

blockchained.

A Intro to Cryptocurrency

12 Mar 2021



\$1.1T USD

Market Cap



“比特币就是**庞氏骗局**”

“虚无缥缈，**专割韭菜**”

“这个模式和**传销**没区别”

“这还能卖钱？这**钱从哪来**？”

“**这是一个被操纵的市场**”

“坐等**泡沫破裂**” “挖矿**纯属浪费电力浪费资源**”

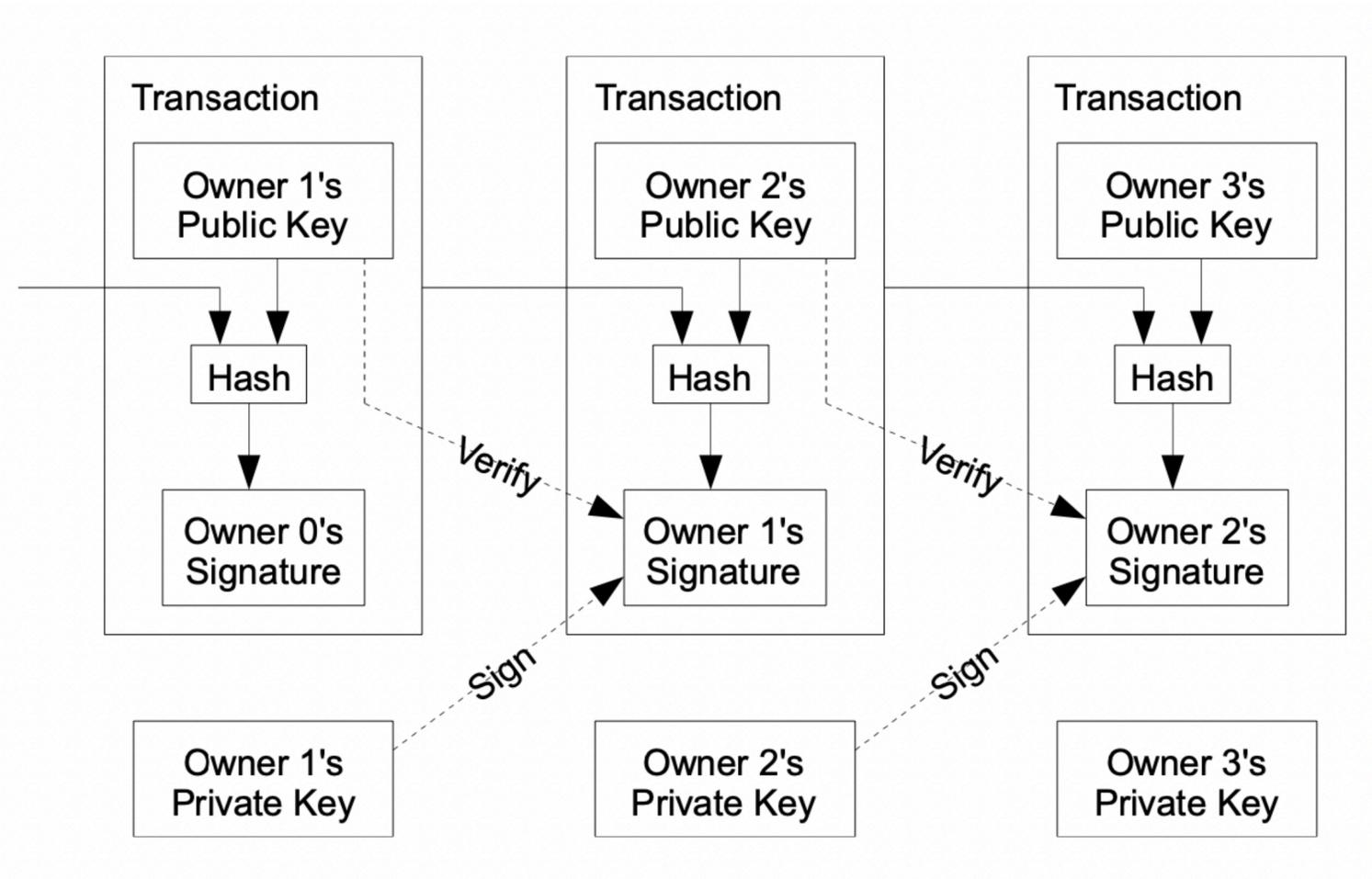
“没有实体支撑，**不如买黄金**”

“信的人**都是傻子**”

来自中文互联网用户

Q&A Session

**区块链更像一台分布式计算机
所有的区块链应用都是个“程序”**



Credit: Satoshi Nakamoto



137d247eca8b99dee58e1e9232014183a5c5a9e338001a0109df32794cdcc92e

Inputs i

HEX

ASM

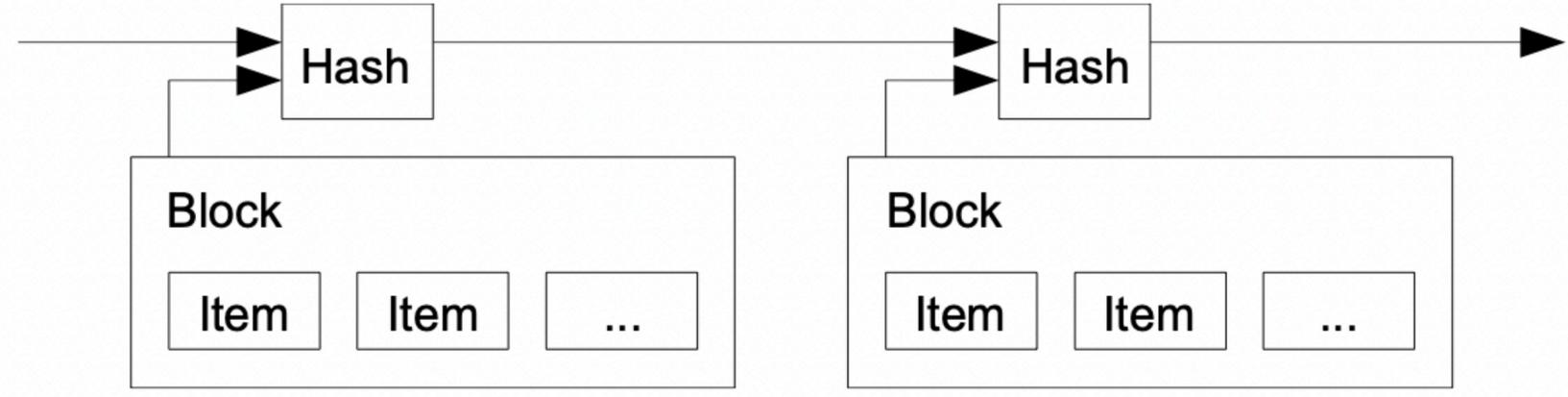
Index	0
Details	Output
Address	1B5AUoAyPpQRBYgcwWXMnqfqCy859jAX7X
Value	50.00000000 BTC
Pkscript	76a9146e7ad5a599e9400c9408d2b0decffa0837dad84988ac
Sigscript	483045022100a616082b724043758a4732dae5461783cb48ccf1b36a7f98d41f3f5f8db577f80220084df7afc2c912c3ef23ea43cfec651ba97ee6c4e4220c0f58b78f374626bdfb01410412aebcb2c5d5625c138c9cdd318ae04a103002b0d1b1541d72cd51dc016bfec885e7b93d73375903acb2731cdb7790b1d969db2684646e6fbeabb0559b6513c1

Outputs i

Index	0
Details	Spent
Address	1Pqth7yp5ZkTSbx6Tr8vmTN2ACedB7MeEV
Value	43.61000000 BTC
Pkscript	76a914fa91e22c8a2a4d1fa592de1cf7aa8f958867a1d288ac
<hr/>	
Index	1
Details	Spent
Address	18Zo31o4GdaFDjmYwfzB5TvwGx9ZLJq7kC
Value	6.39000000 BTC
Pkscript	76a91452fc9e7e1b8be3a61fe20381cb343e62eac105cb88ac

“Mempool”

如何证明我真的有这么多 BTC?

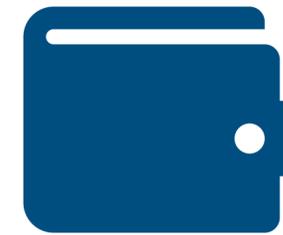


Credit: Satoshi Nakamoto

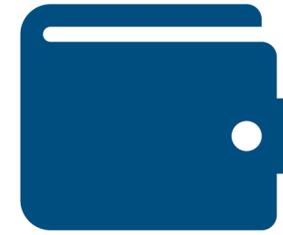
为什么使用工作量证明？

- 隔一段时间产生延长区块链符合我们的实际需求
- 极大增加造假成本，减少造假收益

- > 广播 Transaction
- > 存入 Mempool
- > 被打包进 Blockchain



精妙的平衡



如何维持一个去中心化网络的可持续发展?

- 健康的流通量
- 大量部署的节点
- 配置均衡的算力

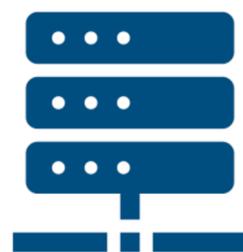


我希望

- 资产具有价值
- 流通量增大

我付出

- 计算资源和电力
- 运行比特币节点



我希望

- 交易能被确认
- 资产收到认可

我付出

- 为矿工提供手续费
- 运行比特币节点

去中心化的
匿名的
不受监管的
资产网络

“挖矿纯属**浪费电力浪费资源**嗷”

“挖矿纯属**浪费电力浪费资源**？”



成本&效益

- 黑市交易、非法收款、洗钱
- 对抗法币高通货膨胀
- 避免外汇管制
- 投资和投机
- 绕过监管的融资 (ICO, Initial Coin Offering)



ethereum

所有的区块链应用都是个“应用”

所有的区块链应用都是个“应用”



区块链应用有一个“编程语言”

Turing Completeness

Smart contract



Filecoin