

比特币与区块链原理介绍

The background is a blue gradient, transitioning from a lighter blue at the top to a darker blue at the bottom. On the right side, there are several thin, white, parallel lines that start from the bottom and extend towards the top right corner, creating a sense of motion or a stylized graphic element.

Bitcoin Charts

Linear Scale Log Scale

Zoom 1d 7d 1m 3m 1y YTD ALL

From Apr 29, 2013 To May 22, 2018



2013~2017年的比特币价格



2013年之前的比特币价格

技术

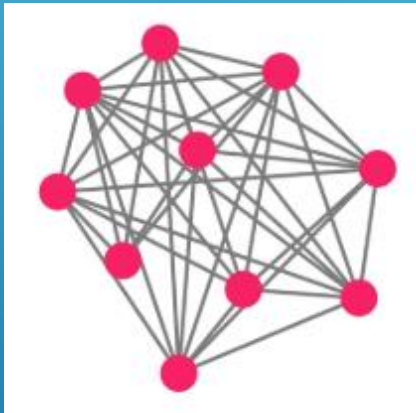
应用

区块链

比特币

碳酸饮料做法

可口可乐



**SATOSHI
NAKAMOTO**

Founder of Bitcoin



**WORLD'S MOST
ENIGMATIC
BILLIONAIRE**

一个署名为“中本聪”的人，
想创造一种不受政府管制的货币，他称之为比特币。
为了实现比特币应用，而发明了区块链技术。
在2008年10月31号发布了论文
在2009年的1月9号网络上第一次生成了50个比特币

货币

贝壳---》金银---》法币（国家未来税收信用背书）



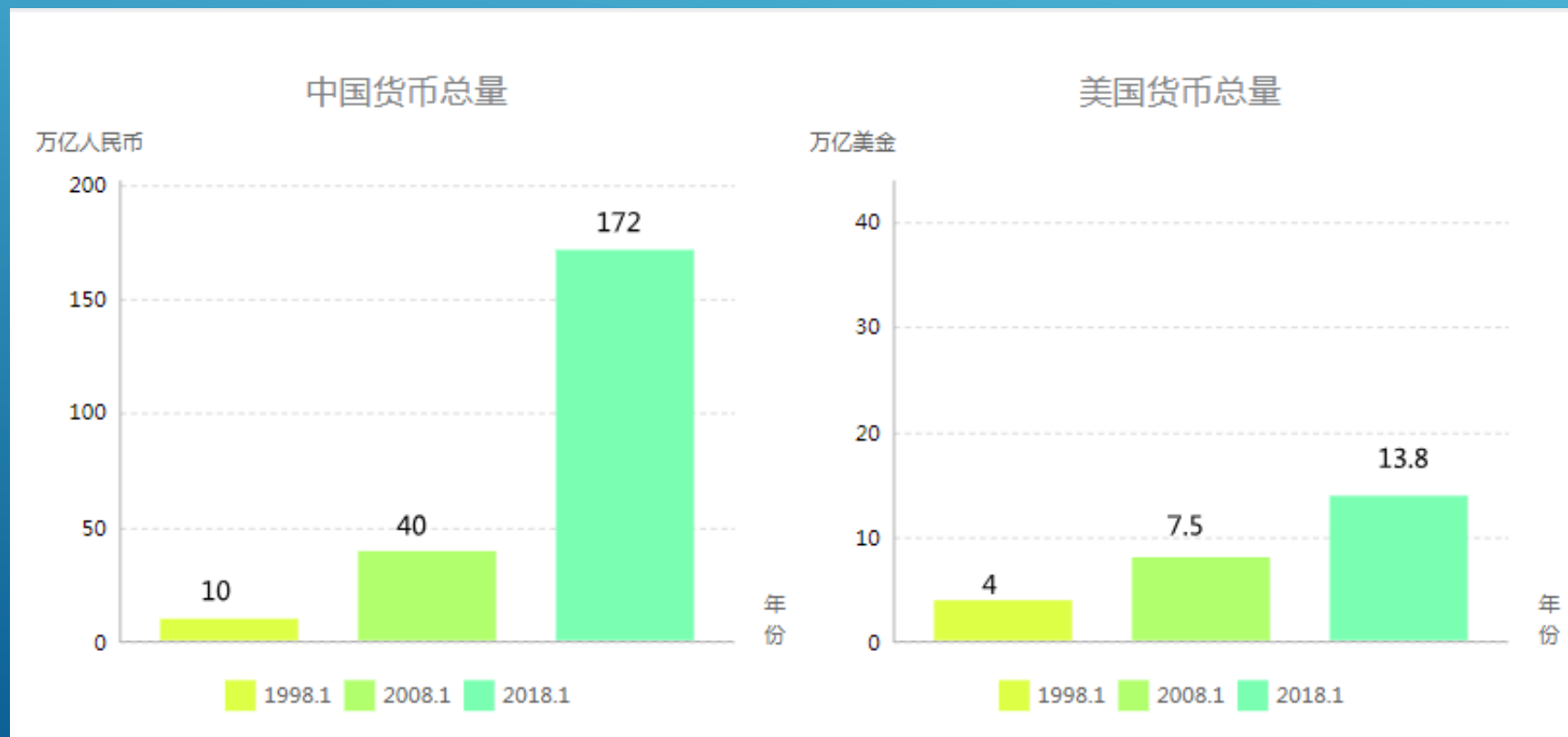
更多资源：高晓松的《晓说》2018年4月5月节目

法币的问题1：滥发

通过通货膨胀稀释和掠夺所有人的财富

中国每10年4倍

美国每10年2倍



法币的问题2：中心化

无法真正拥有自己的财富

场景1.想变成美金到国外，需要提交各种材料，额度最高5万美元

场景2.汇款受限，周末无法大额汇出

场景3.银行服务器维护出故障



法币的问题3：现金使用也不方便


现金纸币虽然可以自由流动，但是必须当面交换，大额的话基本不可能，容易被损毁。



比特币的特点

- 1.总发行量固定（2100万个）
- 2.不受任何人控制的价值交换（去中心化，帐户不被封）
- 3.转帐数量随意，方便（只要有互联网就能进行转帐）

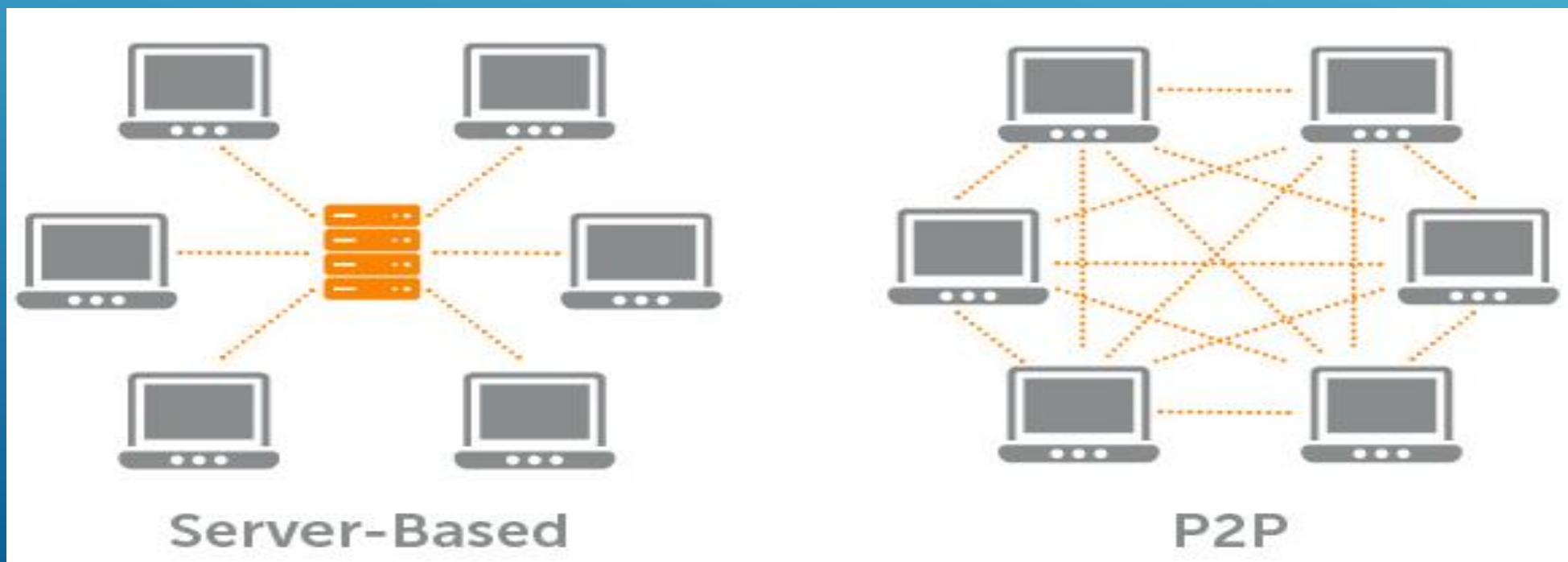
应用场景

- 1.黑市交易 毒品，盗版软件，假护照，黑客攻击，勒索软件
 - 2.互联网服务，域名，服务器，赌博游戏筹码
 - 3.价值存储，富人们的资产配置与转移
 - 4.市场投机
- 
- A series of white lines of varying lengths and slopes are positioned in the bottom right corner of the slide, creating a modern, abstract graphic element.

底层技术基础

分布式网络 p2p

任何一个节点发出的消息都能广播到所有节点
任何一个节点坏掉都不影响其他节点

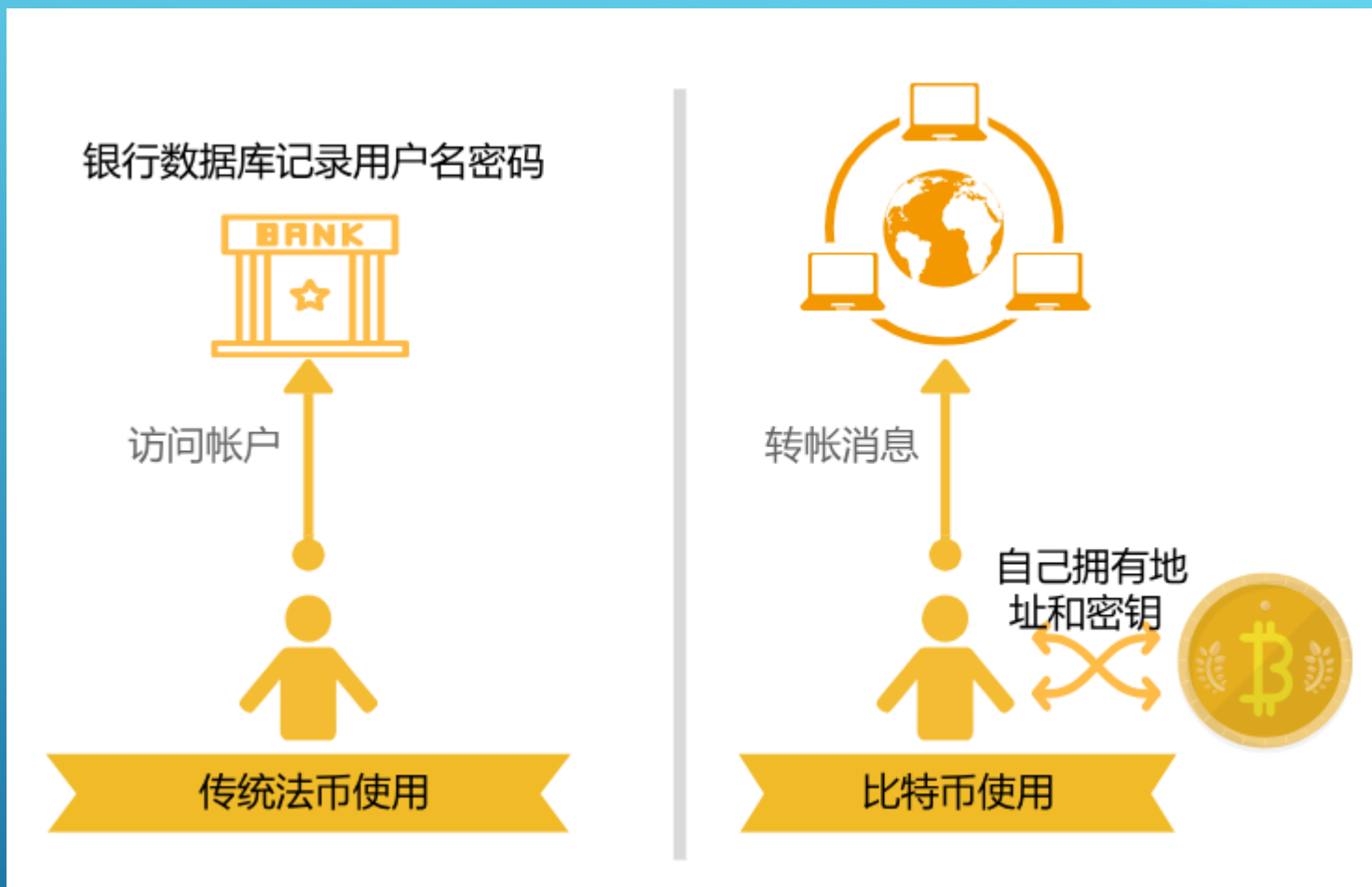


财富的拥有形式

- 传统法币：银行帐号和帐号密码，由银行管理和验证
- 比特币：一个比特币地址和使用这个地址上的钱的密钥或者说密码，由数学公式验证，也不怕被复制

地址：1C1mCxRukix1KfegAY5zQQJV7samAciZpv

密钥：10724fca6db04d038890ddde72ba1cc7adc6ce5fe02850debfa1650f54418cef



比特币网络本质

---转帐消息的集合

如何查有多少钱：

纸币的话看钱包里有多少张

网银直接显示，数据库里记个数

比特币帐户的钱包余额是一系列转帐计算的结果

初始 A:200 B:0 C:0 D:0



最终 A:80 B:0 C:10 D:110

比特币网络

2009年1月9日上午10点54分

第1条



第2条



第320871774条

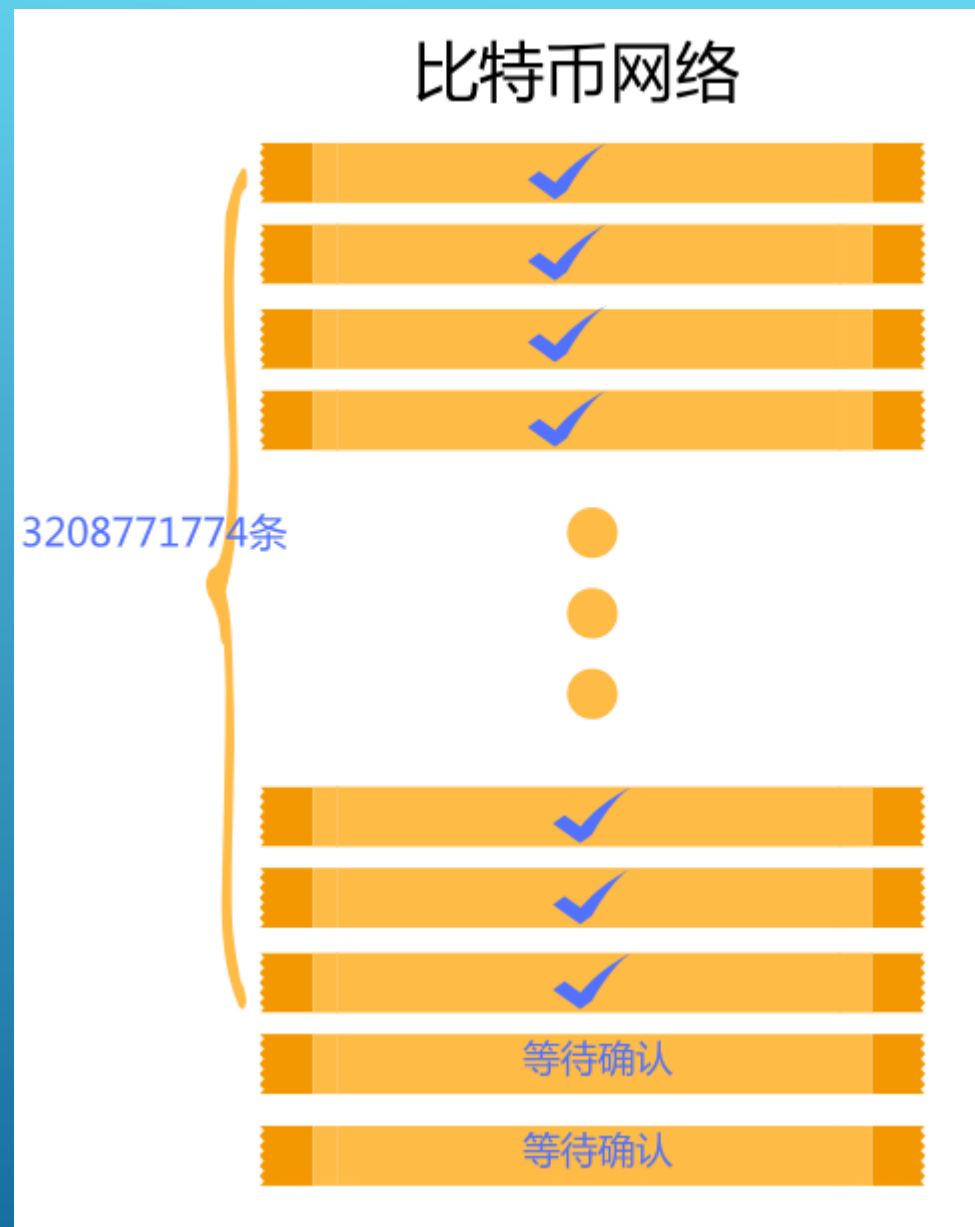


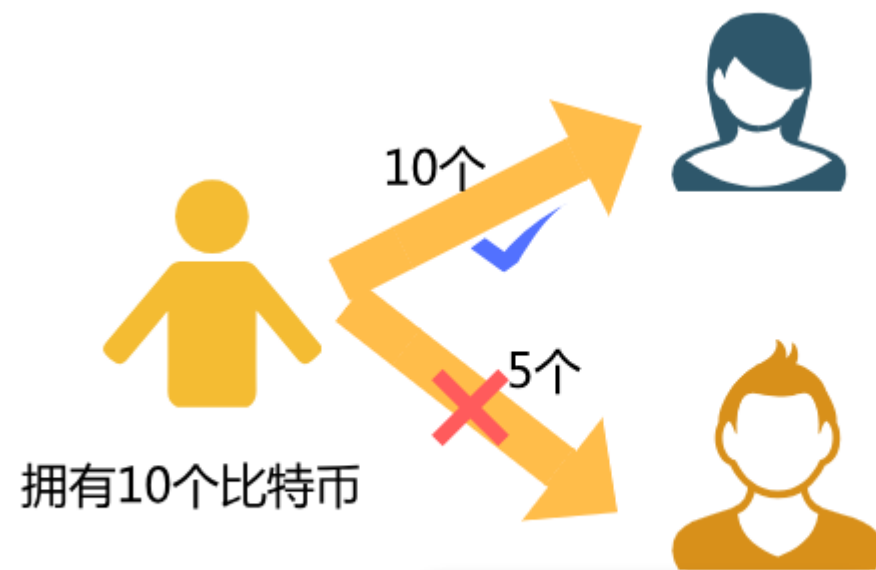
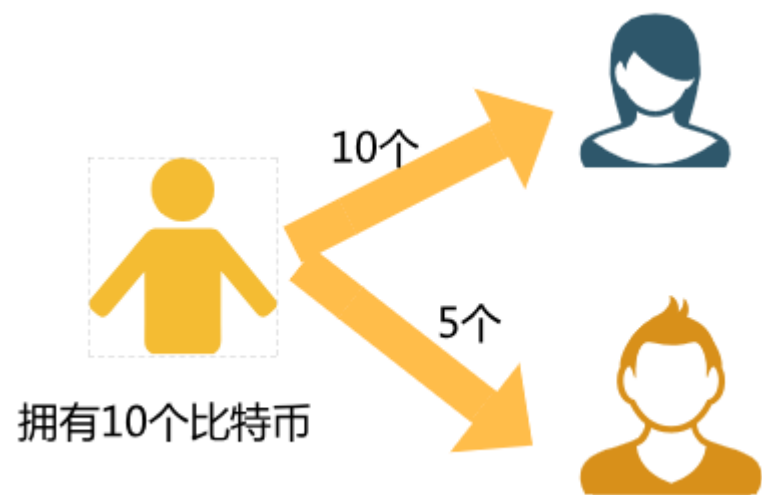
2018年6月7日下午12: 00

转帐确认

转帐消息在分布式网络上需要被确认, 形成共识

没有确认机制的话, 无法判断一条新的转帐消息是否正确, 因为不知道原来地址上真实的钱是多少



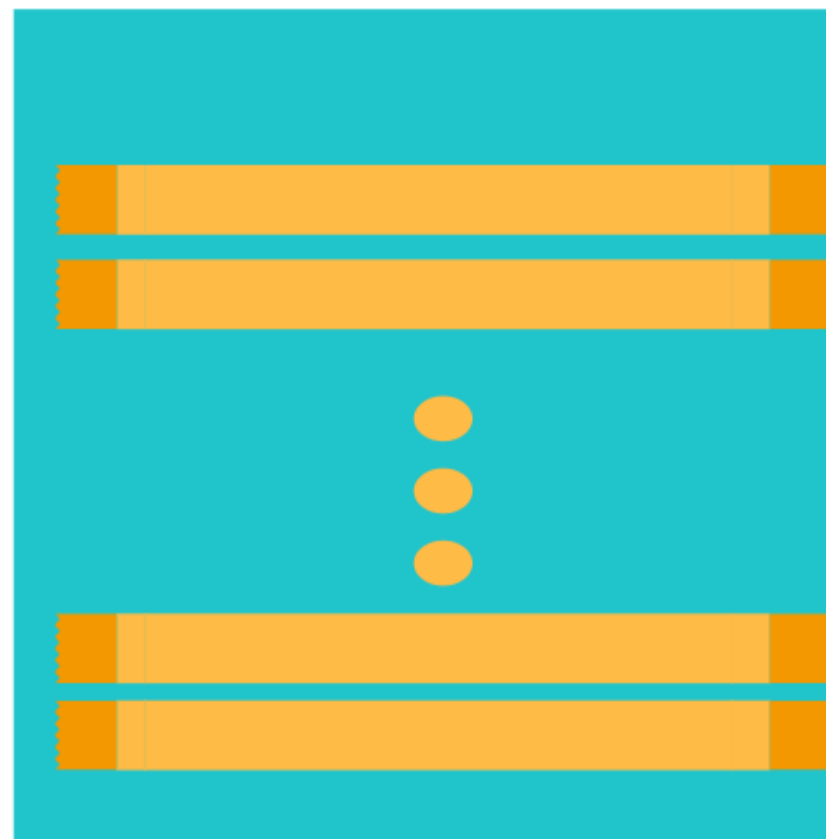


此消息被所有节点丢掉

用区块进行确认 BLOCK

比特币网络平均每10分钟生成一个区块，即将这10分钟内新产生的交易封装到一个数据块中，告诉所有的节点。

区块 BLOCK



平均10分钟产生一个，
目前每个比特币的区块中大约有1000条转帐记录

比特币网络

2009年1月9日上午10点54分

第1条

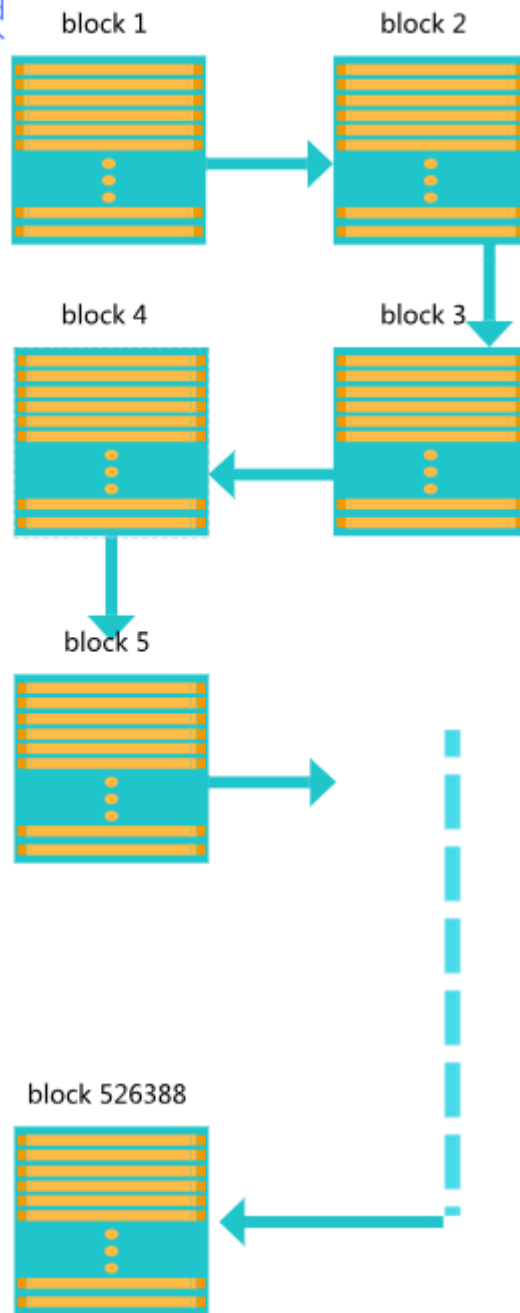
第2条

第320871774条

2018年6月7日下午12: 00

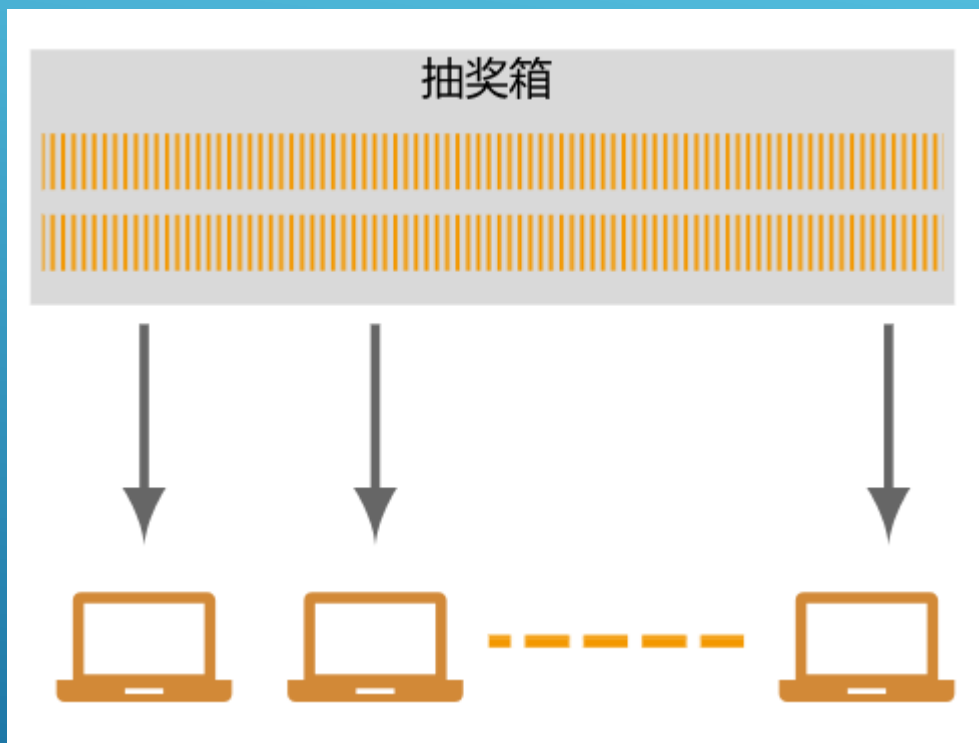


2009年1月9日
上午10点54分

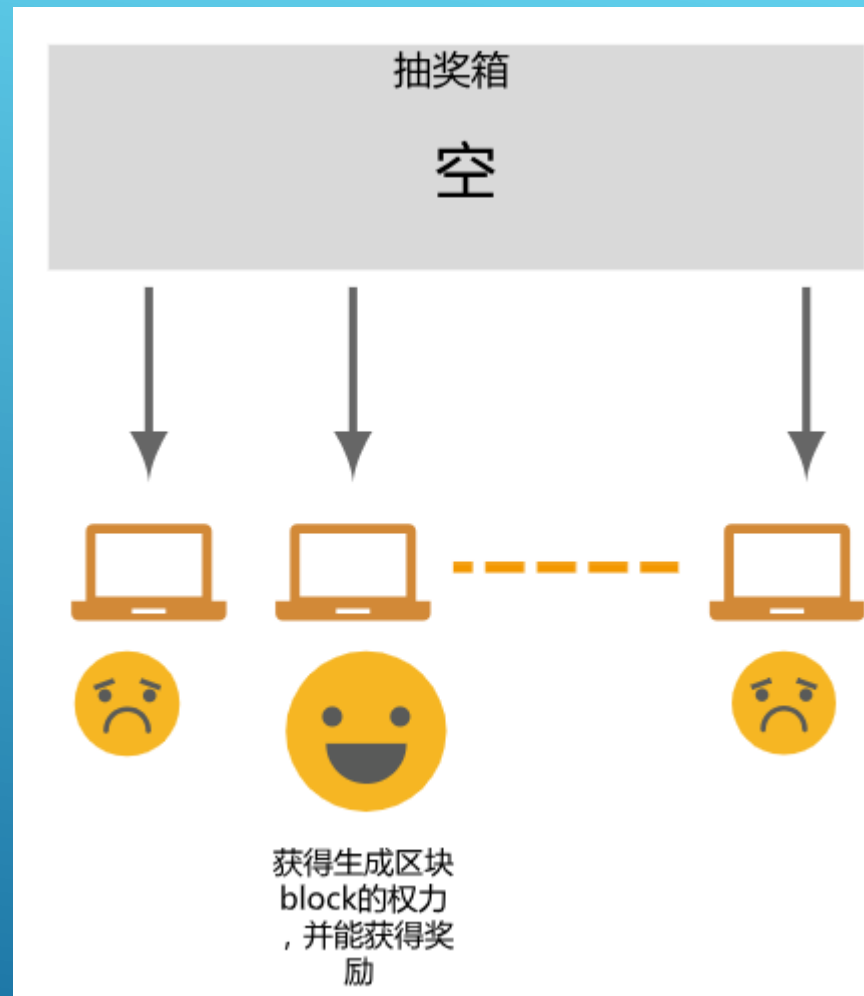


2018年6月7日

产生区块的过程---挖矿

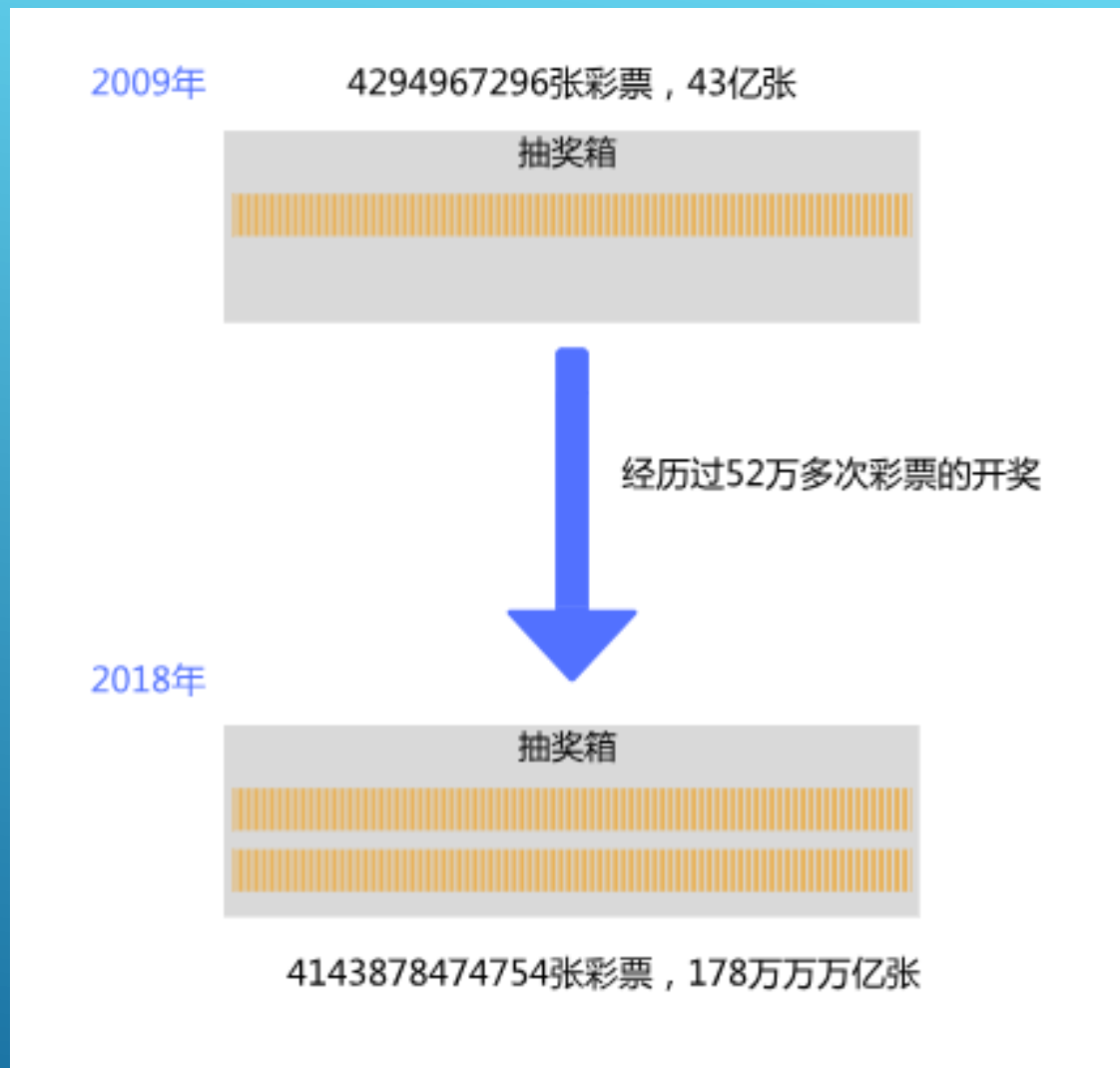


约10分钟后奖箱抽空



而比特币网络在设计时就规定了约每10分钟开一次奖。

为了满足这个要求，难度就需要随着算力的上升要变大。





金贝 X5 矿机
850MH/s

谢谢！

