東莞理工學院
DONGGUAN UNIVERSITY OF TECHNOLOGY

区块链技术与应用

v0.3.11

第二章：区块链核心思想

丁烨，网络空间安全学院 副教授
dingye@dgut.edu.cn

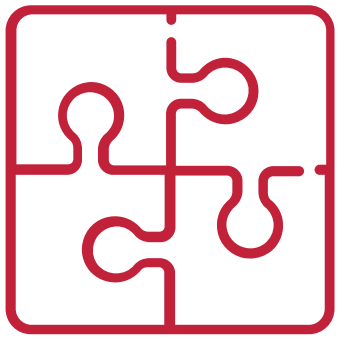
区块链核心思想

"To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the bitcoin currency, the specific blockchain that underpins it and the idea of blockchains in general."

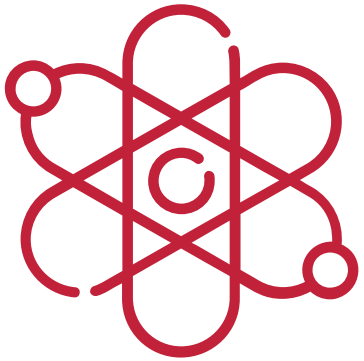
"The Trust Machine," The Economist

Oct. 31, 2015

区块链核心思想



Blockchain

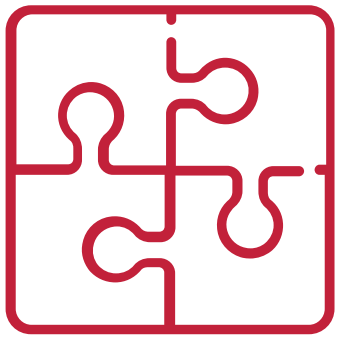


Consensus

Cryptocurrency

目录

区块链核心思想



Blockchain

Consensus

Cryptocurrency

狭义区块链

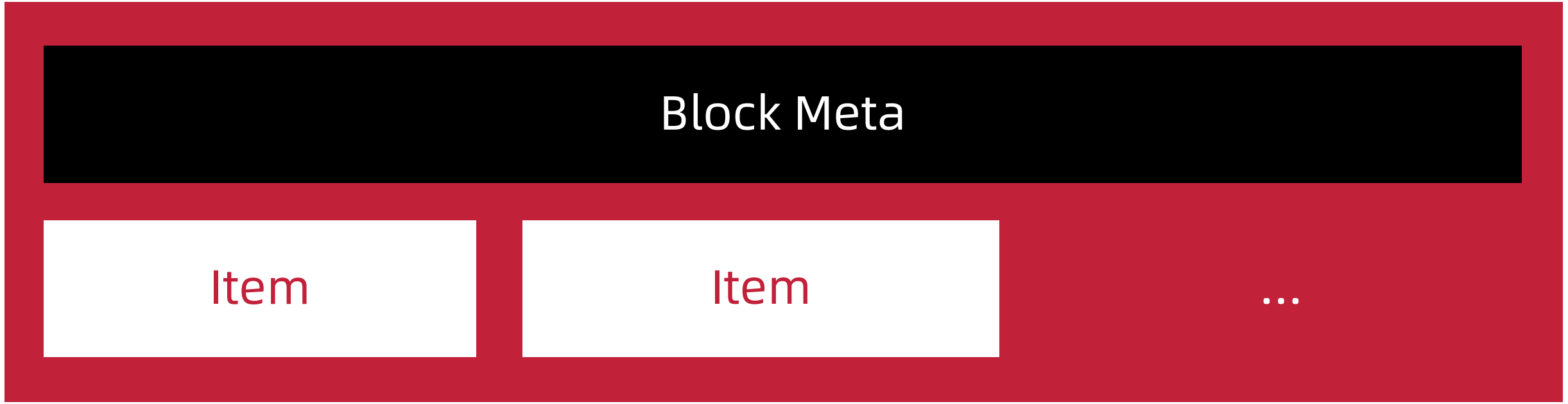
理解区块链

- 区块链（Blockchain）本质上是一个数据库
- 该数据库的设计目的为：安全、防止篡改
- 但是，区块链为了安全付出了运行缓慢的代价

狭义区块链

理解区块链

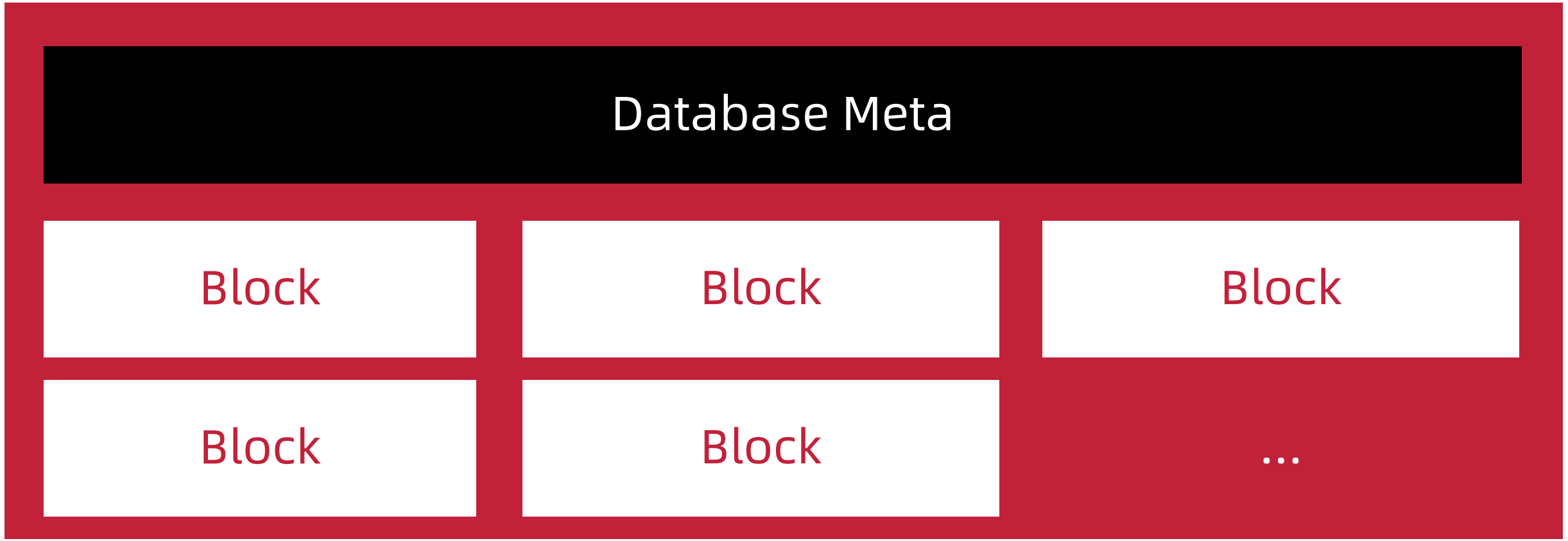
- “区块”（Block）



狭义区块链

理解区块链

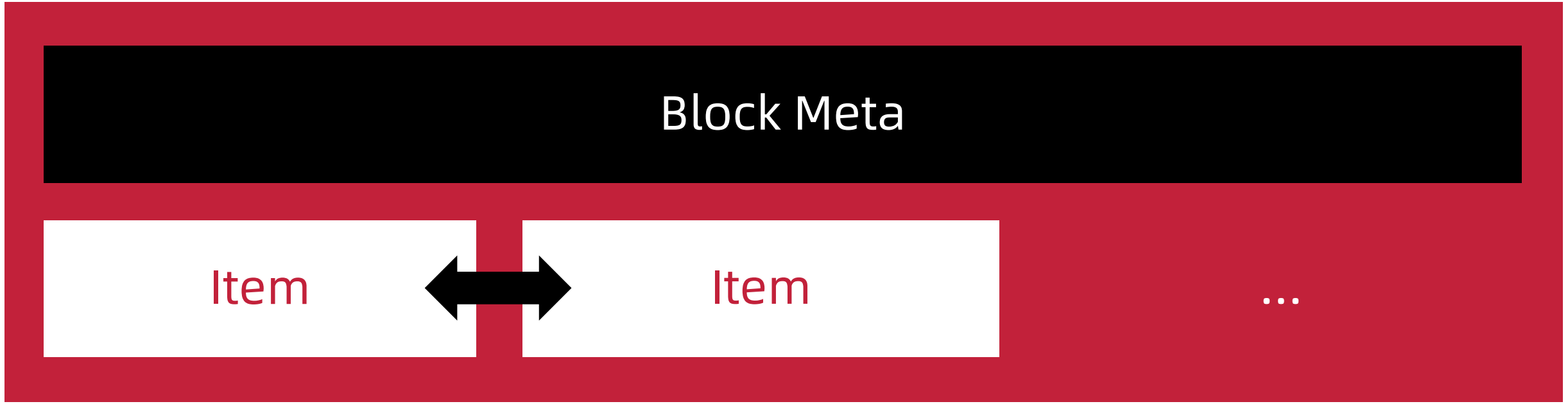
- “区块”（Block）



狭义区块链

理解区块链

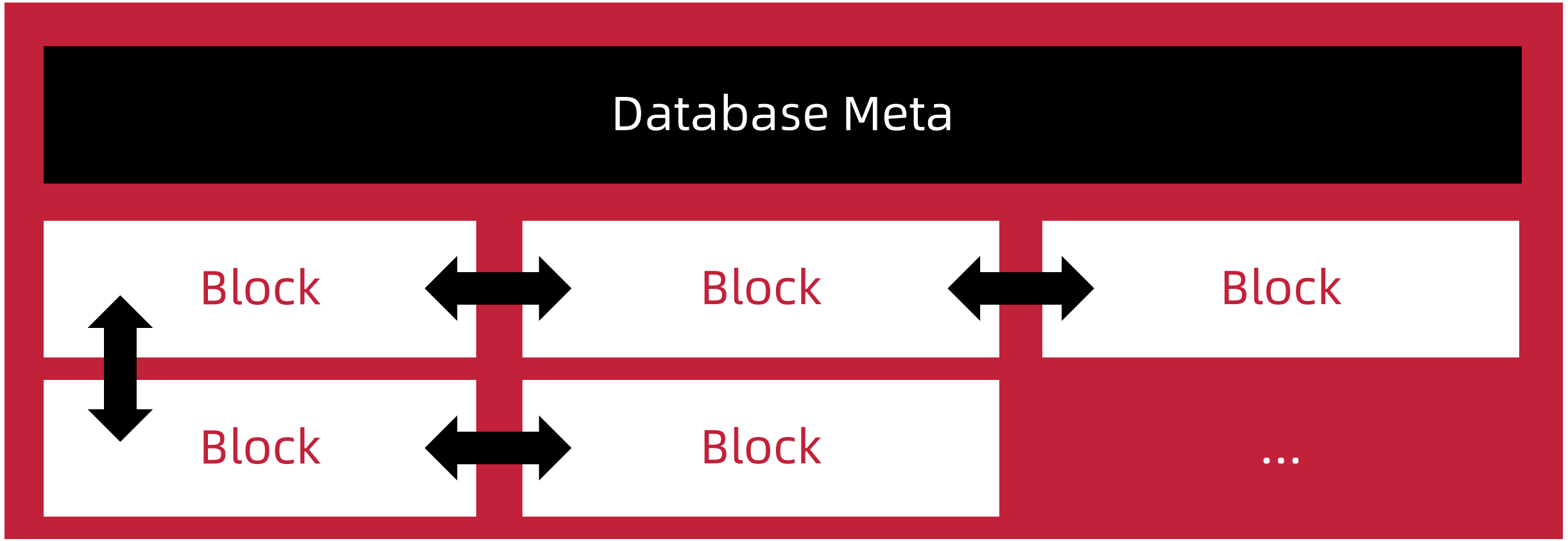
- “链”（Chain）



狭义区块链

理解区块链

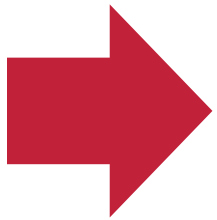
❖ “链”（Chain）



狭义区块链

理解区块链

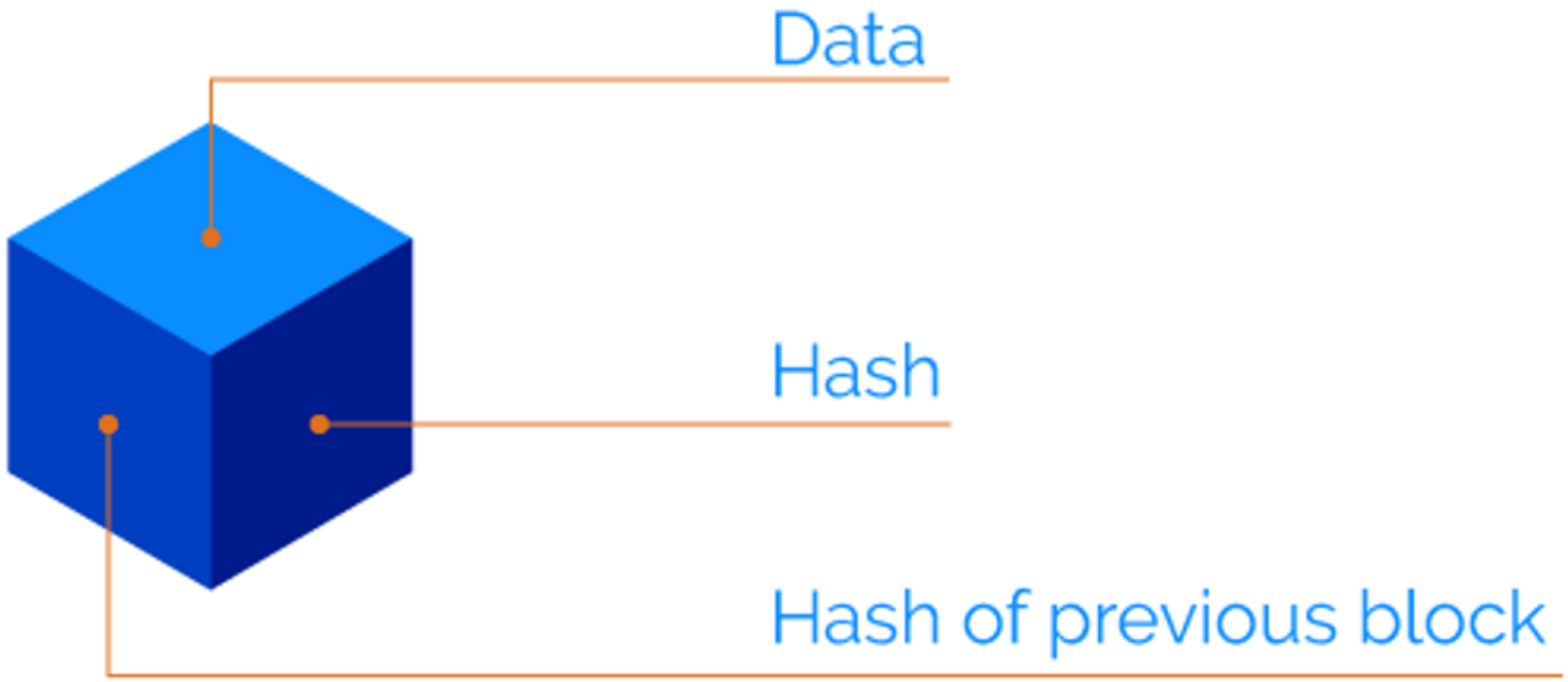
- “区块链”（Blockchain）

Block Chain  Blockchain

~2013

狭义区块链

散列函数



狭义区块链

散列函数


Hash
000dc75a315c77a1f9c98fb6247d03dd18ac52632d7dc6a9920261d8109b37cf

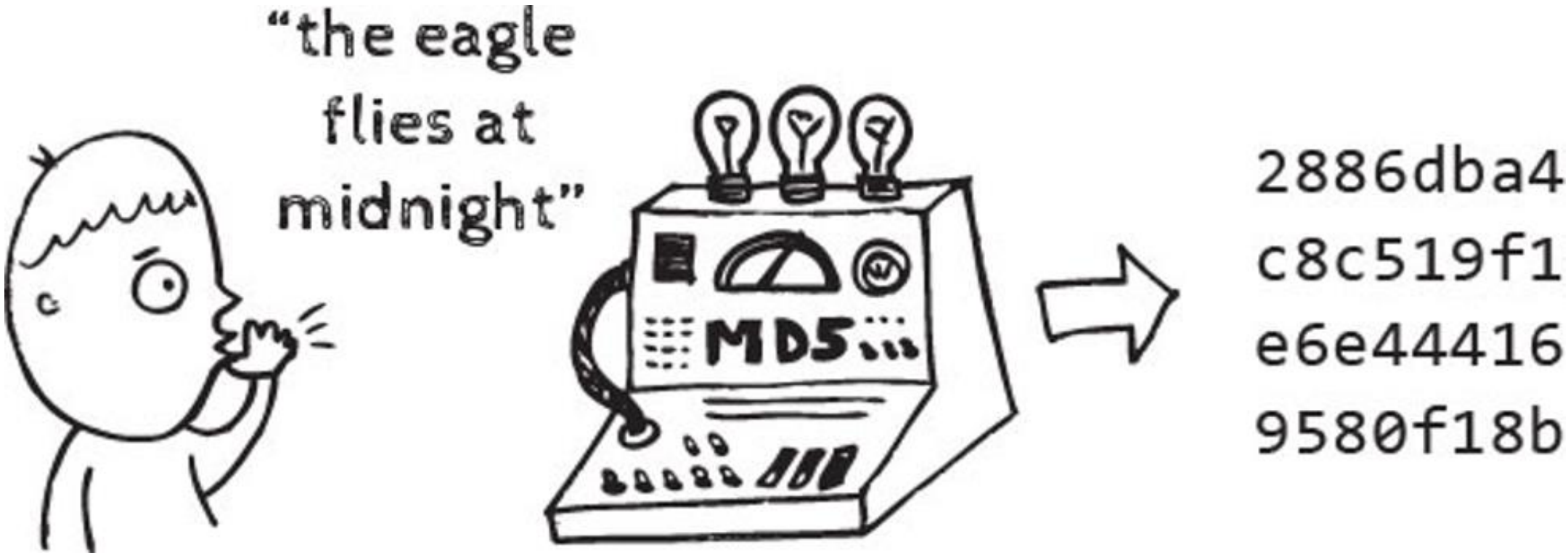
狭义区块链

散列函数


Hash
4f90feb5c789bf7a5d9e667caf9fc4f9b6fce74a9f53735236d29f7f03dc687a

狭义区块链

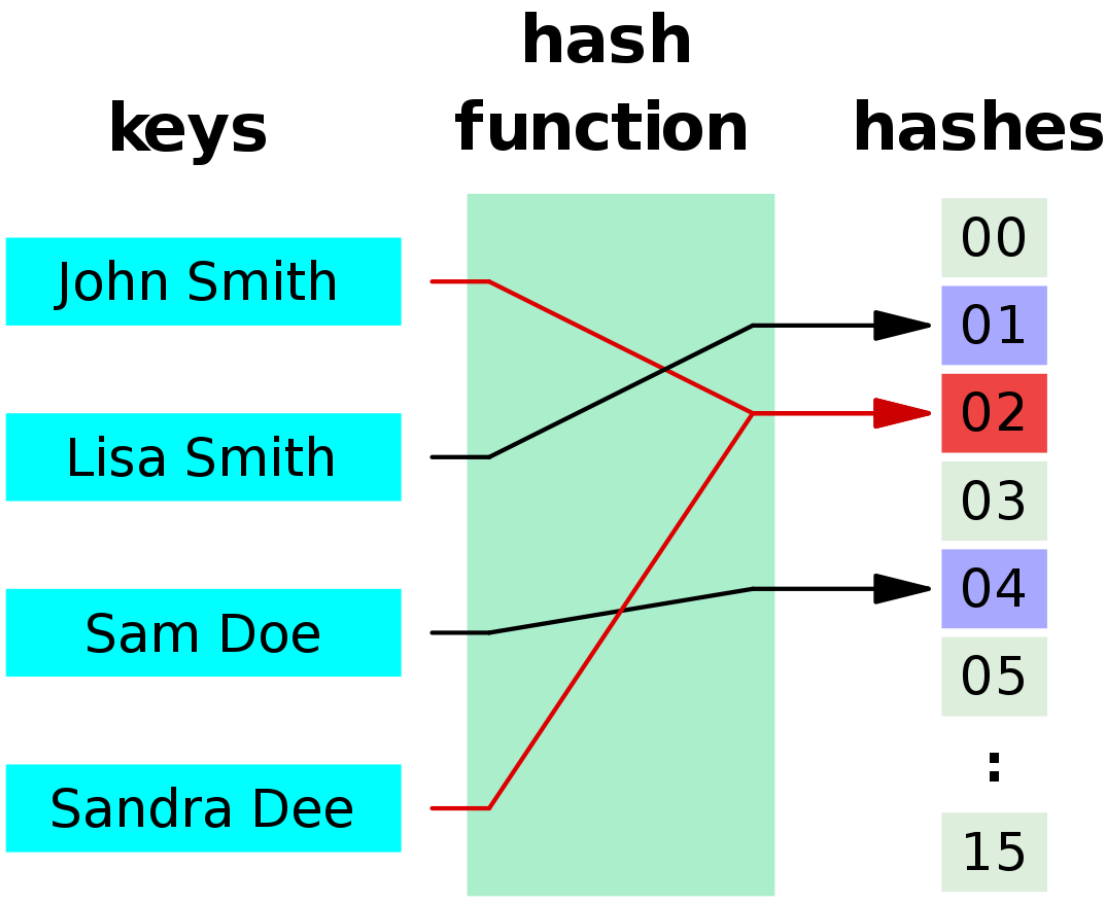
散列函数


"the eagle
flies at
midnight"
MD5
2886dba4
c8c519f1
e6e44416
9580f18b

狭义区块链

散列函数

- CRC-32
- HMAC
- MD5
- SHA-1
- SHA-256



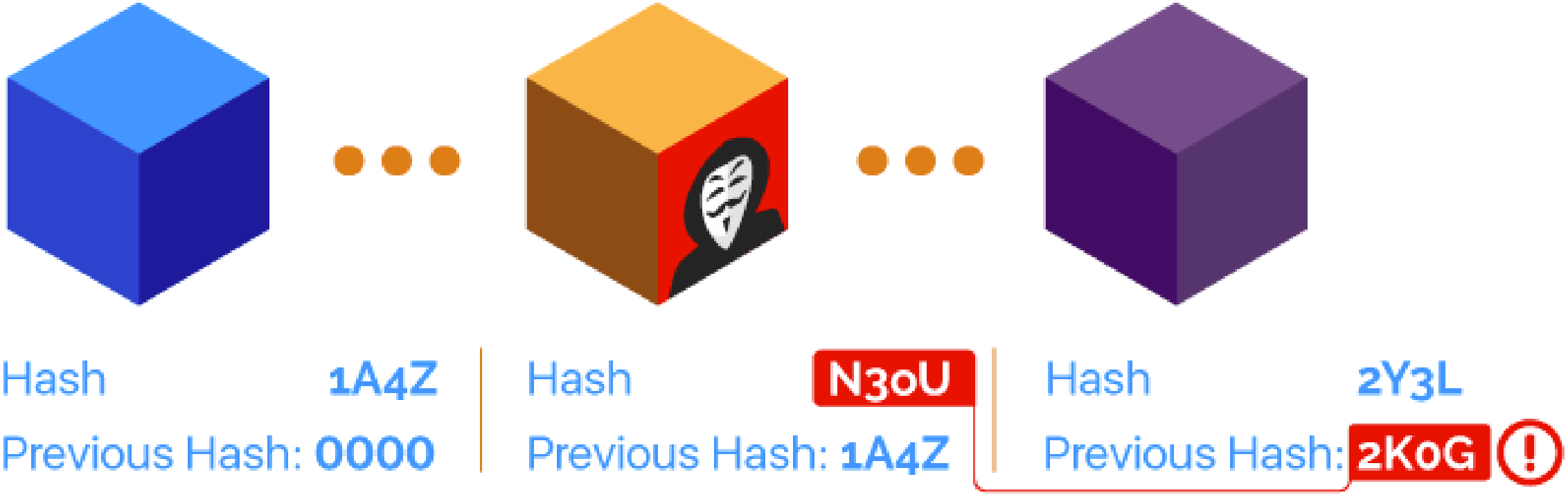
狭义区块链

散列函数


Hash 1A4Z
Previous Hash: 0000
Hash 2K0G
Previous Hash: 1A4Z
Hash 2Y3L
Previous Hash: 2K0G

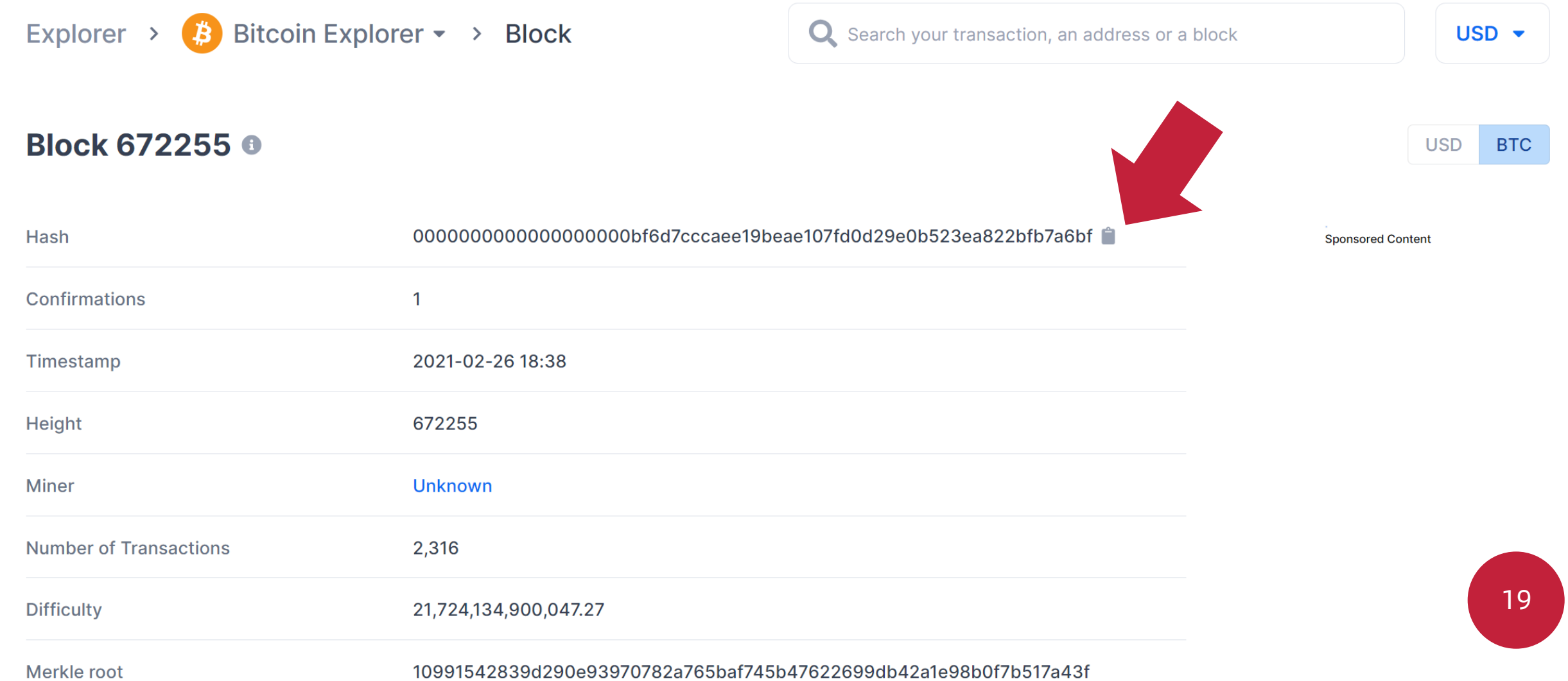
狭义区块链

散列函数


Hash 1A4Z
Previous Hash: 0000
Hash N30U
Previous Hash: 1A4Z
Hash 2Y3L
Previous Hash: 2K0G

狭义区块链

散列函数


Explorer
Bitcoin Explorer
Block
Search your transaction, an address or a block
USD
Block 672255
USD
BTC
Hash
000000000000000000bf6d7cccaee19beae107fd0d29e0b523ea822bfb7a6bf
Sponsored Content
Confirmations
1
Timestamp
2021-02-26 18:38
Height
672255
Miner
Unknown
Number of Transactions
2,316
Difficulty
21,724,134,900,047.27
Merkle root
10991542839d290e93970782a765baf745b47622699db42a1e98b0f7b517a43f

狭义区块链

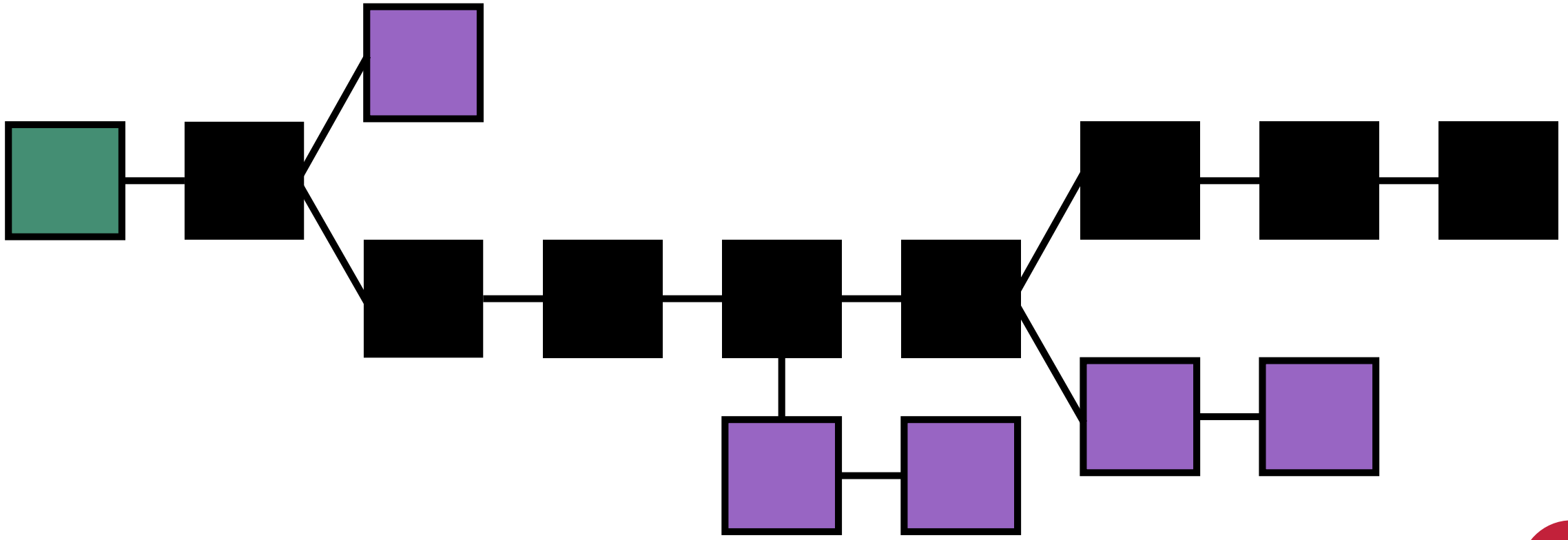
散列函数

Block Transactions

Hash	f8bd2abd818a2b01d8013188fe6acab240ffe31d970c5a5f6b93afac...			2021-02-26 18:38
	COINBASE (Newly Generated Coins)		1DSh7vX6ed2cgTeKPwufV5i4hSi4pp373h	7.13334315 BTC
			OP_RETURN	0.00000000 BTC
			OP_RETURN	0.00000000 BTC
Fee	0.00000000 BTC (0.000 sat/B - 0.000 sat/WU - 291 bytes)			7.13334315 BTC 1 Confirmations
Hash	98945a610cb8c554e4660a9d85b2392e8003cbbd0a863af3be56a...			2021-02-22 14:30
	3L53rUVPf3mXs31uCSzkE45SWvZNsFoD3U	0.09960000 BTC	14TbzLywiFWeL5okjudjtpcWmDCaazT1aW	0.08893577 BTC
			3L53rUVPf3mXs31uCSzkE45SWvZNsFoD3U	0.01063063 BTC
Fee	0.00003360 BTC (13.494 sat/B - 5.022 sat/WU - 249 bytes)			0.09956640 BTC 1 Confirma
Hash	cfb1ab1ab6d75fbe4f894bcd57342ab3bb66790b72f44ba839bdc9...			2021-02-16 12:25

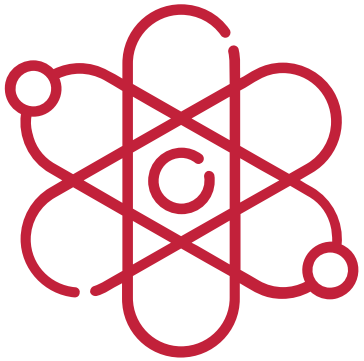
狭义区块链

分叉（Branching）



区块链核心思想

Blockchain



Consensus

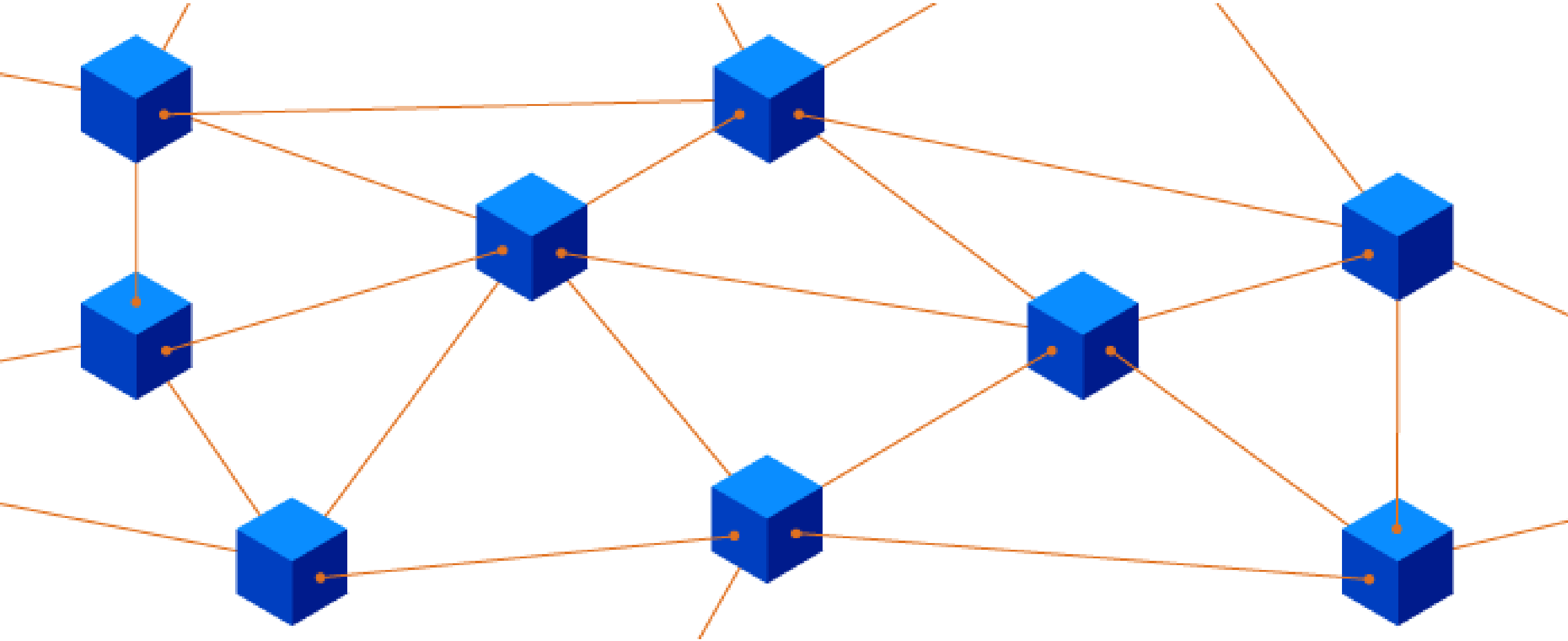
Cryptocurrency

目录

- 狭义区块链
- 共识
- 广义区块链

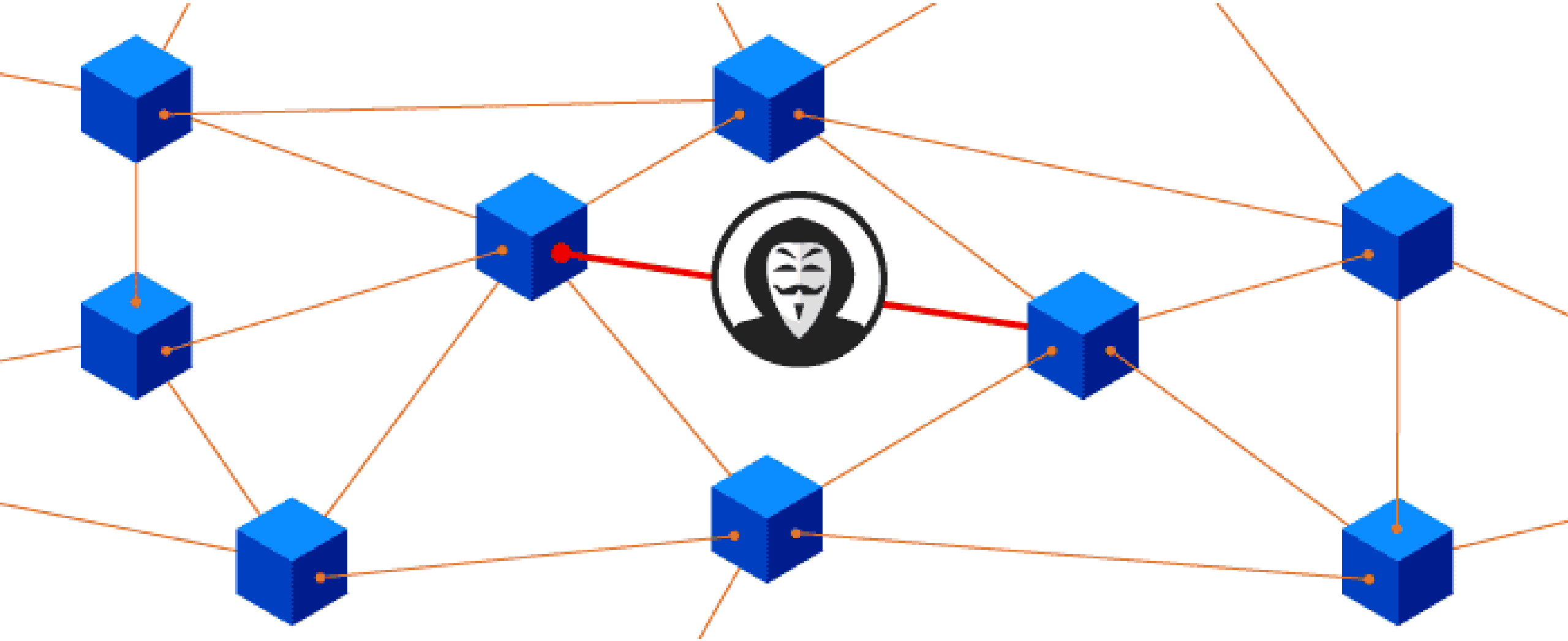
共识

共识的目的



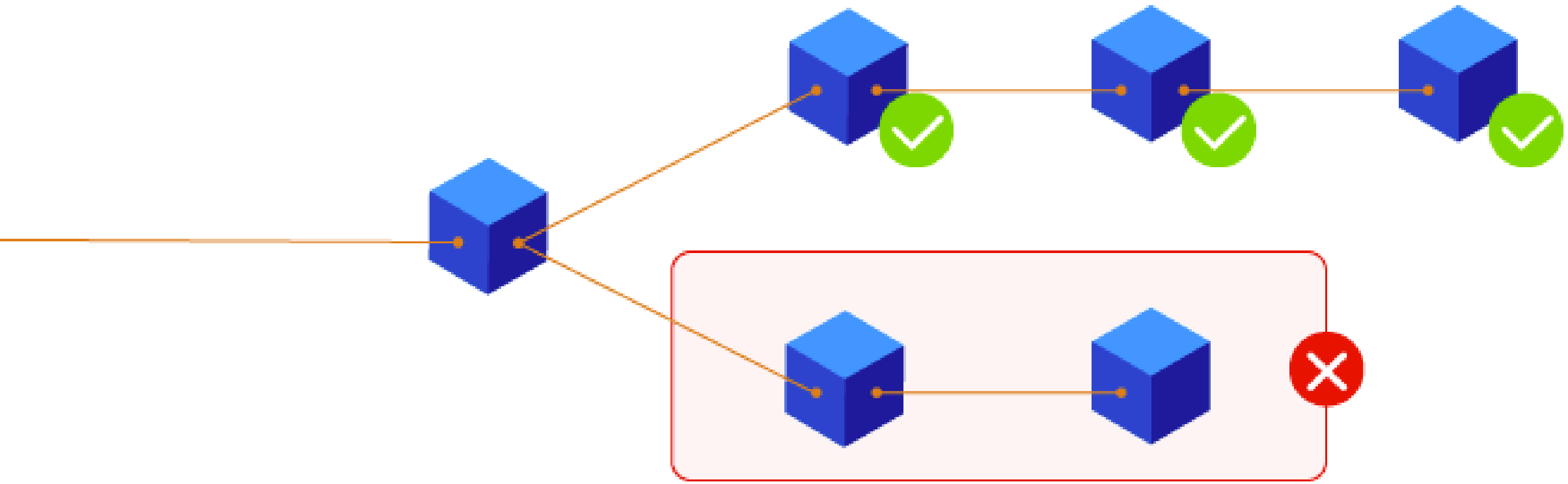
共识

共识的目的



共识

共识一：最长链优先



共识

共识二：写入证明

共识

共识二：写入证明

- 工作量证明（Proof-of-Work，PoW）
- 是一种对应服务与资源滥用、或是拒绝服务攻击的经济对策
- 一般要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源做为担保成本，以确保服务与资源是被真正的需求所使用
- 现时此技术成为了加密货币的主流共识机制之一

共识

共识二：写入证明

- 挖矿（Mining）

共识

共识二：写入证明

- 第一个提供工作量证明的节点将获得写入数据到下一个区块的权限
- 写入成功，且经过其他节点确认后，交易手续费以及一份额外奖励将会自动发送给该节点
- 为了得到这些奖励，区块链节点形成竞争关系
- 为了公平的对待每个竞争者，工作量证明需要解决的复杂运算问题通常为随机问题或存在随机解

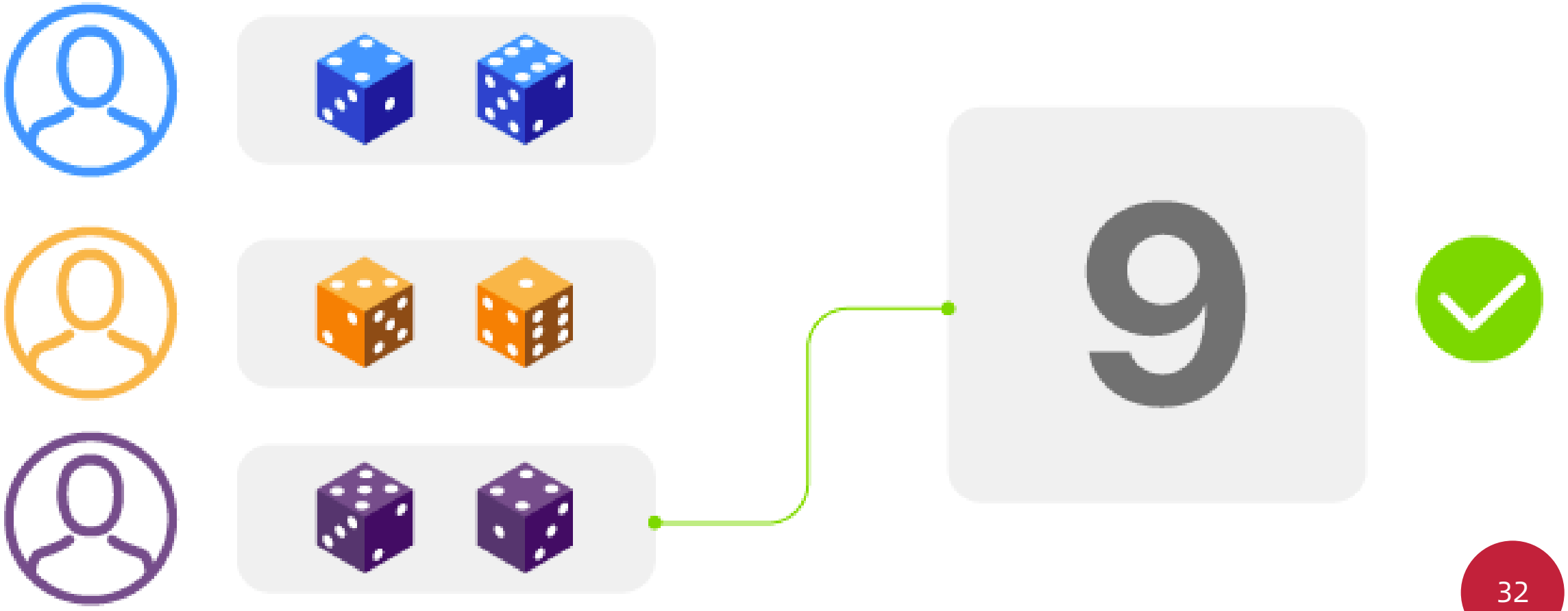
共识

共识二：写入证明

- 工作量证明最常用的技术原理是散列函数
- 由于散列函数的值域变动会引起雪崩效应，所以几乎无法从运算结果反推回输入值，因此通过指定散列函数值域的特征，让用户进行大量的穷举运算，就可以达成工作量证明

共识

共识二：写入证明



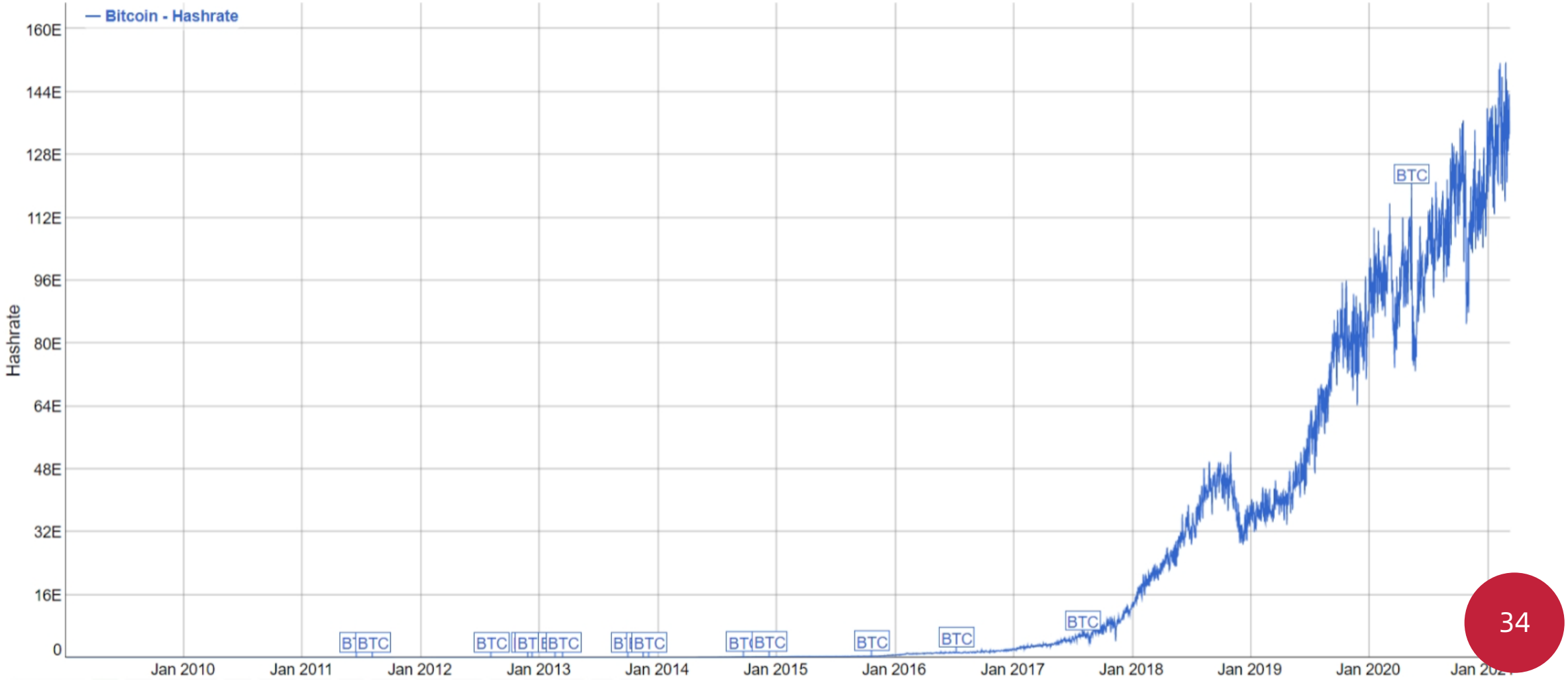
共识

共识二：写入证明

- 散列函数算力（Hashrate）
- 衡量在一定时间内生成新区块所需的总计算能力
- 1 TH/s = 每秒 1,000,000,000,000 次散列函数计算
- 目前，比特币全网算力已经全面进入 E 算力时代

共识

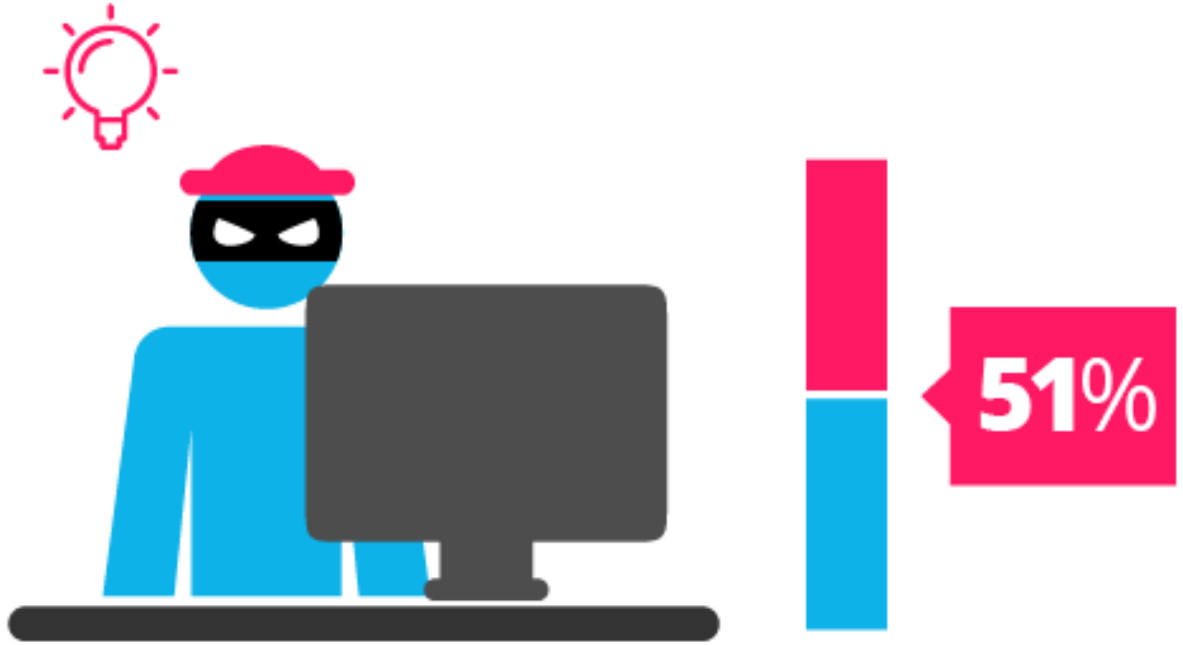
共识二：写入证明


— Bitcoin - Hashrate
160E
144E
128E
112E
96E
80E
64E
48E
32E
16E
0
Hashrate
Jan 2010
Jan 2011
Jan 2012
Jan 2013
Jan 2014
Jan 2015
Jan 2016
Jan 2017
Jan 2018
Jan 2019
Jan 2020
BTC

共识

共识二：写入证明

- 当黑客尝试写入错误的数据时，他需要：
- 拥有全网 50% 以上的算力
- 即“51% 攻击法”



共识

共识二：写入证明

- 权益证明（Proof-of-Stake，PoS）
- 使用选举的方式指定持有权益（Stake）的节点为交易的验证者，并创造新的区块
- 优点：通过缩小选举节点的数量，能够在不增加计算资源的前提下有效减少网络压力
- 缺点：选举固定数量的节点未必能完全实现去中心化；如参选的节点数量少或者投票数量低，选出的节点代点代表性不足

共识

共识二：写入证明

- 每次产生新区块时，将通过选举的方式指定新区块的创建节点
- 由于是通过选举产生的节点，创建区块通常没有奖励
- 交易手续费通常由所有的权益持有节点共享
- 由于 PoS 没有内部竞争，写入数据比 PoW 要高效很多

共识

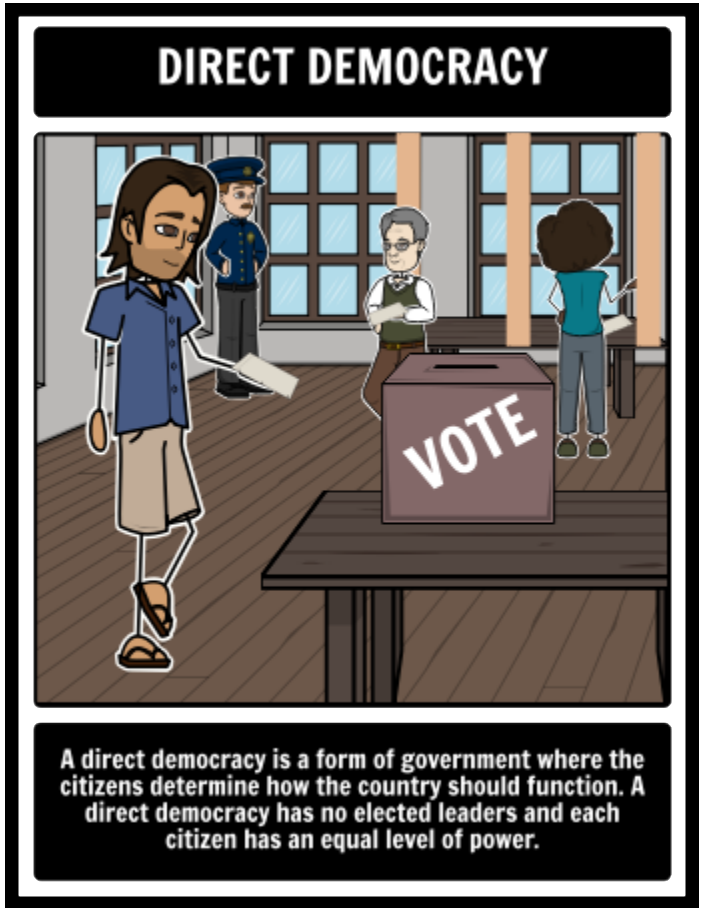
共识二：写入证明

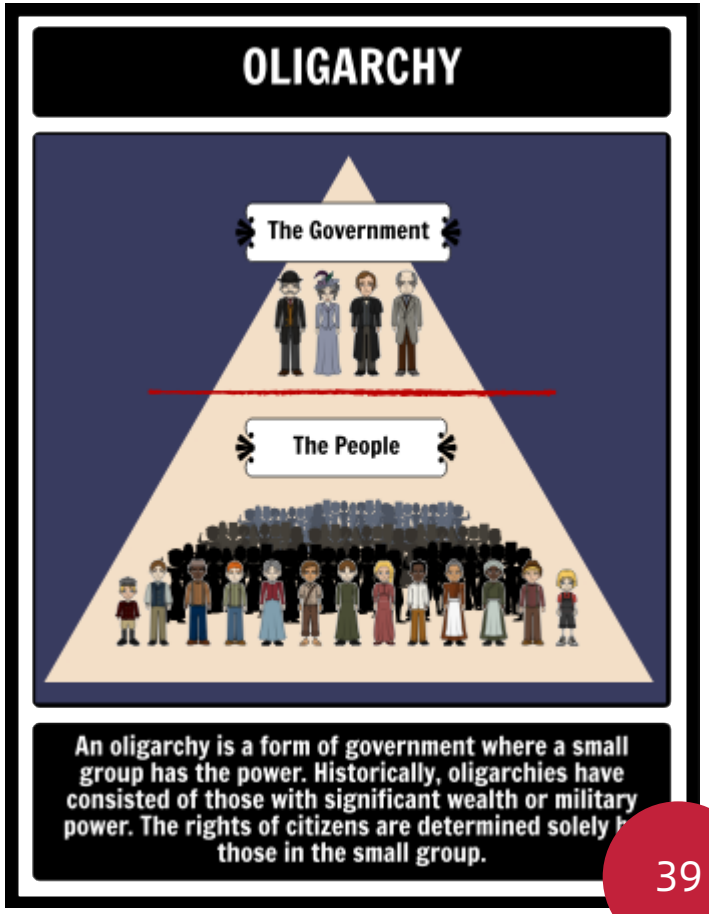
- 当黑客尝试写入错误的数据时，他需要：
- 控制全网 50% 以上的权益持有者
- 即“51% 攻击法”

共识

共识二：写入证明

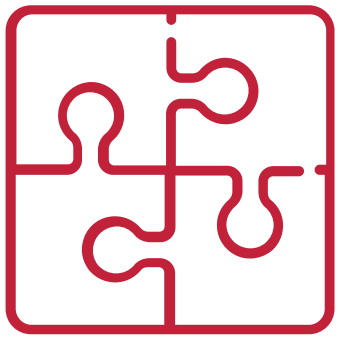

MONARCHY
In a monarchy, a king or queen, "a monarch", rules over the people. Some monarchs have held all of the power, while others have shared their power with other branches of government. A monarch typically comes to power by inheritance. Depending on the monarch, citizens can have numerous rights and privileges, or none at all.


DIRECT DEMOCRACY
VOTE
A direct democracy is a form of government where the citizens determine how the country should function. A direct democracy has no elected leaders and each citizen has an equal level of power.

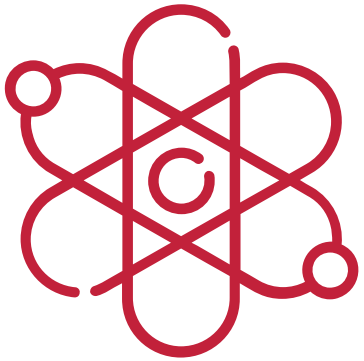

OLIGARCHY
The Government
The People
An oligarchy is a form of government where a small group has the power. Historically, oligarchies have consisted of those with significant wealth or military power. The rights of citizens are determined solely b
those in the small group.

目录

广义区块链



Blockchain



Consensus

Cryptocurrency

总结

- 袁煜明《区块链技术进阶指南》，机械工业出版社
- http://product.dangdang.com/28538836.html

- 安德烈亚斯·安东诺普洛斯《精通区块链编程：加密货币原理、方法和应用开发》第二版，机械工业出版社
- http://product.dangdang.com/27877333.html

总结

- Bitcoin 比特币
- https://bitcoin.org

- Ethereum 以太坊
- https://ethereum.org

東莞理工學院
DONGGUAN UNIVERSITY OF TECHNOLOGY

Thank You!

丁烨，网络空间安全学院 副教授
dingye@dgut.edu.cn