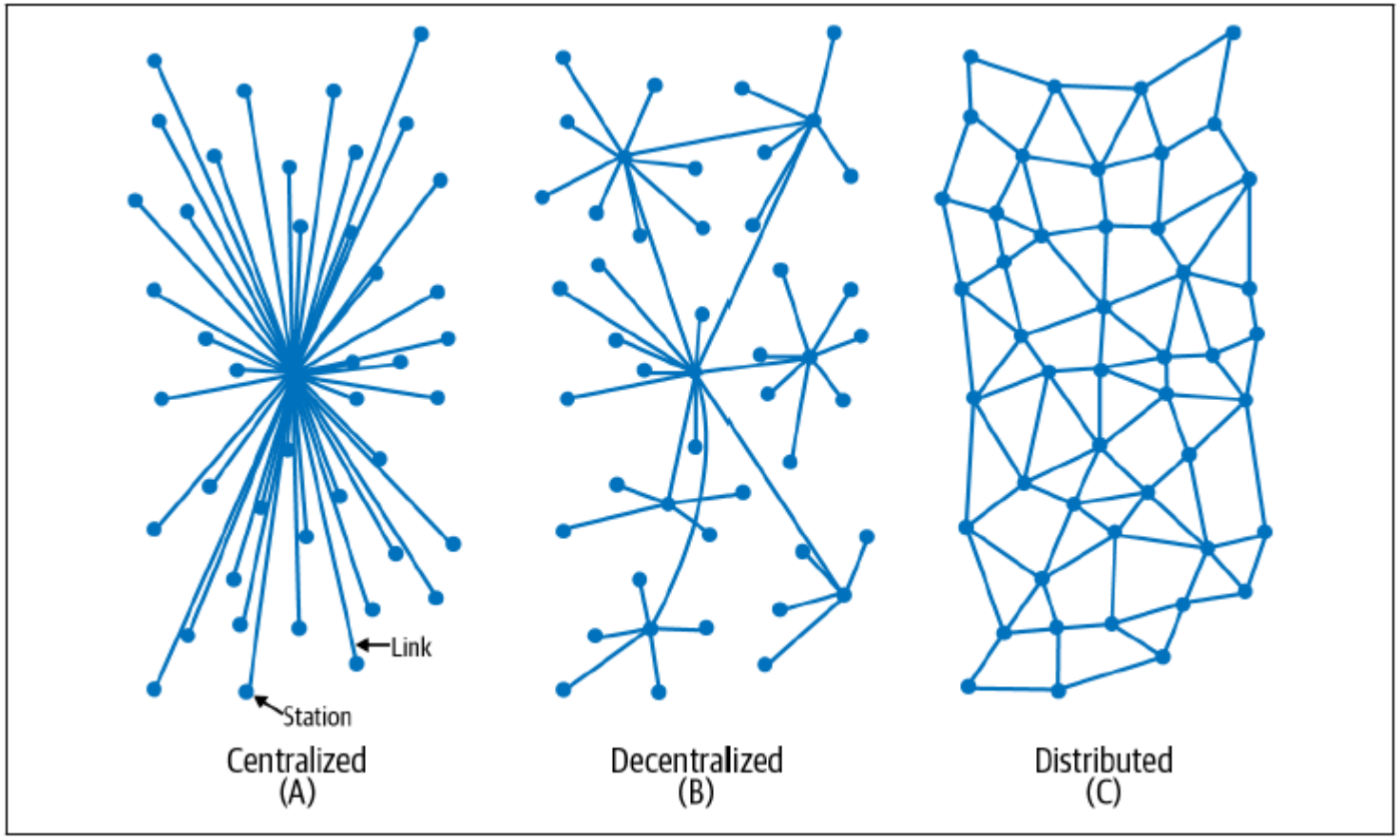
Distributed VS Centralized VS Decentralized

- 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

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.

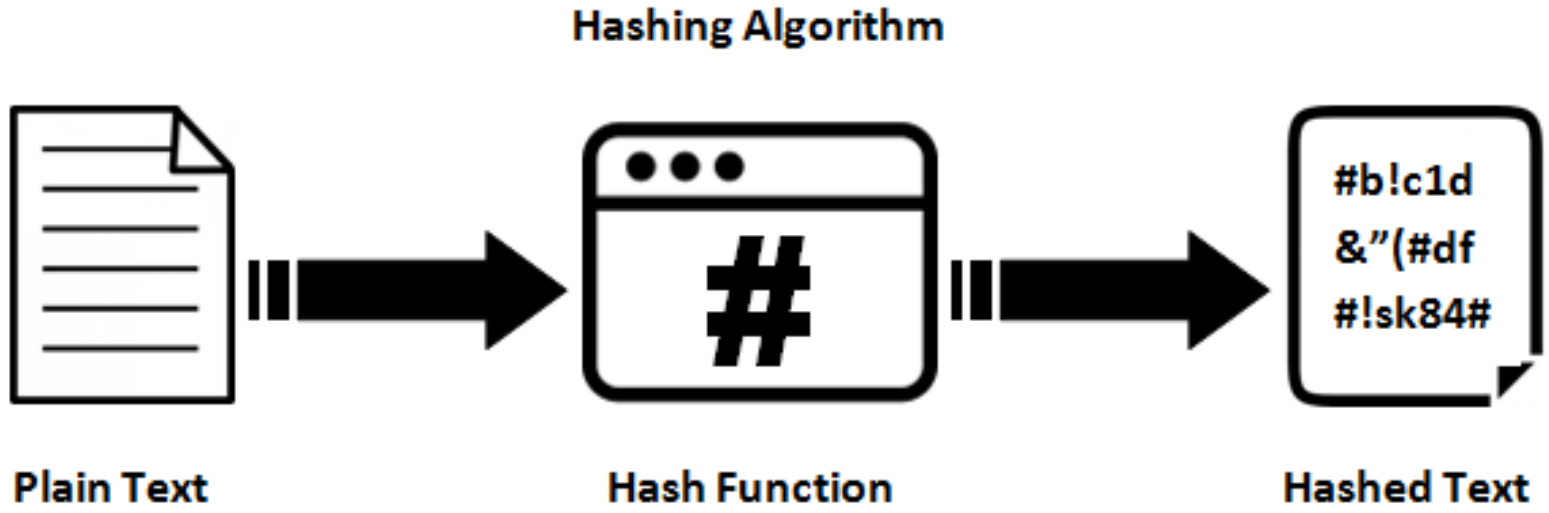
- **Nonces**

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**

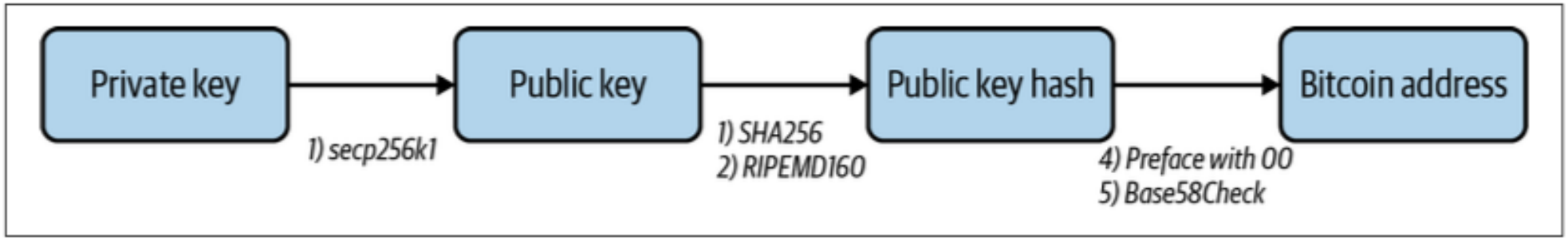
It measures the distance between the referred block and the first block.

- **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
8ae4fa8d6c4de0398a14f3f0000000049483045022100894 9f0
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

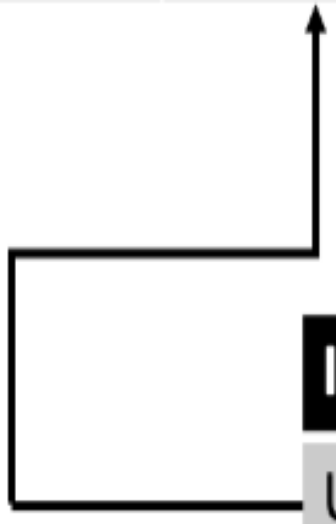
(4) Unlocking-Script

(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):

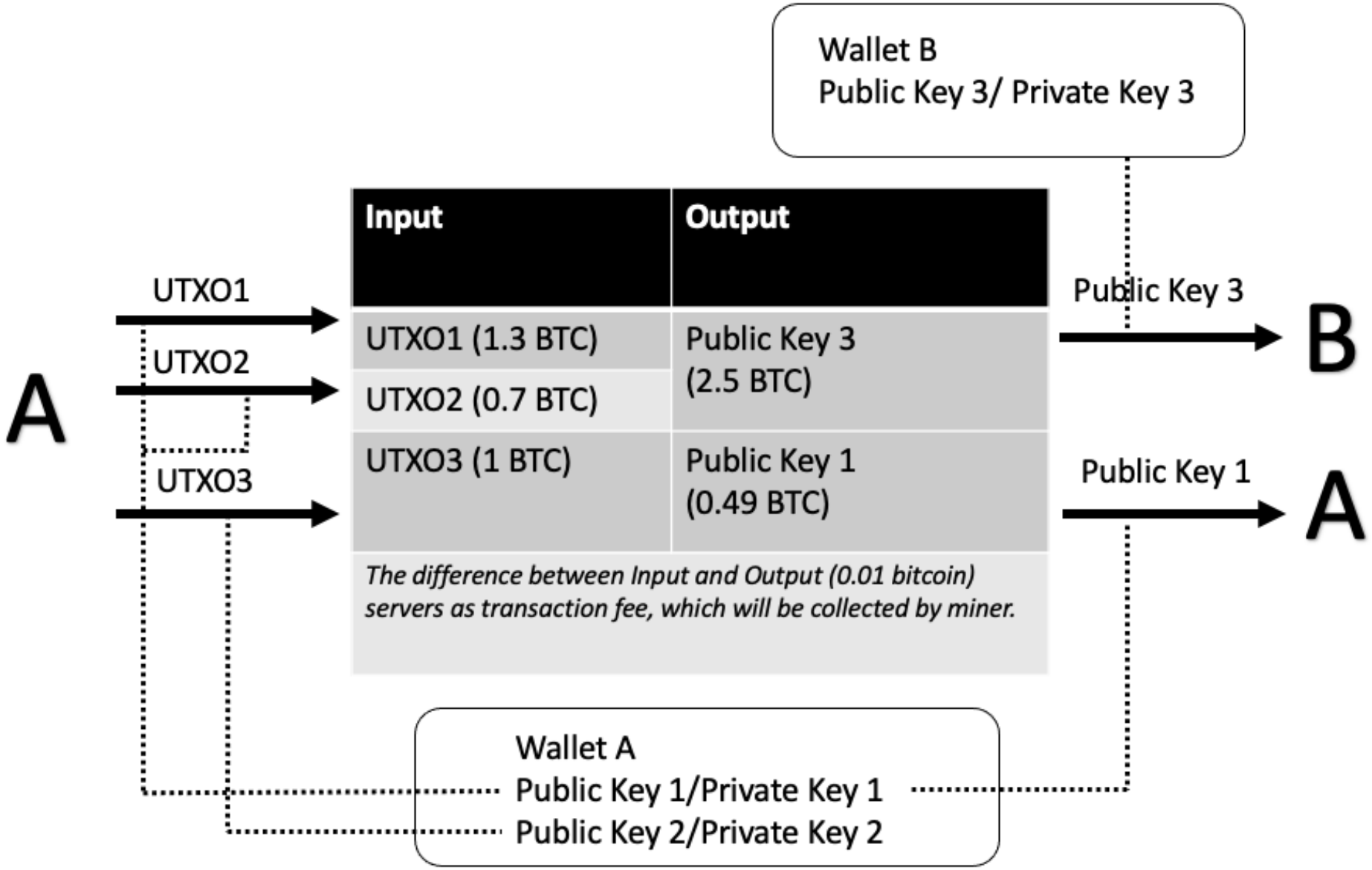
RSR = transaction fee paid in this transaction/the size of this transaction data

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

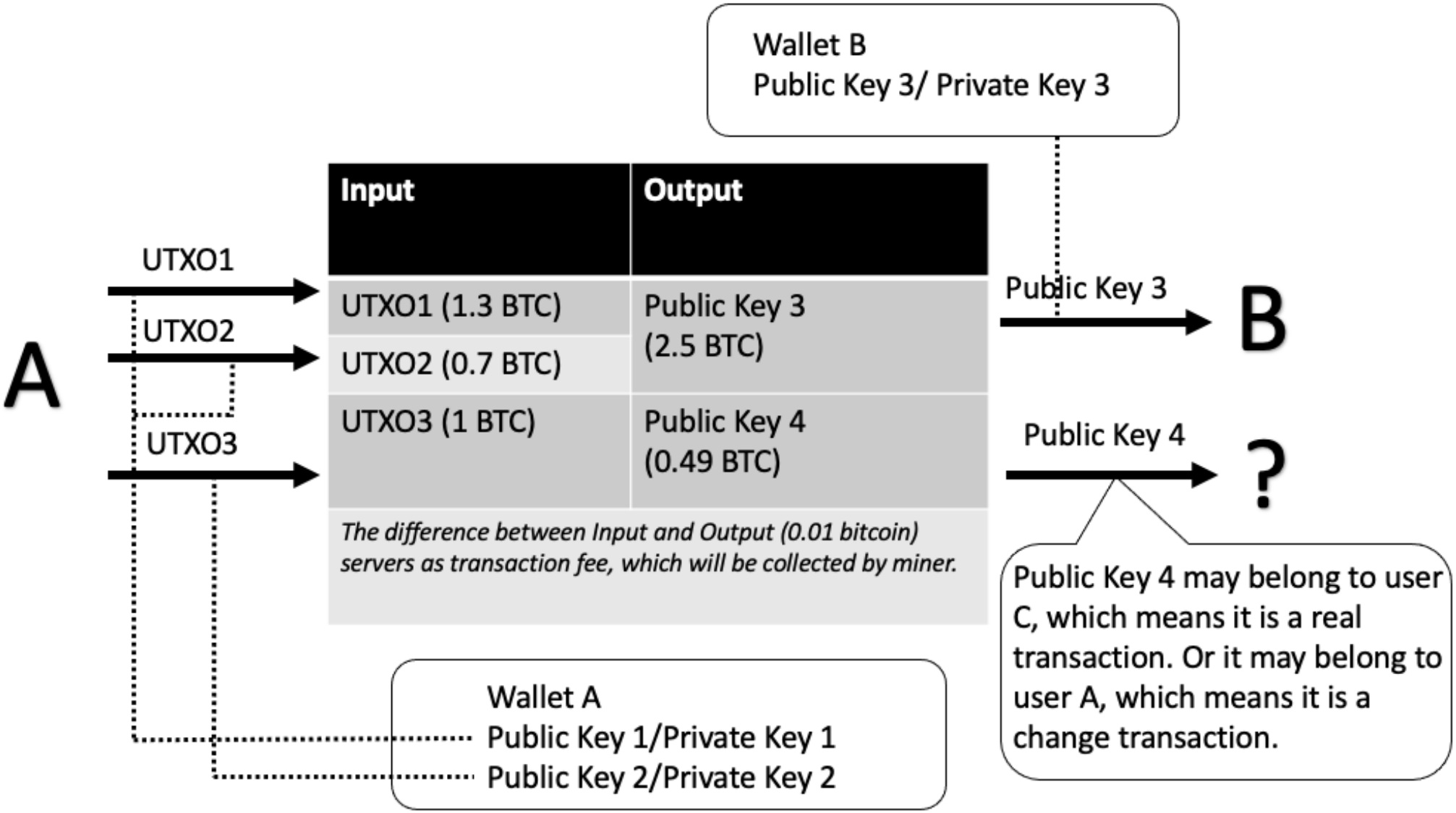
TFR = transaction fee paid in this transaction/the value of this transaction

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

Bitcoin Transactions



Bitcoin Transaction



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.

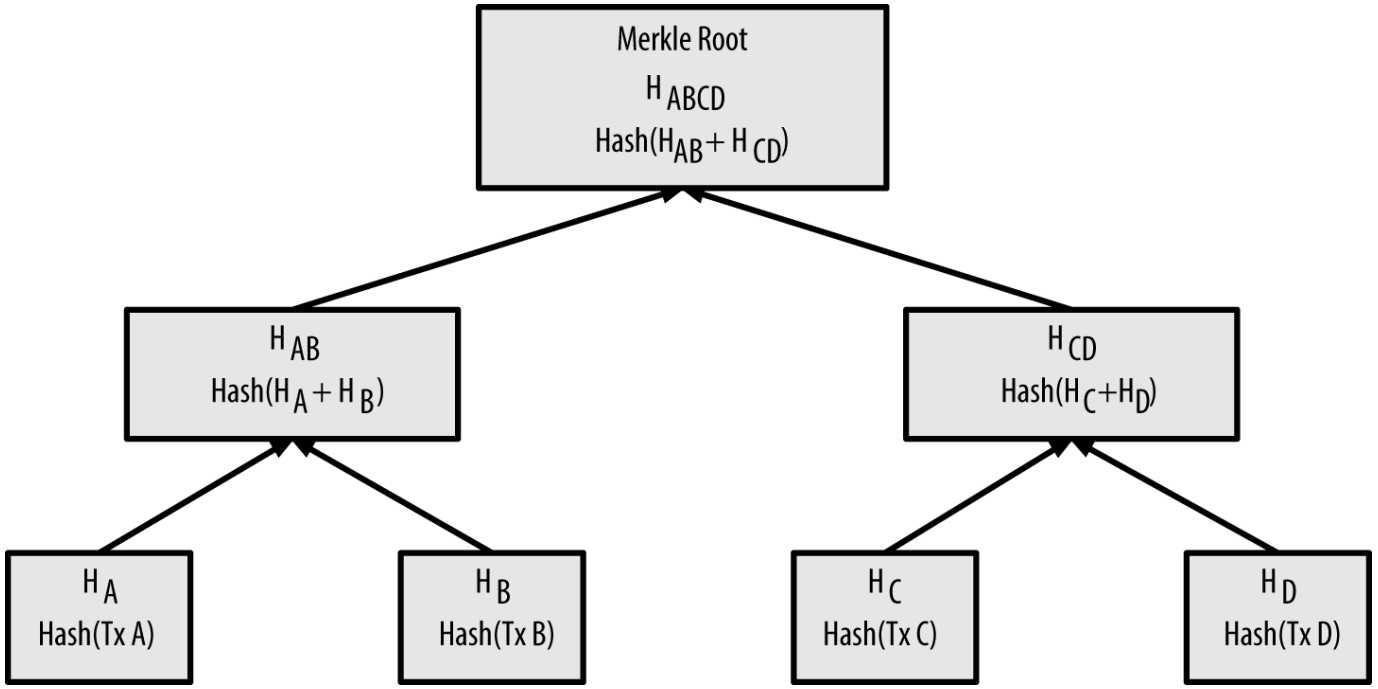
The block hash is **NOT** included in the block's data structure. Miners calculate the block hash by themselves after receiving the block from the network.

- 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

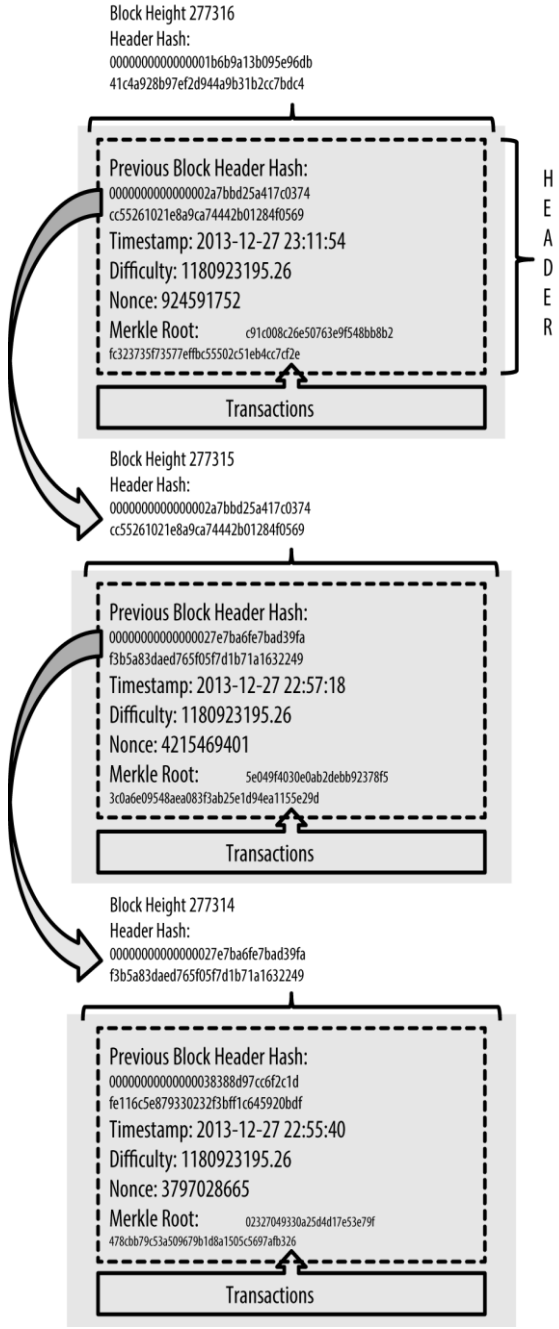
to verify if a transaction is included in a certain block.

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



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

Part IV: Cryptocurrency Fundamentals: Mining

What is mining?

- Block header hash:

0000000000000000000ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

- **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

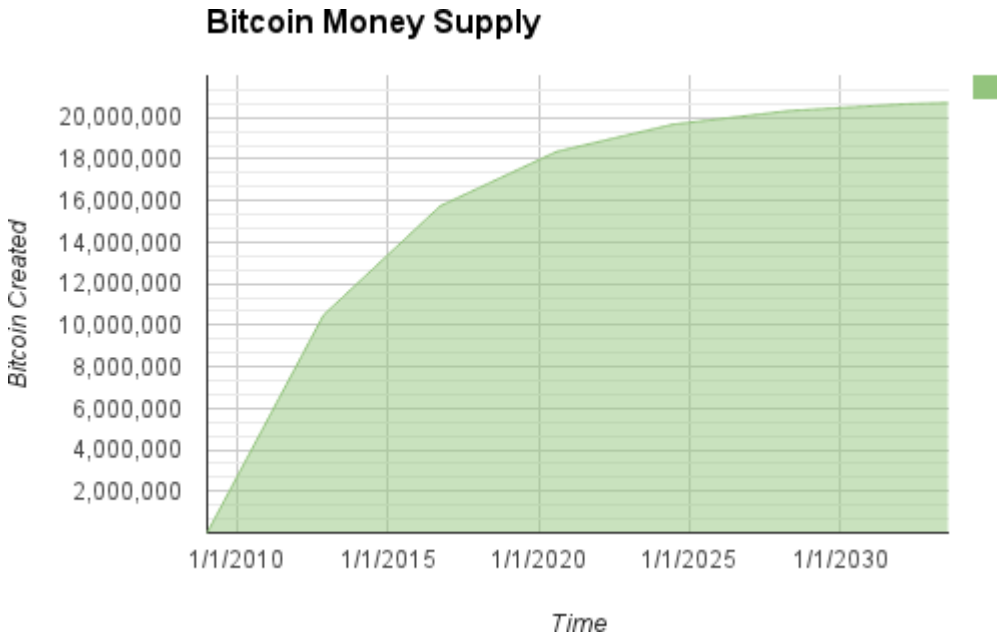
- Coinbase transactions are used to reward miners for confirming blocks.

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

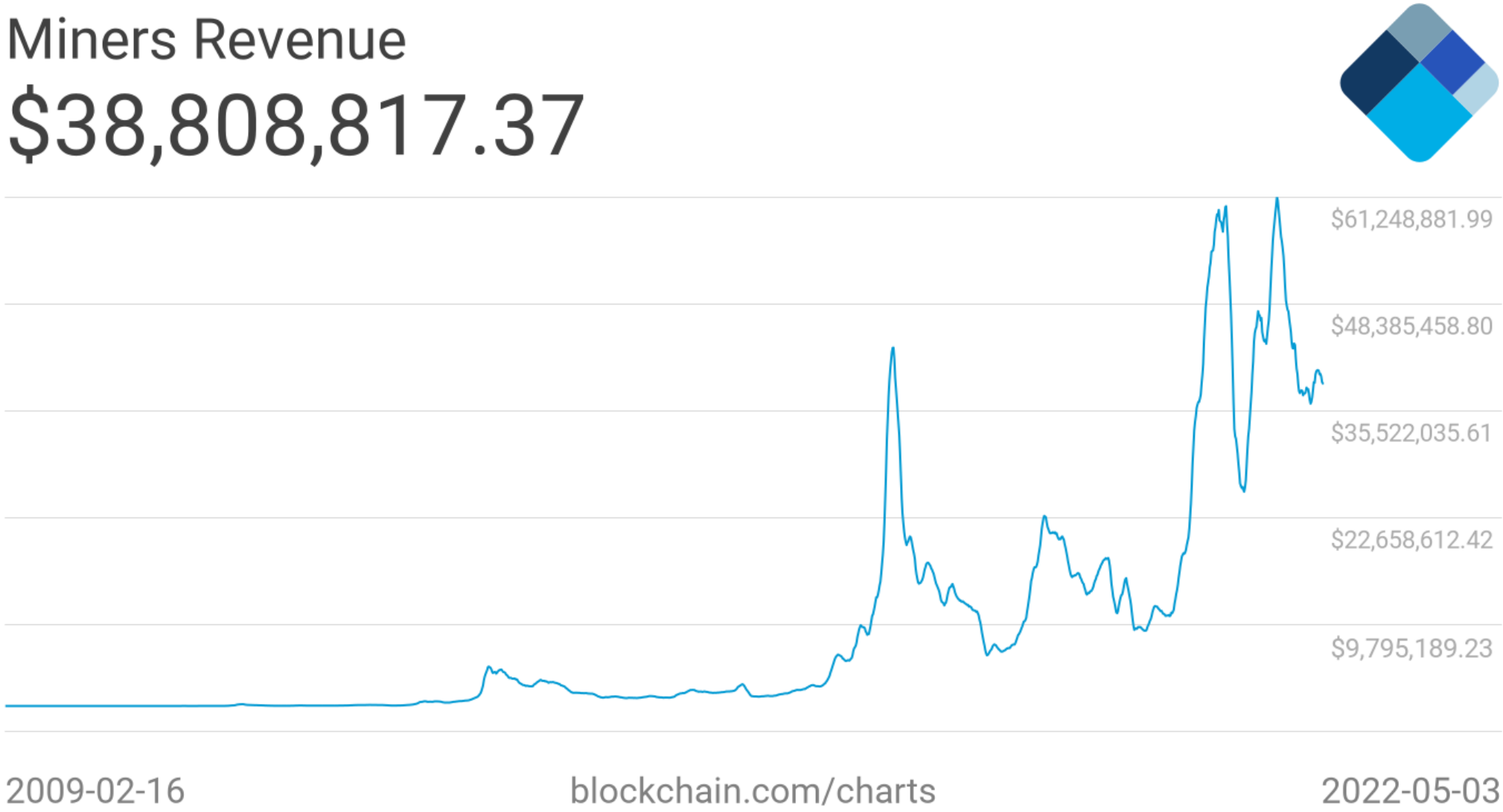
Bitcoin Mining Basics

- 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



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:

000000000000000000ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

- 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

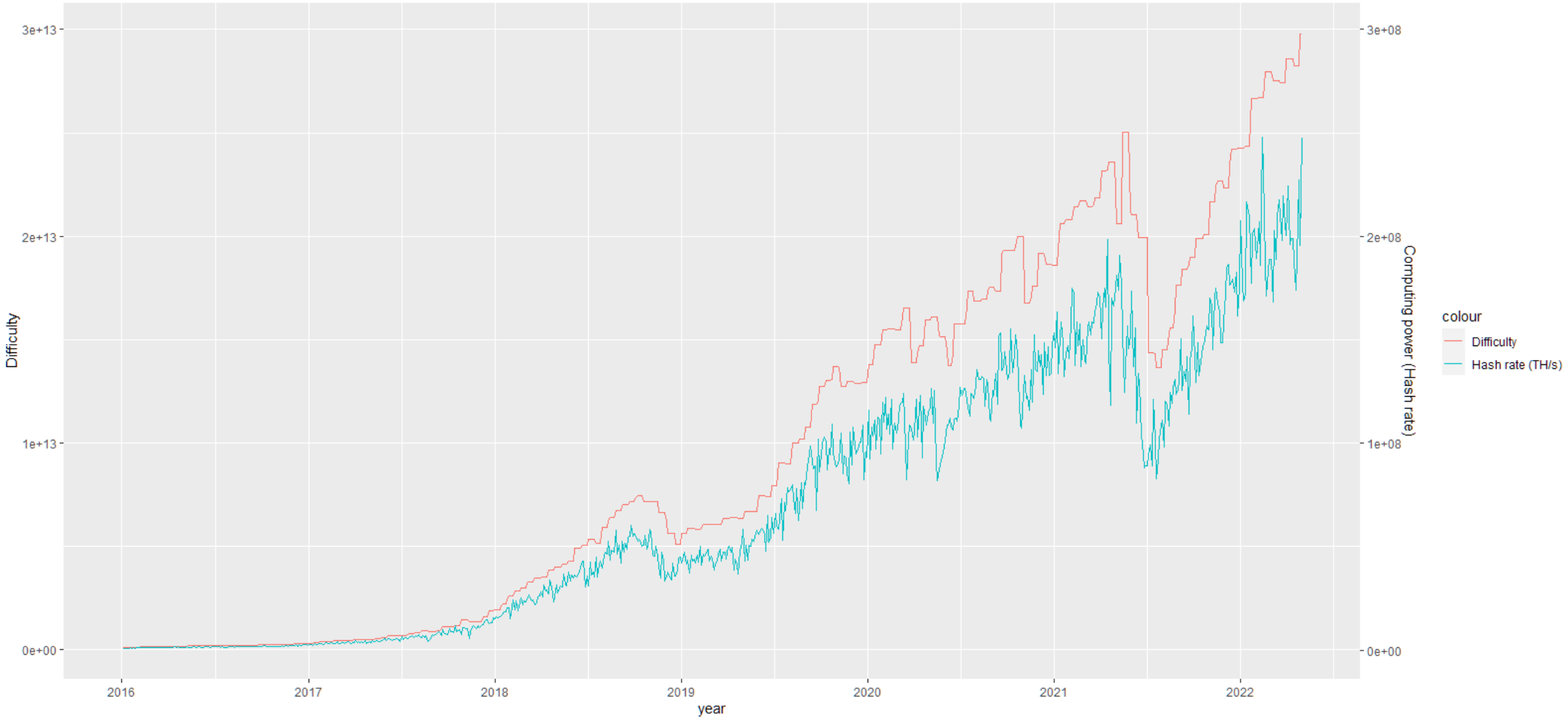
If actually time > 20160 minutes, reduce the difficulty

If actually time < 20160 minutes, increase the difficulty

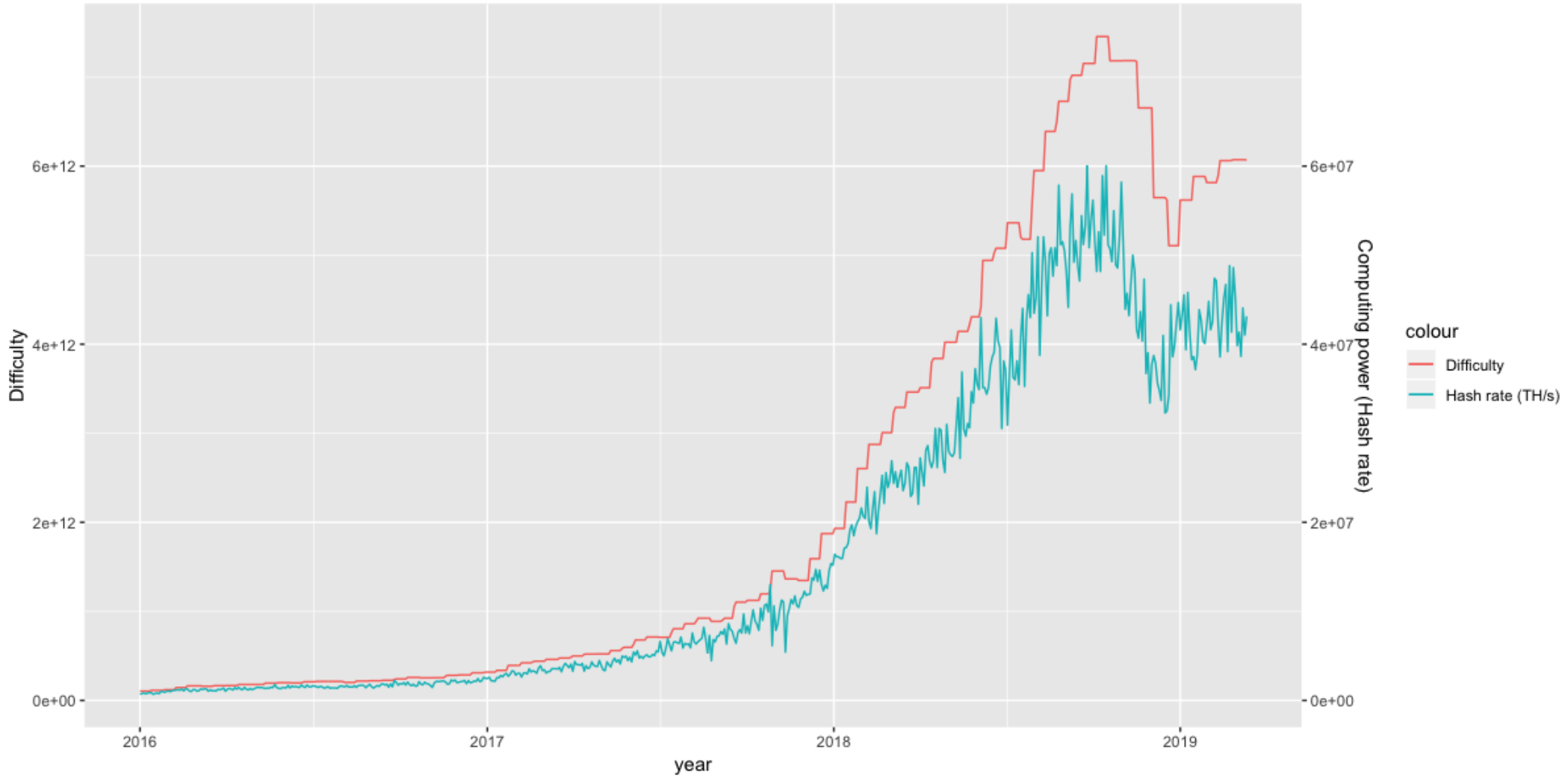
- Difficulty adjustment mechanism makes sure that block are mined, on average, every 10 minutes.

- 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