Bitcoin 社区

黄华威
副教授

中山大学
数据科学与计算机学院
Http://xintelligence.pro

课程大纲

- Week-1 9月2日　课程背景介绍，与区块链应用背景，比特币前传
- -- Part-1: 比特币与以太坊基础知识部分
- Week-2　9月9日　Bitcoin 基础：密码学基础
- Week-3　9月16日　Bitcoin 基础：数据结构
- Week-4　9月23日　Bitcoin 运行机制：交易模型、与共识机制
- Week-5　9月30日　Bitcoin 系统层面的知识（林建入老师上课）
- Week-6　10月7日　Ethereum 概述 与 智能合约（林建入老师上课）
- Week-7　10月14日　比特币的挖矿、分叉的原理
- Week-8　10月21日　比特币社区
- Week-9　10月28日　匿名、监管、与 区块链网络基础
- Week-10　11月4日　考试周（不上课）
- -- Part-2: 区块链工程实践课
- Week-11　11月11日　微众合作开发课程1
- Week-12　11月18日　微众合作开发课程2
- Week-13　11月25日　微众合作开发课程3
- -- Part-3: 区块链研究启发
- Week-14　12月2日　以太坊其他：账户、状态、挖矿算法、可扩展性
- Week-15　12月9日　数据分析与反欺诈
- Week-16　12月16日　区块链的安全问题与攻击模型：攻击与防御
- Week-17　12月23日　区块链的分片技术、与网络“排队理论”
- Week-18　12月30日　区块链的互操作性
- Week-19　1月6日　区块链 与 Game Theory: 以 FruitChain 为例

课前答疑-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。

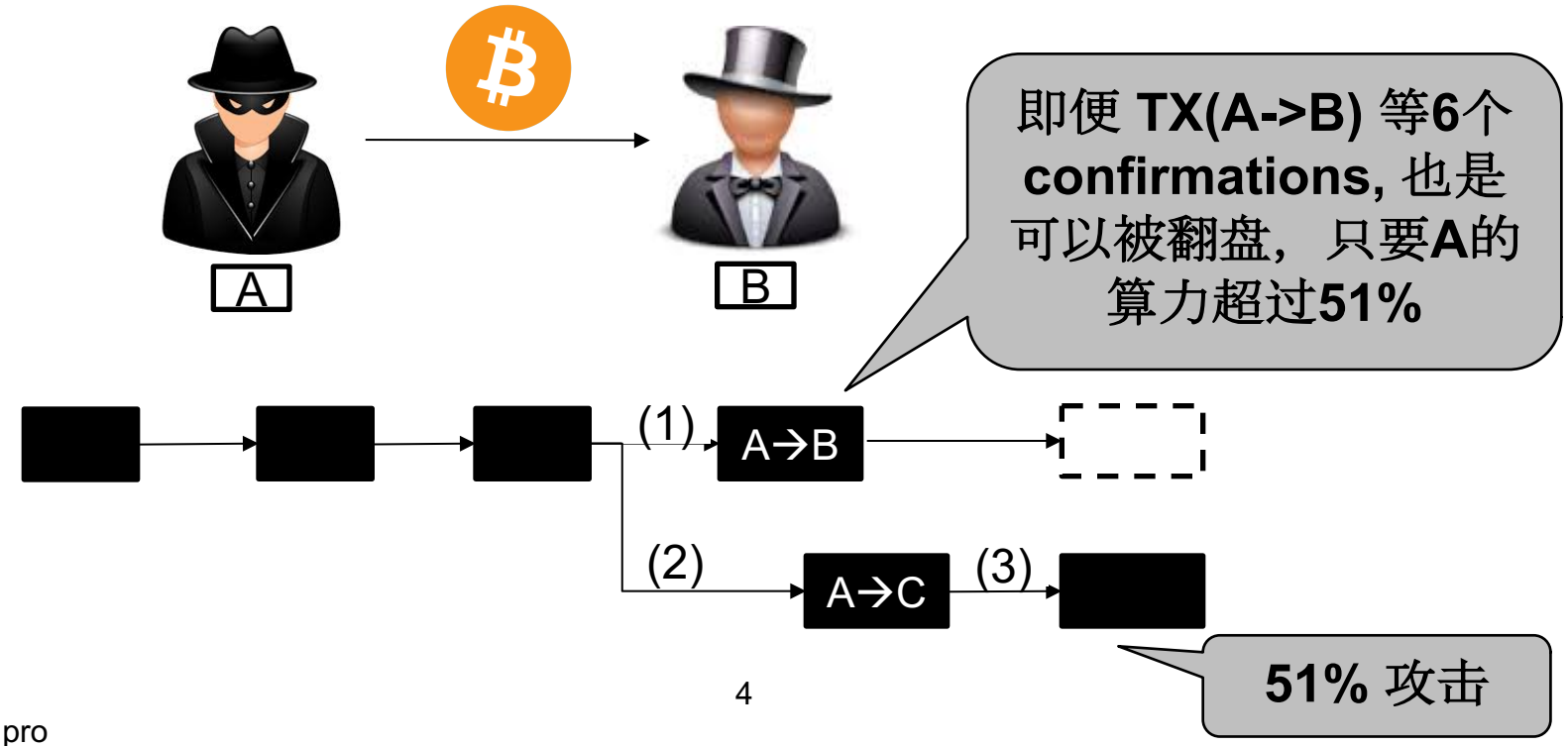
课前答疑：分叉攻击

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



Other Tips of 51% attack

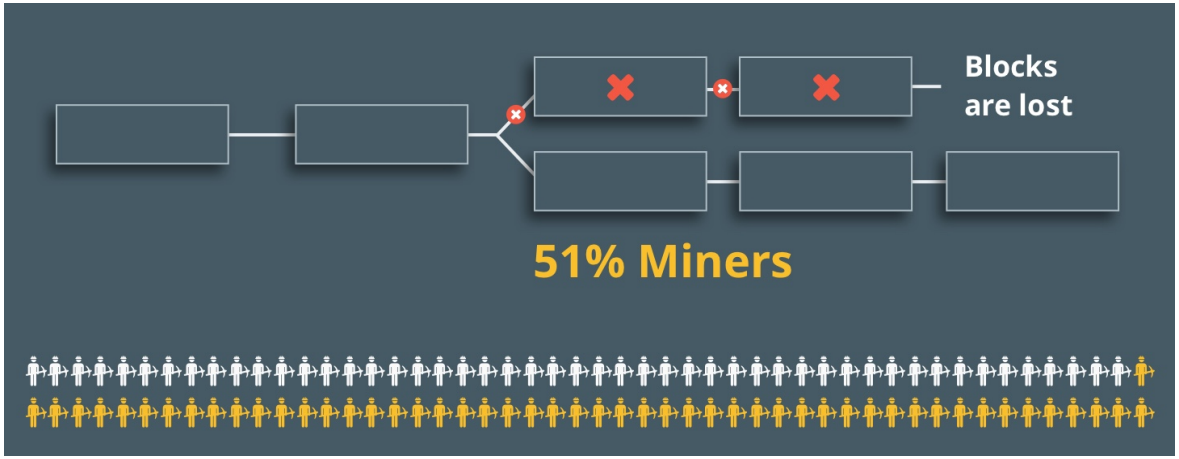
- **Definition**:
  - A 51% attack is an attack on a blockchain by a group of miners who control more than 50% of the network's mining hash rate.

- Changing historical blocks is difficult
  - due to the hard-coding of past transactions into the bitcoin software.

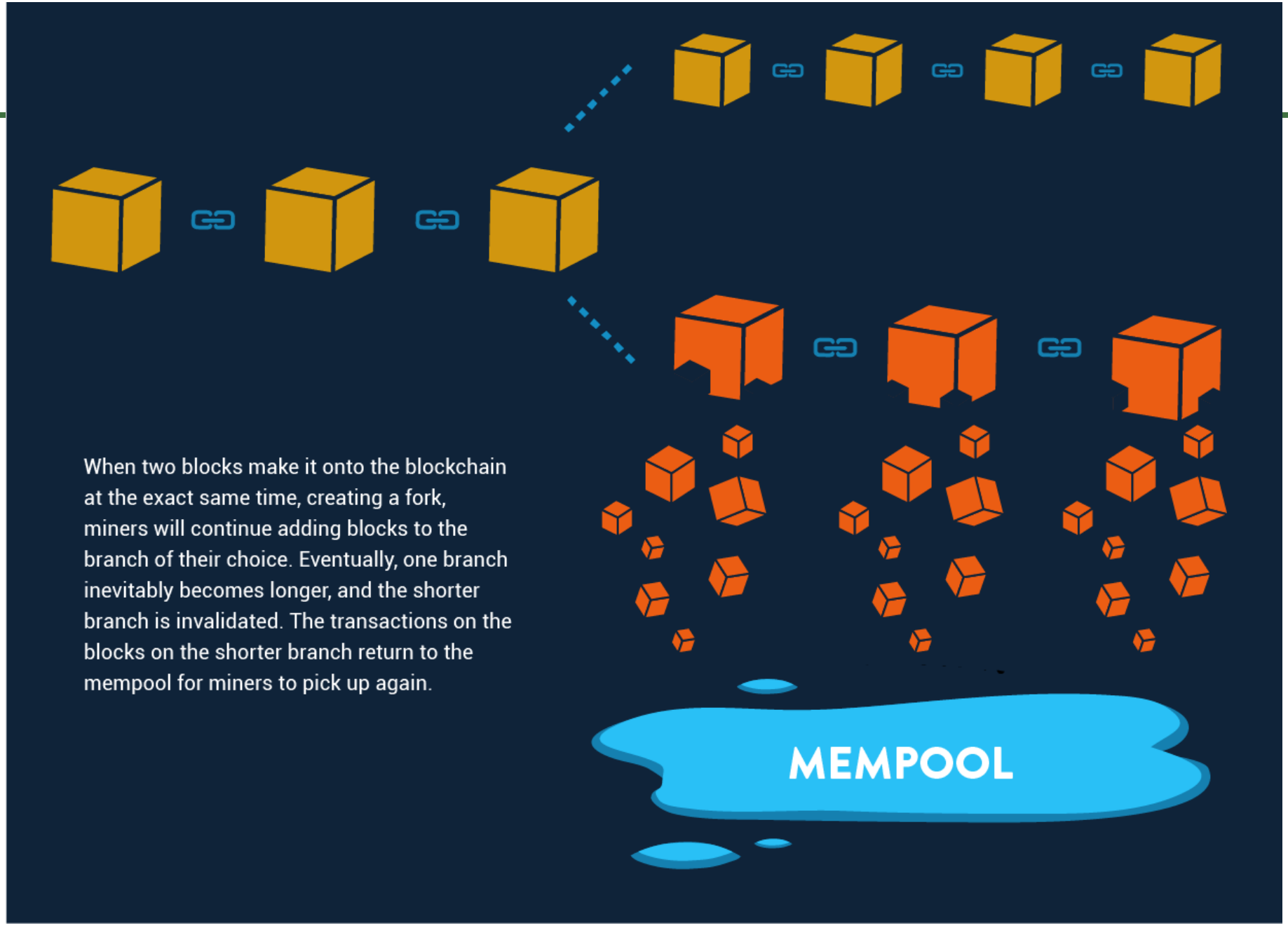
- If an attacker is somehow able to control at least 51% of the hash power of the network,
  - he or she can commit double spending.

51% attack is impossible in reality

- What could a 51% attacker be able to do?
  - he or she could reverse transactions and create a separate private blockchain / a fork



- However, the rapid growth of bitcoin has virtually insured that
  - this type of attack is **impossible**.

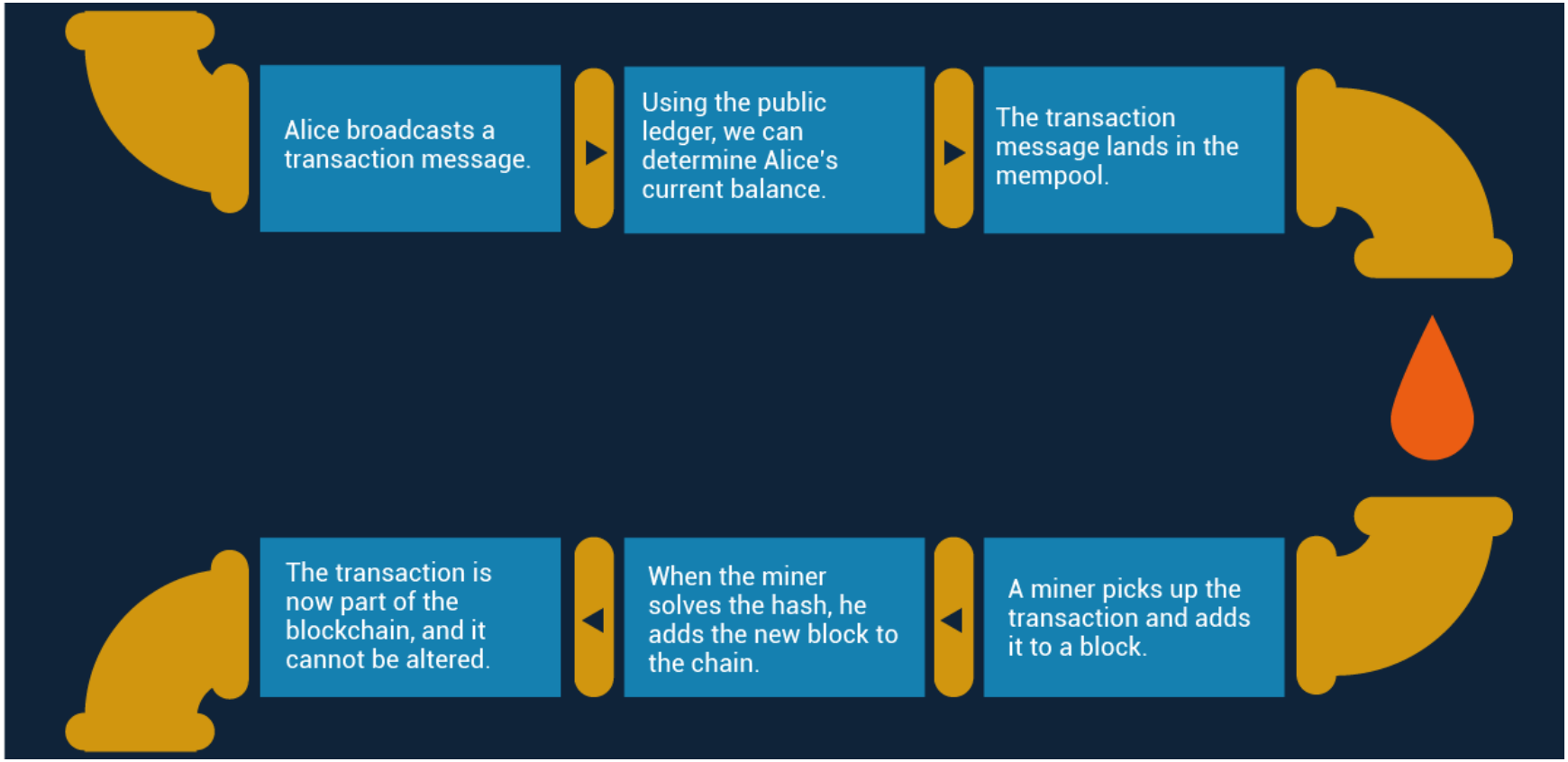

When two blocks make it onto the blockchain at the exact same time, creating a fork, miners will continue adding blocks to the branch of their choice. Eventually, one branch inevitably becomes longer, and the shorter branch is invalidated. The transactions on the blocks on the shorter branch return to the mempool for miners to pick up again.
MEMPOOL

51% attack 引申思考

- 51%攻击可以压制其他交易吗？
  - 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
    - 这个交易被发送到绝大部分节点上，否则，大家就会发现了他的攻击

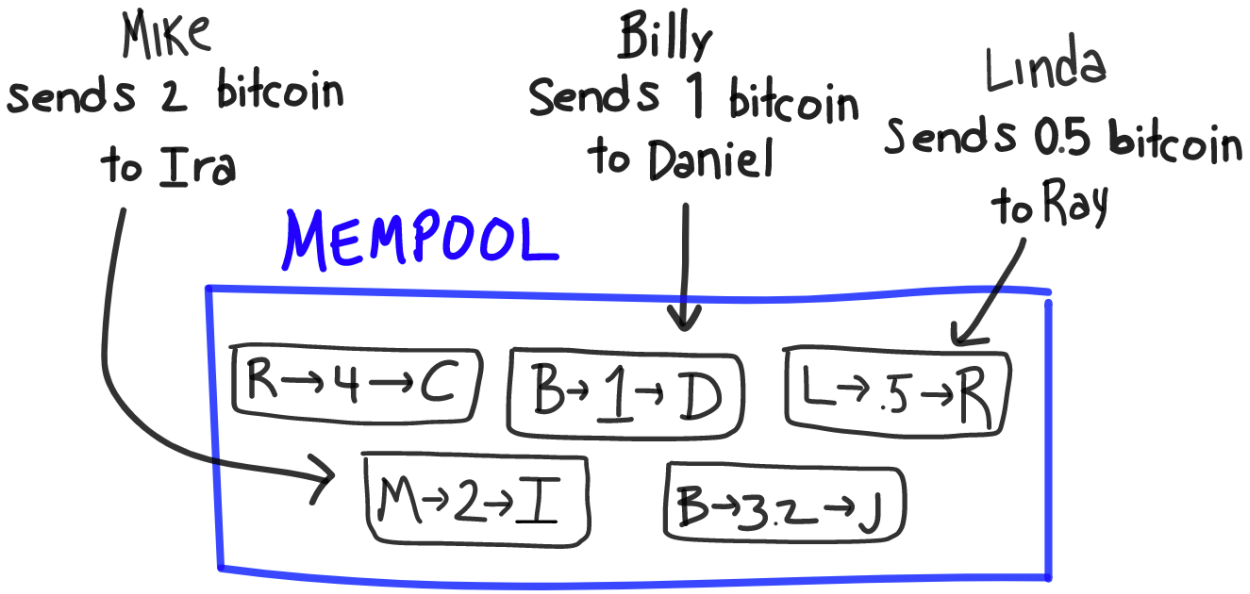
课前答疑-2：比特币交易是如何打包的

- (问) 比特币的交易是如何被选中打包的？遵循什么原则？



课前答疑-2 -- mempool

- 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 transactions.**



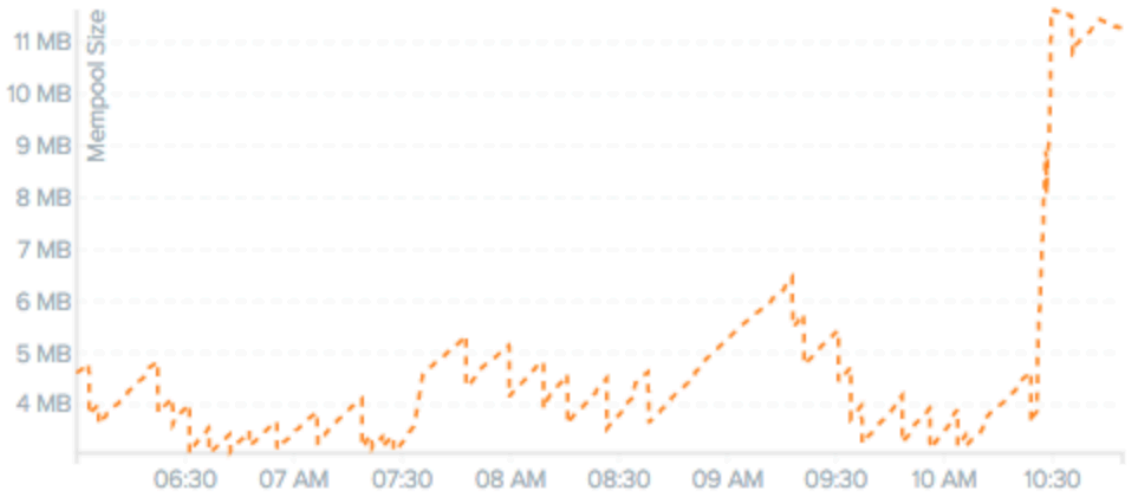
课前答疑-2 -- mempool

- 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 transactions.
  - As a result, **each node has its own version of the pending transactions**
  - This explains the variety of mempool sizes & transactions counts found on different sources.

课前答疑-2 -- mempool

How does a new block impact the Mempool?

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



课前答疑-2 -- mempool

- What happens when the node's memory get full?
  - Unlike mining, there is no financial incentive for running a node.
  - Therefore, the hardware dedicated to it tends to be limited and so a node's Mempool often max out its RAM.
  - When this happens, in former versions of bitcoin, the node would just crash and restart with an empty Mempool.

课前答疑-2 -- mempool

- What happens when the node's memory get full?
  - In recent versions of bitcoin (0.12+), if the Mempool size gets too close to the RAM capacity, the node sets up a minimal fee threshold.
  - Transactions with fees per kB lower than this threshold are immediately removed from the Mempool,
  - only new transactions with a fee per kB large enough are allowed access to the Mempool.

课前推荐 – Github book: Mastering Bitcion

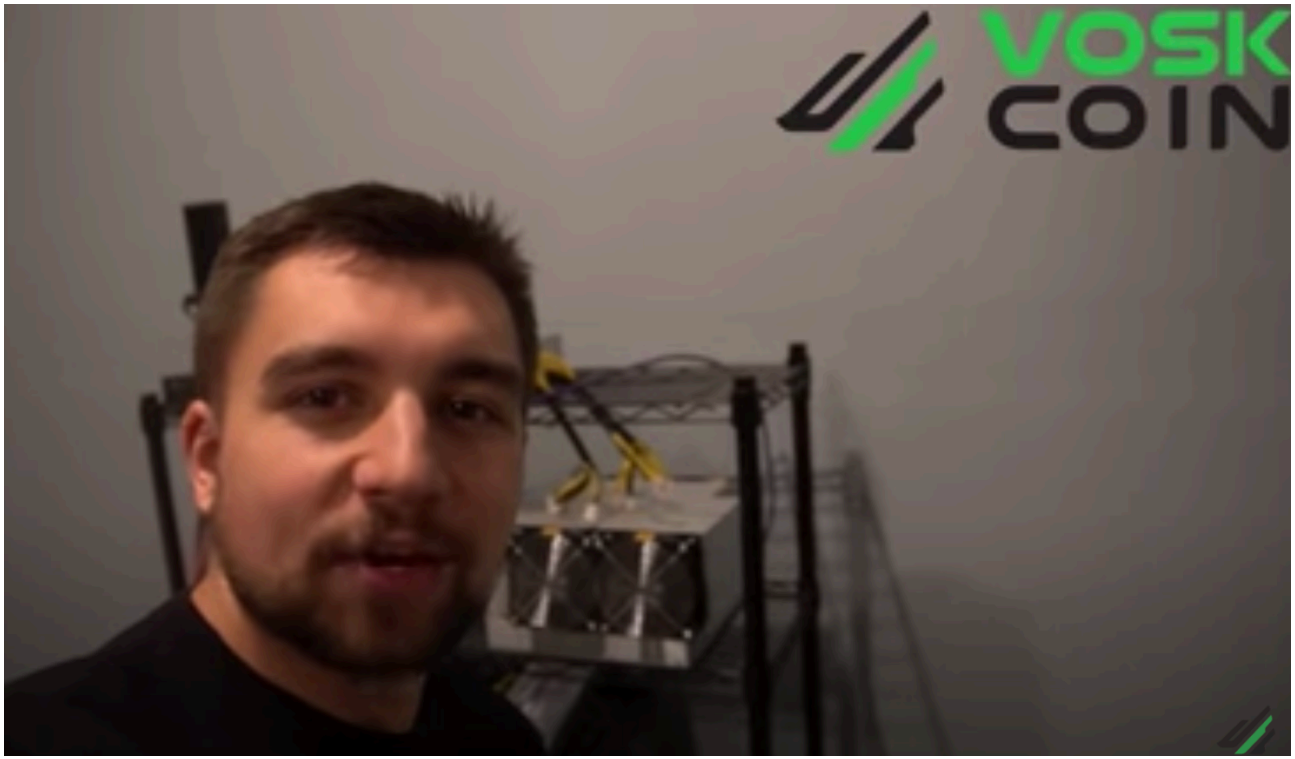
– https://github.com/bitcoinbook/bitcoinbook

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'

课前视频

- What Do YOU Need to MINE ONE BITCOIN In 2020?!
  - https://www.youtube.com/watch?v=5V_Ap0Iy_M0



Outline & Keywords of this Class

- Part 1:比特币安全机制的保障
- Part 2:挖矿的激励与策略
- Part 3: 社区

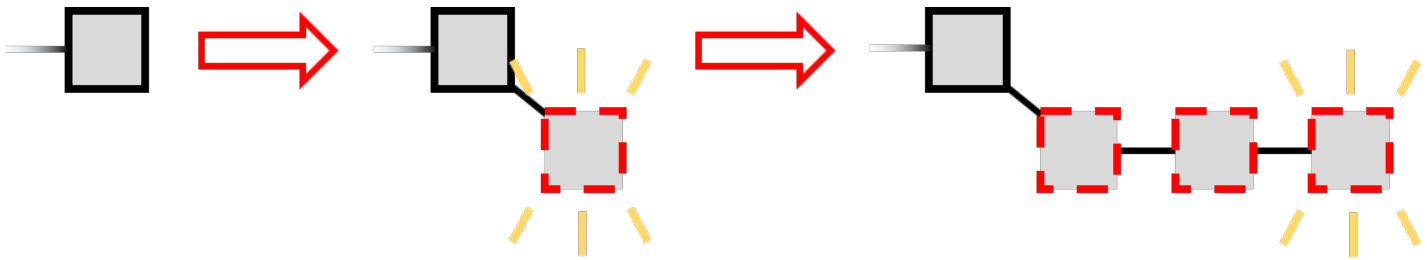
思考：挖矿的安全性分析

- 假设BTC的大部分算力是掌握在 honest 旷工手里，有什么安全保障？
  - #1. 恶意节点可以伪造一个交易把别人的钱转给自己吗？
    - 不能，因为有签名，别的 honest 节点不会承认，把它通过分叉废除了，该恶意节点白费力气又损失了钱
  - #2. 恶意节点可以 double-spending 吗？
    - 很难，除非有 51% 算力
  - #3. 避免 selfish-mining
    - 悄悄挖不发布，为了获取更多的出块奖励，How to？

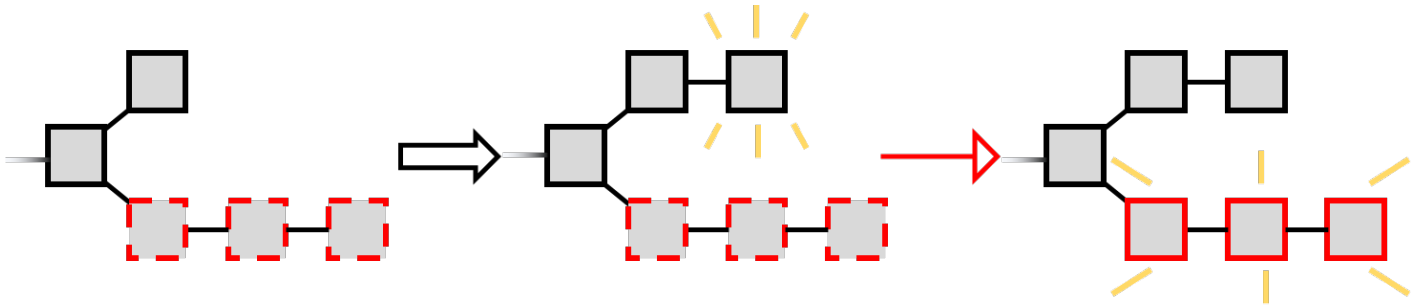
Selfish Mining —— 自私挖矿

- Definition
  - A selfish miner hides the new block it just mined, and keeps to mine the next following this hidden one.

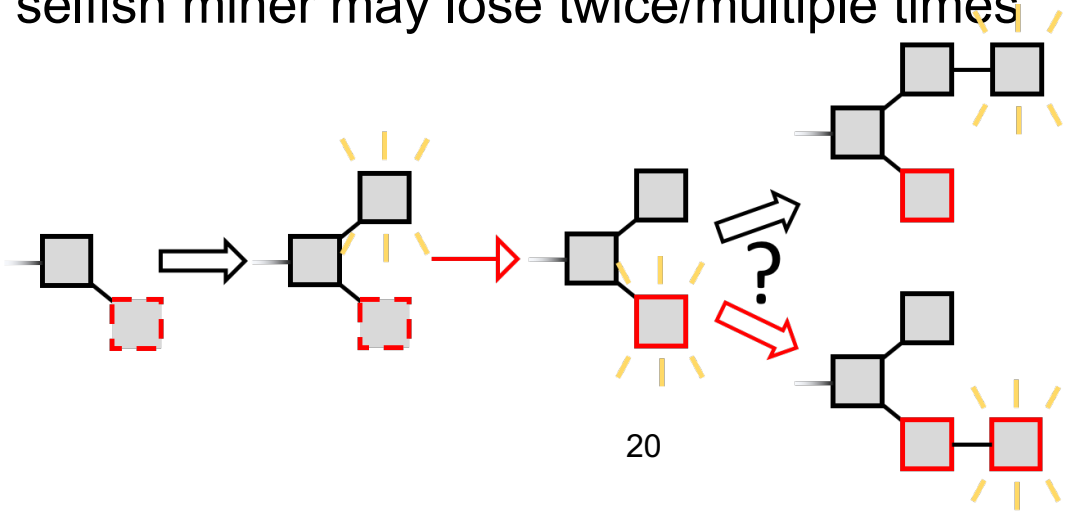
- Motivation: Why mine secretly?
  - Only himself knows a new block was just mined, such that others are mining following the ***wrong / old*** previous block
  - 一旦发布出去，大家都会在新区块后边平等地开始竞争



Selfish Mining —— 自私挖矿

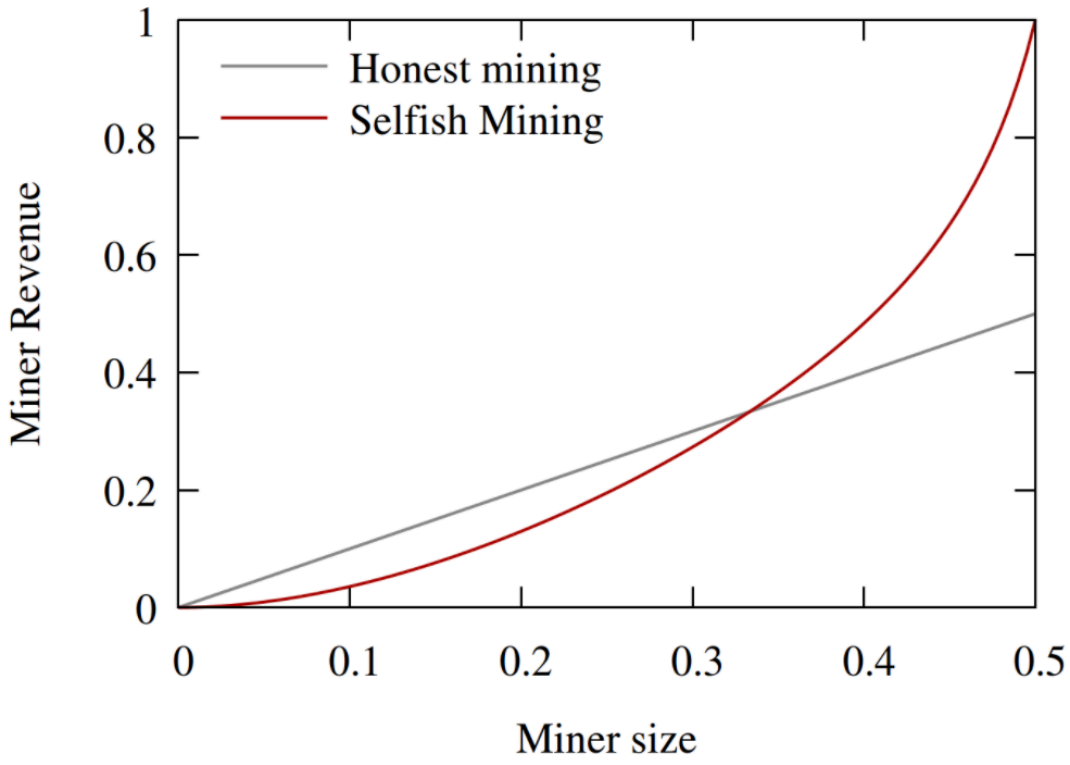


- Risks
  - 不发布的块有可能会浪费掉，所以还不如赶紧发布出去获取当前的出块奖励（落袋为安）
  - The selfish miner may lose twice/multiple times



Selfish Mining —— 自私挖矿

- Revenue
  - A selfish miner larger than 1/3 of the mining power would increase her revenue by deviating from the prescribed protocol and performing Selfish Mining.



思考：挖矿的安全性分析

- 比特币的安全保障是什么？
  - 合谋发动51%-forking 攻击必须要占据系统中超过半数以上的计算力才可能成功 —— 几乎不可能
  - 当一个新区块来了，所有miner 都需要停止当前的挖矿，把新 block 添加后，继续挖；这样可行吗？
    - 不可行，因为 PoW mining 是一个无记忆性的过程，
    - 从任何时候开始挖，成功率都是一样的。
    - 这样就可以防止进行“预挖矿”

Outline & Keywords of this Class

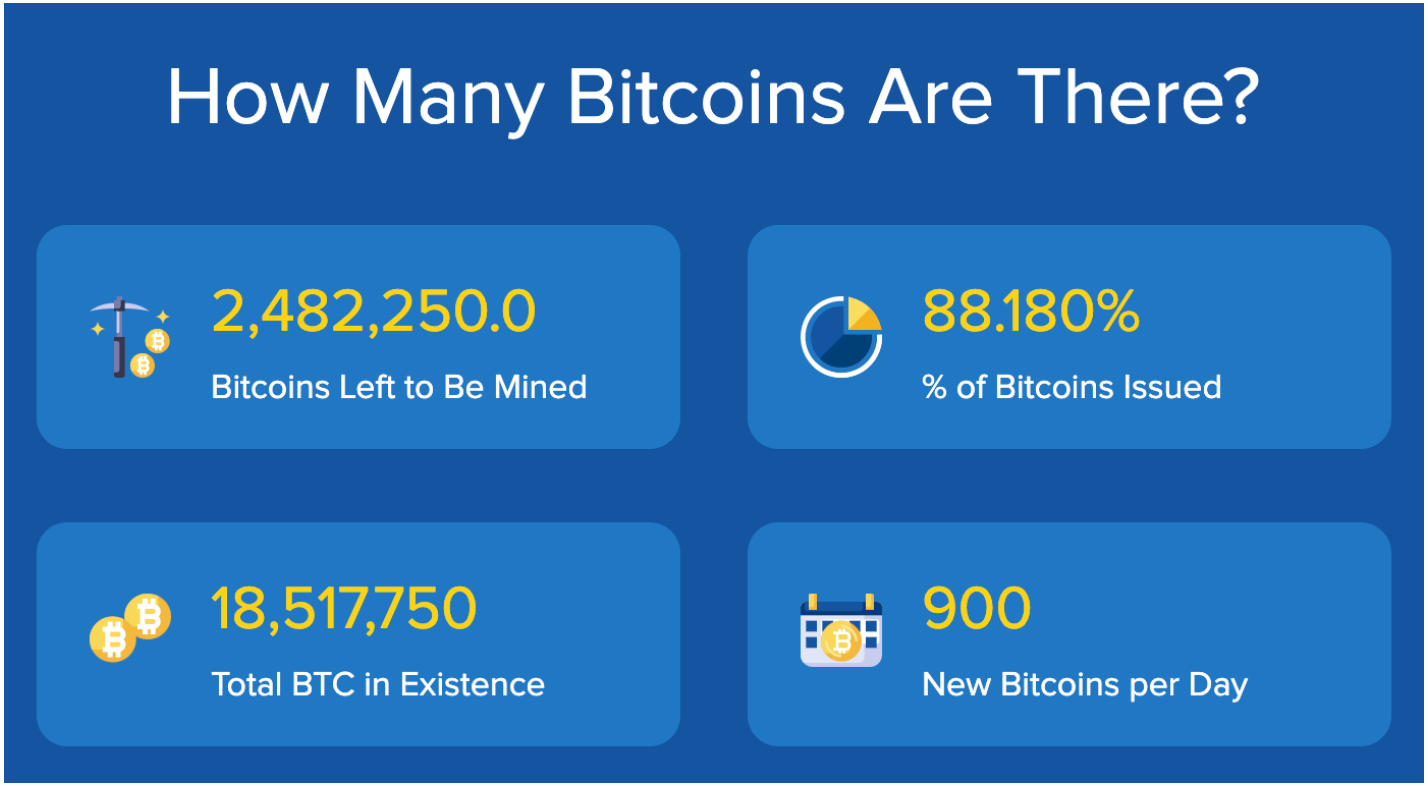
- Part 1:比特币安全机制的保障
- Part 2:挖矿的激励与策略
- Part 3: 社区

首先、几个关于比特币社区的问题：

- 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？

其次，一些事实

- How Many Bitcoins Are There?
  - https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there/



挖矿的激励

- 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.

- 矿工的激励：
  - 出块奖励 block reward (currently 6.25 BTC),
  - 交易手续费：all fees sent with the transactions that were included in the block.

Explaining Bitcoin Transaction Fees

- For this reason, miners have a financial incentive to prioritize the validation of **transactions** that include a higher fee.

- For someone looking to send funds and get a quick confirmation, the appropriate fee to include can vary greatly, depending on a number of factors.

- While the fee **does not** depend on the **amount you're sending**, it does depend on
  - network conditions at the time,
  - and the data size of your transaction.

Explaining Bitcoin Transaction Fees

- **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

- 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 decide the TX fees?
    - Usually, there is **no** simple way to calculate a transaction size by hand.
    - Your BTC Wallet will automatically do this for you, and suggest an appropriate fee.

Explaining Bitcoin Transaction Fees

- 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. 需要包括哪些交易？
  - 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。

- 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。

挖矿的策略

- 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。

- 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

- 空块: empty blocks
  - only header
  - empty TXs included in the block body

  - What is the motivation behind empty blocks?

为了挖到新块采取的策略——Fork Attack

- 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

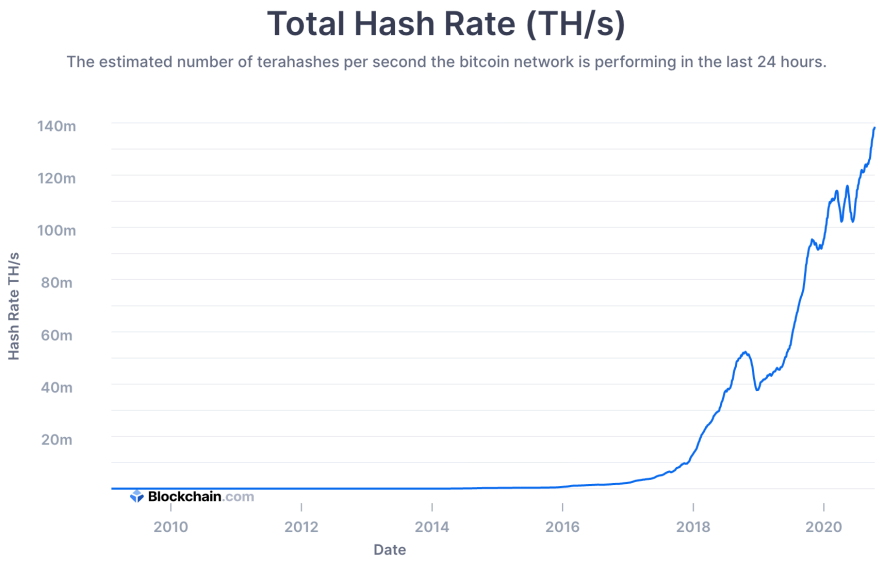
Outline & Keywords of this Class

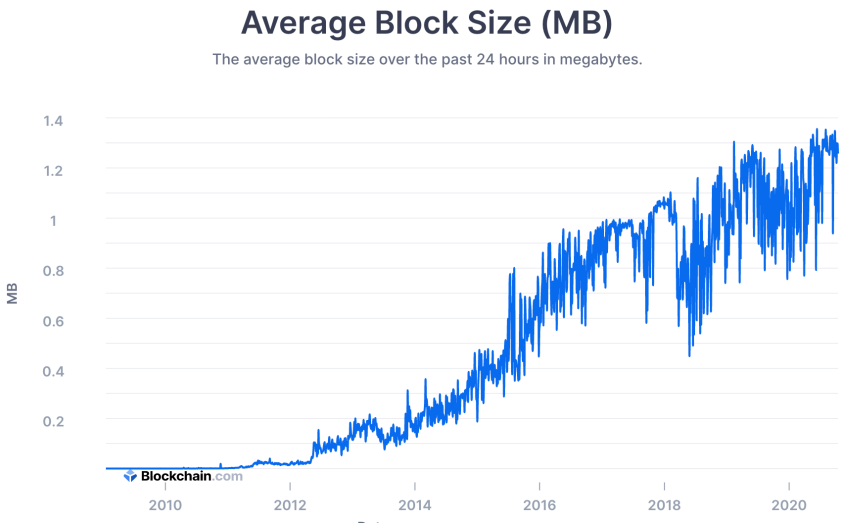
- Part 1:比特币安全机制的保障
- Part 2:挖矿的激励与策略

- Part 3: 社区

启动加密货币

- Bootstrapping 阶段：冷启动



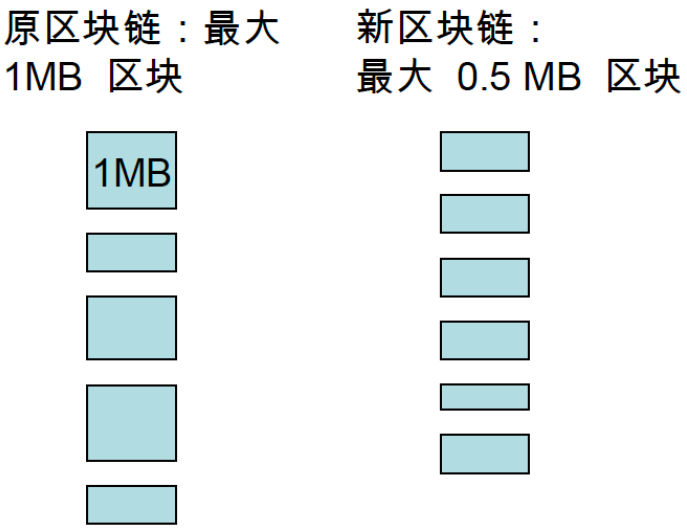


如何维护一个健康的挖矿生态

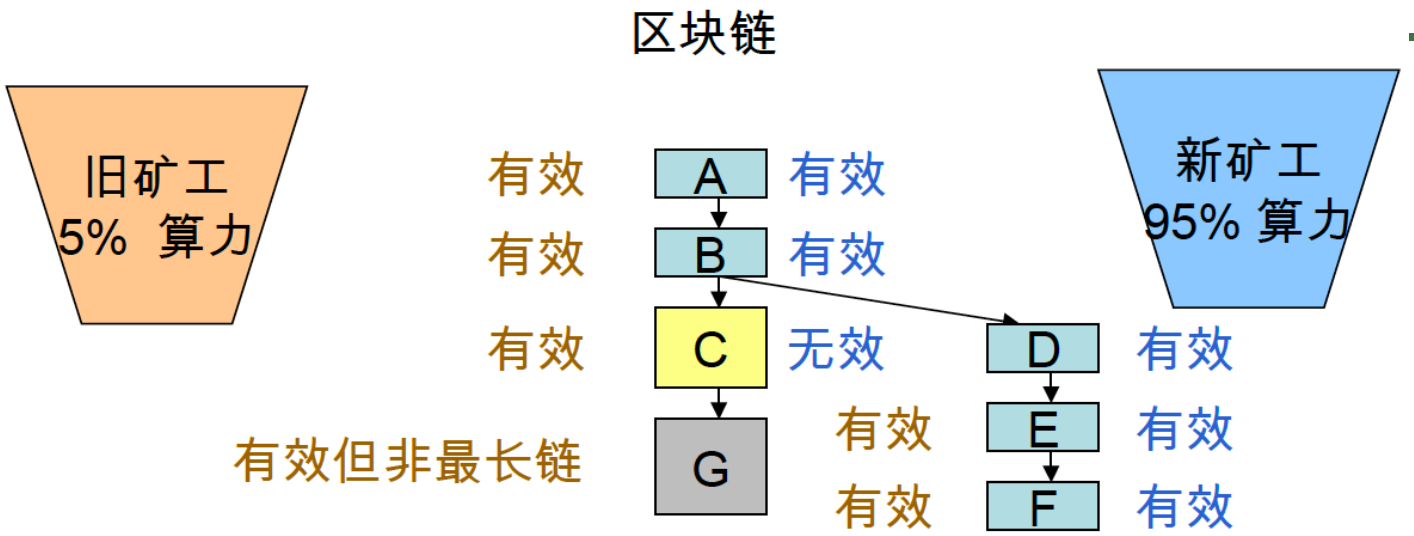
- 什么时候可以保证 miners 会投入大量算力？
  - 得到的奖励是 BTC, 花费的是 $
- 如何保障币的价值持续高稳？
  - 用户普遍相信区块链的安全性
- 安全性、生态健康程度、与BTC Price
  - 相互依赖、相互作用
  - 刚开始只有中本聪，后来知道的人、感兴趣的人越来越多
  - 挖矿的人越多，人们就会对区块链的安全越有信心
  - 每种其他的虚拟货币都要通过 bootstrapping 的考验

社区的发展——规则更新

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



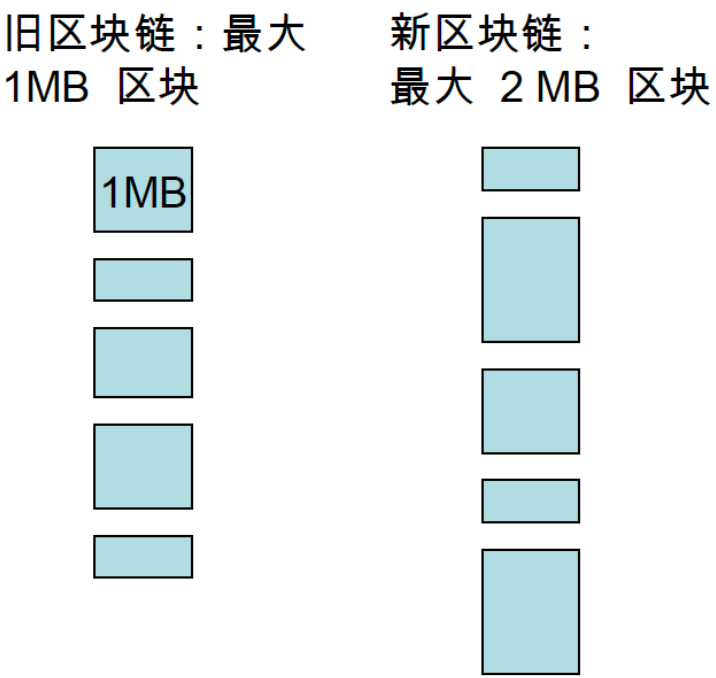
社区的发展——规则更新



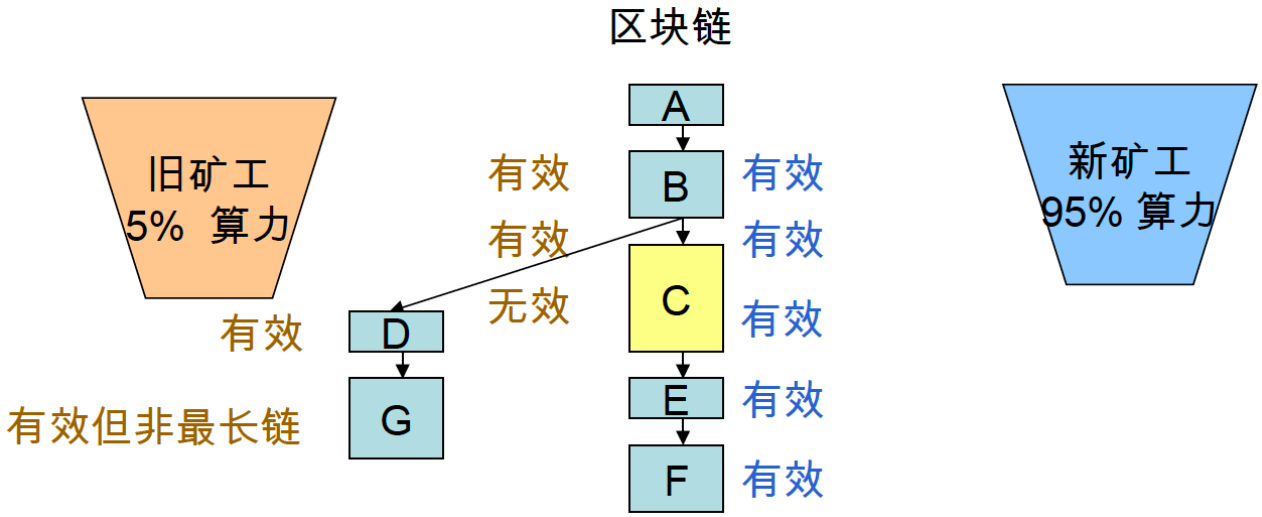
- 软分叉过程
  - 区块 C 大于0.5MB，因此被新矿工拒绝，新矿工另外挖D。但旧矿工仍认为其有效并在其上添加区块。
  - 由于新矿工掌握了绝对优势算力，可以在自己的链上迅速添加区块D,E,F，使其成为最长链。这时旧矿工就会放弃自己挖出的G和C二者，而转到DEF链上去挖矿
  - 结果：两侧矿工都会最终到ABDEF上挖矿，区块链不会分裂。
  - 最重要的是，旧矿工挖出来的大于0.5MB的块都会被孤立掉，所以他们有很强的动机去升级到新版本以避免损失，不久就会达到矿工100%升级的状态

社区的发展——规则更新

- 硬分叉
  - 例如：对现有规则的放宽 (1MB 变为 2MB)
  - 导致：
    - 未升级节点拒绝大于1MB的新区块已升级节点接受所有旧的区块，因为它们都小于2MB



社区的发展——规则更新



- 硬分叉过程
  - 区块 C 大于1MB，所以被旧矿工拒绝而去挖区块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 & Keywords of this Class

- Part 1:比特币安全机制的保障
- Part 2:挖矿的激励与策略
- Part 3: 社区

- (Optional) Part 4:共识的其他认识

再谈比特币共识

- 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，那么旧不存在一个协议，此协议能保证有限时间内使所有进程达成一致

再谈比特币共识

- 可是，FLP不可能结论是分是不是数据库的结论，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

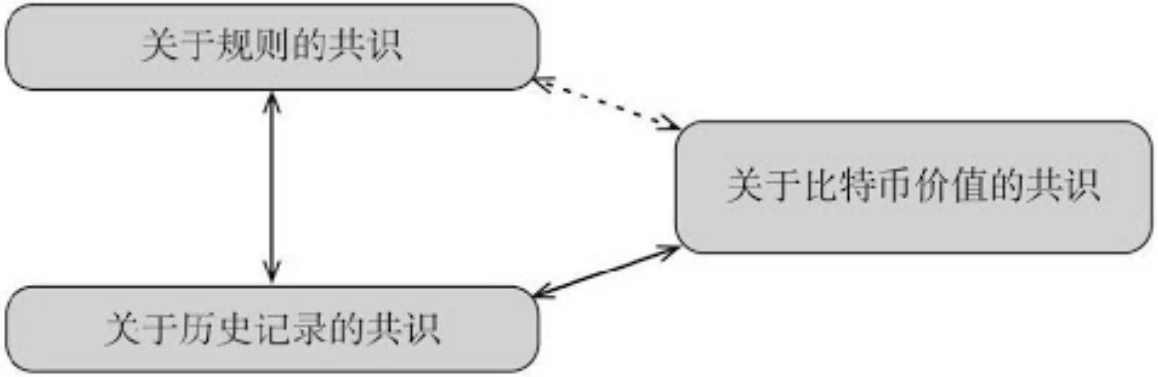
再谈比特币共识

- 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

- 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

- 意义：to ensure
  - Bitcoin participants can communicate with each other for achieving the consensus

比特币共识--三个层面

- 历史记录的共识
  - 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

比特币共识--三个层面

- 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

- 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.