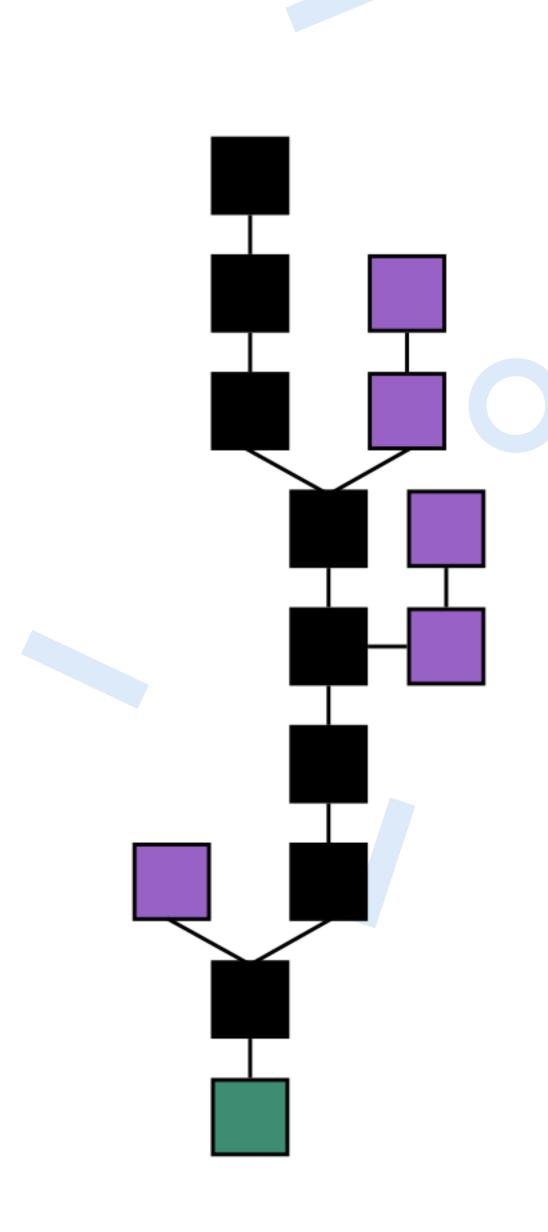


区块链基本原理



A blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. Each block typically contains a cryptographic hash of the previous block, a timestamp and transaction data. By design, a blockchain is inherently resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-topeer network collectively adhering to a protocol for validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which requires collusion of the network majority.

Wikipedia

基本原理

Index 序号(创世区块为 0)

Previous Hash 前一区块是否合法

Timestamp 创建时间

Data

承载的数据

Hash
本区块是否合法

Nonce 重计算次数

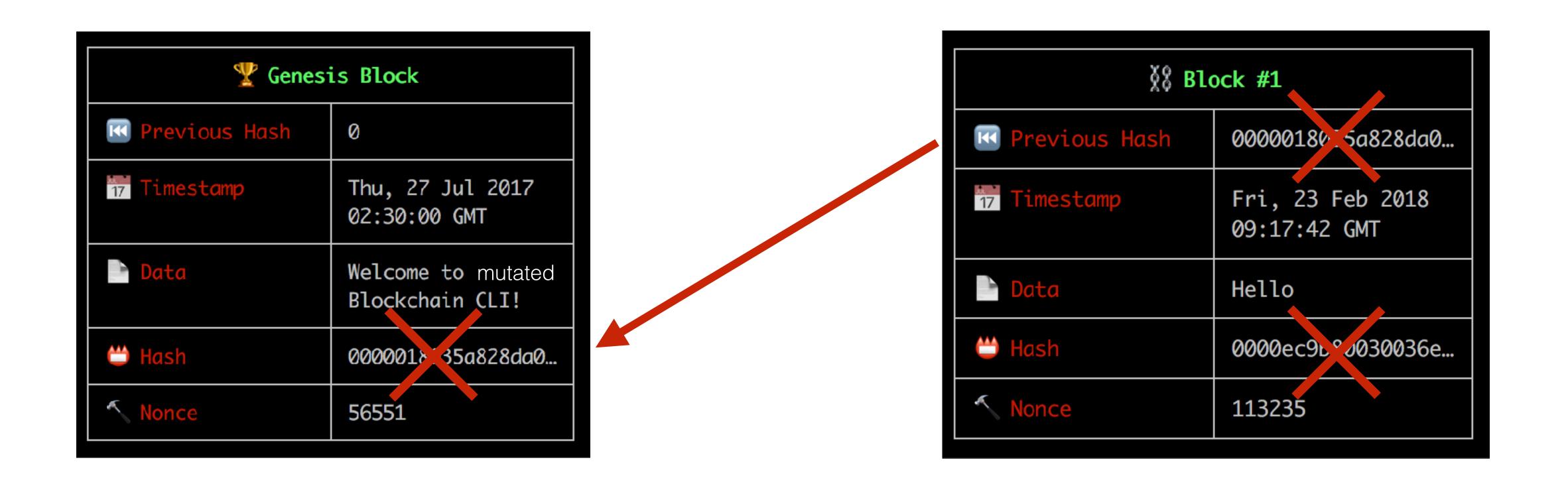
₹ Genesis Block	
M Previous Hash	0
Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
Data	Welcome to Blockchain CLI!
₩ Hash	0000018035a828da0
Nonce	56551

Hash = SHA256(Index + PreviousHash + Timestamp + Data + Nonce)

0000018035… 开头零的个数要求决定计算难度

基本原理

Hash = SHA256(Index + PreviousHash + Timestamp + Data + Nonce)



扩展

```
51% 攻击(Ghash.io)
"Double Spend"(六个区块确认一笔交易)
……
```

THANKS FOR YOUR WATCHING

