Blockchain and Digital Currencies

Lecture 2

PHBS 2024 M3

Background Introduction

This lecture gives a summary of mechanism of the blockchain for bitcoin

Disclaimer

1. The purpose of this course is to introduce the history of cryptocurrencies and blockchain, their underlying mechanisms, some of the risks that have occurred in practice, and some of the possible future directions of these emerging technologies.
2. The information contained in this course does not constitute financial, legal, tax, investment advice, investment advisory or other opinions and should not be relied upon solely for making any investment or other decisions
3. All investments should be made in compliance with local laws and regulations

Participants of Private Digital Currency World

- Three types of participants: miners, users, and speculators
- What is the motivation for users to use digital currencies?
- What is the motivation for speculators to trade digital currencies?
- What is the motivation for miners to maintain digital currencies?

- Who benefits most when the price of digital currencies continues to climb?
- Who will be the first to leave when the price of digital currencies keeps going down?

- Who is most motivated to undermine the mechanics of digital currencies?
- Will a monopoly that runs counter to decentralization lead to a lack of trust?

Who is the most important of the three types of participants?

There is a dynamic weak equilibrium among the three types of participants

What are the Difficulties?

- Double Spending – 双花(双重支付攻击)：电子媒介容易被复制
- Sustainability 运营成本的控制和可持续性
- Challenges to the existing legal currency system 对现有法币体系的挑战
- How to achieve the consistent global anti-money laundering regulatory goals 全球的一致的反洗钱的监管目标如何实现

What Block Chain Can Do

- Avoid double spending 规避双花问题
- Allow anonymous transactions 允许匿名交易
- Guarantee transaction completion 保证交易完成
- Convenient to realize transaction 方便实现转账

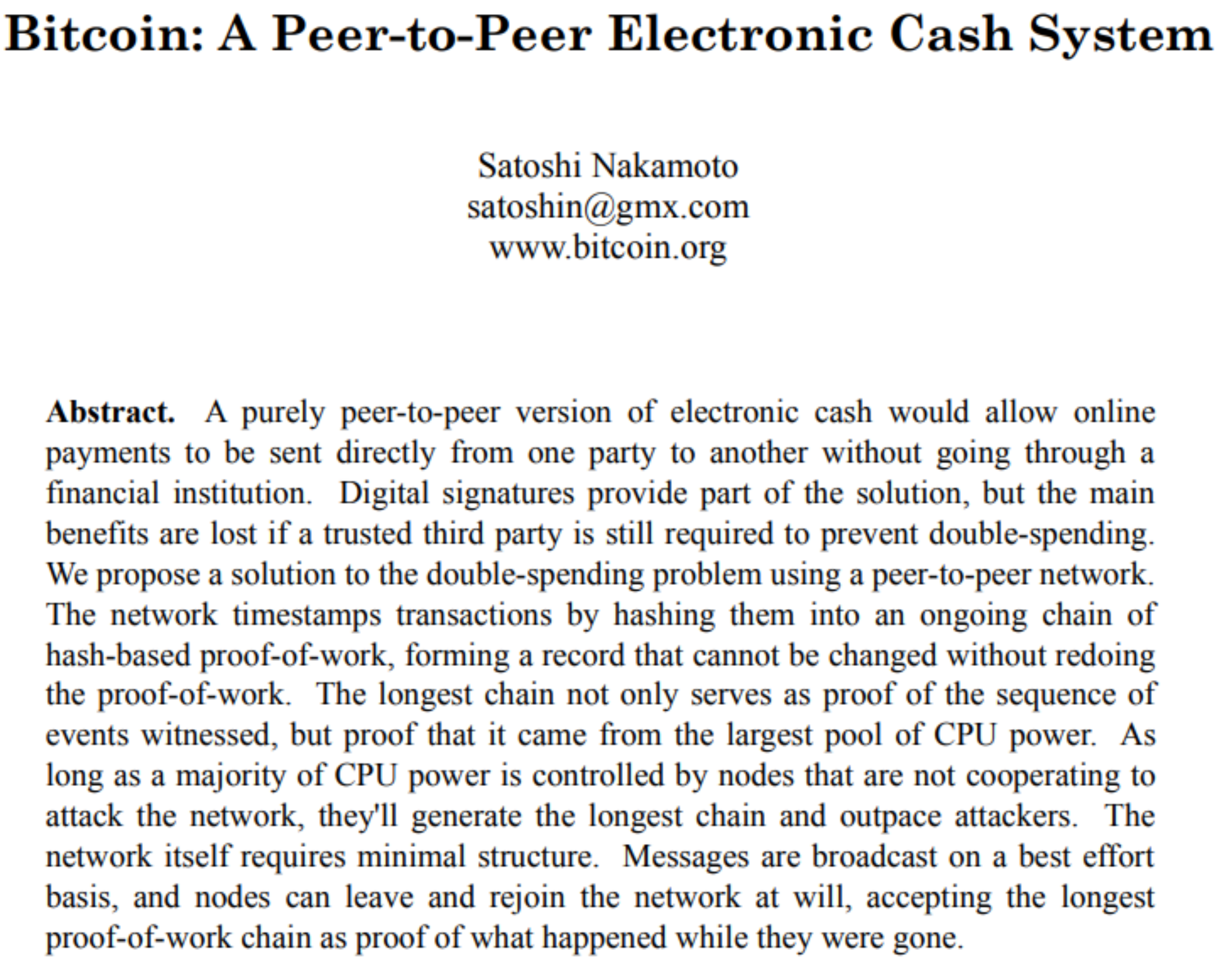
Short History of Block Chain

This technology used to timestamp files was invented in 1991

https://medium.com/@ankit_233/history-of-the-blockchain-1991-38d6d4c3420c

Satoshi Nakamoto used this technique for bitcoin transactions in 2009

Reference (Bitcoin: A Peer-to-Peer Electronic Cash System)



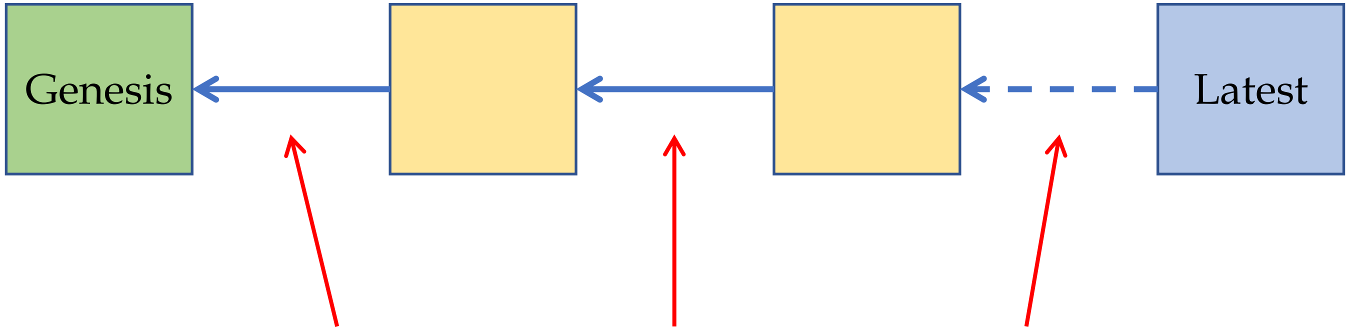
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

What is Blockchain?

- Blockchain is a list of blocks with an order.
- Originally designed to timestamp digital documents in 1991
- Adapted by Satoshi Nakamoto in 2009 to facilitate Bitcoin transactions (Bitcoin: A Peer-to-Peer Electronic Cash System)

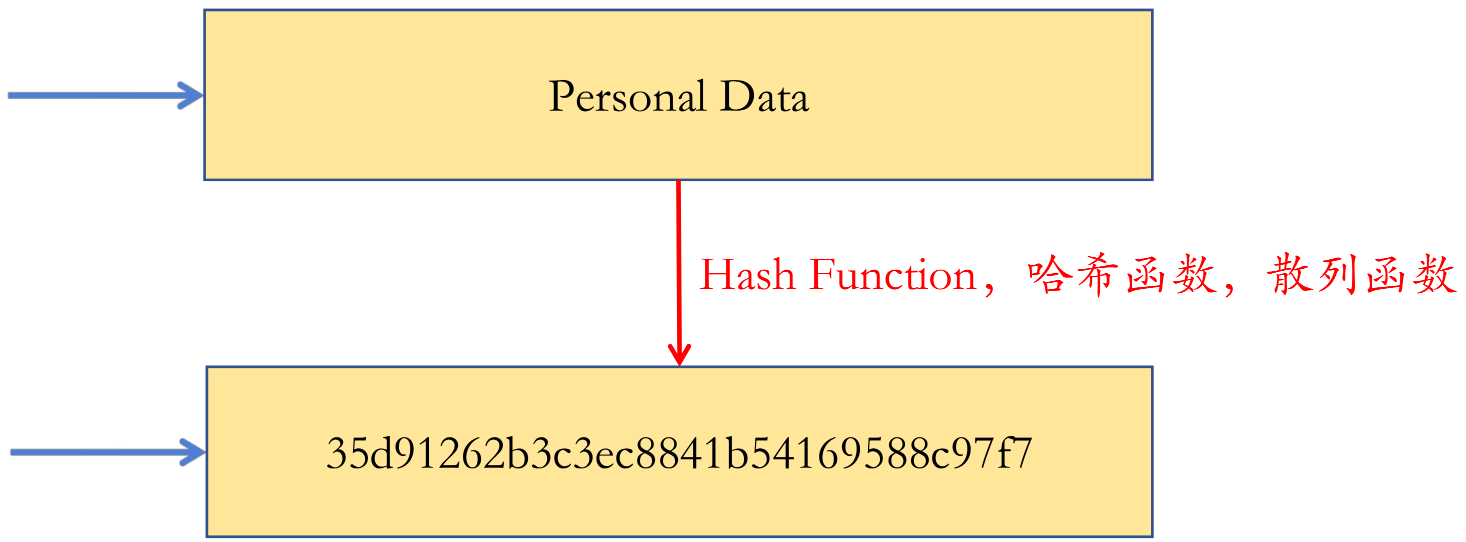


Hash Pointer: a pointer + the hash of the content this pointer refers to.

Hash Pointer 哈希指针

A pointer is essentially an address.

A pointer to a data storage location, and a hash of the data inside that storage location



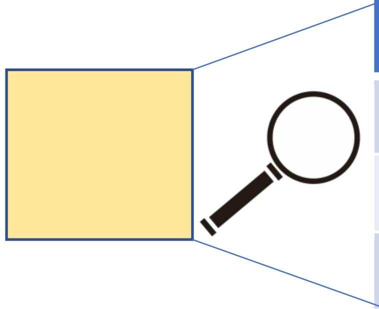
Personal Data

Hash Function，哈希函数，散列函数

35d91262b3c3ec8841b54169588c97f7

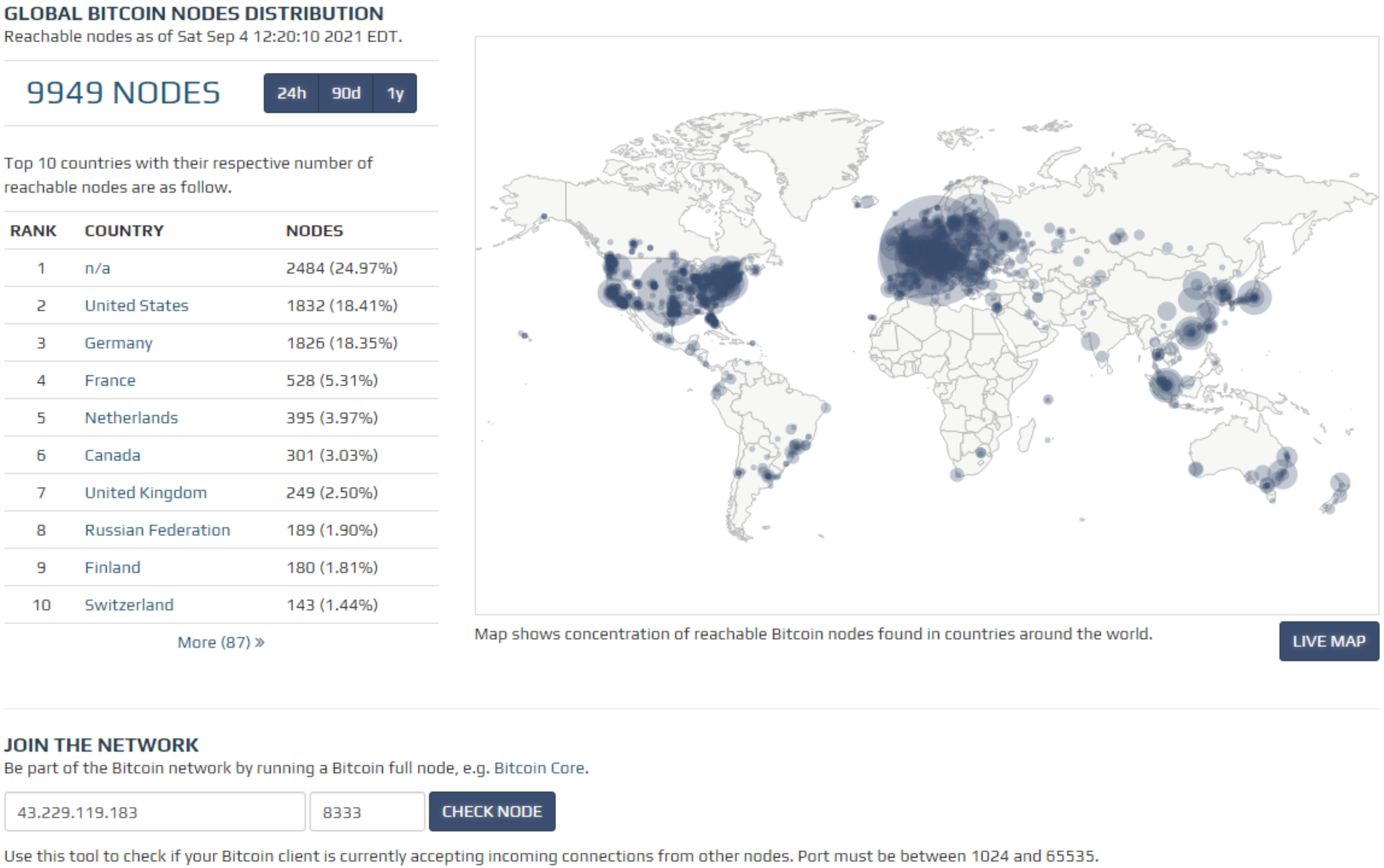
Bitcoin Block

- The blocks contain Bitcoin transactions
- A transaction consists of senders, receivers, and amount of Bitcoins to be transfered
- The transaction is peer to peer without any third party involved
- Bitcoin Blockchain is a Bitcoin transaction ledger



Transaction ID	Sender	Receiver	Bitcoin Amount
1	A	B	100
2	C	B	50
3	B	A	75

The Network Foundation of Bitcoin Blockchain https://bitnodes.io/



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Sep 4 12:20:10 2021 EDT.

9949 NODES

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2484 (24.97%)
2	United States	1832 (18.41%)
3	Germany	1826 (18.35%)
4	France	528 (5.31%)
5	Netherlands	395 (3.97%)
6	Canada	301 (3.03%)
7	United Kingdom	249 (2.50%)
8	Russian Federation	189 (1.90%)
9	Finland	180 (1.81%)
10	Switzerland	143 (1.44%)

More (87) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

JOIN THE NETWORK

Be part of the Bitcoin network by running a Bitcoin full node, e.g. Bitcoin Core.

43.229.119.183 | 8333

Use this tool to check if your Bitcoin client is currently accepting incoming connections from other nodes. Port must be between 1024 and 65535.

Bitcoin Transaction

- Bitcoin transaction is public and transparent, everyone can see it (consists of the sender, the recipient, and the amount of the transaction)
- Each sender and receiver is an address (addresses are also unique hashes that can be created at will, providing anonymity)
- Anyone can send a transaction, but the transaction is only valid if it is acknowledged by everyone (booked into the blockchain)
- The first element for a transaction to be valid is to prove that you have the digital currency of the sender's address
- Each transaction is encrypted with the recipient's public key and can only be decrypted with a signature generated by the recipient with the correct private key (a transaction can be thought of as a letter delivered through a publicly locked mailbox that can only be opened by the recipient with the correct mailbox key (private key))
- The second element for a transaction to be valid is to be recorded in the blockchain

More About Bitcoin Transaction

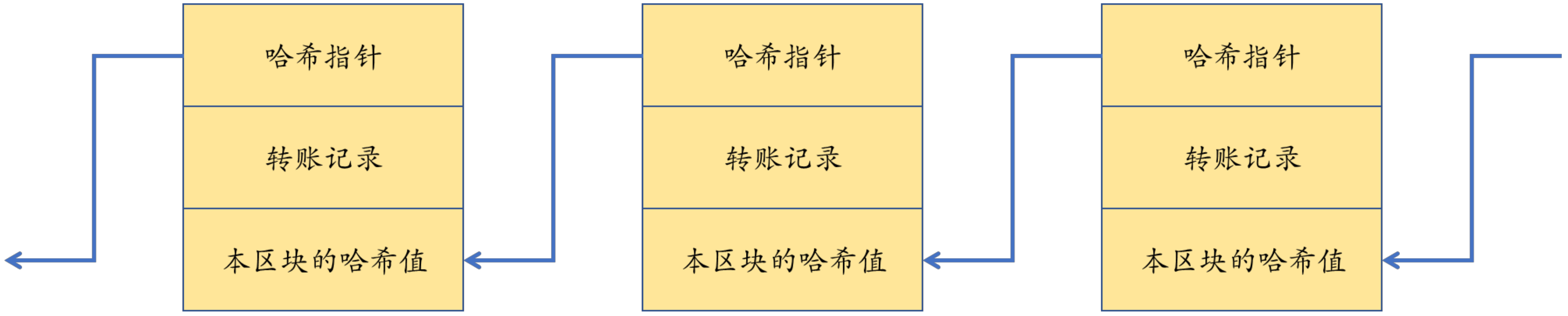
- Each transaction is addressed to the sender and receiver
- Each transaction is encrypted with the recipient's public key, and only the recipient's key can be used to decode
- It can be thought of as a locked mailbox, where the recipient has the key to the mailbox
- Each transaction consumes some digital currencies (spent) and generates one or several digital currencies (unspent)
- A digital currency that has already been consumed cannot be reused (combined with the first element in the previous page)
- A - > A, B
- A, B -> C
- A, A -> A

What Block Chain Can Do

- Avoid double spending 规避双花问题
- Allow anonymous transactions 允许匿名交易 ✓
- Guarantee transaction completion 保证交易完成
- Convenient to realize transaction 方便实现转账 ✓

Important Block Fields

- Each block has 3 key parts:
  - transactions
  - a hash pointer pointing to the previous block
  - hash of the whole block.

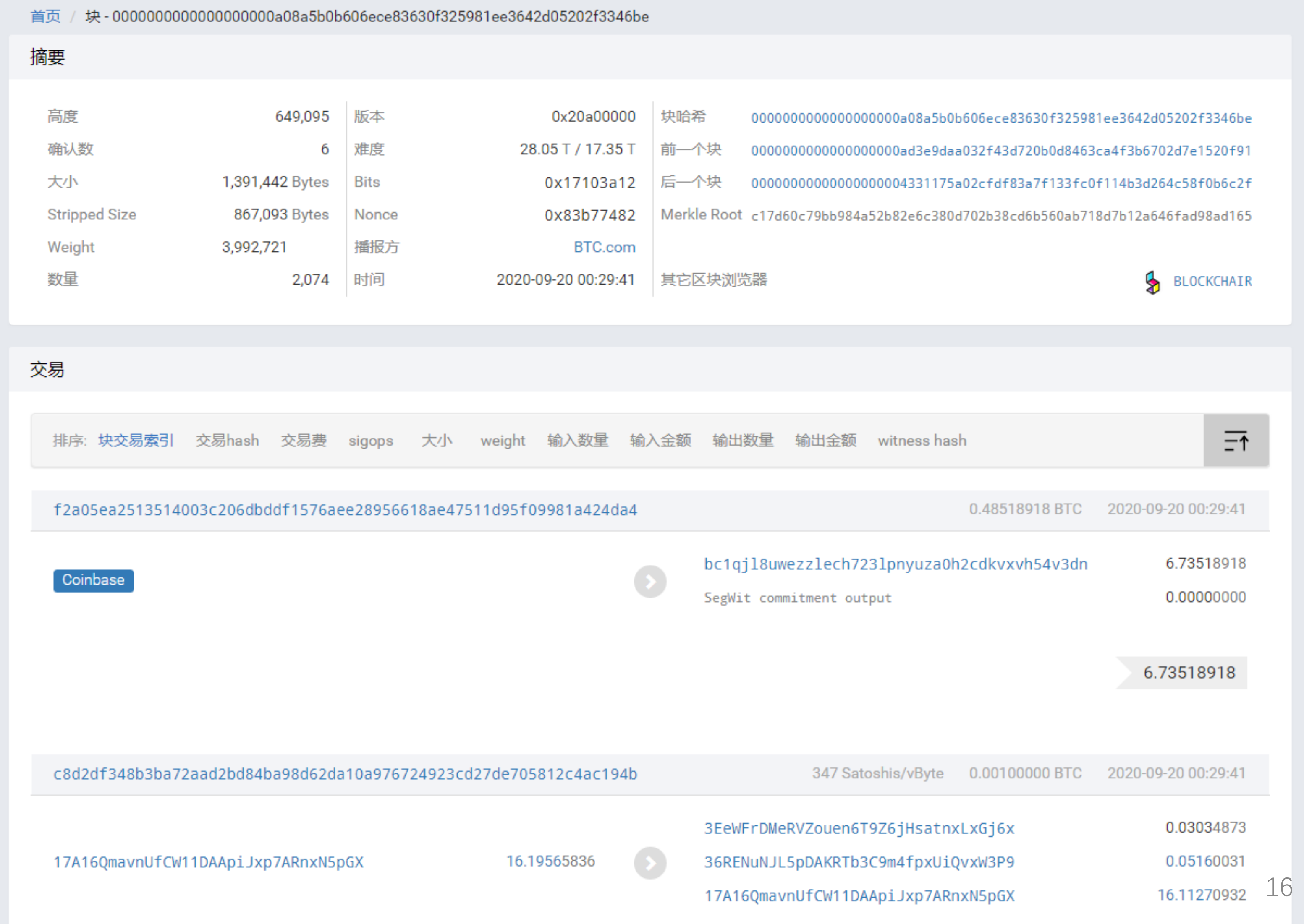


转账记录是其中最关键的部分

Bitcoin Example

https://www.btc.com

https://btc.com/0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be



首页 / 块 - 0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be

摘要

高度	649,095	版本	0x20a00000	块哈希	0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be
确认数	6	难度	28.05 T / 17.35 T	前一个块	0000000000000000000ad3e9daa032f43d720b0d8463ca4f3b6702d7e1520f91
大小	1,391,442 Bytes	Bits	0x17103a12	后一个块	00000000000000000004331175a02cfdf83a7f133fc0f114b3d264c58f0b6c2f
Stripped Size	867,093 Bytes	Nonce	0x83b77482	Merkle Root	c17d60c79bb984a52b82e6c380d702b38cd6b560ab718d7b12a646fad98ad165
Weight	3,992,721	播报方	BTC.com		
数量	2,074	时间	2020-09-20 00:29:41	其它区块浏览器	BLOCKCHAIR

交易

排序: 块交易索引 交易hash 交易费 sigops 大小 weight 输入数量 输入金额 输出数量 输出金额 witness hash

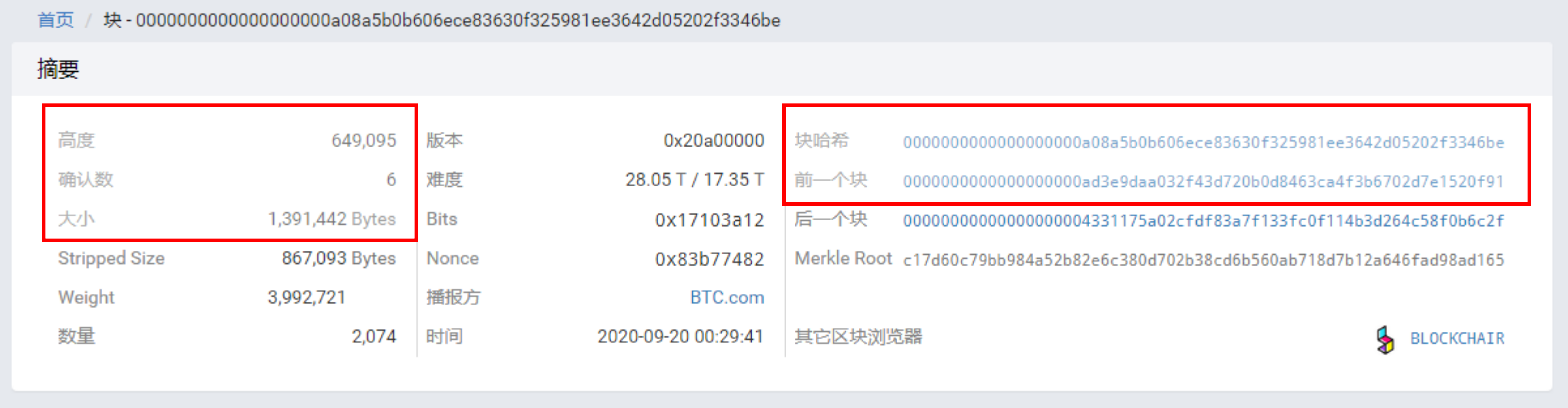
f2a05ea2513514003c206dbddf1576aee28956618ae47511d95f09981a424da4 0.48518918 BTC 2020-09-20 00:29:41

Coinbase	bc1qjl8uwezzlech723lpnyuza0h2cdkvxvh54v3dn	6.73518918
	SegWit commitment output	0.00000000
		6.73518918

c8d2df348b3ba72aad2bd84ba98d62da10a976724923cd27de705812c4ac194b 347 Satoshis/vByte 0.00100000 BTC 2020-09-20 00:29:41

17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	16.19565836	3EeWFrDMeRVZouen6T9Z6jHsatnxLxGj6x	0.03034873
		36RENuNJL5pDAKRTb3C9m4fpxUiQvxW3P9	0.05160031
		17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	16.11270932

Block 649095: Summary



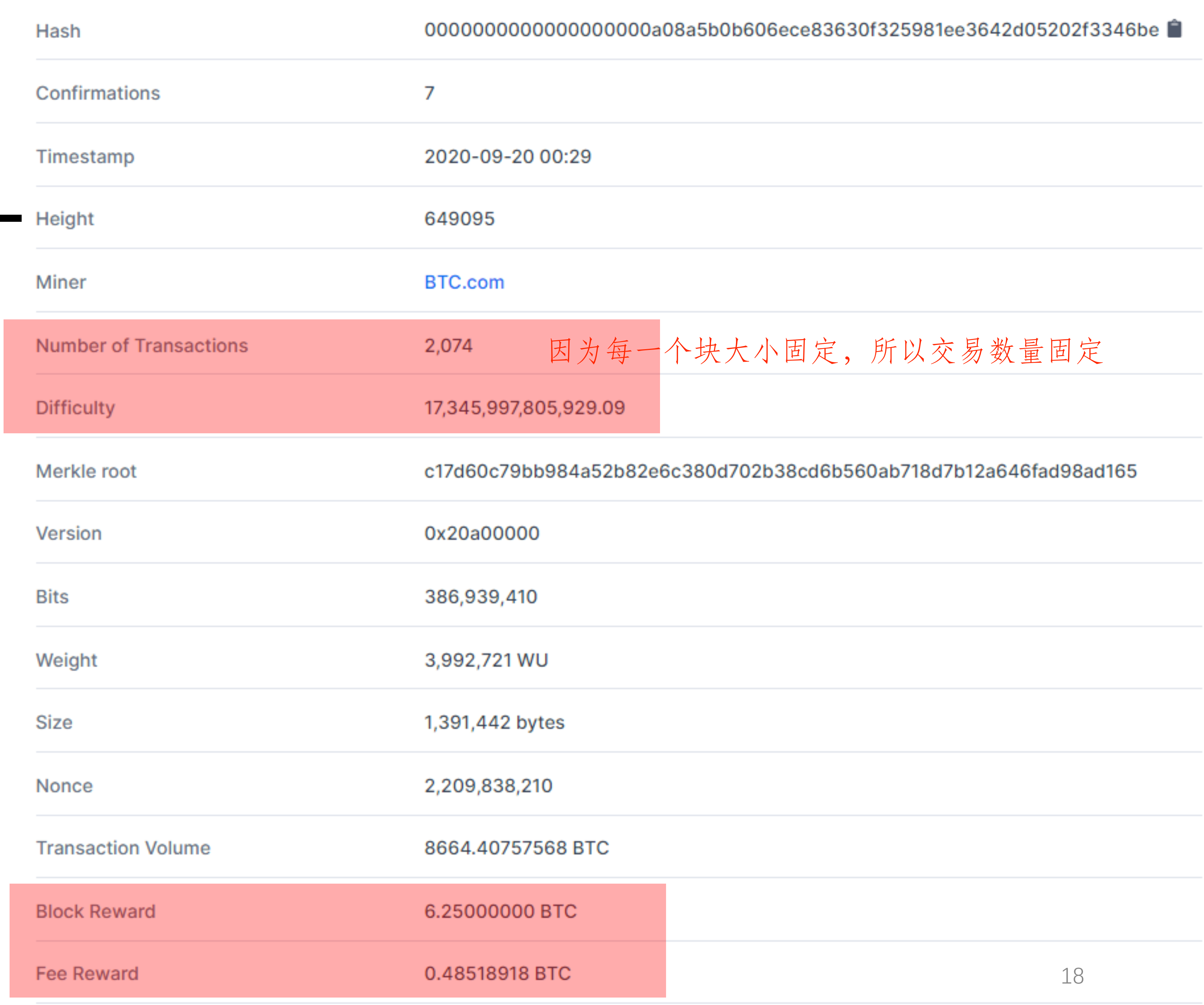
首页 / 块 - 0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be

摘要

高度	649,095	版本	0x20a00000	块哈希	0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be
确认数	6	难度	28.05 T / 17.35 T	前一个块	0000000000000000000ad3e9daa032f43d720b0d8463ca4f3b6702d7e1520f91
大小	1,391,442 Bytes	Bits	0x17103a12	后一个块	00000000000000000004331175a02cfdf83a7f133fc0f114b3d264c58f0b6c2f
Stripped Size	867,093 Bytes	Nonce	0x83b77482	Merkle Root	c17d60c79bb984a52b82e6c380d702b38cd6b560ab718d7b12a646fad98ad165
Weight	3,992,721	播报方	BTC.com		
数量	2,074	时间	2020-09-20 00:29:41	其它区块浏览器	BLOCKCHAIR

第649095区块：

https://www.blockchain.com
https://www.blockchain.com/btc/block/0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be

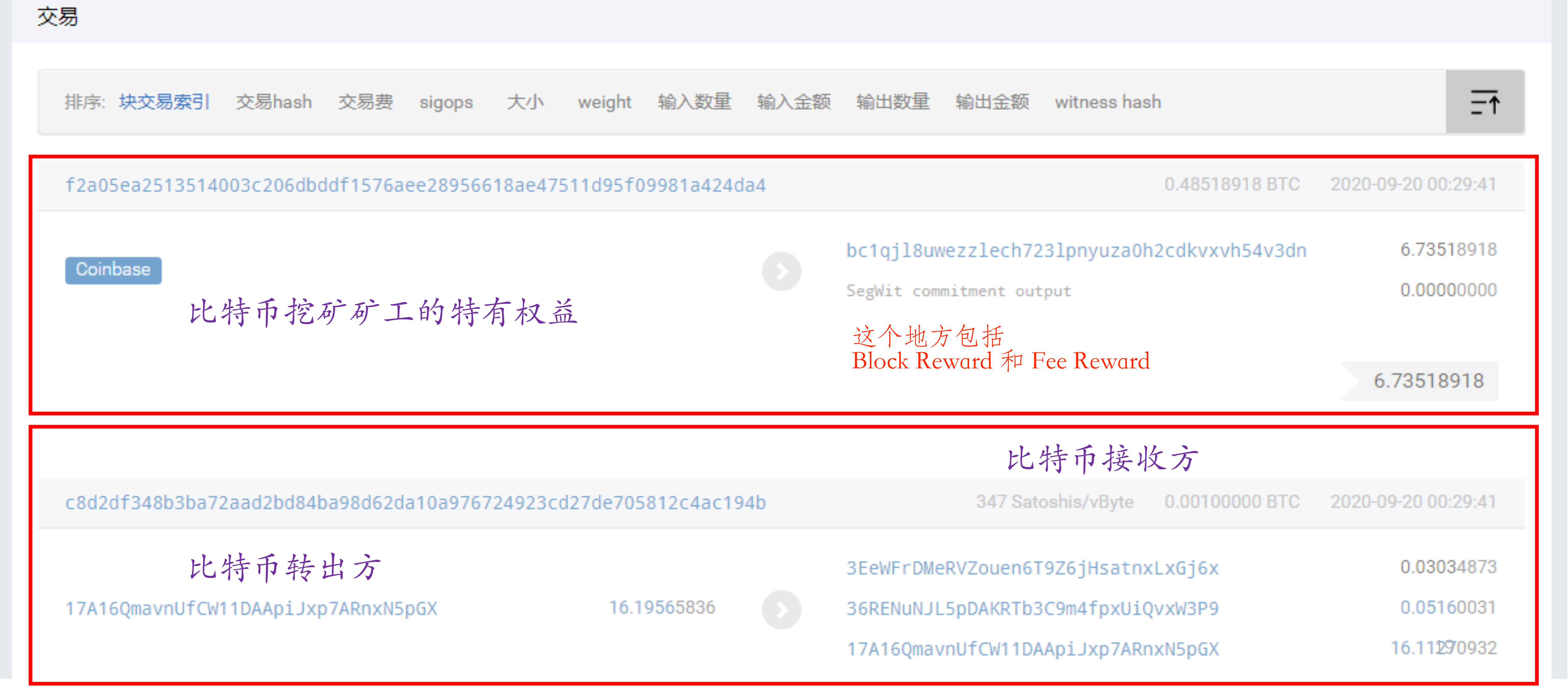


Hash	0000000000000000000a08a5b0b606ece83630f325981ee3642d05202f3346be
Confirmations	7
Timestamp	2020-09-20 00:29
Height	649095
Miner	BTC.com
Number of Transactions	2,074
Difficulty	17,345,997,805,929.09
Merkle root	c17d60c79bb984a52b82e6c380d702b38cd6b560ab718d7b12a646fad98ad165
Version	0x20a00000
Bits	386,939,410
Weight	3,992,721 WU
Size	1,391,442 bytes
Nonce	2,209,838,210
Transaction Volume	8664.40757568 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.48518918 BTC

因为每一个块大小固定，所以交易数量固定

Block 649095: Transaction Records

两种交易方式，一种有转出方，一种没有
没有的就是矿工区块，因此你能明确知道每一个
区块是哪个挖出来的。



交易

排序： 块交易索引 交易hash 交易费 sigops 大小 weight 输入数量 输入金额 输出数量 输出金额 witness hash

f2a05ea2513514003c206dbddf1576aee28956618ae47511d95f09981a424da4 0.48518918 BTC 2020-09-20 00:29:41

Coinbase

比特币挖矿矿工的特有权益

bc1qjl8uwezzlech723lpnyuza0h2cdkvxvh54v3dn	6.73518918
SegWit commitment output	0.00000000

这个地方包括
Block Reward 和 Fee Reward

6.73518918

比特币接收方

c8d2df348b3ba72aad2bd84ba98d62da10a976724923cd27de705812c4ac194b 347 Satoshis/vByte 0.00100000 BTC 2020-09-20 00:29:41

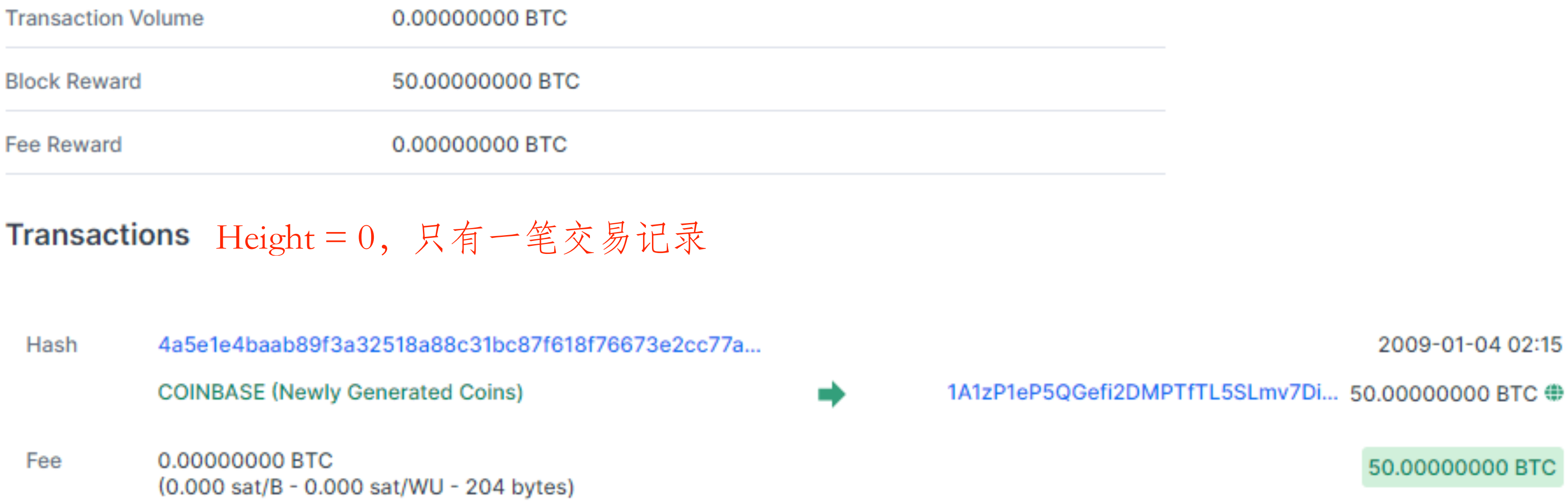
比特币转出方

17A16QmavnUfCW11DAApiJxp7ARnxN5pGX 16.19565836

3EeWFrDMeRVZouen6T9Z6jHsatnxLxGj6x	0.03034873
36RENuNJL5pDAKRTb3C9m4fpxUiQvxW3P9	0.05160031
17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	16.11270932

Why Mining?

- Bitcoins as incentives!
  - Check the blockchain page again – coinbase transaction



Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

Transactions Height = 0，只有一笔交易记录

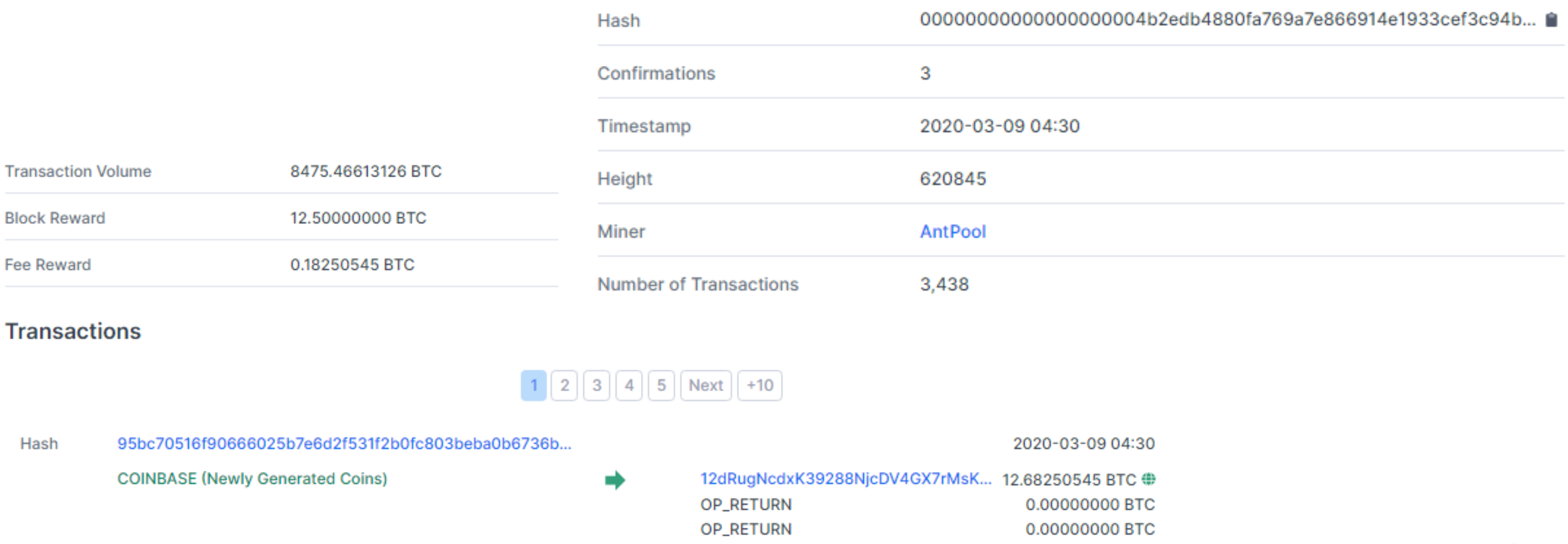
Hash	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77a...			2009-01-04 02:15
	COINBASE (Newly Generated Coins)	➡	1A1zP1eP5QGefi2DMPTfTL5SLmv7Di...	50.00000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 204 bytes)			50.00000000 BTC

Why Mining?

这是设计的规则，10 分钟则是按照算力进行推算的。

- Bitcoins as incentives!
  - Block at depth 620845 in the Bitcoin blockchain – transaction fees

矿工奖励 每210,000个区块减半 按照每10分钟一个区块，
大约四年减半一次 2020.5.12区块链奖励降到6.25BTC



Hash	00000000000000000004b2edb4880fa769a7e866914e1933cef3c94b...
Confirmations	3
Timestamp	2020-03-09 04:30
Height	620845
Miner	AntPool
Number of Transactions	3,438

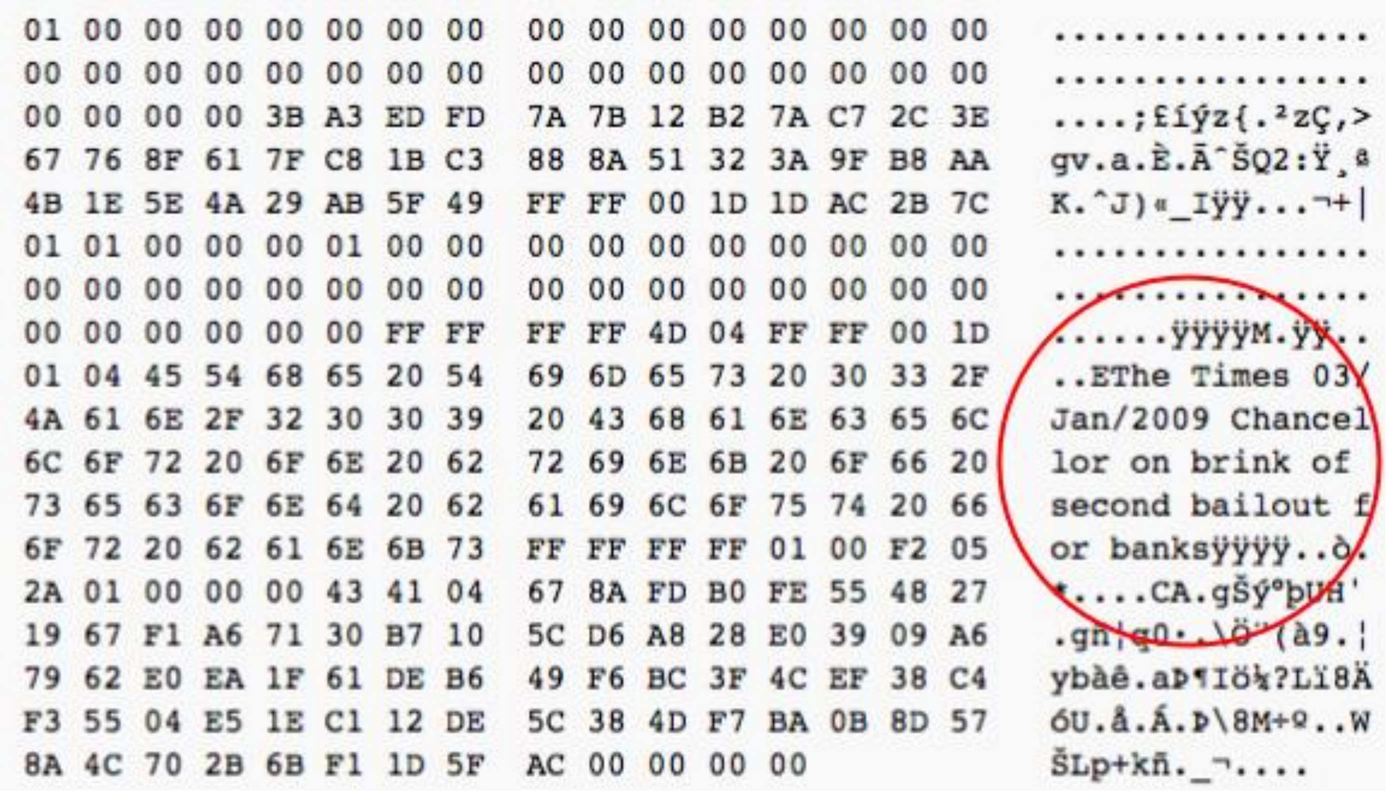
Transaction Volume	8475.46613126 BTC
Block Reward	12.50000000 BTC
Fee Reward	0.18250545 BTC

Transactions

Hash	95bc70516f90666025b7e6d2f531f2b0fc803beba0b6736b...			2020-03-09 04:30
	COINBASE (Newly Generated Coins)	➡	12dRugNcdxK39288NjcDV4GX7rMsK...	12.68250545 BTC
			OP_RETURN	0.00000000 BTC
			OP_RETURN	0.00000000 BTC

Block 0: Genesis Block

- https://www.blockchain.com/btc/block/0
- Generated on January 4, 2009
- Only one transaction 50 bitcoins
- This money is still unspent...
- Flora: contains a hidden message: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks. "
- This is a symbolic pointer to the dangers of centralized issuance of national currencies, in the midst of the global financial crisis.



```
01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of 
73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?Lï8Ä
F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

Blockchain Applications

- All share the same property

  tamper resistant – history is history!

Healthcare

Supply chain

Notary

Clarification of Some Important Concepts

Traditional payment system	Decentralized system
Traditional currencies	Cryptographic digital currencies
Setting up an account at a bank	Address creation through Hash function
Centralized clearing and settlement system	Decentralized and distributed structure
Linked through a network of banks at all levels	Through cooperative blockchain between miners
USD, EURO	Bitcoin, Ethereum

Tech Background

- Cryptographic hash functions
- Proof-of-work
- Distributed consensus

Cryptographic Hash Functions

- A cryptographic hash function takes anything as input **x** and returns a fixed length of string **y**.
- For example, SHA-256 generates a string of 256 bits.

  0000000000000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae

Several important properties:

- Given an input x, it is very easy to find the output y, s.t. y = H(x)
- Given an output y, it is impossible to find an input x, s.t. y = H(x)
- In order to find an output within a range, there is no solving strategy better than trying random inputs

Image courtesy of ratch0013 at FreeDigitalPhotos.net

Cryptographic Hash Functions

- The cryptographic hash function can turn any input value into a fixed length string
- Usually represented by H
- Secure Hash Algorithm (SHA for short) is a family of cryptographic hash functions
- As an example, SHA-256 generates a 256-bit string 这个算法就是 Block Chain 的基础
- 00000000000000000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae
- There are many important applications in information security that use cryptographic hash functions to implement, such as digital signatures, message authentication codes

Characteristics of Cryptographic Hash Function

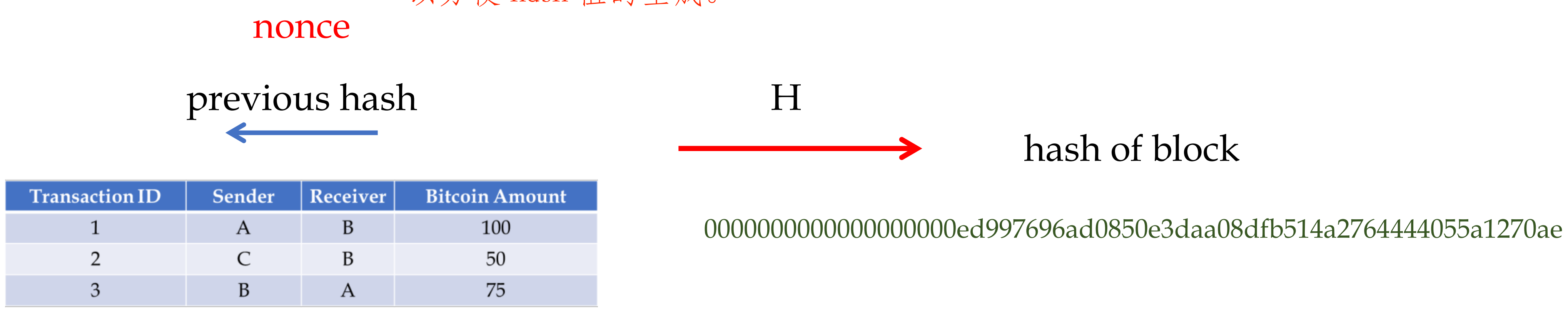
- An ideal cryptographic hash function should have the following main characteristics.
  - For any given input, it can easily compute the hash value.
  - Given a known hash value, it is difficult to derive the original input.
  - It is not feasible to modify the input without changing the hash value.
  - For two different inputs, there is only a very tiny (neglectable) chance that the same hash value will be produced. (Critical)
  - For two subtly different inputs, there is no guarantee that the function will produce a hash value with little difference. 小差异的输入，大差异的输出

Unlike continuous functions commonly known

Hash of Blocks

- hash of block = H (nonce | previous hash | transactions)
- Nonce is the only input variable to be tuned to change output

修改 Nonce 来修改 Block 的 Hash 值，实现目标匹配。
其实也可以修改 transactions，选择小费没那么高的 transactions 进行打包以方便 hash 值的生成。

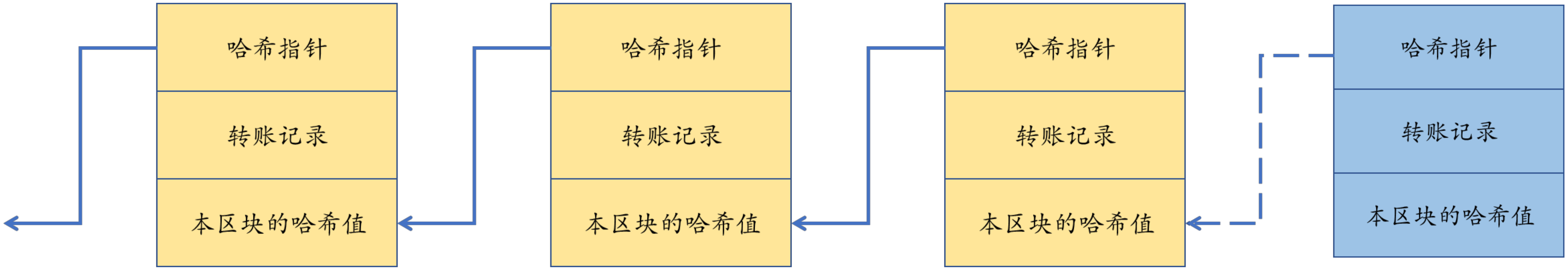


Transaction ID	Sender	Receiver	Bitcoin Amount
1	A	B	100
2	C	B	50
3	B	A	75

0000000000000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae

Block to Blockchain

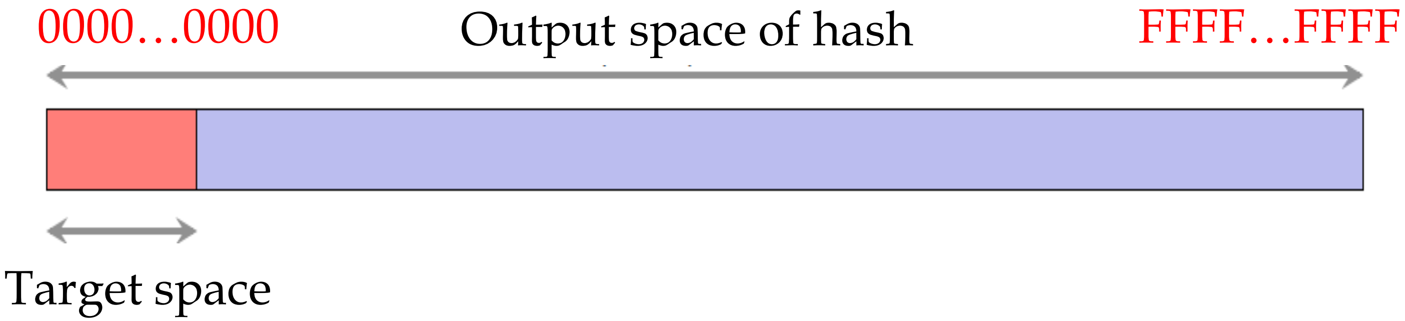
- We now know how to generate the basic content of a single block
- How to generate a blockchain from single blocks? (i.e., to obtain the so-called bookkeeping rights of the blockchain)
- Under the premise of decentralization, anyone can make a block, whose block can be accepted by everyone and thus can be extended at the end of the blockchain?

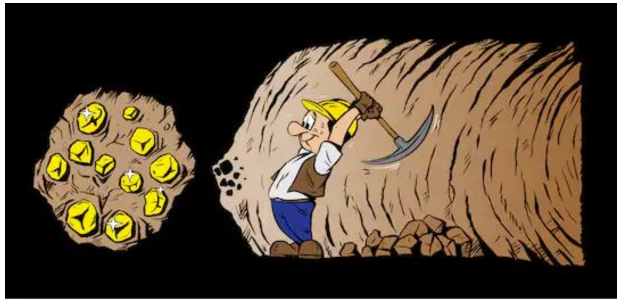


转账记录中也可以只有 Minning Reward 这一条记录，没有人能限制矿工做任何的事情。

Proof of Work – Validating Blocks

- A valid block is a block whose hash falls into the target space
- In practice, the number of leading zeros defines the difficult level. The more zeros, the more difficult.
- The process of finding the satisfying hash is extremely time and energy consuming, thus called mining.

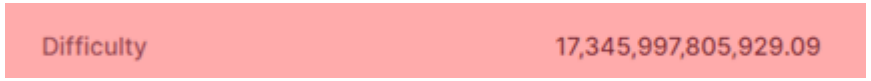




shutterstock.com • 91695749

合格的区块

- 首先，一个区块能被称为合格，必须满足一定的条件
- 对比特币区块链来说，这个条件就是工作量证明，即必须花费一定算力、经过一段时间来找出一个合格的区块
- 合格的量化指标为 难度



Difficulty 17,345,997,805,929.09

区块的哈希值中开头为0的位数 – 位数越多工作量越大

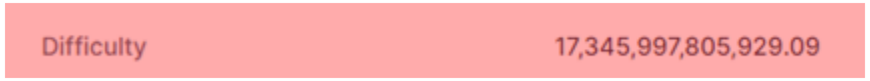
- 0000000000000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae
- 0000000001000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae
- 0100000000000000000000000000000000000000000000000000000000000000

Valid Blocks

- First, for a block to be called valid, it must meet certain conditions
- For the Bitcoin blockchain, this condition is proof of workload, i.e., a certain amount of computing power must be spent over time to find a qualified block
- The quantitative metrics for qualifying are Difficulty

The number of bits in the block's hash that start with a zero - the more bits, the more work

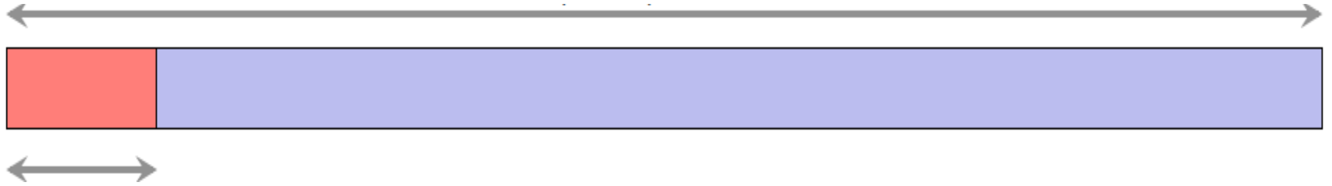
- 0000000000000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae
- 0000000001000000000ed997696ad0850e3daa08dfb514a2764444055a1270ae
- 0100000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000



Difficulty 17,345,997,805,929.09

Illustrations of Difficulty

0000…0000 Range of all hash values from smallest to largest FFFF…FFFF



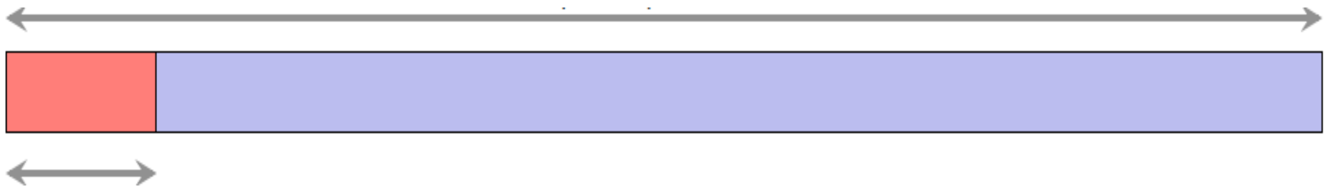
Area that meet the conditions

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

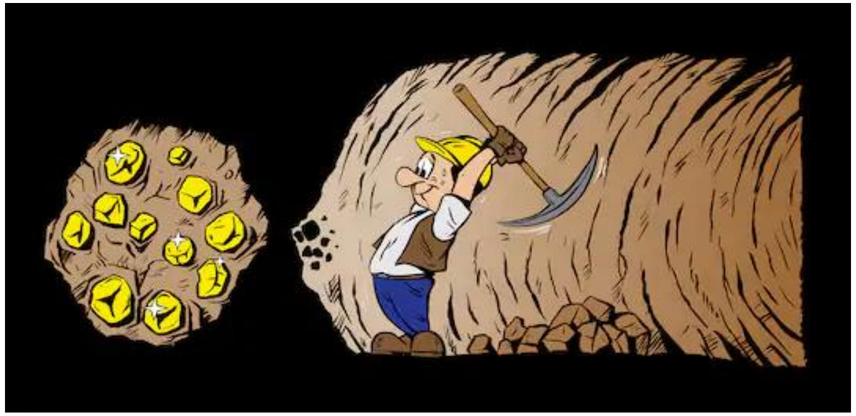
Explanation of the Difficulty

- The more bits in the hash value of a block that starts with a zero, the higher the workload and the corresponding difficulty.
- Finding the qualified hash value, that is, finding the qualified block, is very difficult and requires a lot of time and energy, so it is called mining

0000…0000 Range of all hash values from smallest to largest FFFF…FFFF



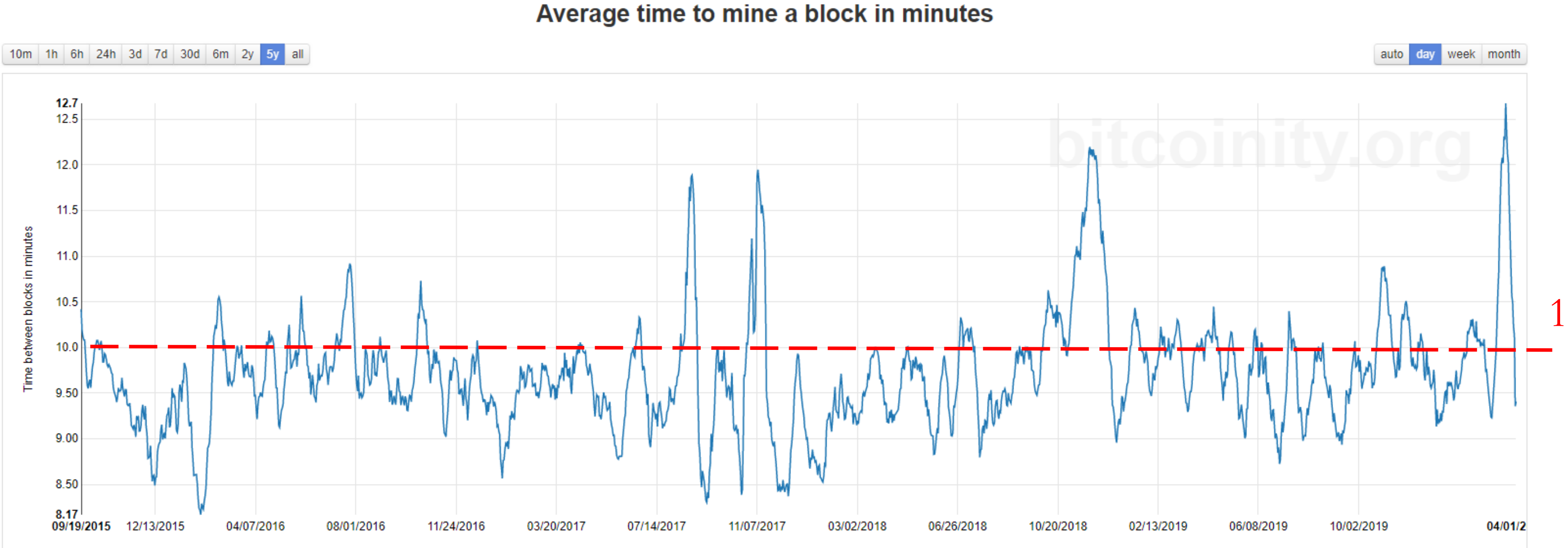
Area that meet the conditions



shutterstock.com • 91695749

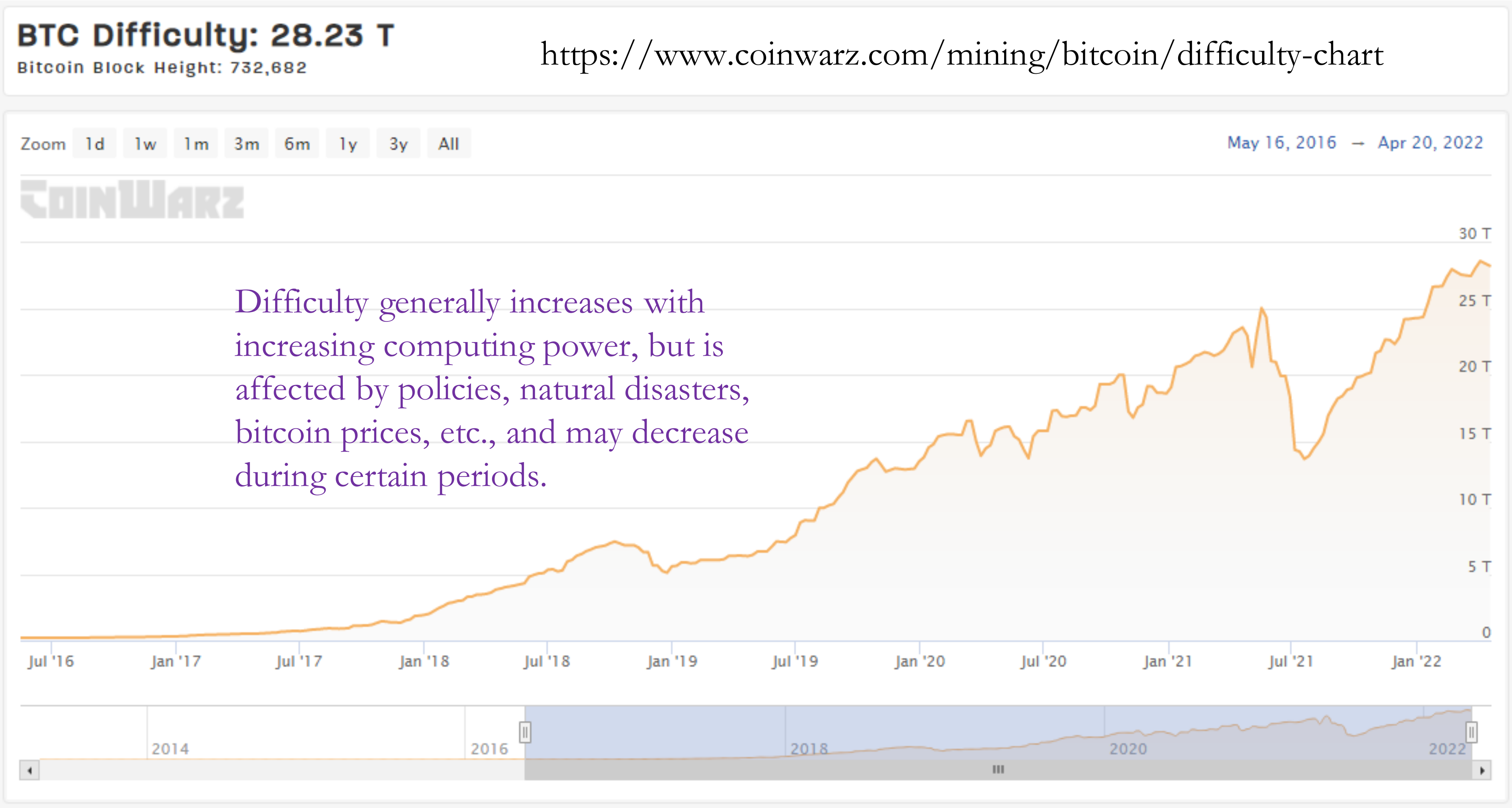
Proof of Work

- The goal of the Bitcoin network is to produce one block in ten minutes on average, so the difficulty criteria (number of leading 0) is adjusted to make that happen
- The only way to find the hash value of a block that meets the above difficulty condition is to change the value of Nonce, given the transaction record and the hash pointer fixed or chosen
- The Bitcoin network requires that the mining difficulty be adjusted every 2016 blocks, and 2016 is exactly two weeks, so the time interval for each difficulty adjustment is about two weeks.



10 minutes

Adjusting Difficulty



BTC Difficulty: 28.23 T

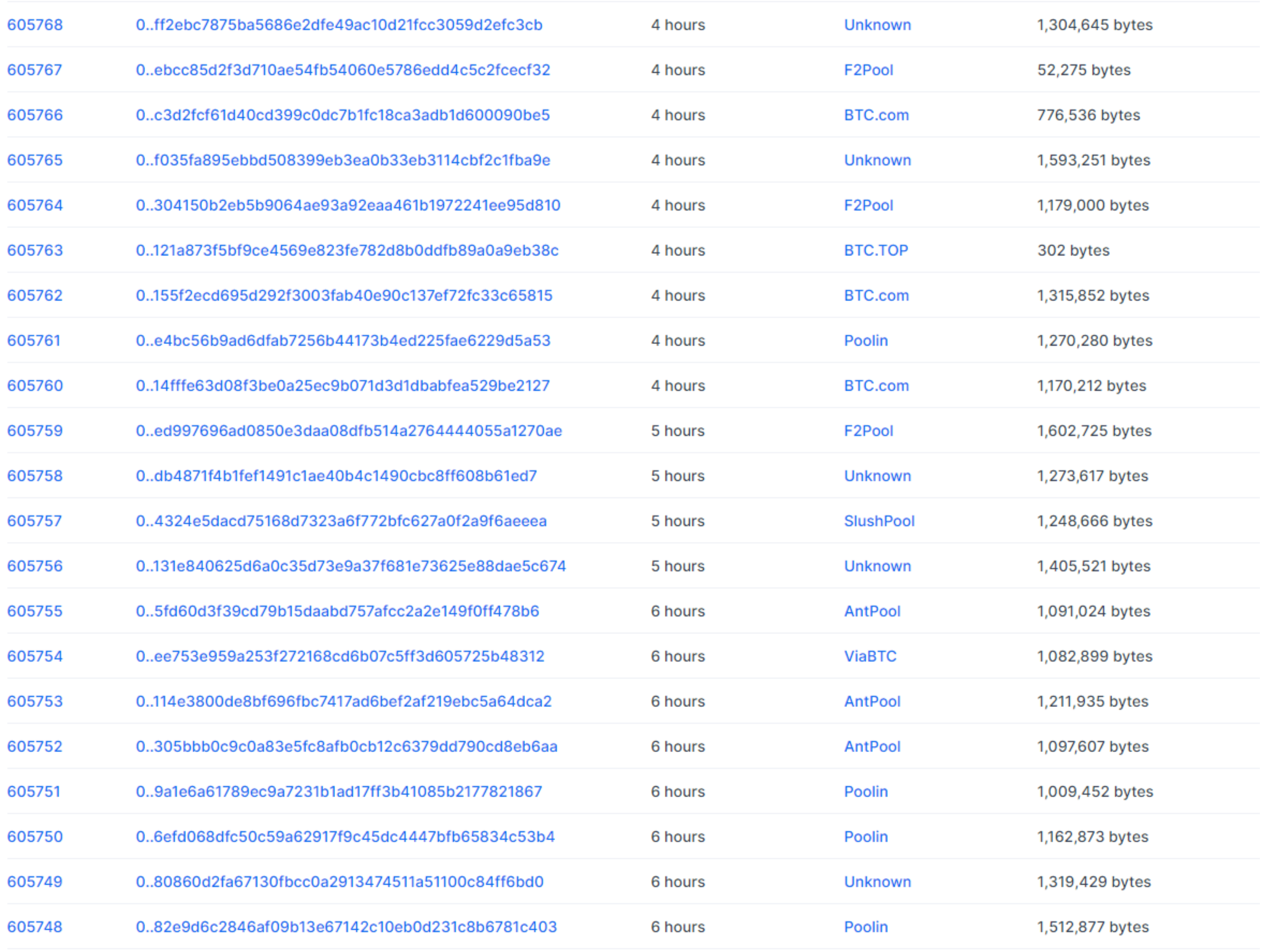
Bitcoin Block Height: 732,682

https://www.coinwarz.com/mining/bitcoin/difficulty-chart

May 16, 2016 → Apr 20, 2022

Difficulty generally increases with increasing computing power, but is affected by policies, natural disasters, bitcoin prices, etc., and may decrease during certain periods.

How Hard is Mining? One block per 10mins



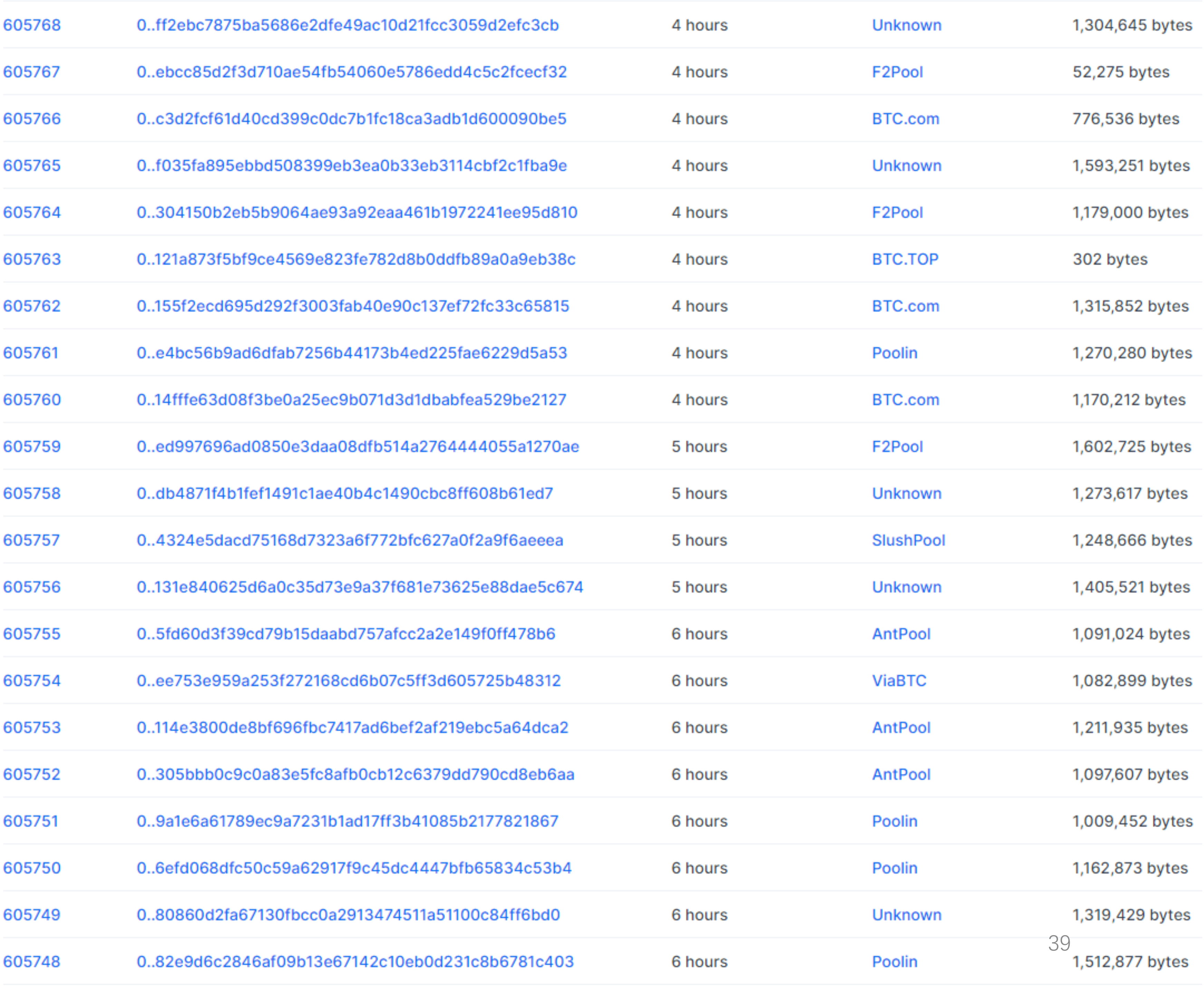
605768	0..ff2ebc7875ba5686e2dfe49ac10d21fcc3059d2efc3cb	4 hours	Unknown	1,304,645 bytes
605767	0..ebcc85d2f3d710ae54fb54060e5786edd4c5c2fcecf32	4 hours	F2Pool	52,275 bytes
605766	0..c3d2fcf61d40cd399c0dc7b1fc18ca3adb1d600090be5	4 hours	BTC.com	776,536 bytes
605765	0..f035fa895ebbd508399eb3ea0b33eb3114cbf2c1fba9e	4 hours	Unknown	1,593,251 bytes
605764	0..304150b2eb5b9064ae93a92eaa461b1972241ee95d810	4 hours	F2Pool	1,179,000 bytes
605763	0..121a873f5bf9ce4569e823fe782d8b0ddfb89a0a9eb38c	4 hours	BTC.TOP	302 bytes
605762	0..155f2ecd695d292f3003fab40e90c137ef72fc33c65815	4 hours	BTC.com	1,315,852 bytes
605761	0..e4bc56b9ad6dfab7256b44173b4ed225fae6229d5a53	4 hours	Poolin	1,270,280 bytes
605760	0..14fffe63d08f3be0a25ec9b071d3d1dbabfea529be2127	4 hours	BTC.com	1,170,212 bytes
605759	0..ed997696ad0850e3daa08dfb514a2764444055a1270ae	5 hours	F2Pool	1,602,725 bytes
605758	0..db4871f4b1fef1491c1ae40b4c1490cbc8ff608b61ed7	5 hours	Unknown	1,273,617 bytes
605757	0..4324e5dacd75168d7323a6f772bfc627a0f2a9f6aeeea	5 hours	SlushPool	1,248,666 bytes
605756	0..131e840625d6a0c35d73e9a37f681e73625e88dae5c674	5 hours	Unknown	1,405,521 bytes
605755	0..5fd60d3f39cd79b15daabd757afcc2a2e149f0ff478b6	6 hours	AntPool	1,091,024 bytes
605754	0..ee753e959a253f272168cd6b07c5ff3d605725b48312	6 hours	ViaBTC	1,082,899 bytes
605753	0..114e3800de8bf696fbc7417ad6bef2af219ebc5a64dca2	6 hours	AntPool	1,211,935 bytes
605752	0..305bbb0c9c0a83e5fc8afb0cb12c6379dd790cd8eb6aa	6 hours	AntPool	1,097,607 bytes
605751	0..9a1e6a61789ec9a7231b1ad17ff3b41085b2177821867	6 hours	Poolin	1,009,452 bytes
605750	0..6efd068dfc50c59a62917f9c45dc4447bfb65834c53b4	6 hours	Poolin	1,162,873 bytes
605749	0..80860d2fa67130fbcc0a2913474511a51100c84ff6bd0	6 hours	Unknown	1,319,429 bytes
605748	0..82e9d6c2846af09b13e67142c10eb0d231c8b6781c403	6 hours	Poolin	1,512,877 bytes

Actual Mining Time

Not strictly one block every 10 minutes

Some blocks take more time to generate and some blocks take less time

On average, a block is generated roughly every 10 minutes

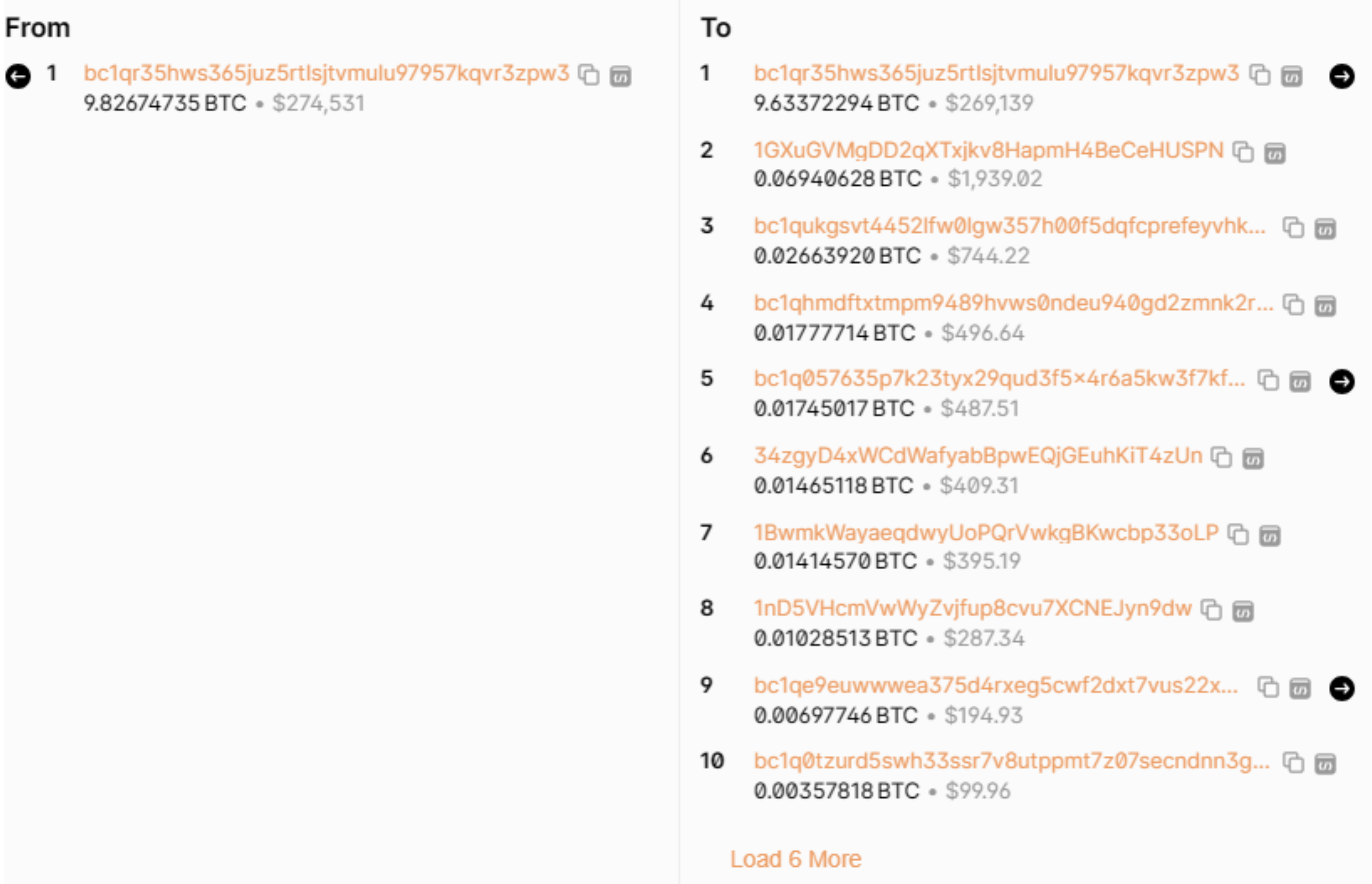


605768	0..ff2ebc7875ba5686e2dfe49ac10d21fcc3059d2efc3cb	4 hours	Unknown	1,304,645 bytes
605767	0..ebcc85d2f3d710ae54fb54060e5786edd4c5c2fcecf32	4 hours	F2Pool	52,275 bytes
605766	0..c3d2fcf61d40cd399c0dc7b1fc18ca3adb1d600090be5	4 hours	BTC.com	776,536 bytes
605765	0..f035fa895ebbd508399eb3ea0b33eb3114cbf2c1fba9e	4 hours	Unknown	1,593,251 bytes
605764	0..304150b2eb5b9064ae93a92eaa461b1972241ee95d810	4 hours	F2Pool	1,179,000 bytes
605763	0..121a873f5bf9ce4569e823fe782d8b0ddfb89a0a9eb38c	4 hours	BTC.TOP	302 bytes
605762	0..155f2ecd695d292f3003fab40e90c137ef72fc33c65815	4 hours	BTC.com	1,315,852 bytes
605761	0..e4bc56b9ad6dfab7256b44173b4ed225fae6229d5a53	4 hours	Poolin	1,270,280 bytes
605760	0..14fffe63d08f3be0a25ec9b071d3d1dbabfea529be2127	4 hours	BTC.com	1,170,212 bytes
605759	0..ed997696ad0850e3daa08dfb514a2764444055a1270ae	5 hours	F2Pool	1,602,725 bytes
605758	0..db4871f4b1fef1491c1ae40b4c1490cbc8ff608b61ed7	5 hours	Unknown	1,273,617 bytes
605757	0..4324e5dacd75168d7323a6f772bfc627a0f2a9f6aeeea	5 hours	SlushPool	1,248,666 bytes
605756	0..131e840625d6a0c35d73e9a37f681e73625e88dae5c674	5 hours	Unknown	1,405,521 bytes
605755	0..5fd60d3f39cd79b15daabd757afcc2a2e149f0ff478b6	6 hours	AntPool	1,091,024 bytes
605754	0..ee753e959a253f272168cd6b07c5ff3d605725b48312	6 hours	ViaBTC	1,082,899 bytes
605753	0..114e3800de8bf696fbc7417ad6bef2af219ebc5a64dca2	6 hours	AntPool	1,211,935 bytes
605752	0..305bbb0c9c0a83e5fc8afb0cb12c6379dd790cd8eb6aa	6 hours	AntPool	1,097,607 bytes
605751	0..9a1e6a61789ec9a7231b1ad17ff3b41085b2177821867	6 hours	Poolin	1,009,452 bytes
605750	0..6efd068dfc50c59a62917f9c45dc4447bfb65834c53b4	6 hours	Poolin	1,162,873 bytes
605749	0..80860d2fa67130fbcc0a2913474511a51100c84ff6bd0	6 hours	Unknown	1,319,429 bytes
605748	0..82e9d6c2846af09b13e67142c10eb0d231c8b6781c403	6 hours	Poolin	1,512,877 bytes

Why Mining?

- Bitcoins as incentives!
    - Check the real block chain page again.
- How to create a block and get rewarded?
    - Identify the last block of the block chain
    - Transaction verification – no double spending (check the status of coin)
    - Find the hash of the block to meet the difficult level
    - Send the block to the internet and pray
    - If the block gets accepted to the end of the longest block chain, block reward is confirmed.

Status of Bitcoin



From

1 bc1qr35hws365juz5rtlsjtvmulu97957kqvr3zpw3
9.82674735 BTC • $274,531

To

1 bc1qr35hws365juz5rtlsjtvmulu97957kqvr3zpw3
9.63372294 BTC • $269,139

2 1GXuGVMgDD2qXTxjkv8HapmH4BeCeHUSPN
0.06940628 BTC • $1,939.02

3 bc1qukgsvt4452lfw0lgw357h00f5dqfcprefeyvhk...
0.02663920 BTC • $744.22

4 bc1qhmdftxtmpm9489hvws0ndeu940gd2zmnk2r...
0.01777714 BTC • $496.64

5 bc1q057635p7k23tyx29qud3f5×4r6a5kw3f7kf...
0.01745017 BTC • $487.51

6 34zgyD4xWCdWafyabBpwEQjGEuhKiT4zUn
0.01465118 BTC • $409.31

7 1BwmkWayaeqdwyUoPQrVwkgBKwcbp33oLP
0.01414570 BTC • $395.19

8 1nD5VHcmVwWyZvjfup8cvu7XCNEJyn9dw
0.01028513 BTC • $287.34

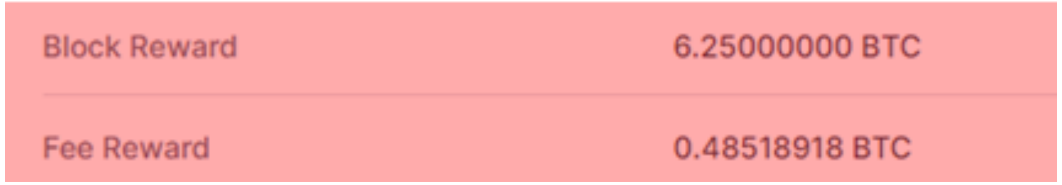
9 bc1qe9euwwwea375d4rxeg5cwf2dxt7vus22x...
0.00697746 BTC • $194.93

10 bc1q0tzurd5swh33ssr7v8utppmt7z07secndnn3g...
0.00357818 BTC • $99.96

https://www.blockchain.com/explorer/blocks/btc/811290

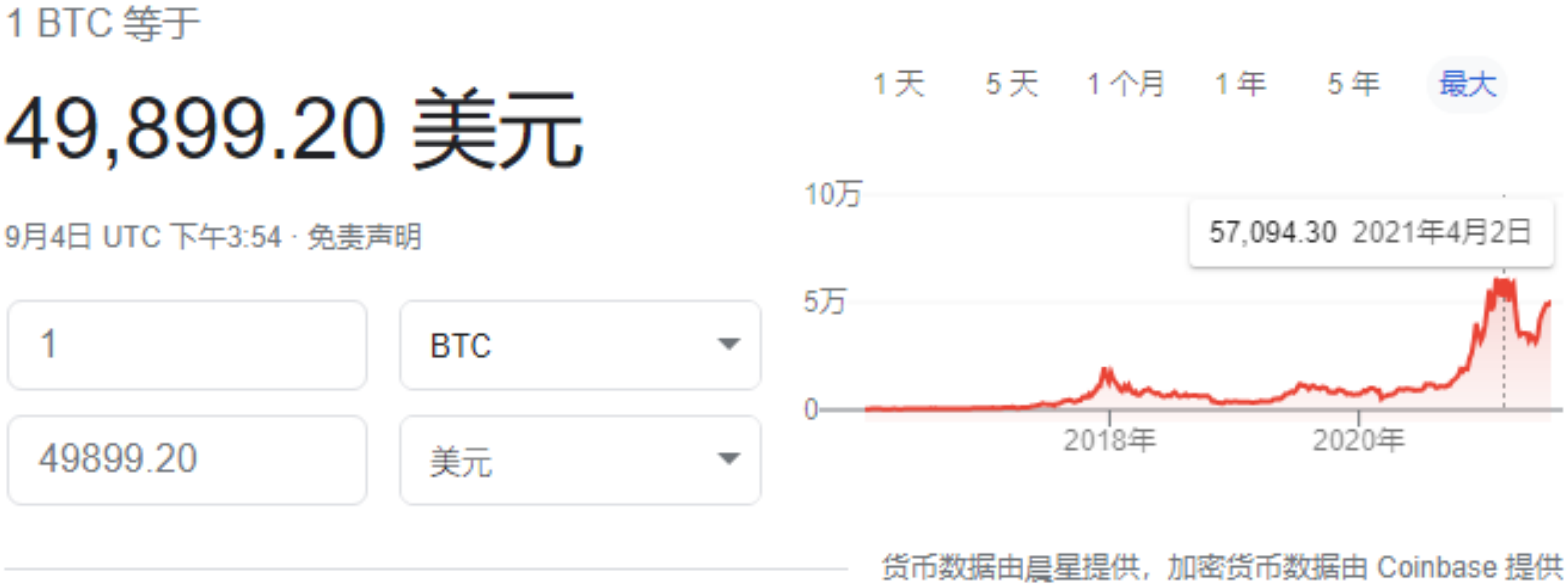
Why Fight for Blockchain Bookkeeping Rights?

- Bitcoins as a reward! Miners deserve to be rewarded for helping users record transactions, including the transaction fees that users give to miners in addition to the block rewards in Bitcoin's initial design



Block Reward	6.25000000 BTC
Fee Reward	0.48518918 BTC

Approximately equal to 2.17 million RMB



1 BTC 等于

49,899.20 美元

9月4日 UTC 下午3:54 · 免责声明

1	BTC
49899.20	美元

货币数据由晨星提供，加密货币数据由 Coinbase 提供

Process of Mining Rewards

- What needs to be done?
  - Find the latest blocks on the blockchain if possible
  - Select some transaction records and do a check on those transactions to make sure there are no double flowers 甚至也可以只有奖励自己的那一个 transaction
  - Put the transaction records together with the hash pointer and find the right block hash by adjusting the Nonce
  - Broadcast the qualified block to everyone as soon as possible, praying that the block is accepted as the latest block
  - By the time the block is officially confirmed as the newest member of the blockchain, the reward is also confirmed by everyone
- The end result is 挖出来某一个特定区块后，可以在挖出来的区块继续往后挖。矿工会用实际行动进行投票，继续挖出来后会广播自己已经挖成功了，让外界知道。
  - Bitcoin transactions are recognized and recorded into the blockchain as consensus
  - Bitcoins are consumed and new Bitcoins are created and ready to use

只有区块被确认后，块上的交易记录也才会被确认

Important Points

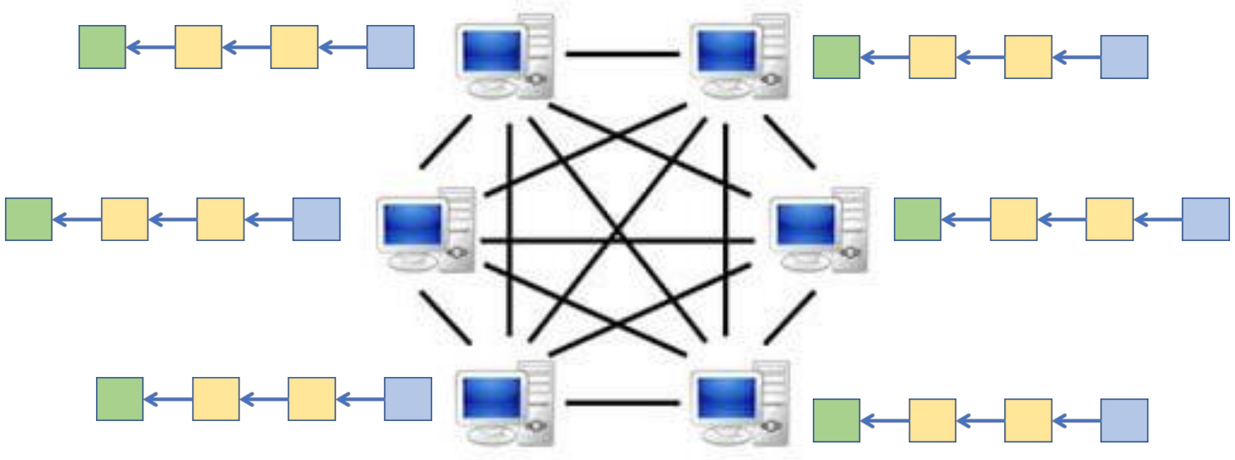
- Here's where the magic comes in: bitcoins are created out of thin air by miners

- Whether or not you own bitcoins is determined by the distributed consensus of others: if everyone says you have money, you have money, if everyone says you don't have money, you don't have money 这个不仅是说笑，如果大部分节点都掌握在一个人手里面的话，就可能出现这个情况

- What are the potential pitfalls?

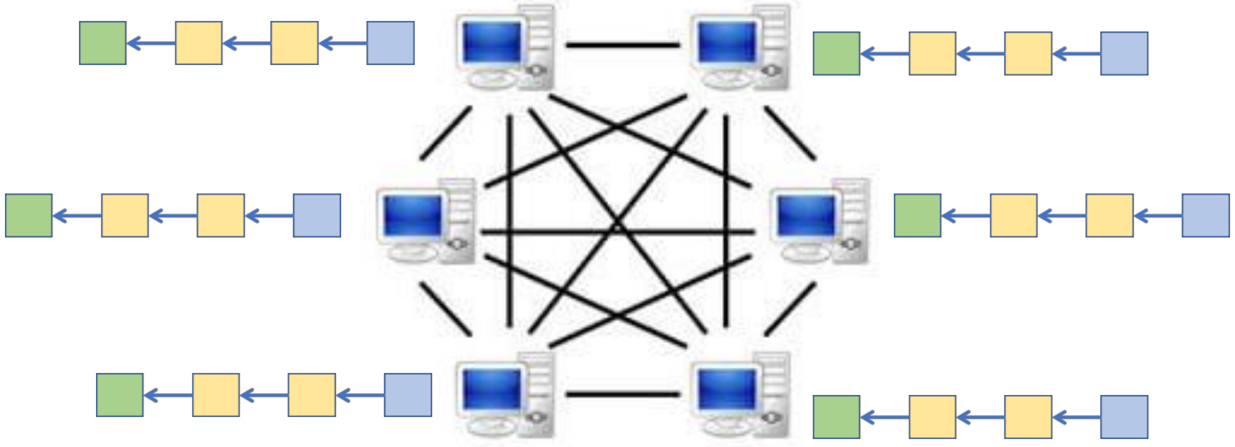
Decentralized Distributed Database

- The blochchain is completely open to anyone on the internet.
- The blockchain is replicated and propagated over the whole network, and therefore is essentially a distributed database.
- There is no central administrator – decentralized.

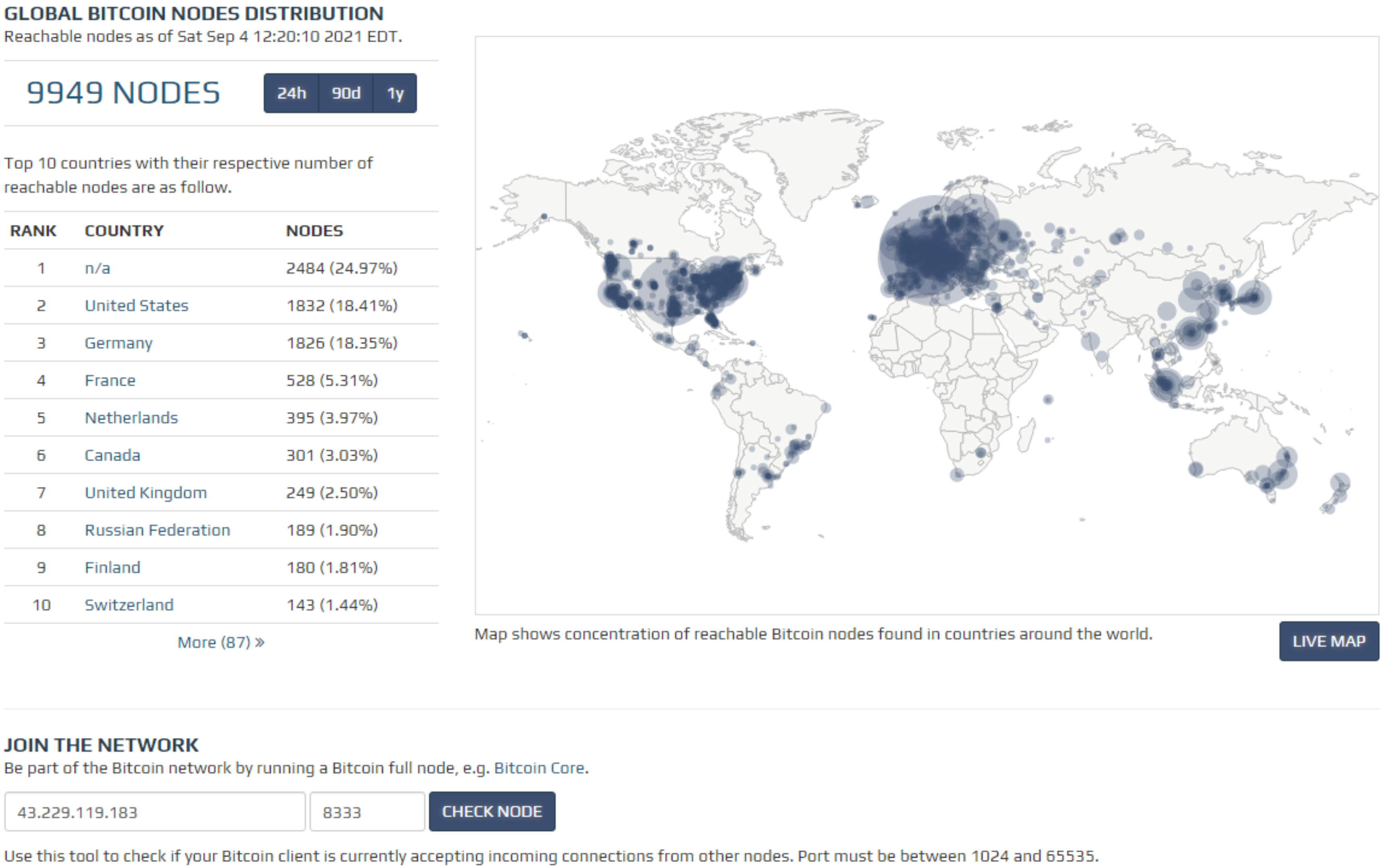


分布式共识

- 比特币区块链的信息对所有人公开
- 比特币的健壮性在于所有信息都被网络重复备份和传播，可以看做一个分布式的数据库系统
- 去中心化的共识机制：多数确认才行，时间优先，最长的链优先
- 信息通过网络的传播需要时间！



Network Foundation of the Bitcoin Blockchain https://bitnodes.io/



GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Sat Sep 4 12:20:10 2021 EDT.

9949 NODES

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	2484 (24.97%)
2	United States	1832 (18.41%)
3	Germany	1826 (18.35%)
4	France	528 (5.31%)
5	Netherlands	395 (3.97%)
6	Canada	301 (3.03%)
7	United Kingdom	249 (2.50%)
8	Russian Federation	189 (1.90%)
9	Finland	180 (1.81%)
10	Switzerland	143 (1.44%)

More (87) »

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

JOIN THE NETWORK

Be part of the Bitcoin network by running a Bitcoin full node, e.g. Bitcoin Core.

43.229.119.183 | 8333

Use this tool to check if your Bitcoin client is currently accepting incoming connections from other nodes. Port must be between 1024 and 65535.

Different Scenarios for Block Chain Extension

How does the block chain extend?

矿工不会相信任何一个人，所以在挖矿的时候会检查前一个 Block 因为 Block 中，完全可能出现 Mining Reward 夸大的情况，这是不能被承认的，因此很难有人作弊成功。

Note from the miners’ point of view

- If there is only one newly generated block?
- If there are 3 newly generated blocks? 选哪一个都可以，关键看在这之后哪一个被挖出来
- If there is only one newly generated block, but this block’s hash pointer points a different block from the previously recognized one?

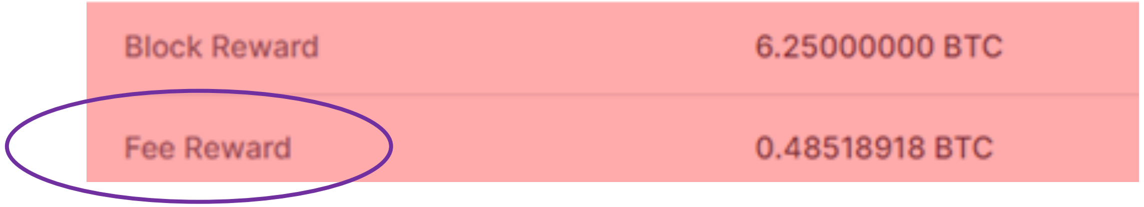
只有交易记录在链上的时候才会被大众所认可，否则不会被接受

Distributed Consensus: More Examples

- What about the following scenarios?
  - You receive a blockchain update message from a person claiming to have mined the latest block, and the hash pointer of the block you are currently mining points to the last block in the same blockchain as that latest block
  - You receive two blockchain updates at the same time, with two different people both claiming to have mined new blocks
  - You receive an update message with the previous message confirming the last block in the blockchain as 600001 and the current message with the last block in the blockchain as 600010

Distributed Consensus: Discussion

- To date, there is no sound theory with solid proof
  - Bitcoin blockchain as a case practice is ahead of the theory
  - It is possible to explain some of the behavior with the help of game theory (the establishment of mining pools and
  - Miners are the key to support the whole blockchain backbone, whether their interests can be satisfied determines whether the bitcoin blockchain is sustainable or not
  - Miners' rewards for mining: halved every 210,000 blocks, or about once every four years at one block every 10 minutes, for a total of 21 million
  - Blockchain rewards dropped to 6.25 BTC on 2020.5.12 and are expected to drop to 3.125 BTC on 2024.5.3. What next? Miners' revenue comes mainly from transaction fees paid by users

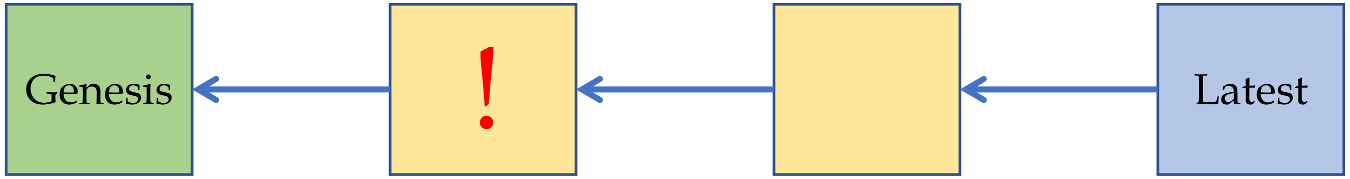


Block Reward	6.25000000 BTC
Fee Reward	0.48518918 BTC

Approximately equal to 2.17 million RMB

Blockchain is Tamper Resistant

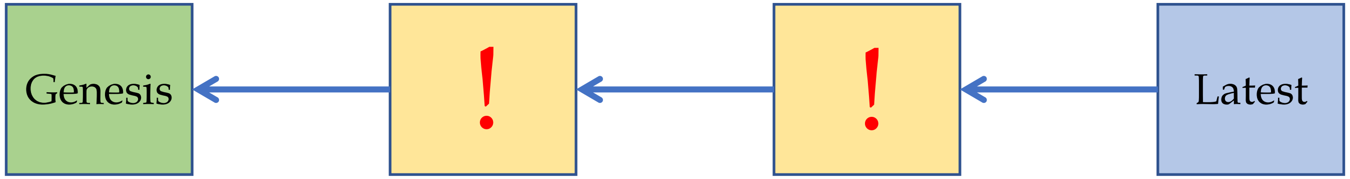
- Once a transaction has been recorded inside a blockchain, it is very difficult to change it.
- If some transaction gets changed, then the hash of the block and the hash pointer contained in the following block won’t match.
- It is easy to identify where the modification happens.



Hash	183F	3T7A	568A	0V67
Previous Hash	0000	183F	7B29	568A

Chained Reactions

- A change of hash pointer will cause the hash of the whole block to change.
- In order to make the blockchain valid again, all following blocks of the downstream of the blockchain have to be altered.
- In reality, technically infeasible! 需要将全链都修改了，这是不可能的！



Hash	183F	3T7A	9557	0V67
Previous Hash	0000	183F	3T7A	568A

What Block Chain Can Do

- Avoid double spending 规避双花问题
- Allow anonymous transactions 允许匿名交易 ✓
- Guarantee transaction completion 保证交易完成 ✓
- Convenient to realize transaction 方便实现转账 ✓

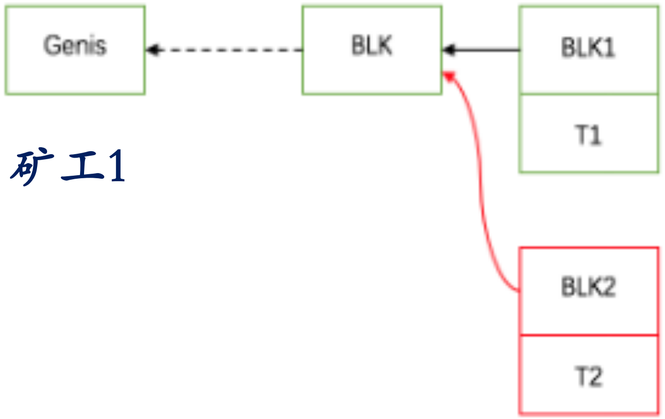
Double Spending 双花问题

- The double spend problem refers to the same amount of money used to make two or more payments
- For traditional currencies or under centralized regulation, it can't happen
- For digital currencies, such as Bitcoin, it is a big problem because the consensus mechanism takes time to reach
- Specific problem description.
  - User A has only 100 bitcoins in total, and he transactions 100 bitcoins to User B and 100 bitcoins to User C. Who gets the 100 bitcoins?
  - The conclusion is uncertain...

https://www.zhihu.com/question/39948446

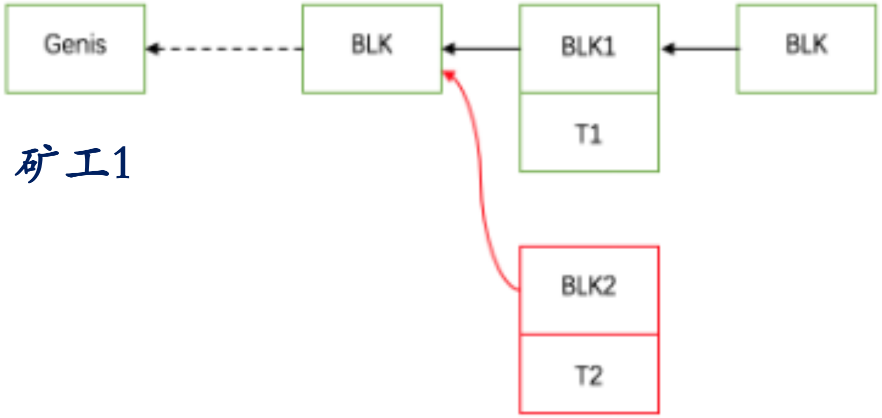
T1, T2 are transactions from A to B, C respectively

节点以 BLK1 延长自己的区块链，BLK2 位于备用链



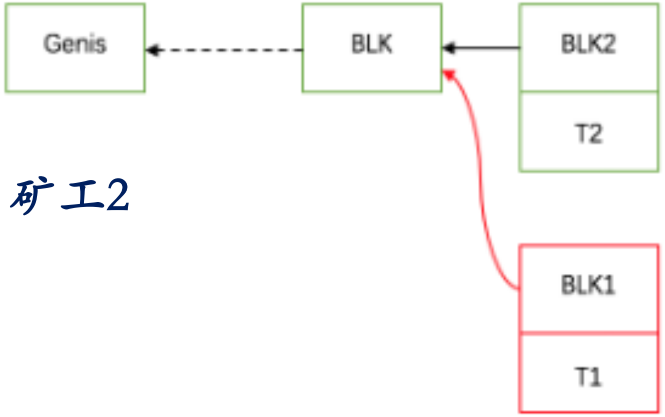
矿工1

节点以 BLK1 延长自己的区块链，BLK2 位于备用链



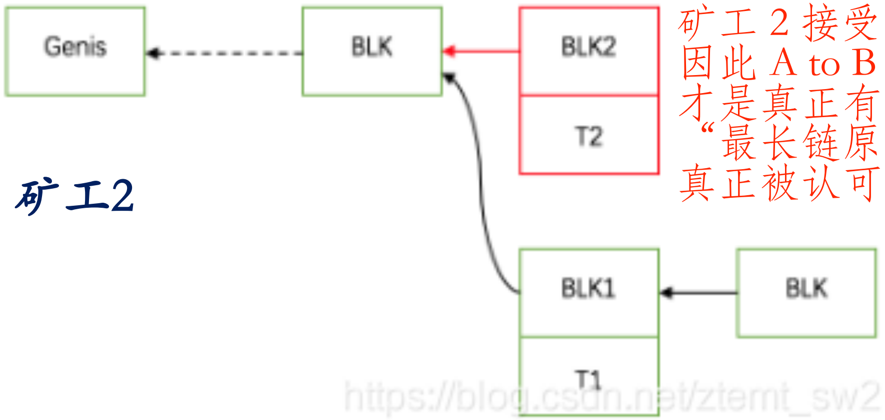
矿工1

节点以 BLK2 延长自己的区块链，BLK1 位于备用链



矿工2

节点以切换主链，BLK1 位于主链，BLK2 位于备用链

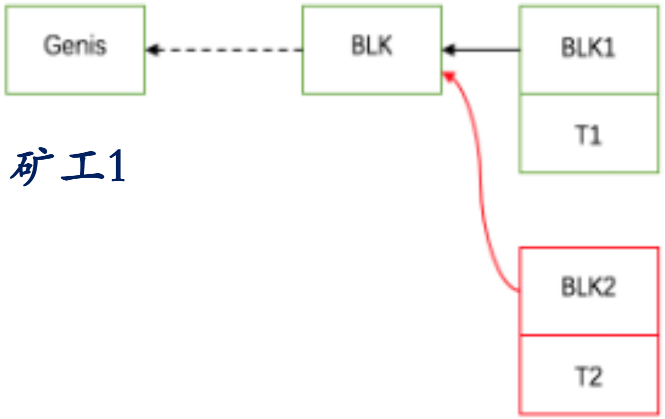


矿工2

矿工 2 接受了 BLK 1
因此 A to B 才真正上链
才是真正有效的
“最长链原则”表示哪些是
真正被认可的块。

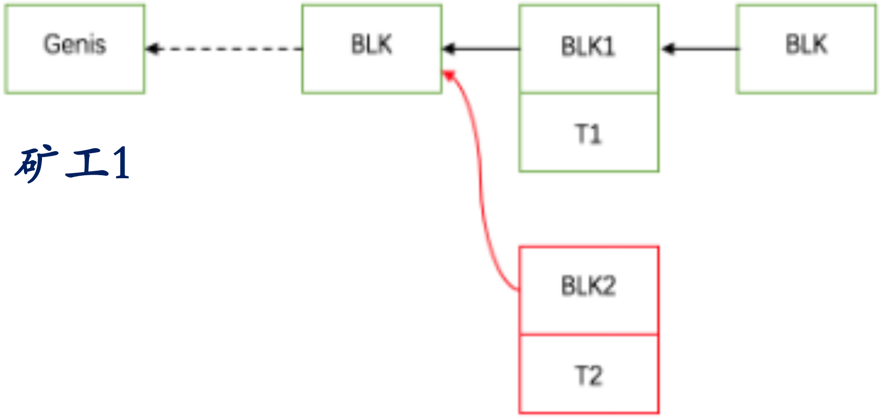
T1, T2 are transactions from A to B, C respectively

节点以 BLK1 延长自己的区块链，BLK2 位于备用链



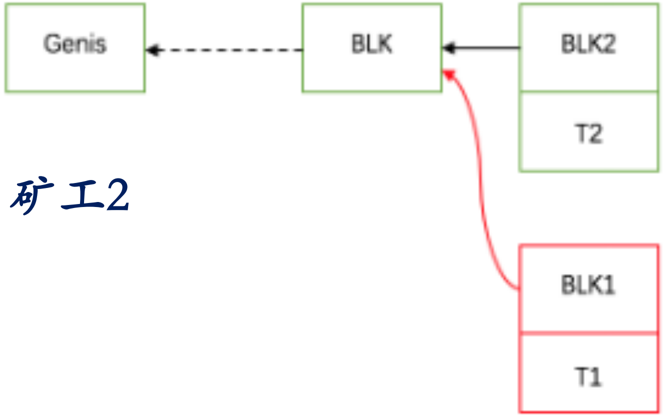
矿工1

节点以 BLK1 延长自己的区块链，BLK2 位于备用链



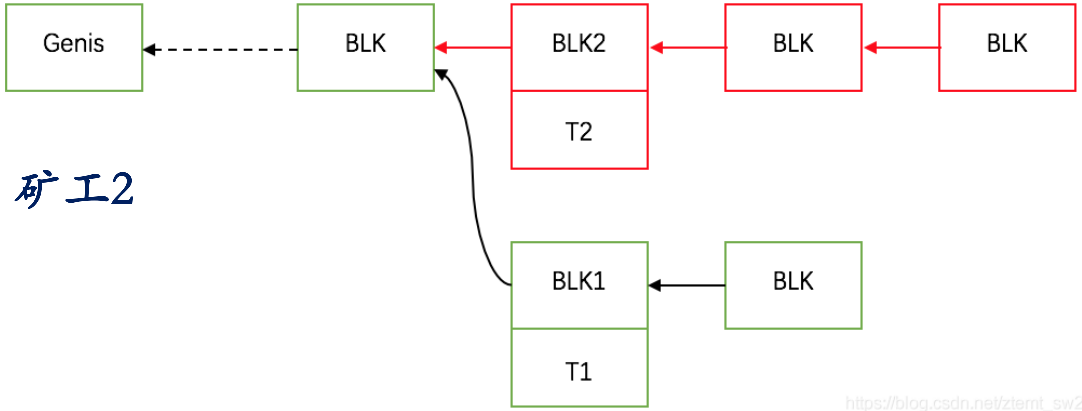
矿工1

节点以 BLK2 延长自己的区块链，BLK1 位于备用链



矿工2

攻击链累计工作量超过主链，导致主链切换



矿工2

Distributed Consensus - Highlights

- Bitcoin blockchain information is public and open to all
- Bitcoin blockchain is robust in that all information is repeatedly backed up and propagated by the network, and can be seen as a distributed database system 空 10 分钟挖出下一个区块，就是想让矿工在真空期获得所有信息。
- Information takes time to propagate through the network!
- Decentralized consensus mechanism: most confirmations to work, time first, longest chain first
- Usually more than 6 confirmations are needed, which corresponds to more than 1 hour 这是 Bitcoin 的一个核心缺陷，但是小交易目前不需要等一个小时确认，大交易需要
  这些缺陷也是其他一些加密货币出现的原因
- Any questions?

Discussion of Centralization and Decentralization

- Decentralization
  - Information has redundancy and is scattered throughout the network
  - Updates to information can be initiated by anyone
  - Benefit: not easily corrupted
  - Problem: consensus is not easy to reach
- Centralized
  - Information generation, updating, and sharing are all initiated by one credit department
  - Benefits: Efficiency and consistency
  - Problem: Dependence on the credit of one central department

Other Options for Consensus Mechanisms

- https://zhuanlan.zhihu.com/p/92228813
- https://www.chaindd.com/3184907.html
- Bit Cash Block Time
- https://www.beekuaibao.com/article/562656933501231104
- https://zhuanlan.zhihu.com/p/35712880
- https://zhuanlan.zhihu.com/p/55278868

What Block Chain Can Do

- Avoid double spending 规避双花问题 √ (部分解决，并不完美)
- Allow anonymous transactions 允许匿名交易 √
- Guarantee transaction completion 保证交易完成 √
- Convenient to realize transaction 方便实现转账 √