



比特币定位和区块链原理

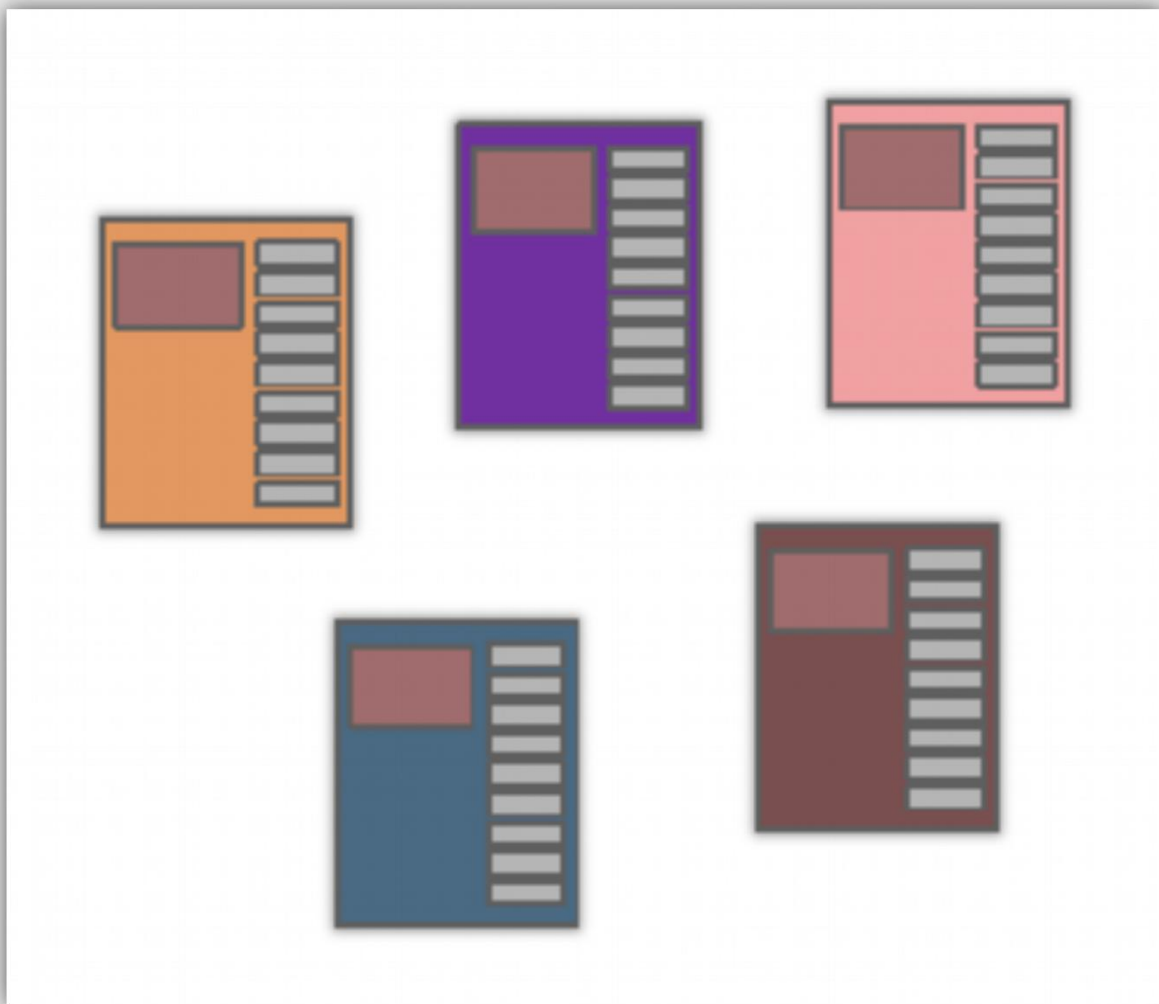
—— 区块链中组块

讲师：康烁

1. 掌握组块的过程
2. 了解组块中的问题以及挖矿的作用



这个块由谁来组成?



1. 所有人都可以组成下一个块
2. 凭什么你能组，我不能组？

1. 每个人都不知道全局的状态
2. 全局状态时时刻刻都在改变
3. 只能依据自己收到的未确认的交易来构造自己的块
4. 组成的块各不相同

关键问题！

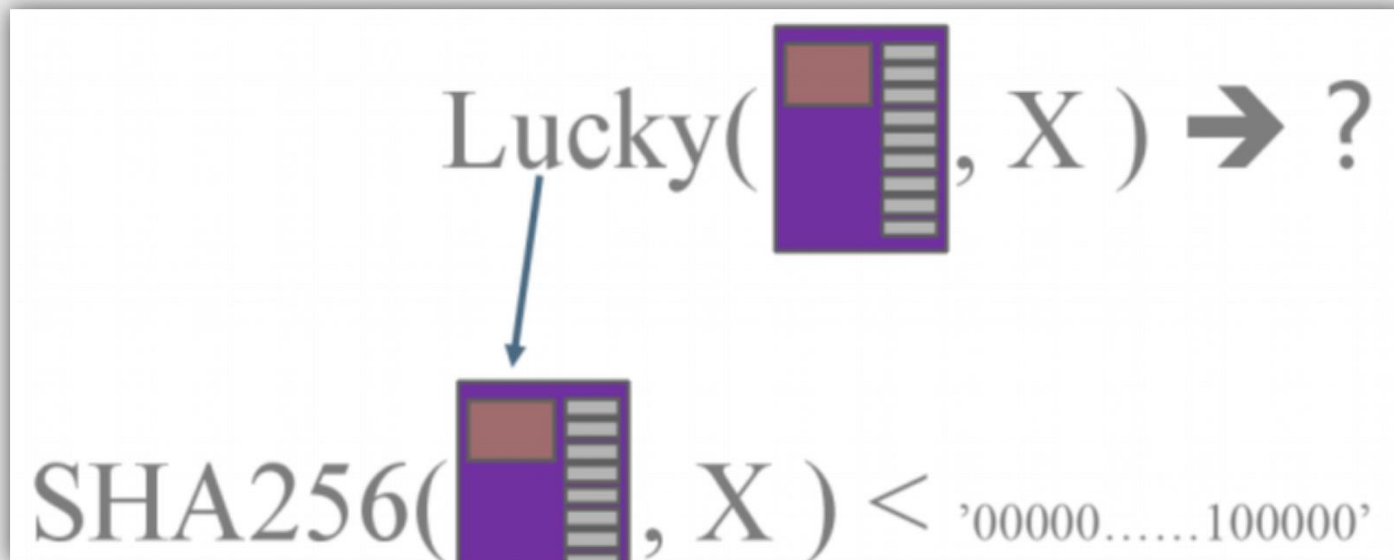


几个选择

- 1.某一个人说了算
- 2.大家投票决定
- 3.抽奖（抓阄）
- 4.弄一个评奖委员会

依据每个人的块的信息大家一起来抽奖

1. 有一个摇奖函数
Lucky
2. 函数的输入是你的块
+ 一个手工填写的号码 X
3. 摇奖函数决定谁中奖



The diagram illustrates the logic of the 'Lucky' function. It shows the function $\text{Lucky}(\text{block}, X) \rightarrow ?$ where the 'block' is represented by a purple icon with a red square and horizontal lines. A blue arrow points from this icon to a similar icon used in the SHA256 formula below. The formula is $\text{SHA256}(\text{block}, X) < '00000.....100000'$, indicating that the function's output is a SHA256 hash that must be less than a specific value to be considered a win.

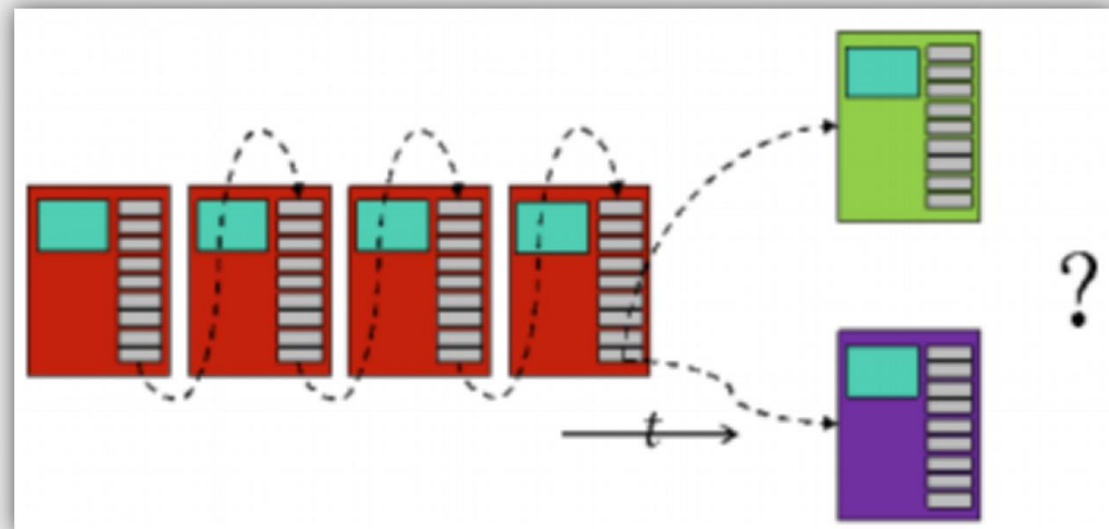
$$\text{Lucky}(\text{block}, X) \rightarrow ?$$
$$\text{SHA256}(\text{block}, X) < '00000.....100000'$$

1. 万一如果所有的人都没有抽中，我系统还工不工作了呀
2. 所以，每个人都有很多次机会去抽奖
3. 因为抽完奖之后，块就放进去了（交易被确认了）必须要有人抽中
4. 没有抽中，继续瞎猜（就是手工换一个X放到抽奖函数里面去）
5. 保证大概10分钟完成一次抽奖，有人抽中的

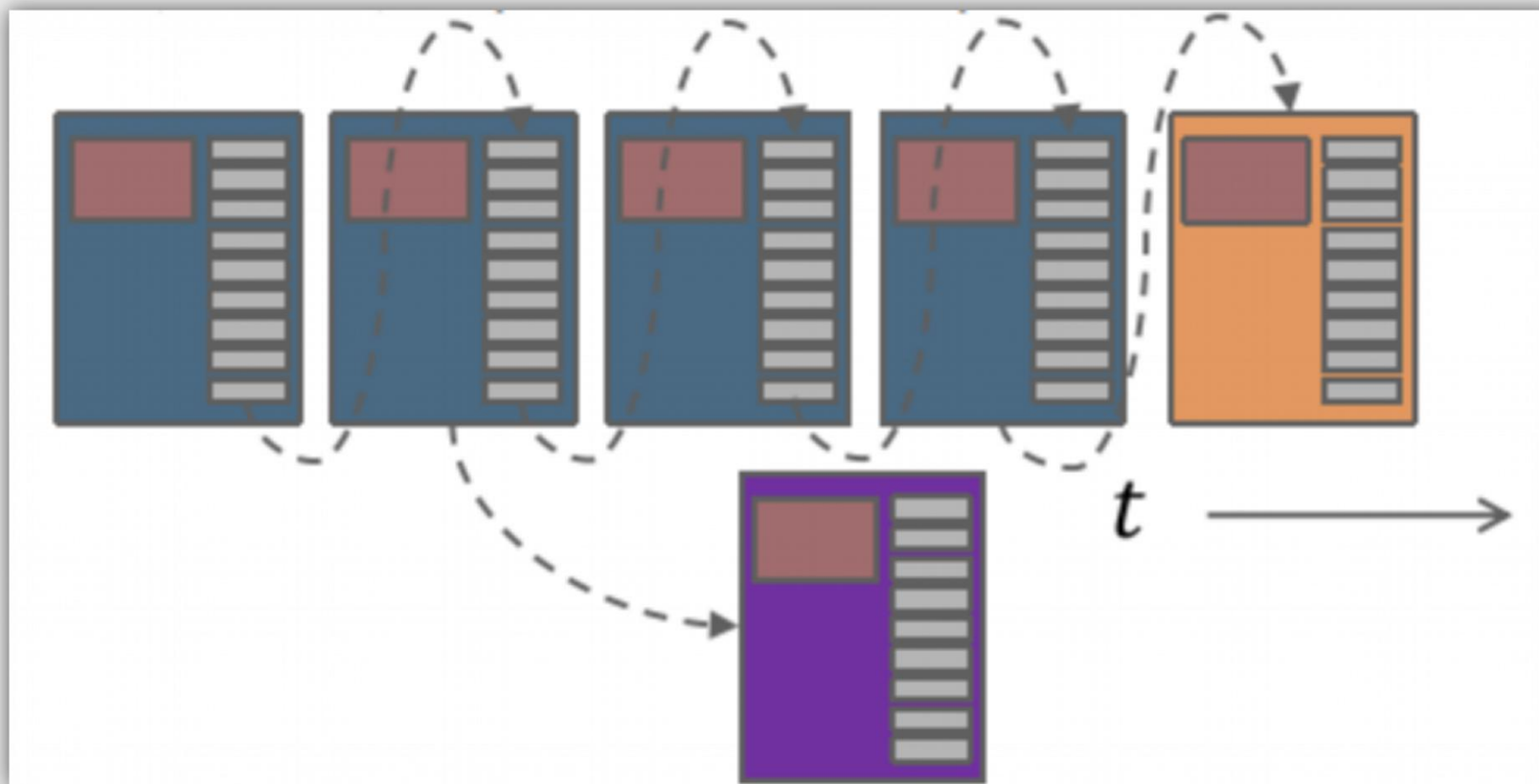
1. 赶紧广播，网络中很多的人都知道有人抽中奖了
2. 在这个时候，抽中奖的人广播，因为抽中了真的有奖，抽中一个奖励12.5个比特币→ 货币发行
3. （因为给你比特币奖励了，所以这个过程又被称为是挖矿）
4. 一次完成：下一个块的确认，货币的发行（奖励确认的工作）

1. 把对应的块放到自己确认列表中
2. 赶紧开始进行下一个抽奖==>所有的人都会在最长的链上进行抽奖的工作
3. 因为协议这样规定，你再在原来的位置上抽奖，别人也不认啊

1. 奖券都是计算出来的，有很小的概率同时抽中
2. 变成两个链了
3. 两个人都广播，每个收到的人都工作在第一个收到的链上（更长）
4. 随时间推移，两个更长的链的概率就更小
5. 迅速回到一个链



放弃，放弃，放弃，（还好概率很小）



1. 破坏部分参与者：没用啊，因为大部分人良好的情况下，可以继续工作
2. 破了全部人：投入太大，没有必要
3. 那怎么办：我也参加抽奖，获得利益（变成好人了）

1. 太多人参加抽奖→中奖速度很快
2. 10分钟获得抽奖结果，不能太快，不能太慢。
3. 人越多，瞎猜的数越多，如果抽奖函数固定的话，时间会越来越短
4. 并且，抽中的人的概率越大，人数越多
5. 不好办-->会分很多叉，系统不稳定
6. 那怎么办：调整抽奖函数，使得抽中的概率降低，人多了也不怕

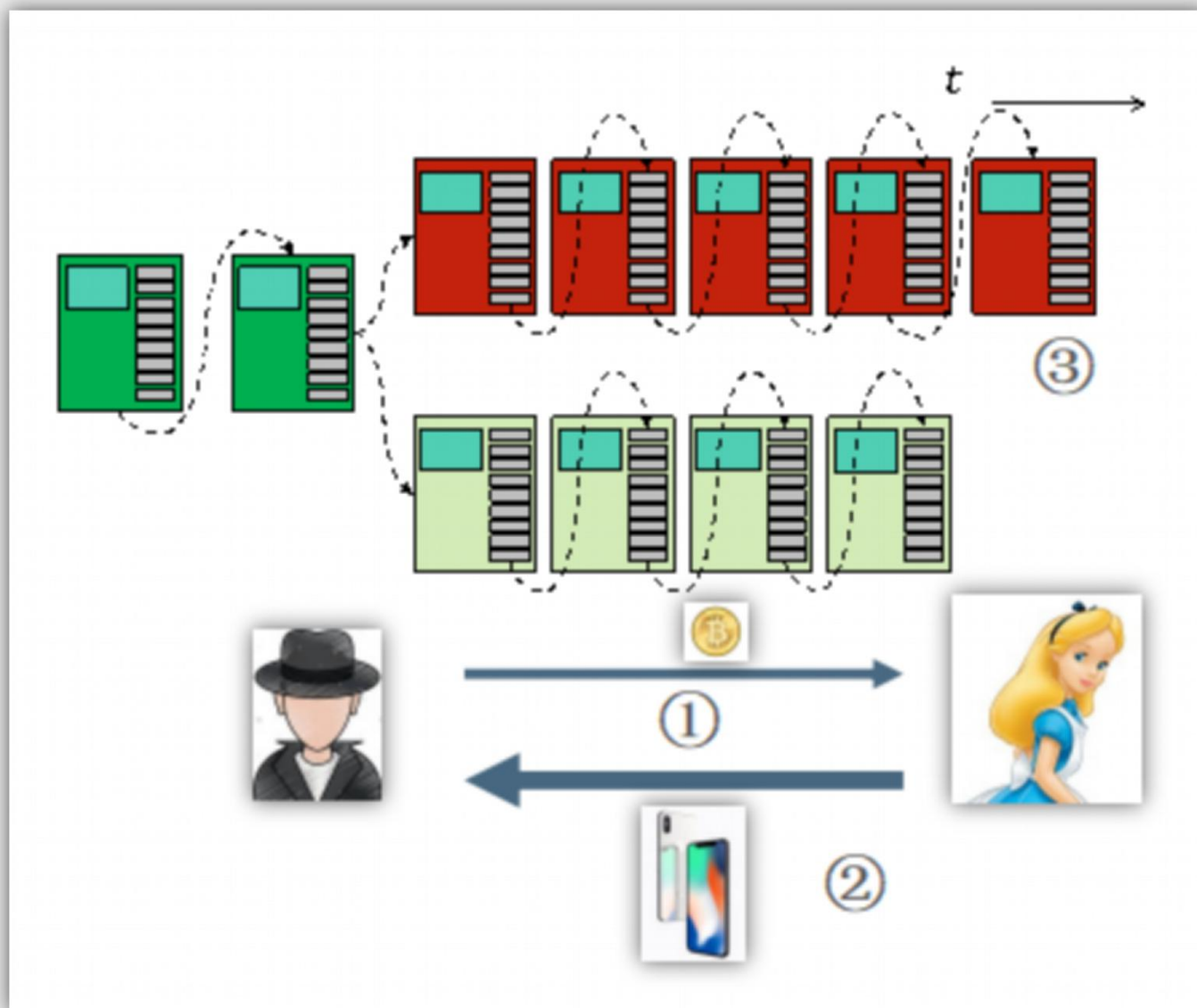
1. 你抽中的概率低怎么办？ 你又想获得比特币
2. 用一台更加强大的机器提高瞎猜的数的个数（提高计算能力），获得更多抽奖的机会
3. ==> 计算机 ==> GPU ==> 矿机（挖矿嘛）
4. 每个人猜中的概率很低，大家一起猜，有福同享==>矿池（挖矿嘛）

我们解决的问题:

- 1.货币发行问题
- 2.货币支付问题
- 3.货币双花问题
- 4.但是, 速度很慢 1MB大小的块, 一秒钟7笔交易最多
- 5.并且, 如果有强大的坏人, 事情也不好办

1. 就是那些能够抽奖抽很多次机会的人（比如一个自建的矿池）
2. 能干啥
3. 我抽中了，但是我不广播

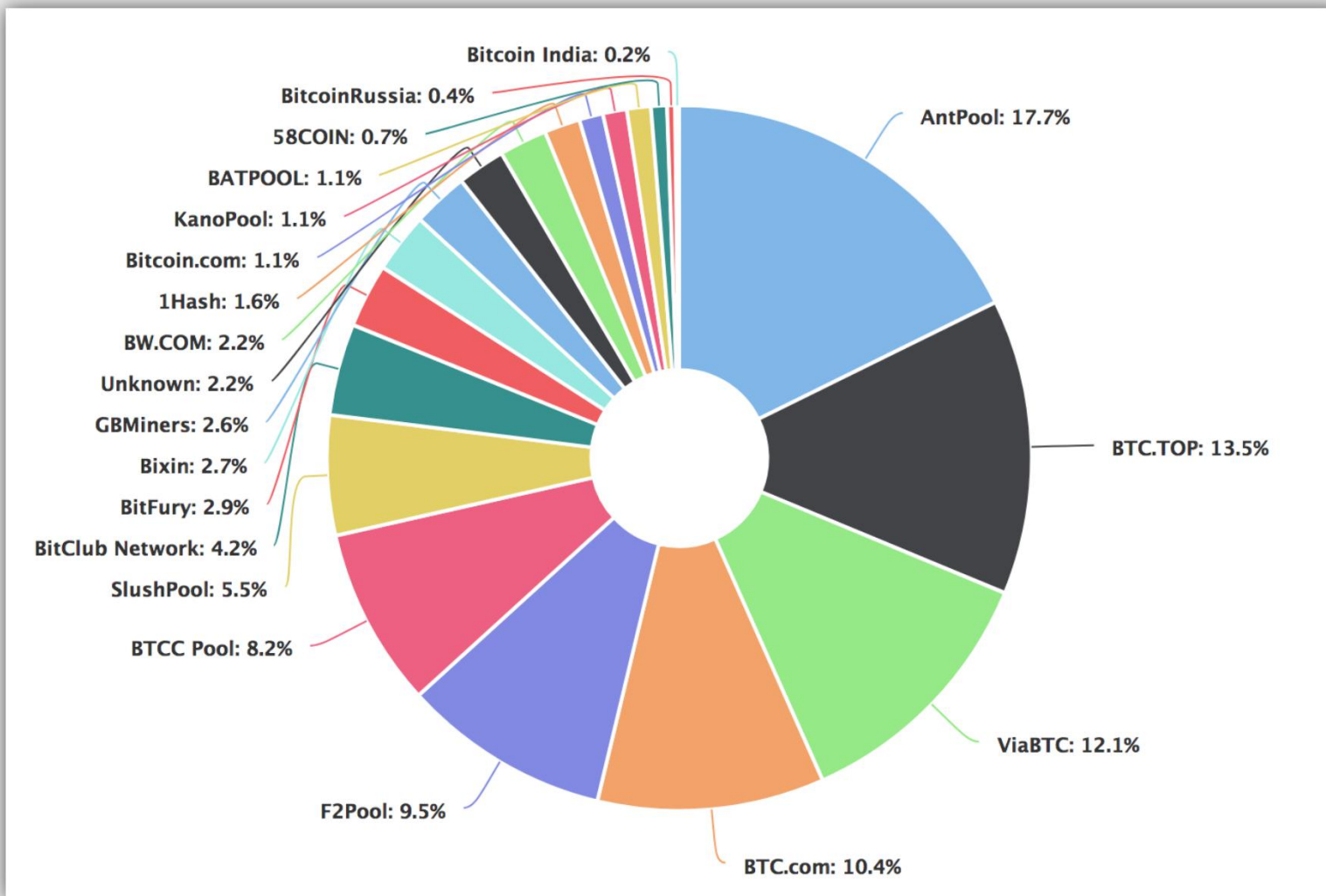
1. 没关系，我可以用作抢钱！！！！
2. 没事，我们可以把别人的块给替换掉，抢钱去



强大的坏人

Rest of the World

1. 小额的交易，没事，放到区块链上就算确认
2. 大额的交易，啊哦，等六个块吧，不太可能被翻过来了，概率非常小
3. 祈祷矿池不要太大（做一个有社会（比特币）责任感的矿池，主动降低计算能力）



1. 2009年50个比特币
2. 2013年25个比特币
3. 2017年12.5个比特币
4. 一共2100万个比特币

December 8, 2017, the Bitcoin supply is 16,669,275 BTC.

5. 货币供应有一个上限的量，这是最多的比特币的个数

1. 还有100年呢，不着急
2. 还有交易费呢，有交易费的交易更容易被确认

(A → B, 100元, 交易费1元) A签名

1. 能，肯定能，并且是彻底的丢了，永远找不回来了
2. 不仅丢了你自己找不回来了，任何人都找不回来了
3. 怎么丢：你丢了你的私钥，你的钱花不出去-->钱丢了
4. 所以，是一个通货紧缩的系统

1. 虽然比特币系统的出发点是最多只有2100万个比特币，看起来是有限的货币
2. 在币值突破 6000 美元 10 天之后，比特币正无限接近 7000 美元（已经超过啦），目前币值为 6960 美元。在这之前，芝加哥商品交易所集团宣布计划推出比特币期货。而在比特币不断刷新新纪录的同时，它正面临新的分裂。在 8 月的 Bitcoin Cash 之后，矿工们准备分裂出 Bitcoin Gold，这次分裂将在 11 月上旬启动。而 11 月中旬比特币还将再次发生分裂。
3. 8月份的分裂：这一计划是由少数比特币持有者发起的，其中主要是中国矿工——他们为比特币网络贡献计算能力获得比特币，这些比特币持有者对比特币技术改进方案不满。

1. 抽奖：通过哈希函数SHA256进行，哈希函数小于某一个阈值，阈值动态调整
2. 形成区块链：通过包含上一个块的哈希到当前块来构成链
3. 交易的签名和验证：非对称的密码学
4. 交易的依赖性：包含当前交易所依赖的交易的哈希值，构成交易的来源情况的验证

1. 选择谁来组块是通过抽奖（挖矿）
2. 比特币的发行是靠挖矿

1. 理解双花和解决方案
2. 理解数字货币发行和挖矿

- 必做内容：
- 理解数字货币发行和挖矿

EDU

CSDN学院 IT实战派

