



# Bitcoin 社区与激励

吴嘉婧  
副教授

中山大学 计算机学院

# 课程大纲



- **Week-1**                    2月22日      课程背景介绍与区块链应用背景
- **-- Part-1: 比特币与以太坊基础知识部分**
- **Week-2**                    3月1日        比特币背后的区块链
- **Week-3**                    3月8日        比特币的密码学基础
- **Week-4**                    3月15日      比特币运行交易模型与共识机制
- **Week-5**                    3月22日      比特币共识机制
- **Week-6**                    3月29日      比特币挖矿和区块链分叉原理
- **Week-7**                    4月5日        清明放假
- **Week-8**                    4月12日      比特币的安全机制、激励策略与比特币社区
- **Week-9**                    4月19日      以太坊介绍
- **Week-10**                  4月26日      以太坊数据结构与共识机制
- **Week-11**                  5月3日        期中考试周（不上课）
- **Week-12**                  5月10日      以太坊与智能合约
- **Week-13**                  5月17日      数字货币与监管
- **-- Part-2: 区块链研究启发**
- **Week-14**                  5月24日      区块链数据分析与反欺诈
- **Week-15**                  5月31日      区块链安全：攻击与防治
- **Week-16**                  6月7日        区块链科研现状概览
- **Week-17**                  6月14日      区块链与Web3和元宇宙
- **Week-18**                  6月21日      区块链与Web3和元宇宙

# 课程大纲



| Week-1      8月30日      课程介绍，与区块链落地应用；比特币前传

## | Part-1: 比特币与以太坊基础知识部分

- Week-2, 9月6日      Bitcoin 的密码学基础
- Week-3, 9月13日      Bitcoin 的数据结构
- Week-4, 9月20日      Bitcoin 运行机制：共识机制
- Week-5, 9月27日      Bitcoin 运行机制：共识机制（续）
- Week-6, 10月4日      停课
- Week-7, 10月11日      比特币的挖矿、区块链的分叉原理
-  – Week-8, 10月18日      比特币的 安全机制、激励策略 与 比特币社区
- Week-9, 10月25日      以太坊数据结构 与 共识机制
- Week-10, 11月1日      考试周（不上课）
- Week-11, 11月8日      区块链网络、匿名、与监管



## I Part-2: 区块链科研启发

- Week-11, 11月8日 区块链 研究现状
- Week-12, 11月15日 数据分析 与 反欺诈
- Week-13, 11月22日 区块链的 安全问题 与 攻击模型
- Week-14, 11月29日 高性能区块链 与 分片技术
- Week-15, 12月6日 区块链 的 互操作性
- Week-16, 12月13日 区块链 与 Game Theory
- Week-17, 12月20日 区块链 与 网络优化、BFT类协议

## I Part-3: 区块链工程实践课

- Week-18, 12月27日 实践开发课程1
- Week-19, 1月3日 实践开发课程2

# Outline of this Class



- | Part 1: 比特币社区
- | Part 2: 挖矿的激励与策略
- | Part 3: 共识的其他知识
- | Part 4: 答疑



# 比特币社区是什么？

# 比特币社区成员——Types of nodes



- | Bitcoin network is a peer-to-peer network
  - nodes exchange transactions and blocks
  - there are different types of nodes on the network
  
- | The role of a node
  - Validate a new block
  
  - Store and save the transaction history of a block
  
  - Update other nodes in the blockchain to ensure all nodes on the blockchain have the latest information



## I 不同的定义

- Intel: 通过系统间的直接交换达成计算机资源与信息的共享
- IBM: 由若干互联协作的计算机构成并具备如下特性之一: 系统依存于边缘化设备的主动协作; 每个成员同时扮演客户端和服务器的角色; 系统应用的用户能意识到彼此的存在而构成一个虚拟或真实的群体

## I 特点

- 节点彼此对等, 既作为服务和资源的提供者, 又作为服务和资源的获取者



# 区块链依靠P2P网络



- | 可扩展性、健壮性
  - P2P网络中的所有对等节点都可以提供带宽、存储空间以及计算能力等资源，随着更多节点的加入，系统整体的资源和服务能力也在同步地得到扩充
- | 负载均衡
  - P2P网络的资源分布在多个节点上，可以实现网络的负载均衡
- | 去中心化
  - 在区块链系统的P2P网络中，节点是信息的发送方和接收方，它们共同维护区块链

# 拓扑形式一

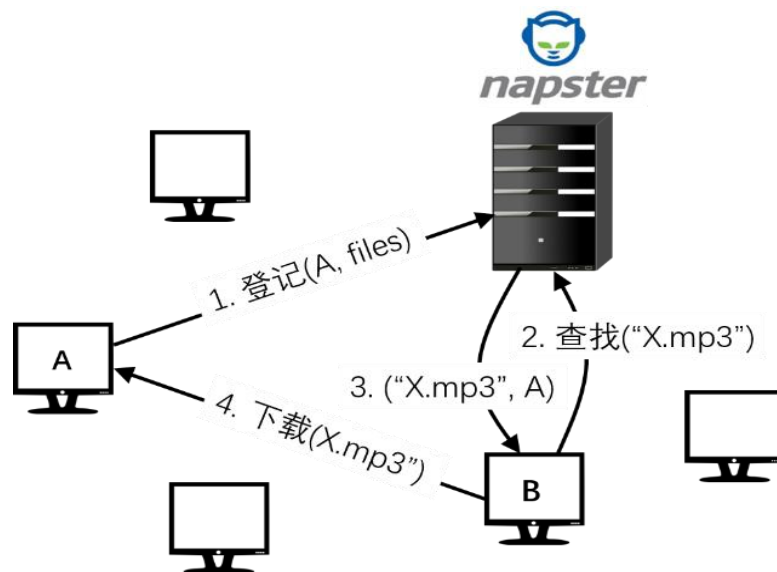


## I 中心化拓扑

- 由一台中心索引服务器和多个客户端节点构成，并非纯粹的P2P网络
- 中心索引服务器用于保存接入节点的地址信息，向其他节点提供地址索引服务

## I 特点

- 实现了文件查询和文件传输的分离，且维护简单
- 一旦中心索引服务器发生了故障，就会导致整个网络无法正常工作



# 拓扑形式二

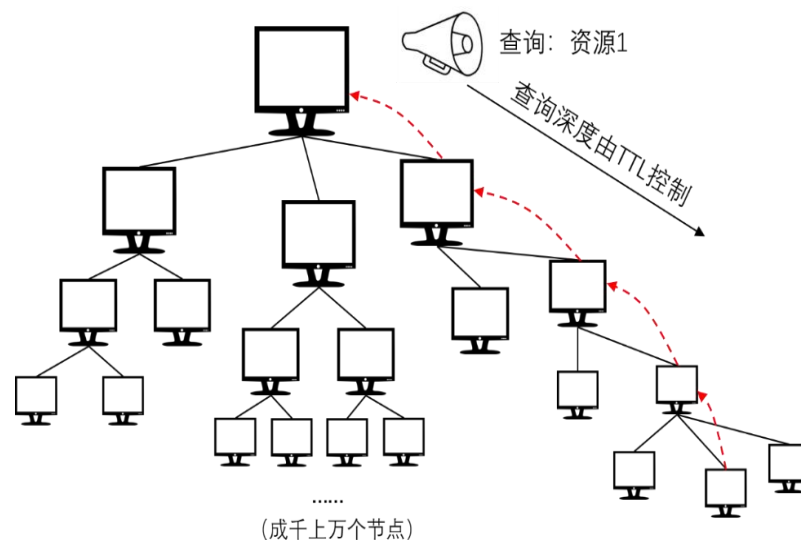


## I 全分布式非结构化拓扑

- 没有使用中心索引服务器，其节点拥有真正的对等关系
- 洪泛 (Flooding) 数据广播，即节点会将接收到的消息向邻居节点转发，直到所有节点都接收到了这个消息或消息传播的深度到达一定的限制

## I 特点

- 可能会出现广播风暴
- 实现快速的消息传播和资源查找

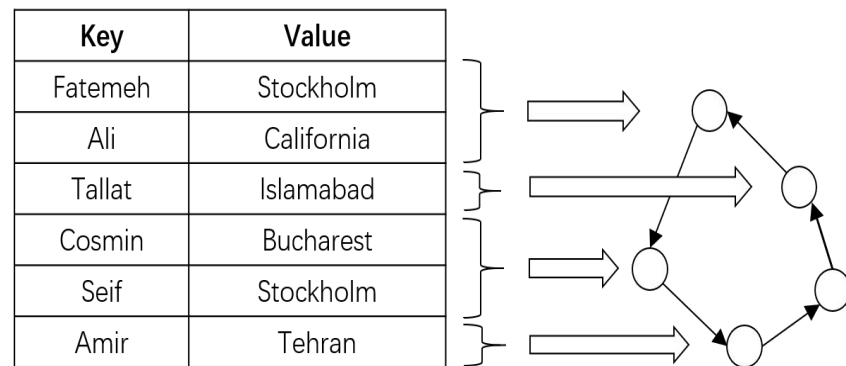


# 拓扑形式三



## 全分布式结构化拓扑

- 采用分布式散列表（**Distributed Hash Tables**, 简称**DHT**）来实现整个网络的寻址和存储，从而结构化地址管理
- 分布式散列表将存储着网络中所有资源信息的散列表划分成很多不连续的小块，分散地存储在多个节点上



## 特点

- 维护机制较为复杂
- 良好的健壮性、可扩展性和动态适应性

# 拓扑形式四

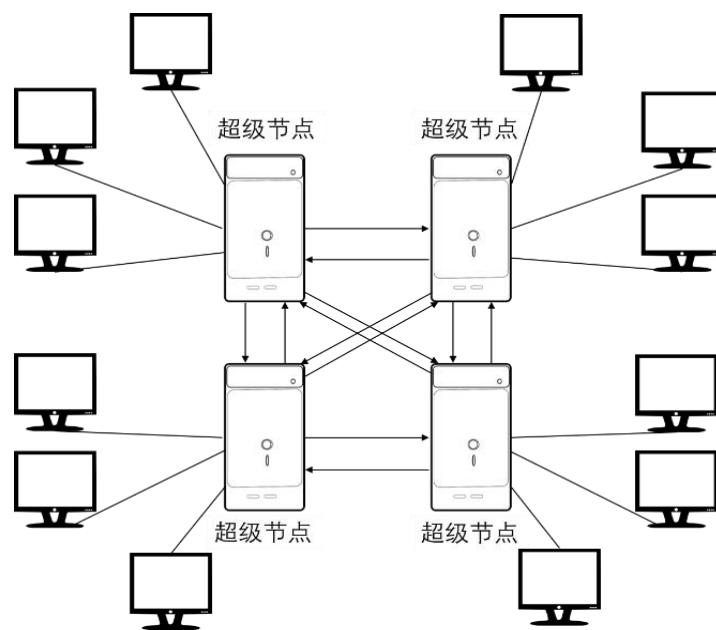


## 半分布式拓扑

- 将网络中性能较高的机器作为超级节点，每个超级节点存储着系统中其他部分节点的文件信息，执行维护这些节点的地址、文件索引等工作
- 超级节点之间形成一个高速的转发层，并与接入的普通节点形成一个自治的簇，簇内采用中心拓扑的P2P网络

## 特点

- 消除了网络拥塞的隐患，并在性能和可扩展性上具有一定的优势
- 对超级节点的依赖性较大



## I 基于全分布式非结构化拓扑

- 网络中的节点彼此对等，不存在特权节点和索引服务器，通过共识机制使所有诚实的节点保存一致的区块链视图，从而实现去中心化控制

## I 协议

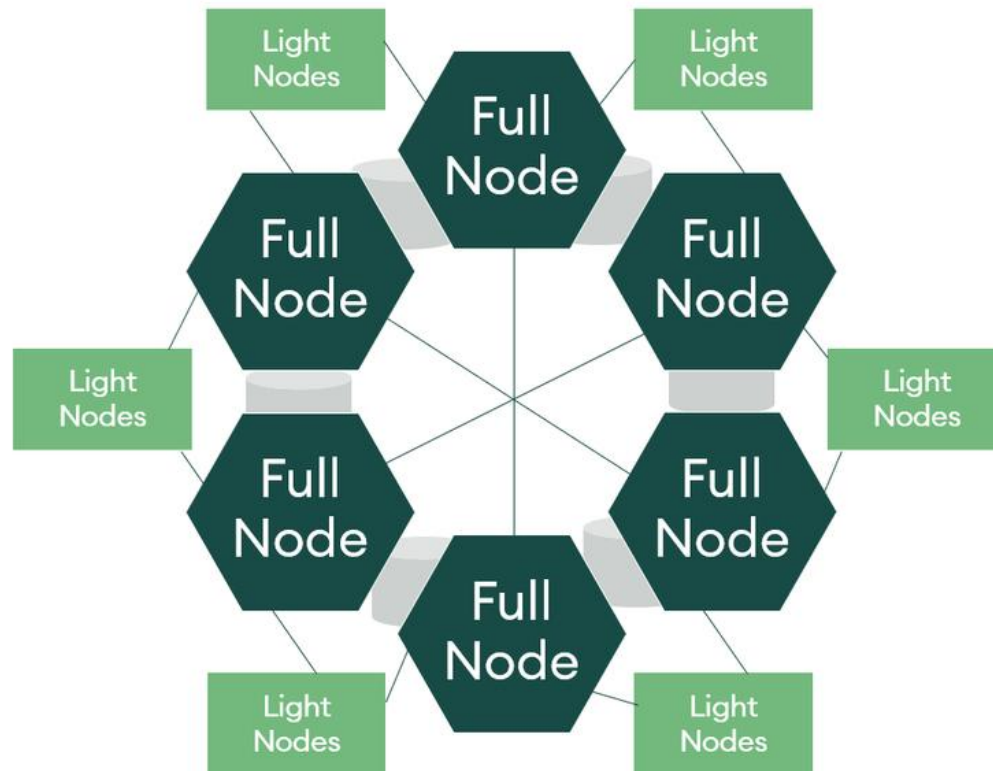
- 比特币网络是依照比特币P2P协议运行的一系列节点的集合，其P2P协议建立在传输层的TCP协议之上，采用8333端口作为主网默认通信端口
- 比特币还运行着其他协议，如应用于矿池挖矿、轻量级或移动端比特币钱包中的Stratum协议。这些协议由网关路由服务器提供，通过比特币P2P协议接入到比特币网络，使得运行着扩展功能的网络节点连接到比特币主网络

# 比特币社区成员——Types of nodes (cont.)



## Two typical types of nodes

- Full nodes,
- SPV (Simple Payment Verification建议支付验证) nodes

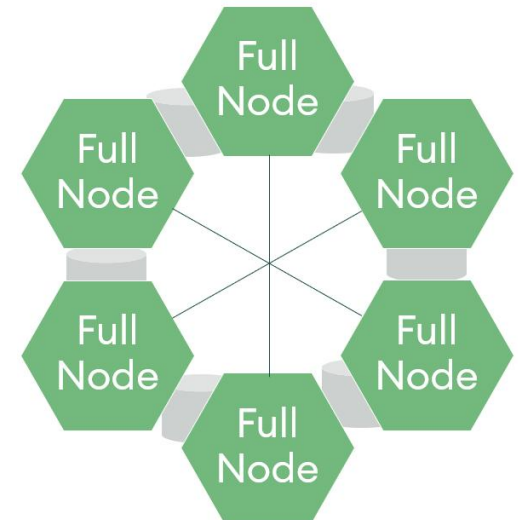


# 比特币社区成员——Types of nodes (cont.)



## I 全节点 (Full nodes)

- 拥有完整的数据: host a single copy of an entire blockchain history including transactions, timestamps and all created blocks.
- 负责全部功能: wallet, miner, full blockchain storage, and network routing functions
- they require more advanced computing power and energy and thus, are expensive
- It is estimated that the Bitcoin network has over 10,000 operational full nodes.



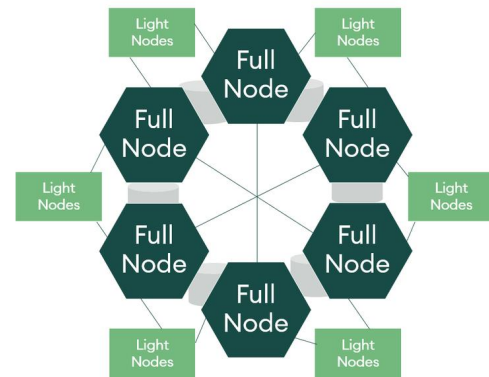


# 比特币社区成员——Types of nodes (cont.)



## 轻节点 (SPV nodes, or lightweight clients)

- download wallets and connect to full nodes to further validate information stored on the blockchain.
- They are much smaller in size and only hold information of partial blockchain histories.
- perform only **wallet** and **network routing** functionality.
- SPV 客户端只需要下载所有区块的区块头 (Block Header)，并进行简单的定位和计算工作就可以给出验证结论。
- SPV nodes 能够以较小的代价判断**某个支付交易**是否已经被验证过 (存在于区块链中)，以及得到了多少算力保护 (定位包含该交易的区块在区块链中的位置)
- 进一步应用：SPV proof，侧链协议中，用 SPV 来证明一个交易确实已经在区块链中发生过，称为 SPV 证明 (SPV Proof)，以后在“区块链的互操作性”课程中会讲



# 比特币社区成员——节点承载的功能



- | 钱包 (Wallet)
  - 可以支持比特币交易、查询等功能
- | 矿工 (Miner)
  - 可以运行工作量证明算法来争夺创建新块的资格，从而赚取系统奖励的比特币以及交易手续费
- | 完整区块数据存储 (Full Blockchain)
  - 存储着区块链的完整数据，可以独立地验证所有交易，不需要借助任何外来参考
- | 网络路由 (Network Routing Node)
  - 连接着一定数量的节点，能帮助转发交易和区块数据，发现和维持节点间的连接

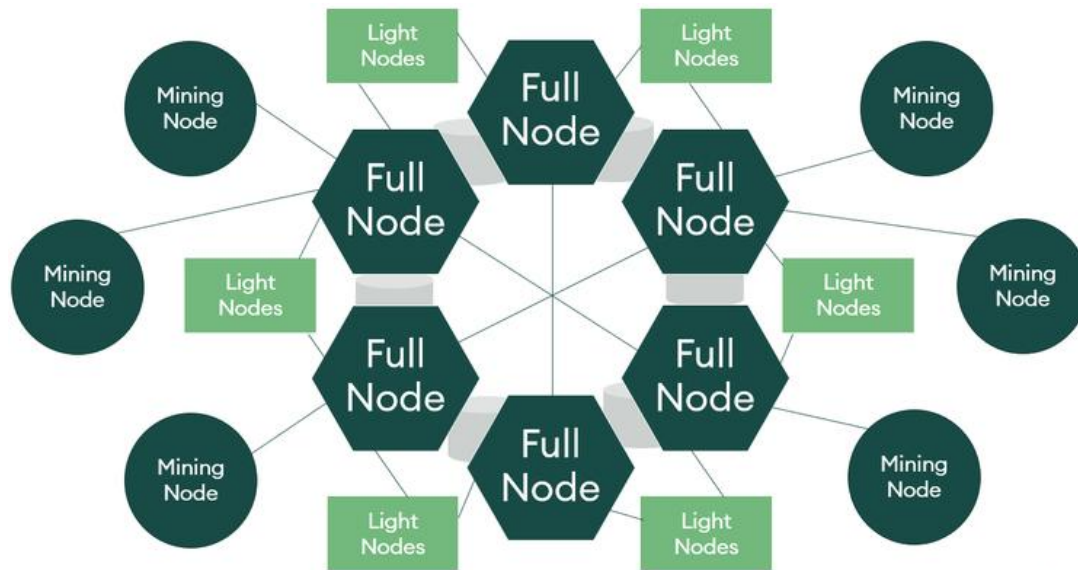
# 节点类型



- | 依照节点的功能进行划分
- | 核心客户端节点 (Reference Client (Bitcoin Core) )
  - 包含钱包、矿工、完整区块存储、网络路由四种功能
- | 全节点 (Full Block Chain Node)
  - 拥有完整的区块链数据，具有网络路由功能
- | 独立矿工节点 (Solo Miner)
  - 拥有完整区块链数据，具有路由功能和挖矿能力，能不依赖其他节点的算力单独进行挖矿
- | 轻量级钱包 (Lightweight (SPV) Wallet)
  - 包含钱包与路由转发功能

## I 矿工节点 (mining nodes, or miners)

- Mining nodes are only responsible for creating blocks to add to the blockchain,
- they are not responsible for the maintenance or validity of future blocks (unlike full nodes).



**Full, Light and Mining Nodes illustrated on a Blockchain**



## | Miners

- are typically rewarded through coinbase rewards
- not necessarily to host all historical TXs to identify the validity of new TXs, 除非这个矿工很有责任心
- 一个急功近利的 miner 有可能为了竞争出块奖励而打包“空块（不包含任何交易的 block）”

## | Full nodes

- are not rewarded,
- are volunteers of the P2P network,
- they are incentivized on preserving and further decentralizing the blockchain.
- a full node does not require a miner to exist.



**Table: Key Characteristics of Node Types**

	Can propose new blocks	Send new transactions	Holds wallet balance information	Holds the complete data history of the blockchain
Mining Nodes	Yes	No	No	No
Full Nodes	No	Yes	Yes	Yes
Light Nodes	No	Yes	Yes	No

Source: SEBA Research



## I 矿池 (Mining Pools)

- the process of mining consumes energy and miners typically have high start-up costs in purchasing the computer power required.
- This has led to the popularity of **mining pools**, which exist to **pool (集中)** hashrate from multiple sources/users.
- 矿工们抱团取暖，按照一定的管理规则参与挖矿，遵守某种利益分配规则获得一定的挖矿奖励



# 比特币社区有什么问题？



# 如何维护一个健康的挖矿生态？



- | 什么时候可以保证 miners 会投入大量算力？
  - 得到的奖励是 BTC, 花费的是 \$, 当奖励大于花费的时候才有动力
- | 如何保障币的价值持续高稳？
  - 当用户普遍相信区块链的安全性时
  - 没有政策的干预时
- | 区块链的安全性、生态健康程度、与 BTC Price
  - 相互依赖、相互作用
  - 刚开始只有中本聪, 后来知道的人、感兴趣的人越来越多
  - 挖矿的人越多, 人们就会对区块链的安全越有信心
  - 每种其他的虚拟货币都要通过 bootstrapping 的考验

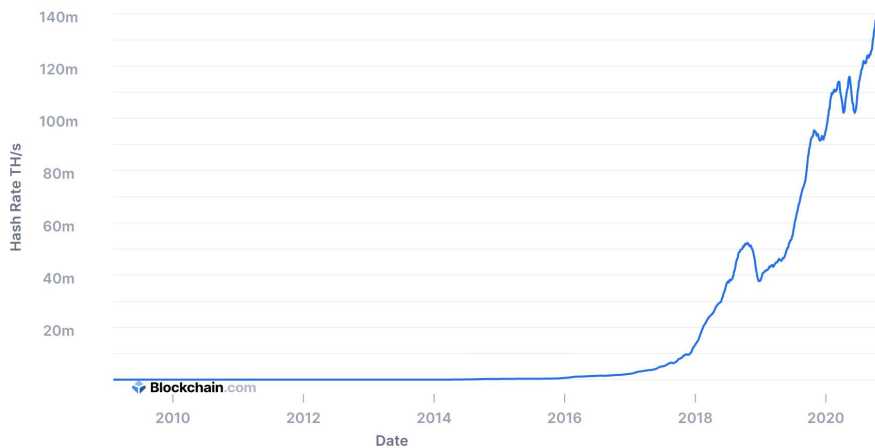
# 启动一个加密货币



## I Bootstrapping 阶段: 冷启动

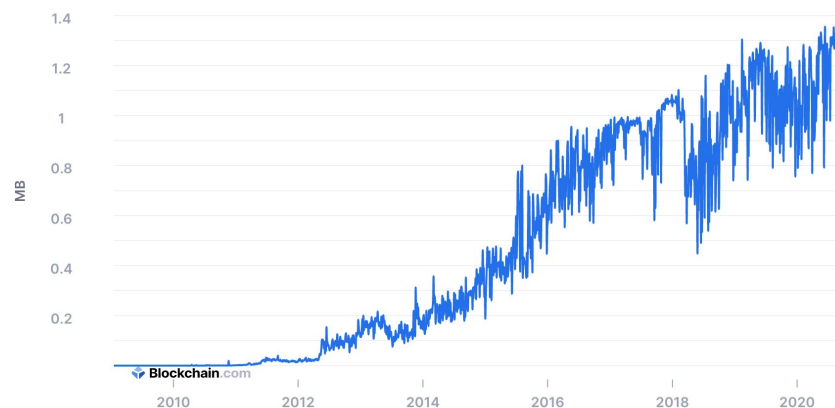
### Total Hash Rate (TH/s)

The estimated number of terahashes per second the bitcoin network is performing in the last 24 hours.



### Average Block Size (MB)

The average block size over the past 24 hours in megabytes.



# 社区的发展——规则更新



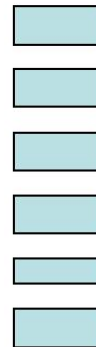
## I 软分叉

- 例如：对现有规则的收紧 (1MB 变为0.5MB)
- 导致：
  - ◆ 未升级 (old) 节点接受 所有的新区块，因为它们都小于1MB；
  - ◆ 已升级 (new) 节点拒绝大于0.5MB的旧区块

原区块链：最大  
1MB 区块

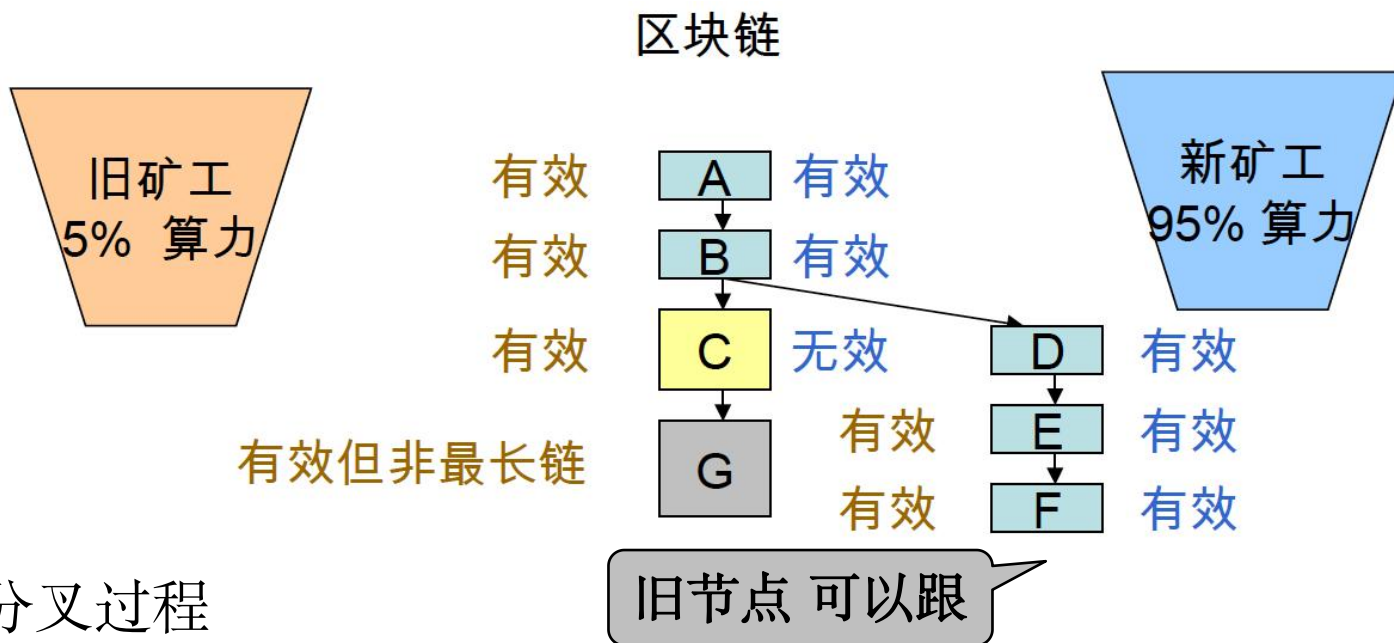


新区块链：  
最大 0.5 MB 区块



旧节点 接受

# 社区的发展——规则更新 (cont.)



## I 软分叉过程

- 旧矿工产生的区块 C 大于0.5MB，因此被新矿工拒绝，新矿工另外挖D。但旧矿工仍认为其有效并在其上添加区块。
- 由于新矿工掌握了绝对优势算力，可以在自己的链上迅速添加区块D,E,F，使其成为最长链。这时旧矿工就会放弃自己挖出的G和C二者，而转到DEF链上去挖矿。
- 结果：
  - ◆ 两侧矿工都会最终到ABDEF上挖矿，区块链不会分裂。
  - ◆ 最重要的是，旧矿工挖出来的大于0.5MB的块都会被孤立掉，所以他们有很强的动机去升级到新版本以避免损失，不久就会达到矿工100%升级的状态

# 社区的发展——规则更新 (cont.)

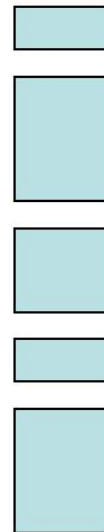


## I 硬分叉

- 例如：对现有规则的放宽 (1MB 变为 2MB)
- 导致：
  - ◆ 未升级 (old) 节点**拒绝** 大于1MB的新区块；
  - ◆ 已升级 (new) 节点接受所有旧的区块，因为它们都小于2MB

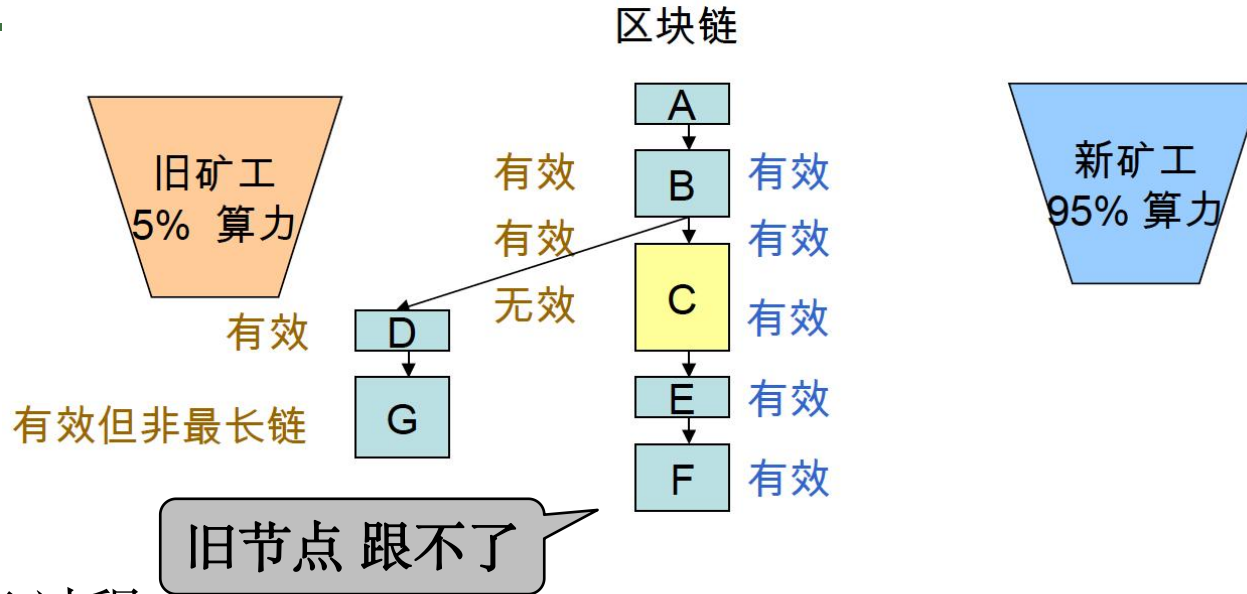
旧区块链：最大  
1MB 区块

新区块链：  
最大 2 MB 区块



旧节点 拒绝

# 社区的发展——规则更新 (cont.)



## I 硬分叉过程

- 新矿工产生区块 C 大于1MB，被旧矿工拒绝，旧矿工转去挖区块D和G。
- 新矿工掌握了优势算力，此后迅速添加了区块E、F并成为最长链。
- 但是，旧矿工无法抛弃DG而转到最长链CEF上挖矿，因为CEF中包含了一个不符合他们规则要求的无效区块C
- 结果：
  - ◆ 旧矿工就在ABDG基础上继续添加区块，
  - ◆ 新矿工则在ABCEF上添加区块，导致区块链的分裂

# Outline of this Class



| Part 1: 比特币社区



| Part 2: 挖矿的激励与策略

| Part 3: 共识的其他知识

| Part 4: 答疑



比特币社区参与者最关心什么？





# 一个引子

# 为什么矿工们如此疯狂地挖矿？



< **yahoo!finance**

## This electric vehicle mines crypto in its free time



Thomas Hum

Sat, 2 October 2021, 3:17 am · 3-min read

### In this article:

ETH-USD  
+1.90% ☆

DOGE-USD  
-2.20% ☆

TSLA  
-0.03% ☆



< **yahoo!finance**

Toronto-based personal light electric vehicle (LEV) producer [Daymak](#) plans to launch a cryptocurrency-mining car that will allow owners to make money when parked, plugged in, or wireless charging.

The car, known as the [Spiritus](#), is a three-wheeled all-electric vehicle able to seat two adults aimed at being a daily commuter “designed with the track in mind,” according to Daymak’s website. The base model Spiritus Deluxe has a top speed of over 85 mph, a 0-to-60 time of 6.9 seconds, and a range of 180 miles. The upgraded sport model Spiritus Ultimate has a top speed of over 130 mph, a 0-to-60 time of 1.8 seconds and a range of 300 miles.

“I think that in the future, we’ll see [cryptocurrency] replacing banks and transactions,” Aldo Baiocchi, president and founder of Daymak, [told Yahoo Finance Live](#). “So it was just logical [to incorporate crypto mining capabilities] since the car comes with computers on board, and most cars, as you know, they depreciate.”



# 比特币设计者需要考虑的几个问题

# 比特币设计者需要考虑的问题:



- | 谁在维护交易账本?
- | 谁在制造新的比特币?
- | 谁有权利批准哪个交易是正当有效的?

# 首先，让我们看一些事实



## I How Many Bitcoins Are There?

- <https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/>



*All data/stats on this page are real-time.*



## | 谁在制造新的比特币？

- 挖到矿的矿工
- 挖矿的整体目的

◆ Every bitcoin transaction must be added to the blockchain, in order to be considered successfully completed or valid.

## | 矿工的“出块激励”，包含两部分：

- 出块奖励 **block reward** (currently 6.25 BTC),
- 交易手续费: all fees sent with the transactions included in the proposed new block.

# Explaining Bitcoin Transaction Fees



- | For this reason, miners have a **financial incentive** to **prioritize** the validation of **TXs** that **include a higher fee**.
- | For someone looking to send funds and get a quick confirmation, **the appropriate fee** to include can **vary greatly**
- | While the fee **does not** depend on the **amount you're sending**, it depends on
  - **network conditions** at the time,
  - and the **data size** of your TX.

# Explaining Bitcoin Transaction Fees (cont.)



## I Network Conditions

- a block on the bitcoin blockchain can only contain up to 1 MB of information
- the # of TXs included in a block is limited
- during the times of congestion, more TXs are waiting in the pool
- miners choose which transactions to include, prioritizing the ones with higher fees
- When the mempool is full
  - ◆ users compete to get their TXs into the next block by including higher and higher fees
  - ◆ Eventually, the market will reach a maximum equilibrium fee that users are willing to pay and the miners will work through the entire mempool in order
- Once network traffic has decreased
  - ◆ the equilibrium fee will go back down



# Explaining Bitcoin Transaction Fees (cont.)



## I Transaction Size

- **block size**: 1 MB of information
- **TX size** is an important consideration for miners
  - ◆ Smaller TXs are easier to validate; larger TXs take more work, and take up more space in the block.
- For this reason, **miners prefer** to include **smaller TXs**.
- A **larger TX** will **require** a **larger fee** to be included in the next block.
  
- Q: Who calculates the TX fees?
  - ◆ Your BTC Wallet will automatically do this for you, and suggest an appropriate fee.

# Explaining Bitcoin Transaction Fees (cont.)



## I Fees in your BTC Wallet

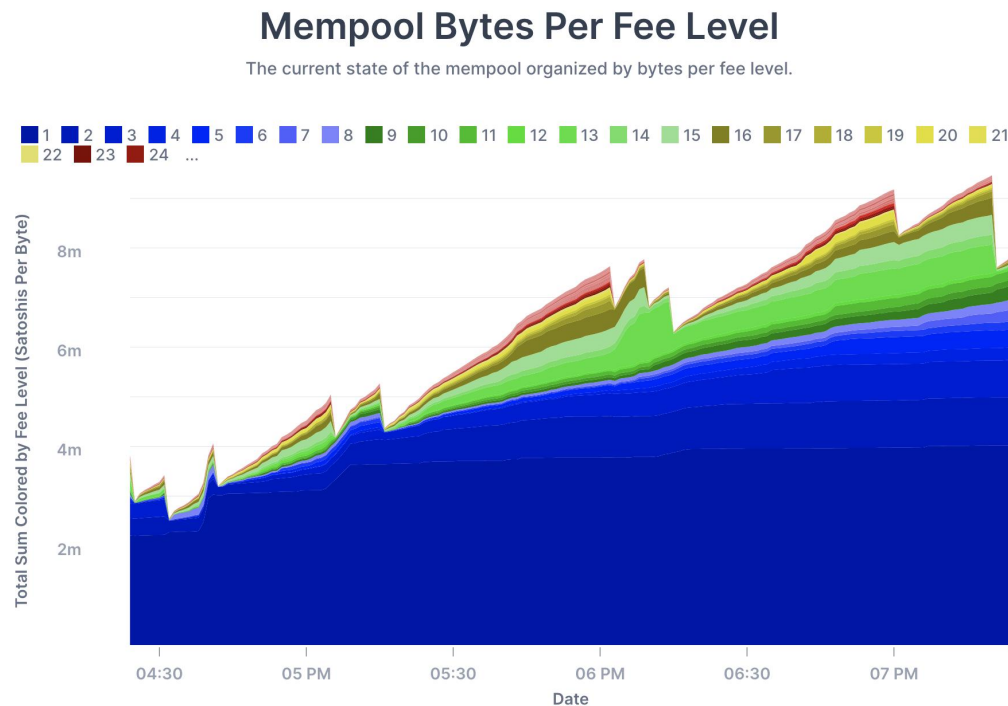
- **dynamic fees**: **wallet** will **calculate** the appropriate **fee** for your TX taking into account **current network conditions** and **TX size**.
- You can choose between a **Priority fee** and a **Regular fee**.
  - ◆ The **Priority fee** is calculated to get your TX included in a block within the hour.
  - ◆ The **Regular fee** is **lower**, and is for users who can afford to be a bit more patient; This type of TXs will typically take a bit more than an hour.
- **Advanced users** can **set custom fees** for their TX in units of satoshi per byte (sat/b)
  - ◆ At a Risk: setting too low a fee may cause your TX to remain **unconfirmed** for a **long time** and possibly be **rejected**.
  - ◆ Q: What will happen when all BTC are out-of-mining?

# 挖矿的策略



## 1. 要打包哪些交易？

- 矿工可以选择将哪些交易放进他的区块里。
- **默认的规则**是选择那些交易费比较高的交易。



该图展示 mempool 中，交易手续费的高低决定了交易被优先处理的程度不一样：颜色越深代表每单位交易的 fee 越高。

按照时间流逝的顺序我们发现，每隔大概10分钟 竖坐标指标会有一次断崖式的下降（代表每次出块），结果显示总是那些交易费比较高的 Bytes (of TX) 从 mempool 中消失了。

# 挖矿的策略 (cont.)



- | 2. 对哪一个区块进行挖矿运算?
  - 矿工可以选择在哪个区块上进行挖矿。
  - **默认的做法**是在最长的那条区块链上继续挖下去。
  
- | 3. 如何在同一高度的多个区块中做选择?
  - 如果两个不同的区块在同一时间被宣布发现，这就造成了一个区块的分叉，每个分叉的区块都是可以被延续下去的，因为它们都符合最长区块链原则。
  - 矿工必须选择其中一个区块接龙下去。
  - **默认的做法**是选择最先被监听到的那一个区块。



## 4. 什么时候宣布新的区块?

- 矿工找到一个有效区块之后，他们要决定什么时候向比特币网络宣布这一个区块。
- **默认的做法**是立刻宣布，
- 但他们也可以选择等一下 —— **自私挖矿** or **block withholding attack**

# 为了挖到新块采取的策略——挖空块现象



I 空块: an empty block

- only includes **block header**
- is with **empty TXs** in the **block body**
  
- What is the **motivation** behind empty blocks?
  - ◆ 更快拿到出块奖励

# 挖矿社区可能采取的恶意策略 — 合谋

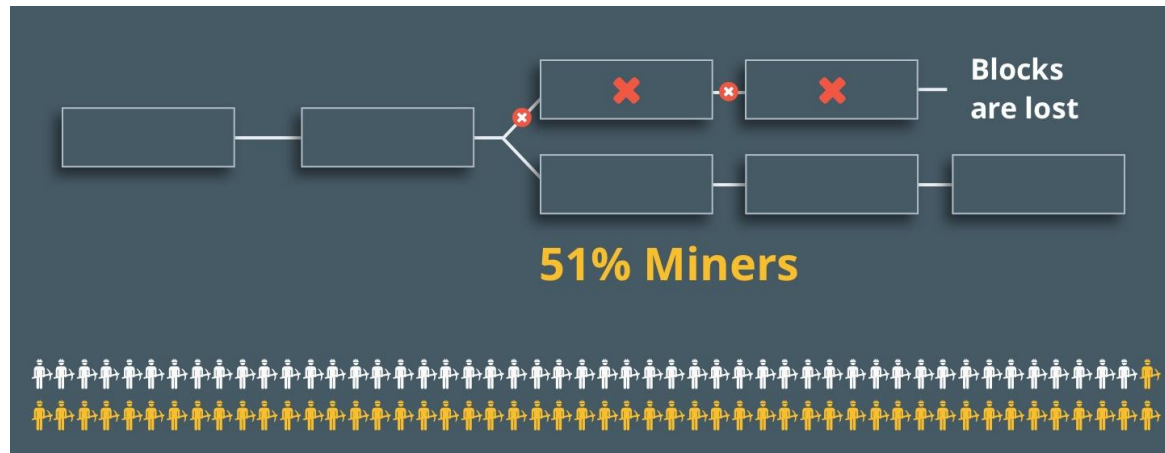


- | 一种合谋: 51% Forking Attack
  - What strategies can help attackers make it?
  
- | 通过贿赂进行分叉攻击
  - 抱团取暖: 矿池, 吸引别的 Miner 加入进来
  - 通过 Out-of-band 方式贿赂、给小费, 争取把分叉链变成最长链
  - 这种攻击能否成功?
    - ◆ 有的矿工会反对: 不要配合, 要维护整体币圈生态
    - ◆ 有的矿工会心动: 短期利益, who care 集体利益

# 一种合谋 —— 51% 攻击



- | A 51% attack is an attack on a blockchain by **a group of miners** who control more than 50% of the network's mining hash rate.



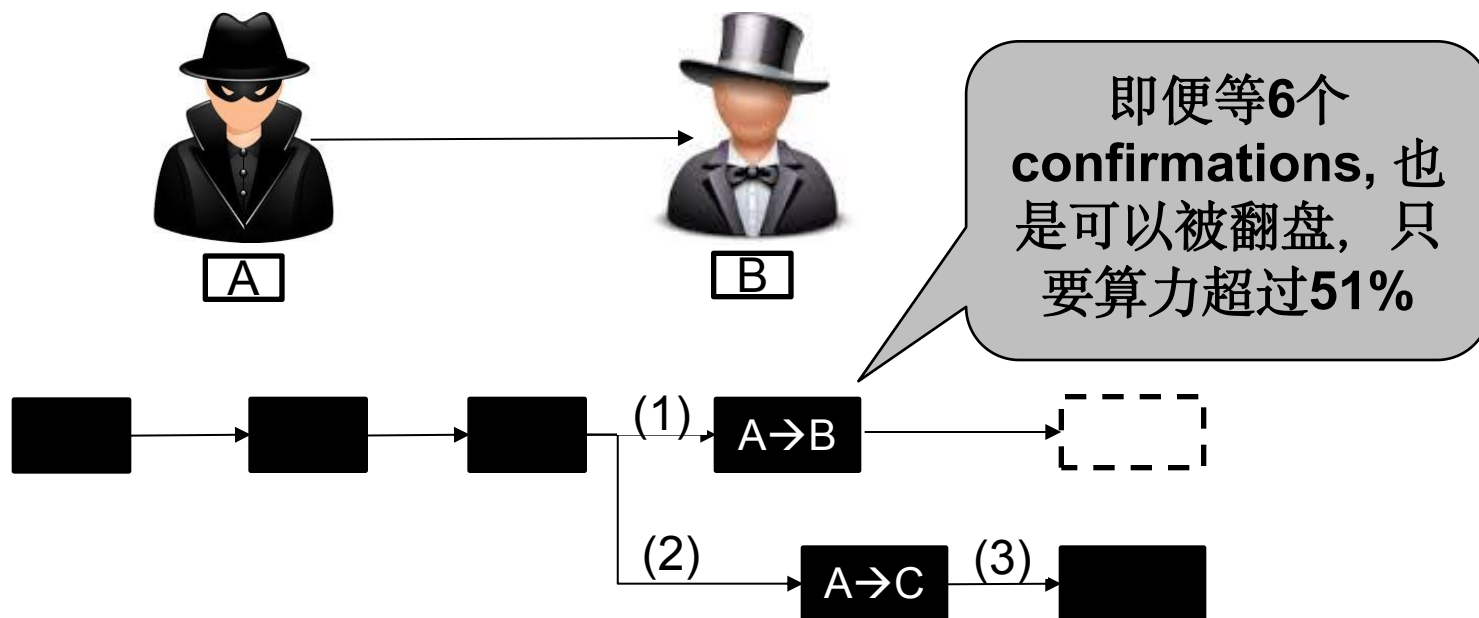


# 一种合谋 —— 51% 攻击 (cont.)



通过51%攻击，可以实现 double-spending attack

- (1) A给B支付比特币，交易在一个块中确认
- (2) A重新构造一笔交易A→C，并打包进区块公布（分叉）
- (3) 包含双重支付的块率先找到下一个块，全网认可A→C，交易A→B无效



# 如何防范 51%攻击？



- | 除了尽量**避免算力放到同一个组织**手里，没太好的办法
  - 这是目前 PoW 机制自身造成的
- | 绝大多数的矿工，都会通过**诚实挖矿**来维持整个比特币系统
  - 如果他们集体伪造交易，用户对比特币失去了信心，没人再去使用比特币。那么矿工伪造了交易盗取比特币就失去了意义
- | **6个确认机制**
  - 如果真有这样的**51%攻击**，建议是收款方等到全网的**6个区块确认**之后再交付商品
  - 按照**10分钟**一个区块的速度，只需一个小时就可以保证你的钱是否基本肯定收到
  - **6个区块后再对全网进行篡改的难度很高**
  - **A tradeoff**: 确认的块数不一定是**6**，可以为了更安全而采取更大的确认块数，但是需要等待的时间也越长

# 交易的确认次数 - 以太坊的交易例子



All Filters ▾

Search by /

Ropsten Testnet Network

Home BI

## Transaction Details

Overview State

[ This is a Ropsten **Testnet** transaction only ]

Transaction Hash:	0xb6a70ffc9bc1d864fd776abd973b05418937d819665e1ab0f5a1dc79756928e7
Status:	<span>✔ Success</span>
Block:	8854537 <span>14 Block Confirmations</span>
Timestamp:	⌚ 3 mins ago (Oct-11-2020 04:43:46 AM +UTC)
From:	0x81b7e08f65bdf5648606c89998a9cc8164397647
To:	0x8554a40e3ae79e388c5c3b735b4a2fc64765c919
Value:	<span>1 Ether</span> (\$0.00)
Transaction Fee:	0.000042 Ether (\$0.000000)
Gas Price:	0.000000002 Ether (2 Gwei)

# 51% 攻击的引申思考



- | 51%攻击可以压制 (阻止) 其他交易吗?
  - 如果他知道某些讨厌的人 (比如, Peter) 的地址, 攻击者可以让源于 Peter 地址的币都无法使用吗?
  
  - 攻击者可以做到:
    - ◆ 不打包那些包含来自Peter 的交易,
    - ◆ 轻易拒绝 create 包含来自 Peter 地址的交易的 new block
    - ◆ 拒绝在含有类似交易的 block 上延展
  
  - 但是, 他不可以阻止 Peter 的交易
    - ◆ 因为 Peter 的交易会被发送到绝大部分节点上。如果攻击者作恶, 大家会轻易发现他的恶意行为

# Outline of this Class



| Part 1: 比特币社区

| Part 2: 挖矿的激励与策略



| Part 3: 共识的其他知识

| Part 4: 答疑



- | 比特币协议达成共识两大障碍
  - 不完美的网络：信息延迟 与 节点down机
  - 某些节点故意搞破坏
  
- | 分布式协议：FLP不可能结论
  - 由 Michael J. Fischer, Nance A. Lynch 与 Michael S. Paterson 在论文 *Impossibility of distributed consensus with one faulty process* 中证明的一个结论
  
  - 分布式理论中**最为深刻的结论**：在一个多进程异步系统中，只要有一个进程不可靠，那么就不存在一个协议，此协议能保证有限时间内使所有进程达成一致



- | 可是，FLP不可能结论是分布式数据库的结论，不能完全套用到比特币
- | 比特币打破了很多分布式数据库所做的假设
  - 比特币或许对分布式共识给出解决方案
  - 比特币实际运行远比理论上预示的好得多
  - 插曲：那么分布式理论研究是不是没有用了？
    - ◆ 理论结果可以让我们预测、预防未来可能出现的攻击和其他问题
    - ◆ 一旦完善了比特币分布式共识背后的理论运作机制，我们才能对比特币的安全性和稳定性做出保证



## I 比特币打破了哪些经典模型所做的假设？

1. 比特币引进了奖励的理念：人们为了金钱奖励会变得诚实起来
  - ◆ 可以说比特币是在特定的货币系统下解决了分布式共识问题
2. 比特币体系包含随机性
  - ◆ 不用管一个共识的起点与终点
  - ◆ 随着时间流逝，比特币网络对某一个 **Block** 的认识与最终总体共识相吻合的概率会越来越大

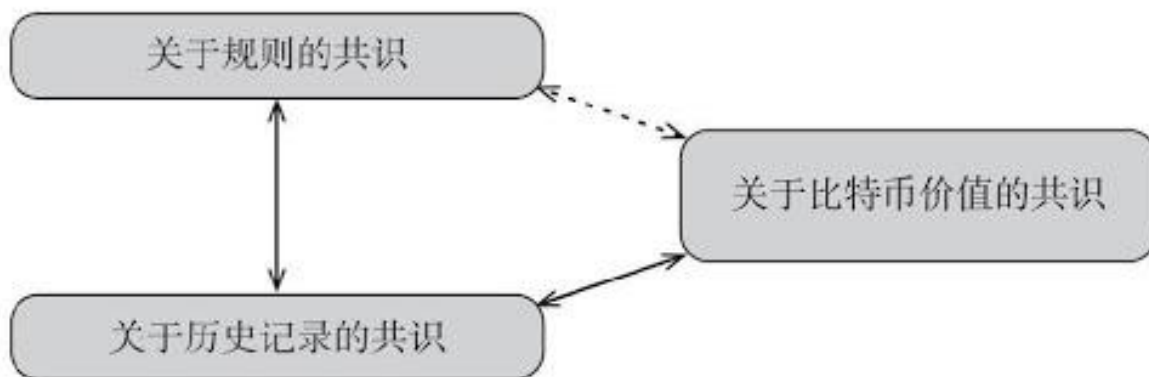
– **Bitcoin overcomes FLP results!**



# 比特币共识—三个层面



- | 比特币设计简单，但是它能顺畅运行，背后有什么原因？
- | 三个问题达成了共识
  - 规则的共识
  - 历史记录的共识
  - 比特币价值的共识



# 比特币共识--三个层面



## I 规则的共识

- 规则：确保交易/block 有效的机制
- 比特币运行的核心协议、数据结构

## I 意义：to ensure

- Bitcoin participants can communicate with each other **to achieve the consensus**

# 比特币共识—三个层面



## | 历史记录的一致

- 记录：已发生的交易

## | 意义：to agree with

- Bitcoin owners' unspent # of coins

# 比特币共识--三个层面



- | Bitcoin's Price 的共识
  - Price: measured in \$
  
- | 意义: to ensure that
  - Everyone wants Bitcoin
  - Everyone can trade with Bitcoin



## I The **genius** of Bitcoin's Design


- It realizes that **it is hard to achieve** any of the three perspectives of consensus,
- because it is **impossible** to guarantee the consensus of rules in a *decentralized*, *anonymous*, and *worldwide* system

## I However, we see that

- Bitcoin **somehow** combine those 3 perspectives of consensus together and make them support each other
- But **don't to be too optimistic!** This consensus is **fragile**: it is mixed with **technologies** and **social network issues**.

# Outline of this Class



- | Part 1: 比特币社区
- | Part 2: 挖矿的激励与策略
- | Part 3: 共识的其他知识
-  | Part 4: 答疑



# 答疑

# 答疑1: 51%-based Double Spending



- | (问) 老师, 我还是不是很理解双花, 既然失败的链的交易还是会回滚到交易池, 那同一笔钱怎么能花两次呢?
  - A付钱给B, B等交易确认再交货给A, 交易确认了, B就收到钱了。为什么会存在双花?
  - (追问) 这个过程中A- >B不是还没确认吗? 感觉B只要不交货给A那就对B没有损失才对。

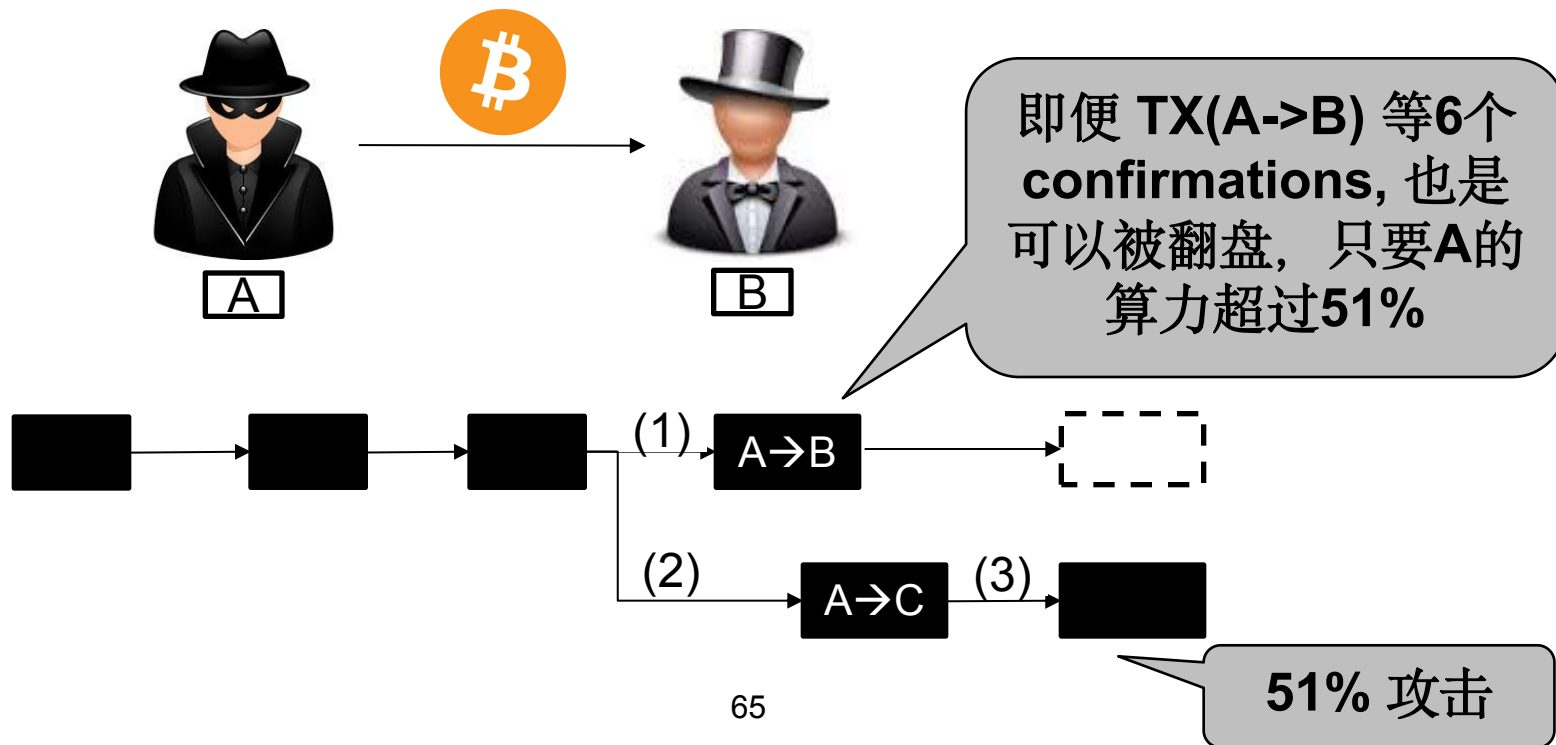


# 答疑1: 分叉攻击



## 回顾双花支付：如何做到 一笔钱花两次？

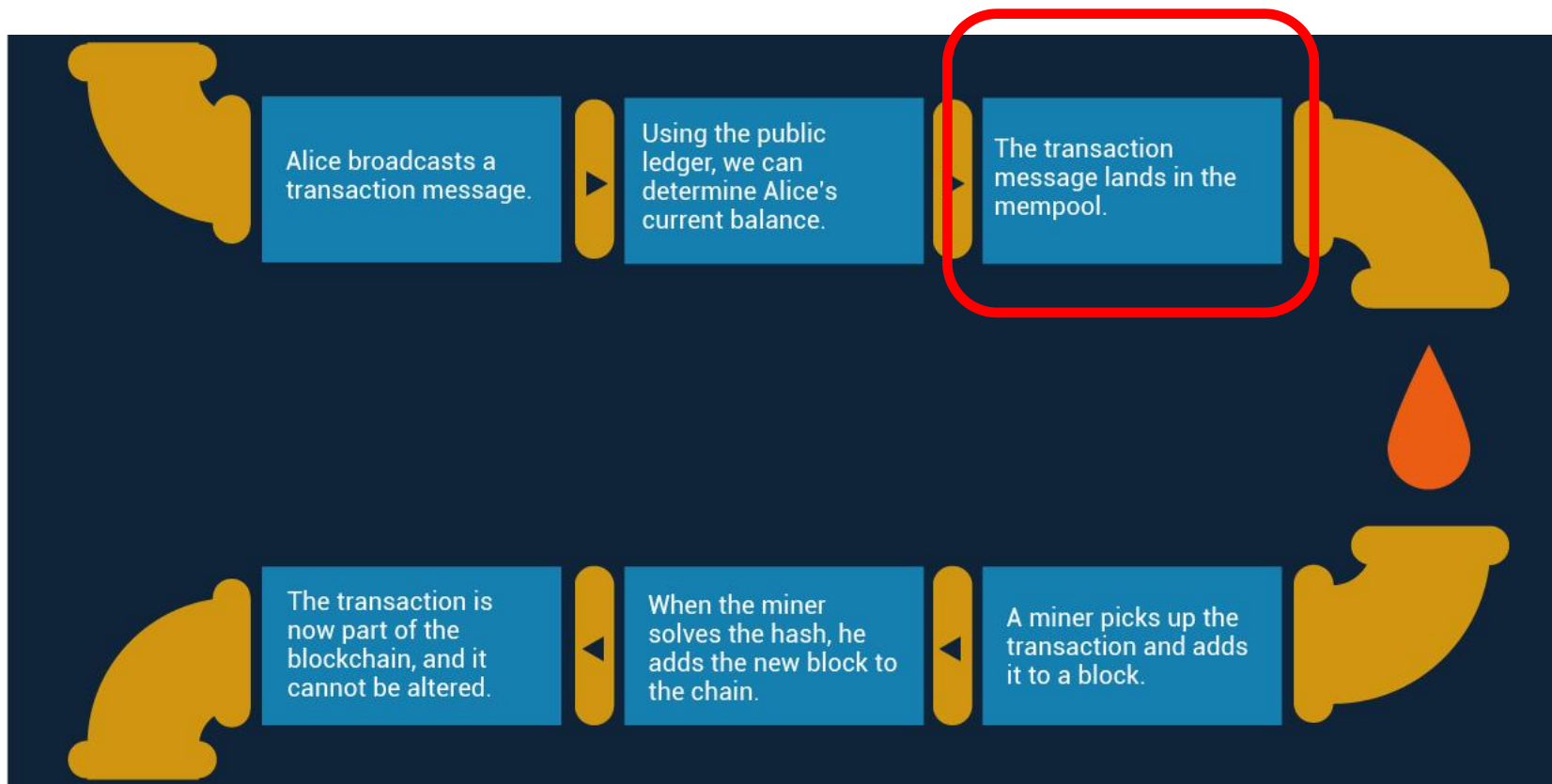
- (1) A支付比特币给B，交易在一个块中确认（如何阻止或者逆转TX(A→B)?)
- (2) A重新构造一笔交易A→C，并打包进区块公布（分叉攻击，双重支付）
- (3) 包含双重支付的块率先找到下一个块，全网认可A→C，交易A→B无效



# 答疑2: 比特币交易是如何打包的



- 1 (问) 比特币的交易是如何被选中打包的? 遵循什么原则?
- 过程如下图所示; 遵循的规则本节课会讲到一部分
  - Tx打包之前需要先提交到 mempool。先来了解 mempool 的一些细节

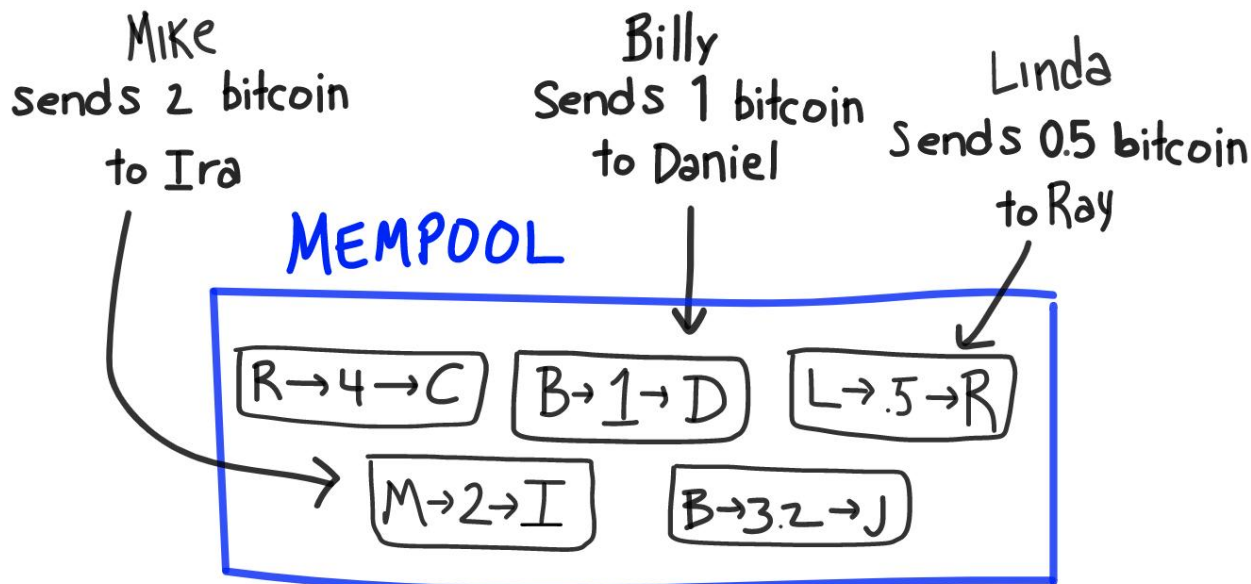


# 答疑 – mempool (上节课提到过)



## I Mempool

- <https://blog.kaiko.com/an-in-depth-guide-into-how-the-mempool-works-c758b781c608>
- The mempool is the node's holding area for all the **pending TXs**.



# 答疑 – mempool (cont.)



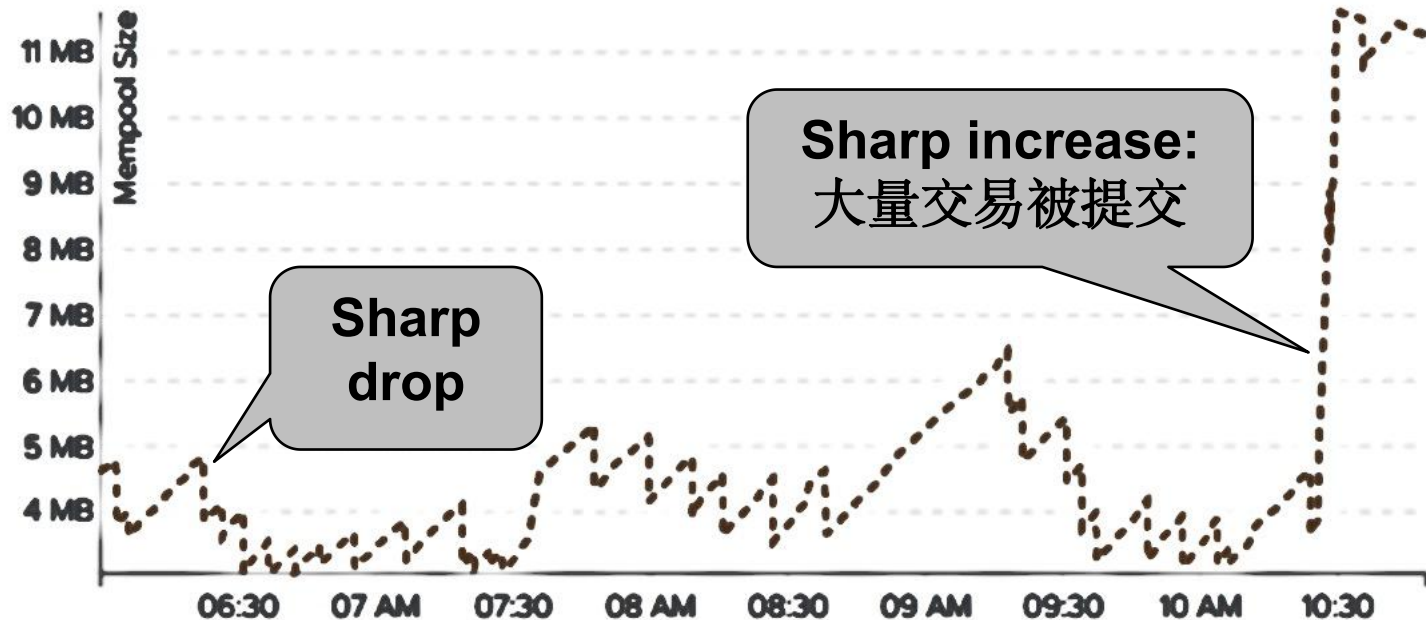
- | **There are as many mempools as there are as nodes**
  - As the Bitcoin network is **distributed**, not all nodes receive the same transactions at the same time,
  - so **some nodes store more TXs than others** at some time.
  
  - Plus, everyone can run its own node **with the hardware of his choice**; so all nodes have a **different RAM capacity** to store unconfirmed TXs.
  
  - As a result, **each node has its own version of the pending TXs**
  
  - This explains the variety of **mempool sizes & TX counts** found on different sources.

# 答疑 – mempool (cont.)

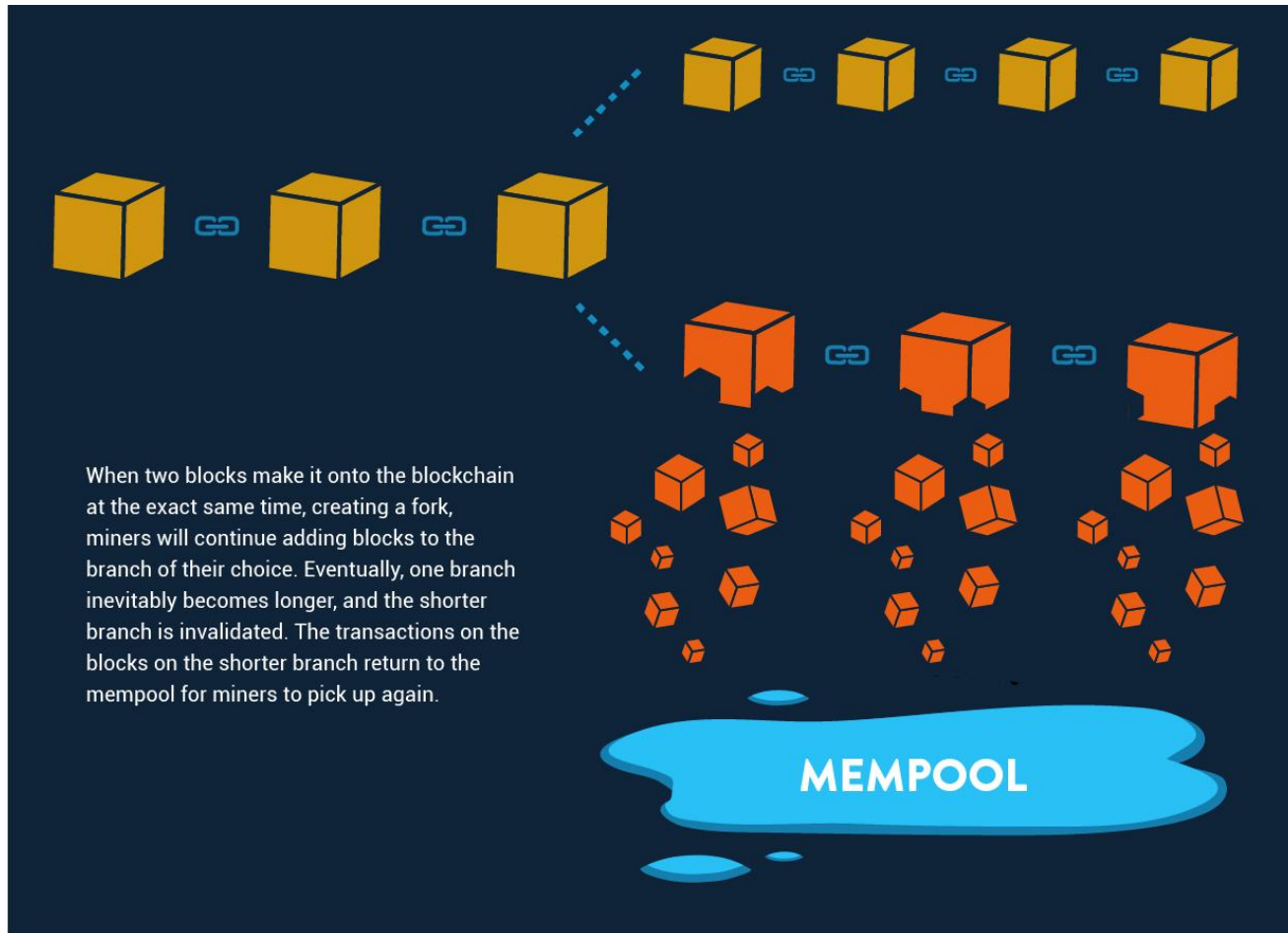


## I How does a new block impact the Mempool?

- When a node receives a **new valid block**, it removes all the **TXs contained in this block** from its **local mempool**, as well as the **TXs that have conflicting UTXO inputs**.
- This results in a **sharp drop** in the Mempool size



# 答疑3: 那么被撤销的交易是如何处理的?



答案: 重新回到了 mempool, 等待后续的打包上链



# More materials

# 推荐 – Github book: Mastering Bitcoin



– <https://github.com/bitcoinbook/bitcoinbook>

## Chapters

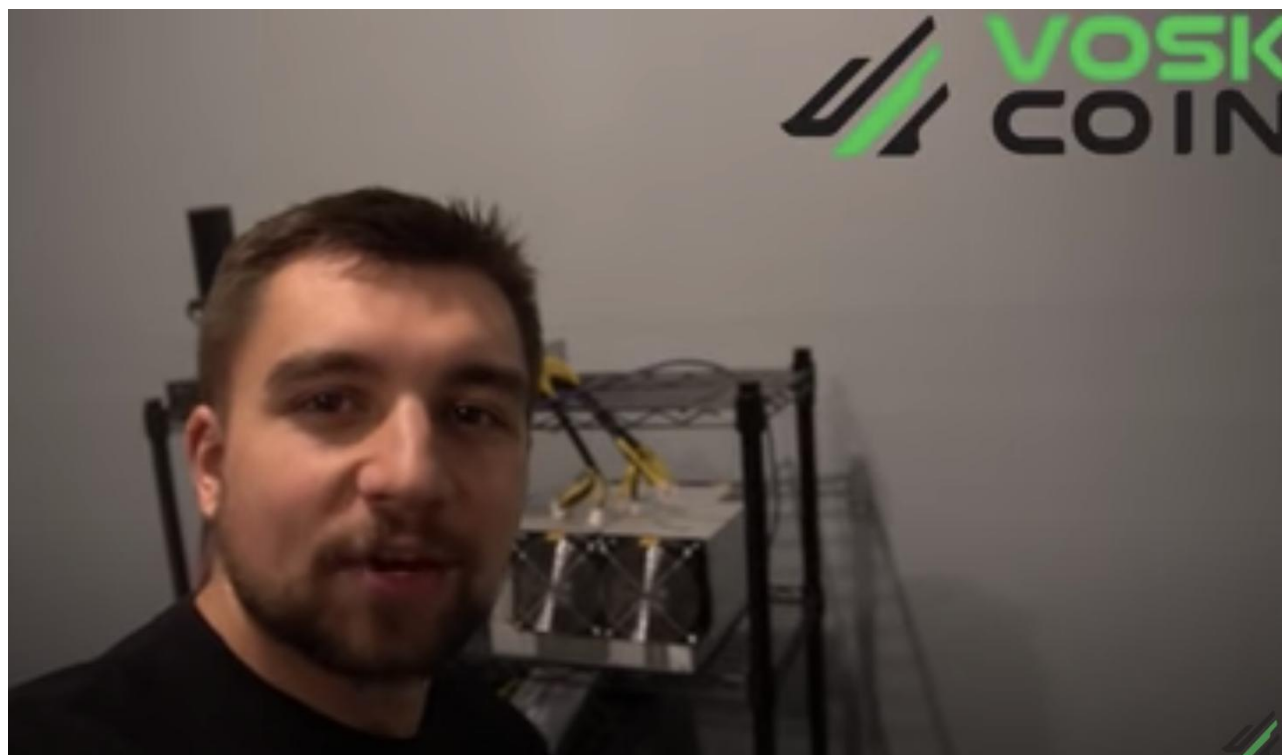
---

- Chapter 1: 'Introduction'
- Chapter 2: 'How Bitcoin Works'
- Chapter 3: 'Bitcoin Core: The Reference Implementation'
- Chapter 4: 'Keys, Addresses'
- Chapter 5: 'Wallets'
- Chapter 6: 'Transactions'
- Chapter 7: 'Advanced Transactions and Scripting'
- Chapter 8: 'The Bitcoin Network'
- Chapter 9: 'The Blockchain'
- Chapter 10: 'Mining and Consensus'
- Chapter 11: 'Bitcoin Security'
- Chapter 12: 'Blockchain Applications'



## | What Do YOU Need to MINE ONE BITCOIN In 2020?!

- [https://www.youtube.com/watch?v=5V\\_Ap0Iy\\_M0](https://www.youtube.com/watch?v=5V_Ap0Iy_M0)



# 作业2-Due 11.15



## 作业内容:

- | 阅读: 阅读“Monoxide: Scale Out Blockchain with Asynchronized Consensus Zones”, 2019年由计算机网络顶级学术会议 NSDI 所接收。
- | 总结与思考: 比特币设计简单, 但是它能顺畅运行, 背后有什么原因? Monoxide 提出的共识机制与比特币的共识机制有哪些不一样? 思考: 连弩挖矿机制存在什么样的潜在问题?

# 作业2-Due 11.15



## | 2、参考文献:

| Monoxide: Scale Out Blockchain with Asynchronized Consensus Zones

| Majority Is Not Enough Bitcoin: Mining Is Vulnerable

| “ Proof-of-Work ” Proves Not to Work; version 0.2

## | 3、作业要求:

| 要求写出自己的观点，字数不限。

| 截止提交时间11月15日24:00。