

02

OPEN ORIENTED

凹凸实验室

区块链基本原理

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

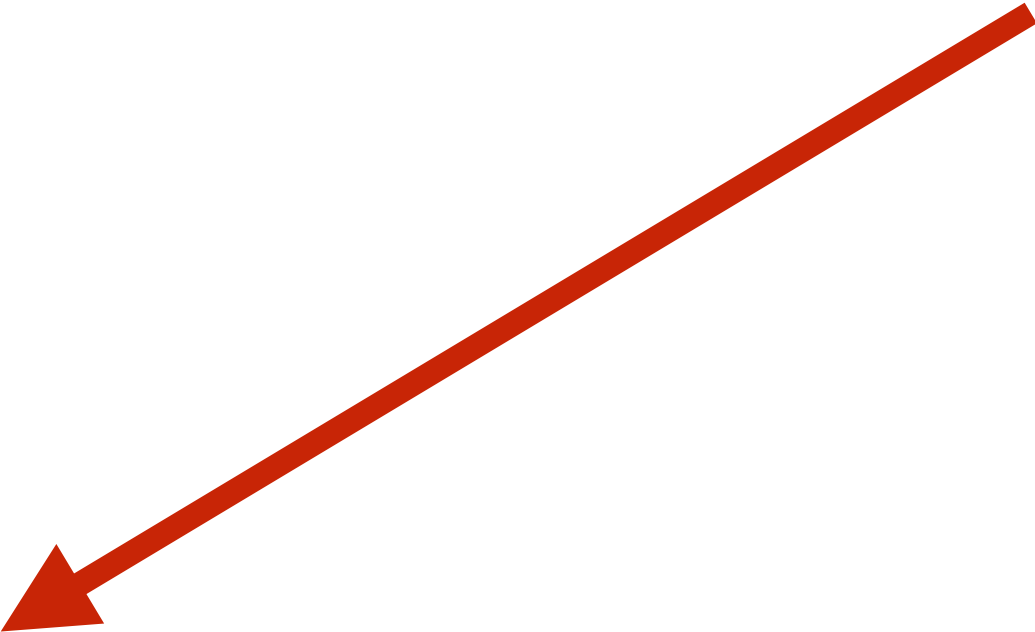
🏆 Genesis Block	
⏮ Previous Hash	0
📅 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
📄 Data	Welcome to Blockchain CLI!
🔥 Hash	0000018035a828da0...
🔨 Nonce	56551

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

0000018035... 开头零的个数要求决定计算难度

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

🏆 Genesis Block	
⏮ Previous Hash	0
📅 Timestamp	Thu, 27 Jul 2017 02:30:00 GMT
📄 Data	Welcome to mutated Blockchain CLI!
🔥 Hash	0000018...35a828da0...
🔨 Nonce	56551



🔗 Block #1	
⏮ Previous Hash	0000018...35a828da0...
📅 Timestamp	Fri, 23 Feb 2018 09:17:42 GMT
📄 Data	Hello
🔥 Hash	0000ec9b...0030036e...
🔨 Nonce	113235

51% 攻击 (Ghash.io)

“Double Spend” (六个区块确认一笔交易)

.....

T H A N K S
FOR YOUR WATCHING



OPEN ORIENTED

凹凸实验室