比特币基础

-- 比特币协议和共识

概述

- 比特币概念
- 建立共识
- 挖掘概述
- 加密货币开采

基本概念-什么是比特币？

- **加密货币: "一种数字货币, 其中使用加密技术来调节货币单位的生成, 并核实资金的转移, 运作独立一个中央银行。**
  - 建立在计算机科学、密码学和经济学相结合的基础上
- **比特币是一种加密货币**
  - "比特币" 可以指:
    - 比特币 (大写)-协议、软件和社区
    - 比特币 (通常小写)-单位
- **社区术语**
  - **"加密"**-加密货币, 以太
  - **"私人区块链"**-私人区块链、许可分类账、大型金融机构
  - **"区块链"**-伞式术语

区块链技术的影响

- **Altcoins 2 (dash, dogecoin, Dogecoin)**
- **比特币 2.0/earum-应用区块链金融以外**
- **汇款----规避传统的银行基础设施**
  - 以5美分的价格在世界任何地方汇款
- **成为您自己的银行-100% 正常运行时间**
- **当前热门话题: 治理与 "区块链"**
  - 块大小辩论
  - 对所涉经费问题感兴趣的银行
- **私人区块链-降低成本 + 传统银行基础设施的结算时间**

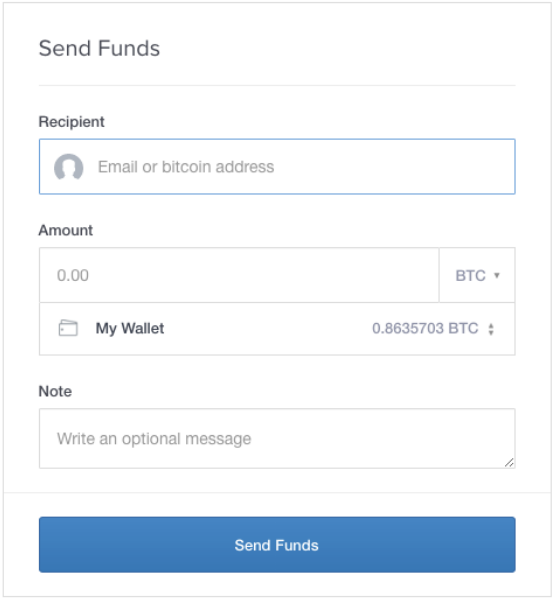
基本概念-比特币中的标识

- 在假名之间汇款
  - 假名 = = 地址 = = 公钥
- 加密原语
  - 数字签名方案 (ecdsa: 椭圆曲线数字签名算法)
    - 公用密钥/私钥对;喜欢电子邮件地址 + 密码
  - 单向哈希函数 (sha-256)
- 比特币隐藏在大量的公钥中
  - 用户可以任意生成多个密钥对
  - 示例地址: 1ftquew9x78hdchngcbw9tbe2myp87elt
  - 2 ^ 160 可能的地址(1461561516633302929292929183636848828282828282928659932542976 地址)
  - 地球上的沙子颗粒: 2 ^ 63
  - 2 ^ 126 实际上只有0.00000058% 的 2 ^ 160

比特币交易-基本版本

- **比特币作为软件存在**
  - 交易是通过钱包软件进行的
  - 钱包创建生成一个比特币地址
- **要收到钱，您可以分享您的地址**
  - 发件人指定地址和金额
- **交易被广播到网络，"矿工" 在网络中验证并将其添加到交易历史记录中**

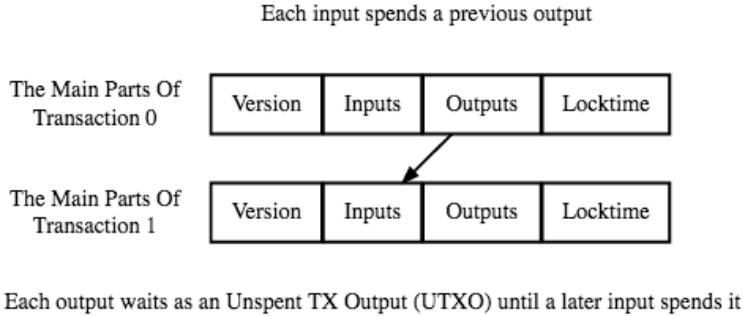
1LNnJDNTUXYUfmbiVcngKGg52N8TKNPw6J



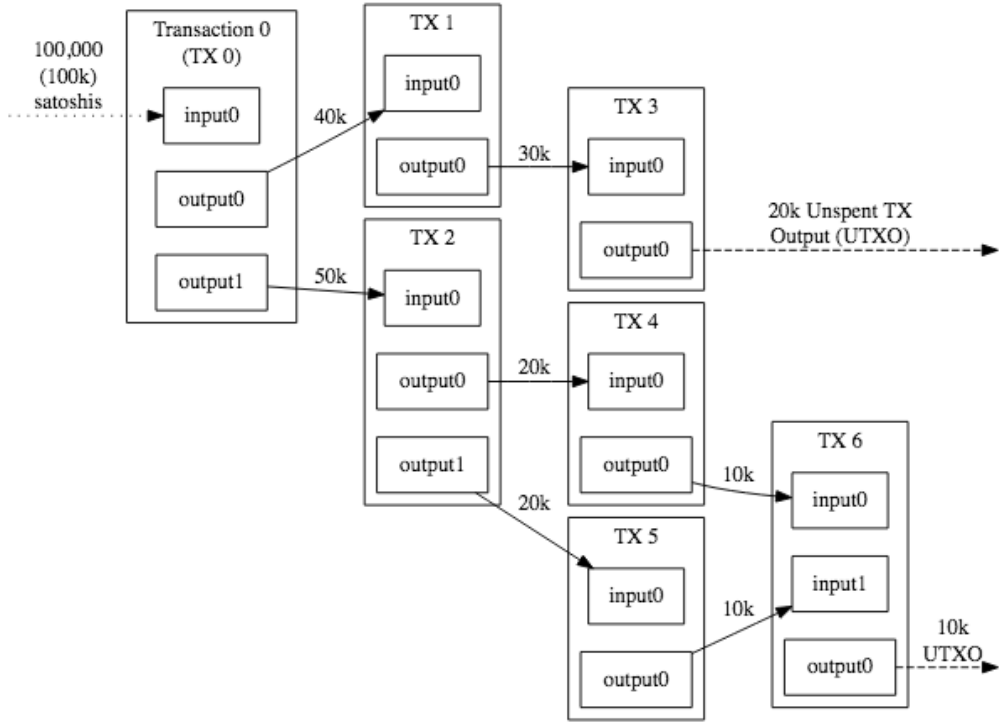
基于库的接口

基本概念-事务

- **将输入地址映射到输出地址**
  - 输出只能使用一次
- **典型 tx: 一个输入, 两个输出**
- **费用是隐式的**



Each output waits as an Unspent TX Output (UTXO) until a later input spends it



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

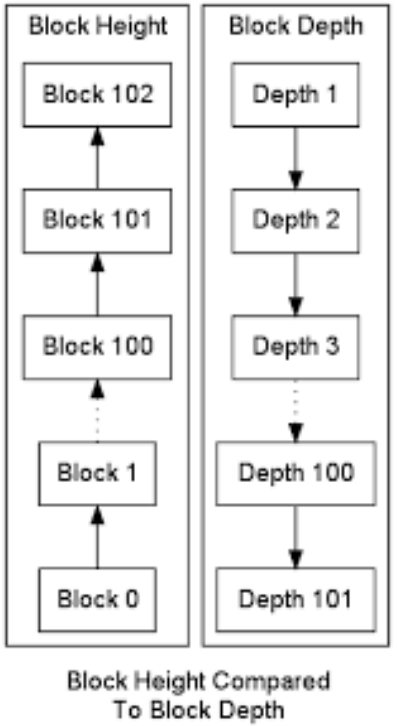
基本概念-块 + 区块链

块

- **包含一组已排序的事务**
  - 时间戳的事务, 是不可变的
- **每个块引用前一个块**
- **每个方块都有高度和深度 (确认)**
  - 目前428k 块

区块链

- **整个系列的块 "链接" 在一起**



Block Height Compared To Block Depth

源：比特币开发者指南

Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac10551802075f053208fe995204a145197e2904bb9

3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v (44,000 BTC - Output)	3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
	3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
	3Qd7hXZoZ1iyXZznrbdUwUQBxHMmujdqhJ - (Spent)	333.33328889 BTC
	3ECJwvx9VgfotcUuEJMVNvmWnTGVMk179L - (Spent)	333.33328889 BTC
	3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
	3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
	3GEaT8ZRXELcjMSFvGro6eZcC5S1LSLZuN - (Spent)	333.33328889 BTC
	35DVAzDtZDKAU94kFT9sxoscnuLCTxgwYc - (Spent)	333.33328889 BTC
	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v - (Unspent)	38,000 BTC
	35mwqShnStDro6uEB4bmsgbyBo8en6Byfm - (Spent)	333.33328889 BTC
	39pvSqfNcUosc8RGVWxyzKM3ny96a3uSkW - (Spent)	333.33328889 BTC
	39QNJSgQg5JnBXAtbF8ezkDn72VqWdPZPJ - (Spent)	333.33328889 BTC
	3L9qAGBQLbXkFAB2GpijnJXPScSVjuiJio - (Spent)	333.33328889 BTC
	37WSkANPVUQ8uuktf8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
	3EEwPZZ6pYRJSotCz9RBoVYPRnoWyGWEka - (Spent)	333.33328889 BTC
	3C4ABC7iPcAAKBh6SJXfvUSDBew3abCtw3 - (Spent)	333.33328889 BTC
	3HpQozfTzoXAsHf87m2mwJXUQ14LVtLgK4 - (Spent)	333.33328889 BTC
	337RfngTLRTpU7RT9sKWQWDdmfcdmWnugi - (Spent)	333.33328889 BTC
	3P2eoKr3vAeZhJcTzon3VFkv5r7DqSXW9G - (Spent)	333.33328889 BTC
		43,999.9992 BTC

Summary	
Size	1055 (bytes)
Received Time	2016-08-30 11:45:03
Included In Blocks	427512 (2016-08-30 11:51:09 + 6 minutes)
Confirmations	854 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	44,000 BTC
Total Output	43,999.9992 BTC
Fees	0.0008 BTC
Estimated BTC Transacted	333.33328887 BTC
Scripts	Hide scripts & coinbase

基本概念-utxo 类比

utxo 代表 "未使用的交易输出"

- 全球一组未使用的比特币
- "我在花这个比特币", 而不是 "我在花一个比特币"。

与雅浦群岛的拉伊石类似

- 拉伊·斯通从未动过
- 相反: 同意改变所有权

源：维基 百科

回顾--中本佐藤的创新

比特币是中本佐藤于2009年创立的

- **首次分散、不可信任的交易系统**
  - 只需要互联网连接的低成本金融体系
- **中本解决了双倍支出问题**
  - 防止某人两次花费同一资产
  - 解决 方案？区块链 + pow

dorian satoshi nakamoto
(实际上不是中本佐藤)

概述

- 比特币概念
- 建立共识
- 挖掘概述
- 加密货币开采

建立准备:拜占庭发电机问题

围绕一个城市的将军小组必须投票并商定一项行动计划

约束:

- **将军们在身体上是分开的;必须使用信使**
  - 信使可能会失败
- **将军们可能是忠诚的, 也可能是故意叛国的**
- **假设大多数将军都很忠诚**
- **"拜占庭容错" 实现, 如果忠诚的将军们一致同意的战略**

在比特币中, 这是一个关于交易历史的协议

在这个版本中，如果爱丽丝想给鲍勃送一个比特币，她应该写并签署这条信息："我，爱丽丝，给鲍勃一个比特币"

v1

爱丽丝写并签署了一条描述她交易的信息

"我，爱丽丝，给鲍勃一个比特币。

接下来, alice 应该将交易发送给运行比特币软件的每个人。
现在大家都知道鲍勃还有一个比特币, 爱丽丝少了一个。

v1

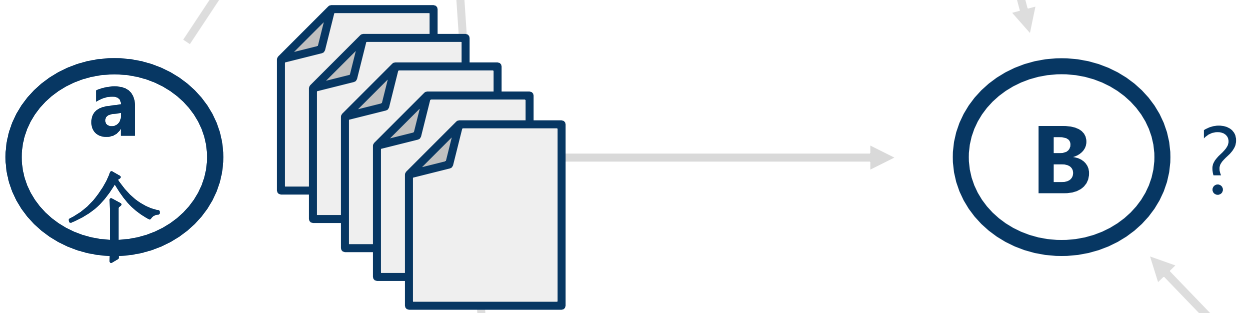
爱丽丝向全世界传递她的信息

第一个版本有一个主要缺陷:
爱丽丝可以继续发送同一笔交易五次。

= 那是什么意思？鲍勃现在有五种不同的比特币或五个相同比特币的副本？

v1

爱丽丝发送五个相同的消息



在版本2中, 我们将通过引入序列号来解决双倍支出的问题, 以使比特币唯一可识别。

现在, 如果爱丽丝想给鲍勃送一个比特币, 她应该给鲍勃发一个信息: "我, 爱丽丝, 我给鲍勃一个比特币, 序列号8732。

这样, 爱丽丝只能花每一个比特币一次。

v2

介绍唯一可识别的序列号

有一个问题:

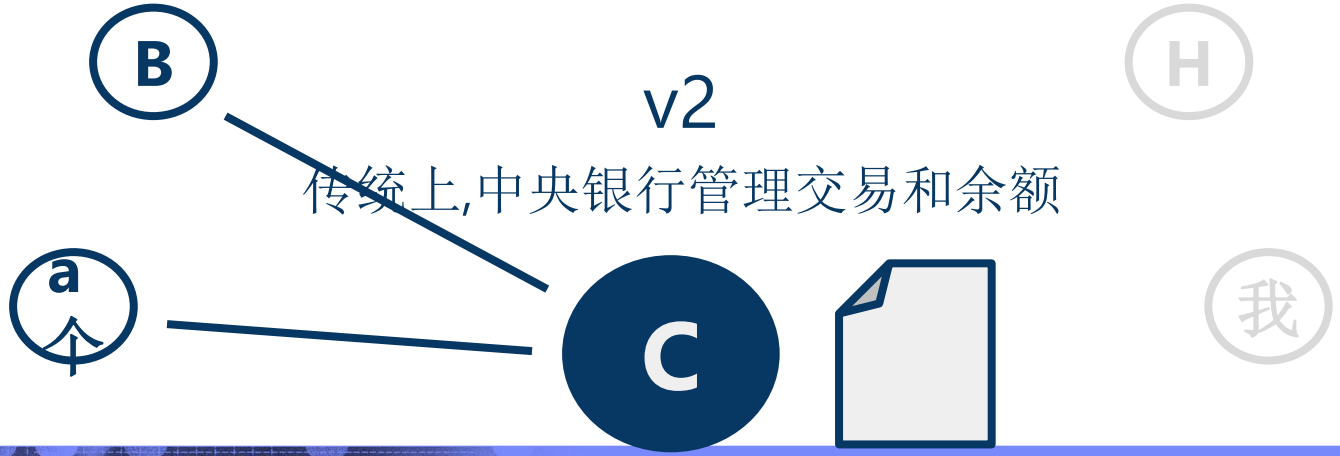
= 这些序列号从何而来?
= 我们如何管理谁拥有哪枚比特币?
= 使用序列号, bob 可以确保 alice 不会两次向他发送相同的比特币, 但他怎么能确定比特币首先属于她呢?

v2

序列号从何而来?

?

要使版本2正常工作，需要有一个受信任的序列号来源。
传统的来源是银行。
该银行将提供比特币的序列号，跟踪谁拥有哪些比特币，并验证交易是否合法。
现在，当爱丽丝将她的交易发送给鲍勃时，他可以向银行核实比特币是否真的属于她，它是独一无二的。



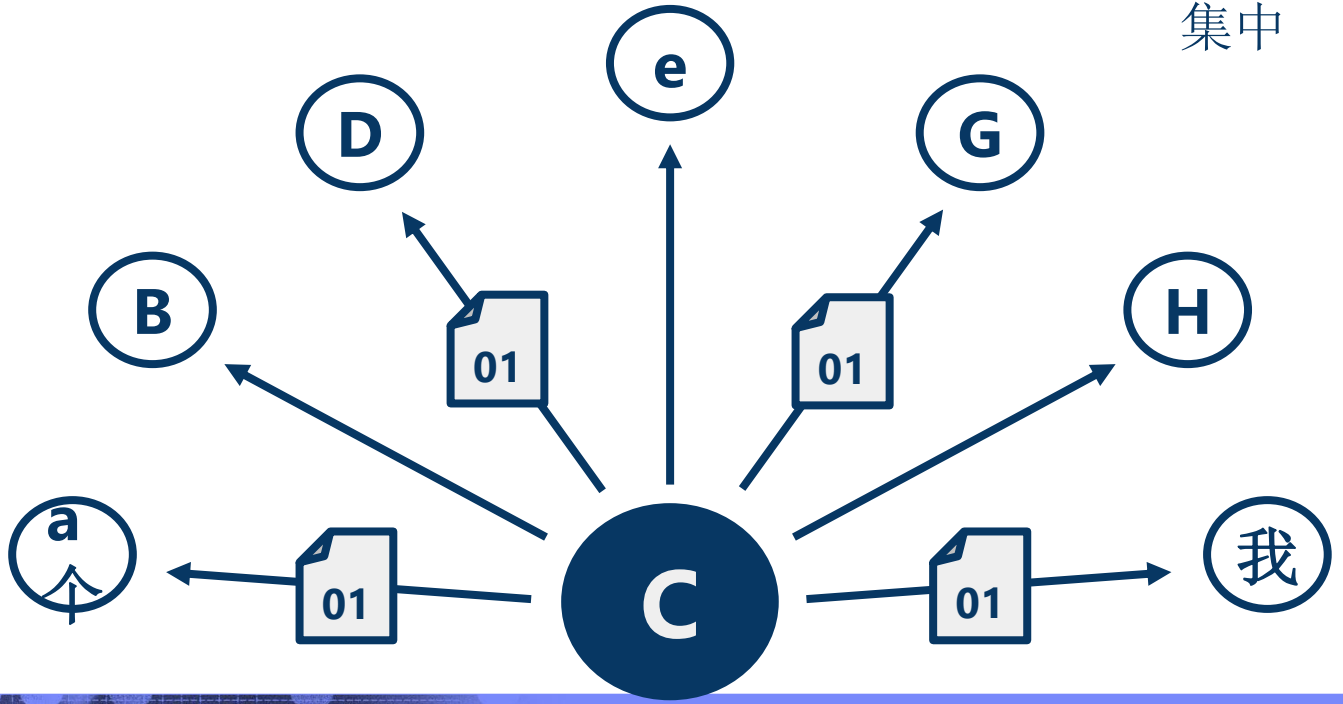
v2

传统上,中央银行管理交易和余额

有一个问题:
版本2确实解决了重复问题, 但它失去了版本1的分散性质, 在该版本中, 交易向没有银行的每个人宣布。

v2

集中



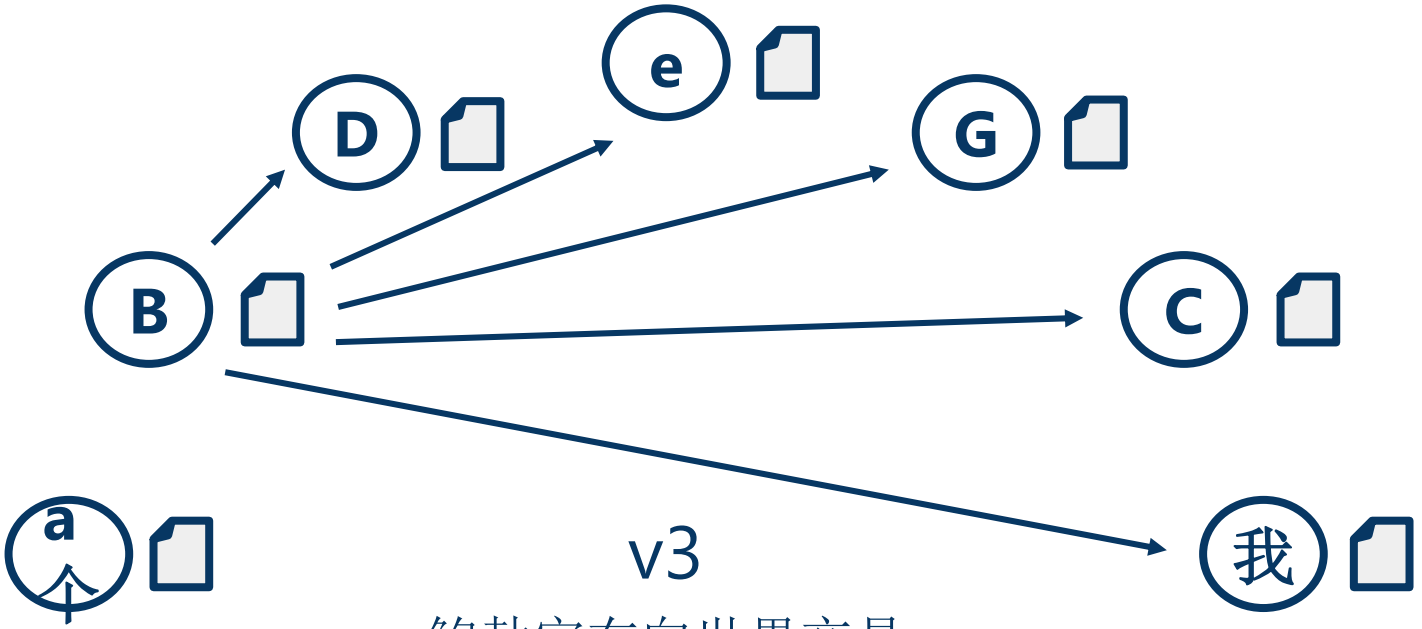
在第3版中，我们将通过让每个人都成为银行来带回这种分散的结构。
现在每个人都有所有交易的完整记录。
在比特币中，这被称为**区块链**.

现在，当爱丽丝把她的交易寄给鲍勃，他可以检查**他的副本**封锁链，以确保比特币实际上属于爱丽丝。

v3

爱丽丝把她的交易寄给鲍勃

如果这样做，鲍勃宣布交易向世界，每个人都更新他们的块链的副本。

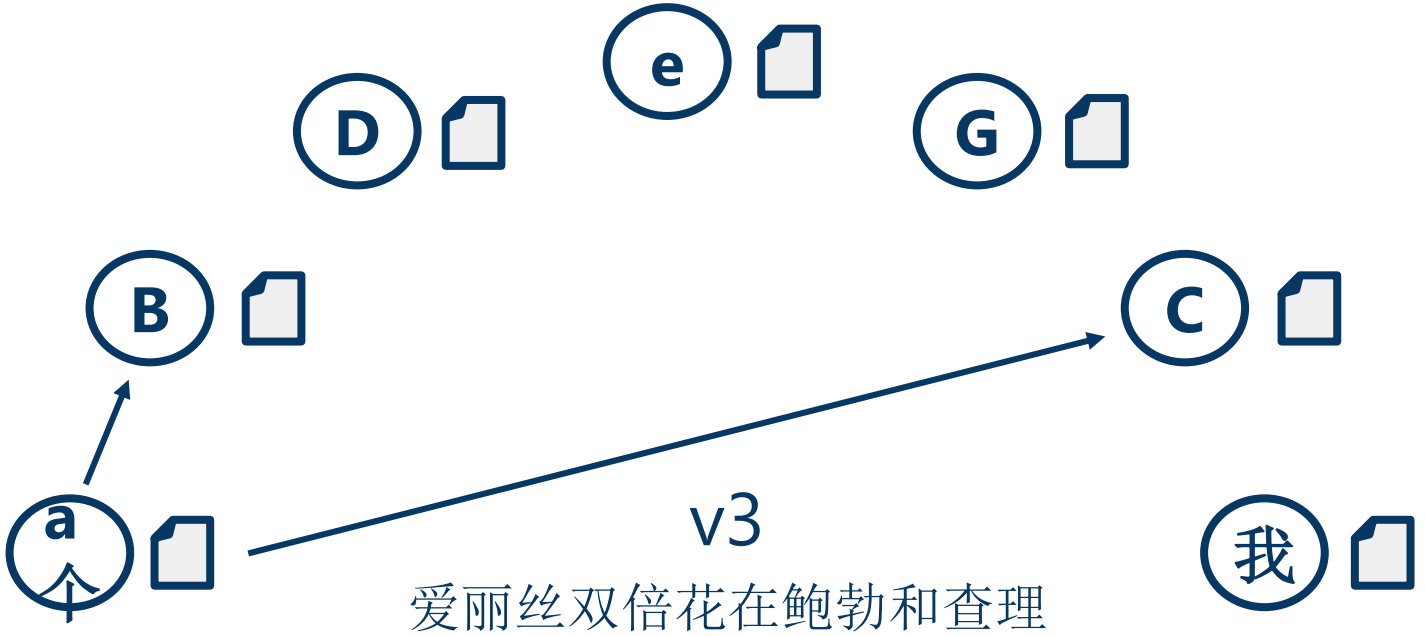


v3

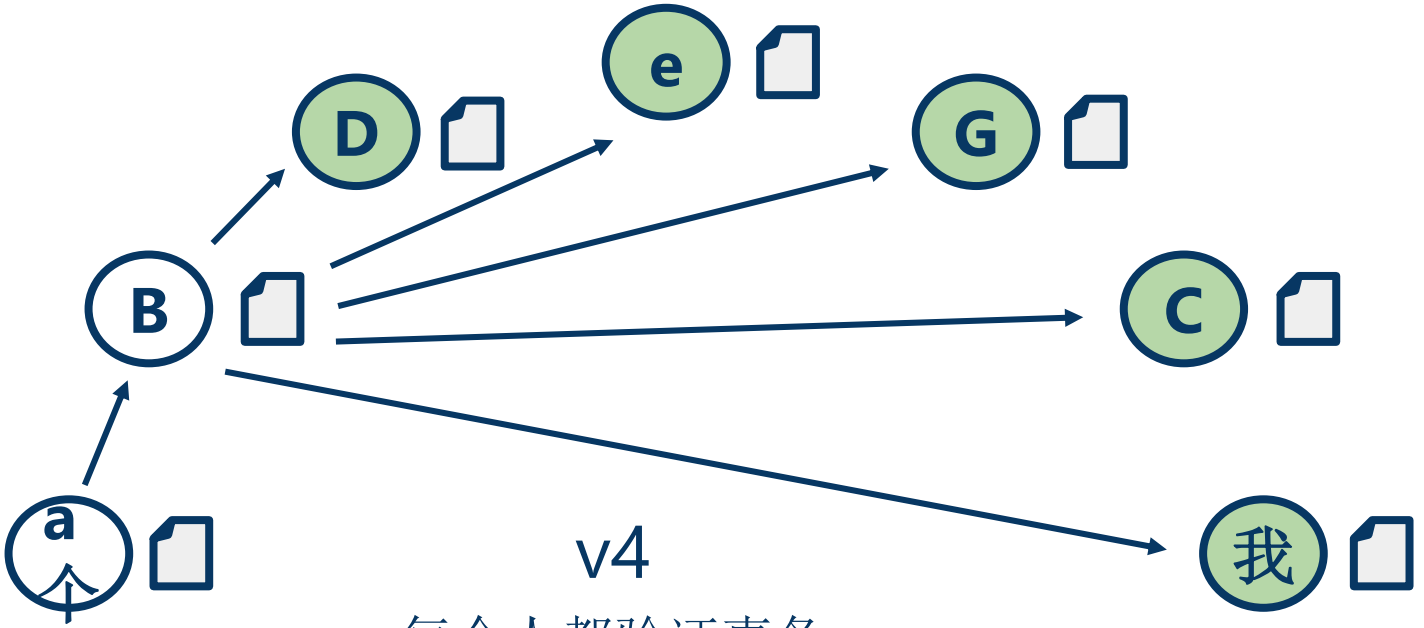
鲍勃宣布向世界交易

有一个问题:

如果爱丽丝同时把她的交易寄给鲍勃和查理呢?
两人都会发现比特币属于爱丽丝, 接受交易, 并向世界宣布。
其他人应该如何更新他们的区块链副本?
显然, 鲍勃和查理不能拥有同样的比特币, 所以我们有问题。



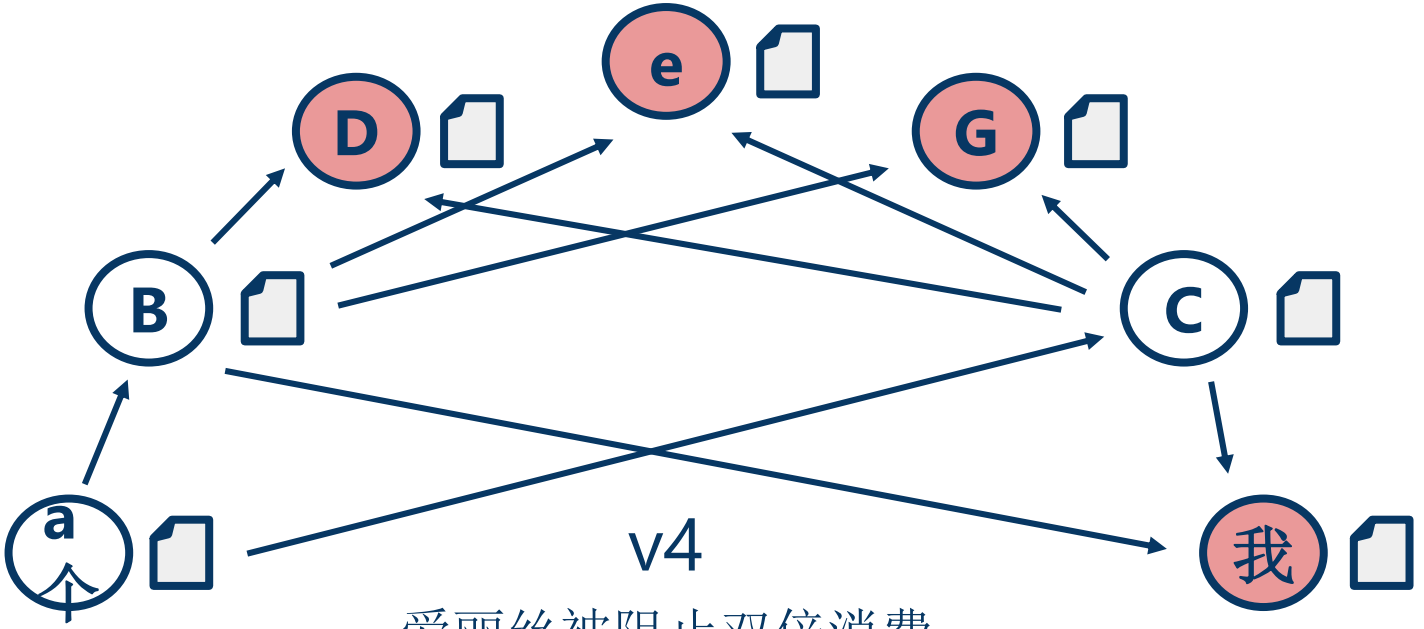
我们可以通过赋予每个人验证交易的权力来解决版本4中的双倍支出问题。
现在, 当 alice 将她的事务发送给 bob 时, bob 不应该试图单独验证事务。
相反, 他应该向整个比特币用户网络广播可能的交易, 并请他们帮助核实。
如果有足够多的用户验证交易, bob 可以接受比特币, 每个人都会更新他们的区块链。



v4

每个人都验证事务

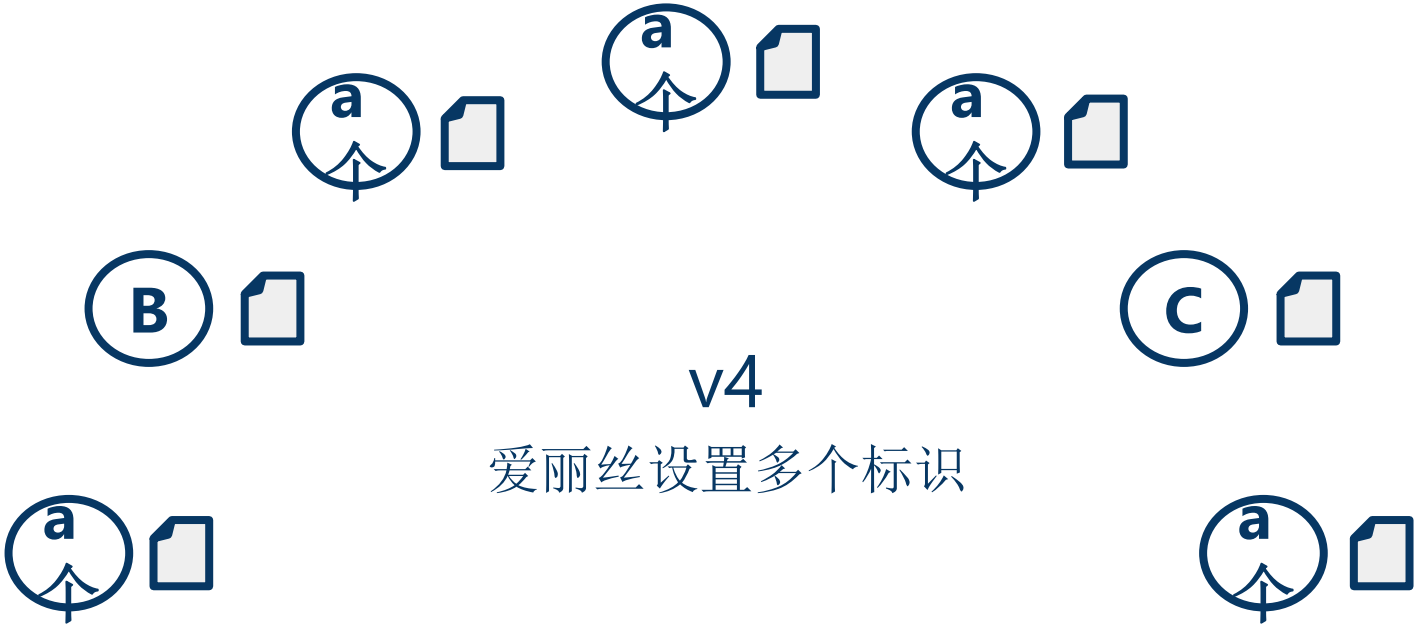
这样, 如果 alice 试图在鲍勃和查理身上双倍花费, 其他比特币用户会注意到并拒绝交易。



爱丽丝被阻止双倍消费

此方法有问题:

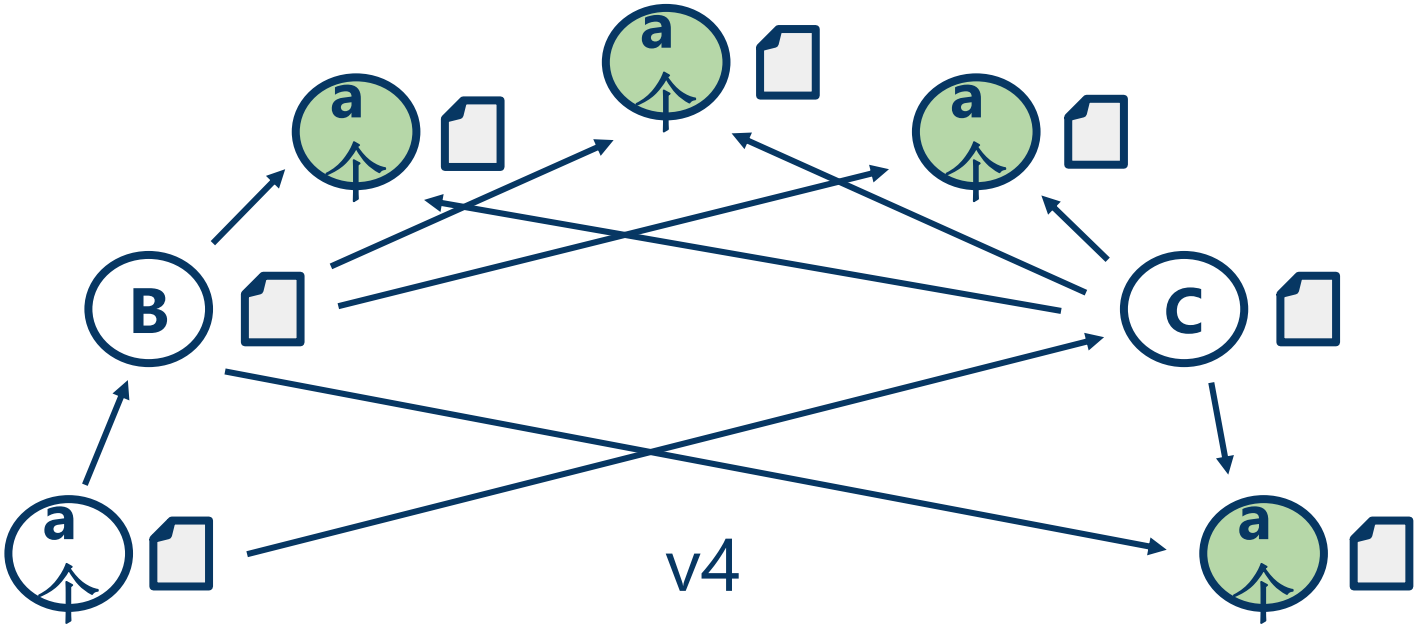
爱丽丝可以通过接管比特币网络在鲍勃和查理身上花双倍的钱。
她可以使用自动化系统来建立大量的独立身份, 压倒比特币网络。



v4

爱丽丝设置多个标识

现在当鲍勃和查理要求网络核实他们的交易时
爱丽丝的许多身份淹没了网络，并宣布鲍勃和查理的交易是好的，愚弄他们接受相同的比特币。



爱丽丝花了她的多重身份

西比尔袭击: 通过创建许多假身份来完成

我们可以通过实施工作证明来解决版本5中的双倍支出问题。
在一个工作证明系统中，当 alice 想要给 bob 一些比特币时，她宣布她的交易作为一条消息给整个网络。

v5

工作证明

当其他用户收到 alice 的事务消息时，他们会将其添加到已被告知的待处理事务列表中，但尚未由网络验证。

任何用户都可以维护自己的挂起事务列表

v5

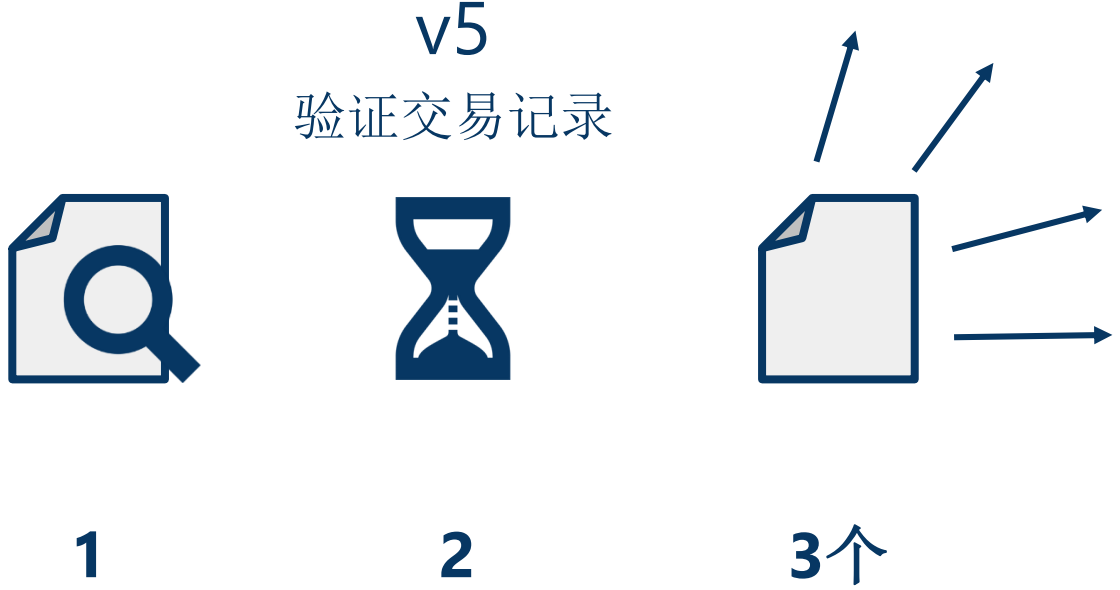
待处理的交易记录

1. 我，汤姆，给苏一枚比特币，序列号3920。
2. 我，悉尼，给辛西娅一个比特币，序列号1325。
3. 我，爱丽丝，给鲍勃一个比特币，序列号1234。

如果 david 想要在工作证明系统中验证这些挂起的事务, 他必须执行以下三项操作:

- 首先, 大卫必须检查他的区块链副本, 以确保交易是合法的。
- 其次, 他的电脑必须利用资源来解决一个难题。
- 第三, 他必须向网络宣布交易块。

在我们仔细观察之前, 请记住, 如果 david 不想验证任何事务, 他不必验证-他可以让其他用户这样做!



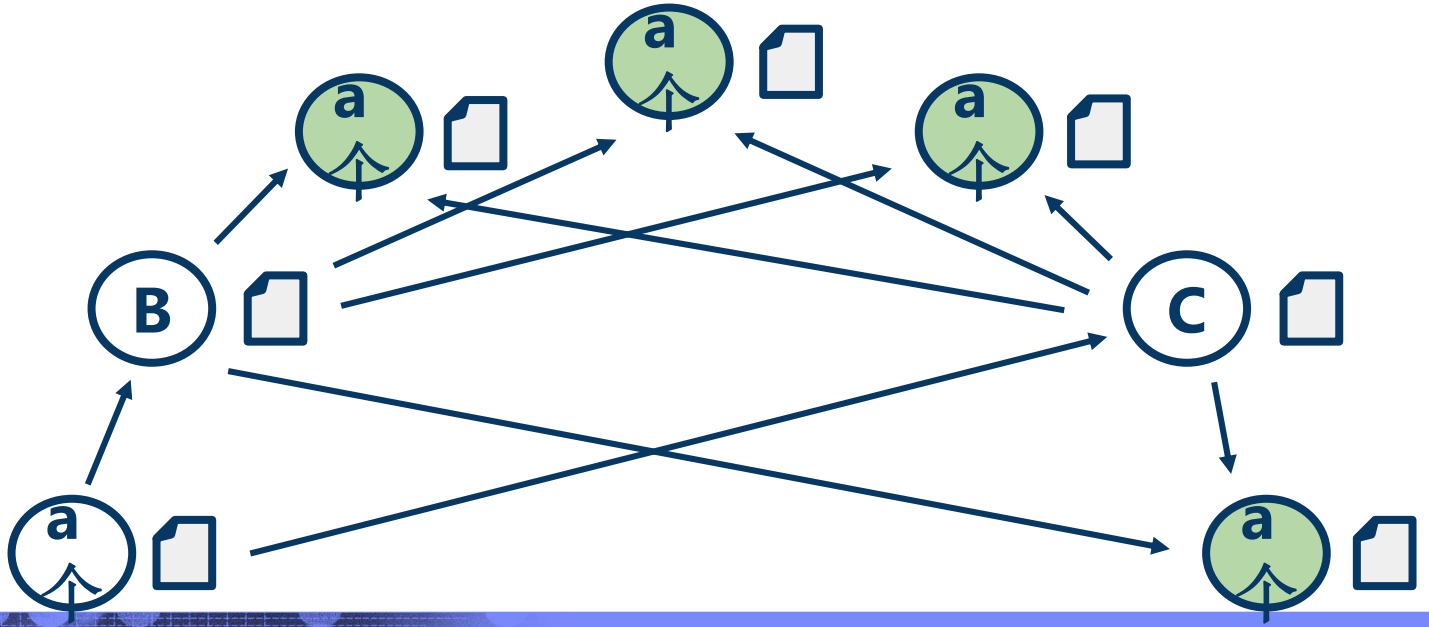
v5

为什么要做数学？

这是一个重要的问题。通过要求大卫的电脑来解决一个数学难题，我们实际上是在解决双倍支出的问题。让我们再看看那个问题。

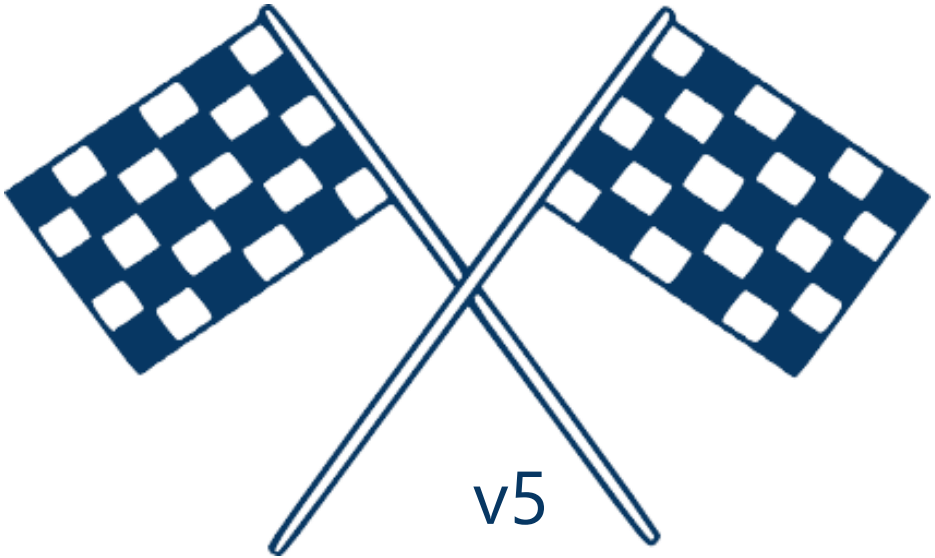
v4

爱丽丝花了她的多重身份



您可以将工作证明视为验证交易的竞争。 在比特币中，人们称之为**挖掘**.
如果您的计算机在网络上的其他计算机之前解决了数学难题，您将验证挂起的交易，并收到一些比特币作为奖励。

校对可以防止像 alice 这样的坏演员双倍支出，因为这会使他们与其他试图验证交易的人竞争。 只要网络上的大部分计算能力都是由诚实的人控制的，像爱丽丝这样的恶意行为者就很难做一些不诚实的事情，比如双倍消费。



v5

作为竞争的工作证明

总结

版本	主要特点	增值服务
1	向网络发布的签名消息	整个系统的基础
2	序列号	唯一可识别的交易记录
3个	块链	共享的交易记录
4个	每个人都验证事务	更高的安全性
5	工作证明	防止双倍支出

概述

- 比特币概念
- 建立共识
- 挖掘概述
- 加密货币开采

比特币采矿素描. 工作证明

- **拜占庭将军问题的解决方案: 工作证明 (pow)**
  - "矿工" 不断竞争, 以解决一个非常计算难题
  - 工作证明是 "拜占庭共识算法" 的一个例子
- **工作标准证明:**
  - 易于验证
  - 难以计算
- **sha-256 哈希函数满足这些要求**
  - 单向哈希函数;可以哈希任何任意数据
  - 相当随机 (非常有用的属性)
- **例子**
  - SHA256("Donaldt臀部 ")= "e4f2f2f2e2e2e2e2e2e2e2e4e3d3c70c3b4f35777c9977bdc9f4a4ac28e3e7c2c505db6c"
  - SHA256("Donaldt臀部 ")= "6ad2fa6a5caaee9143578931456322c4433a92ae2af8f0d5c9b4f9bb080f49d6"

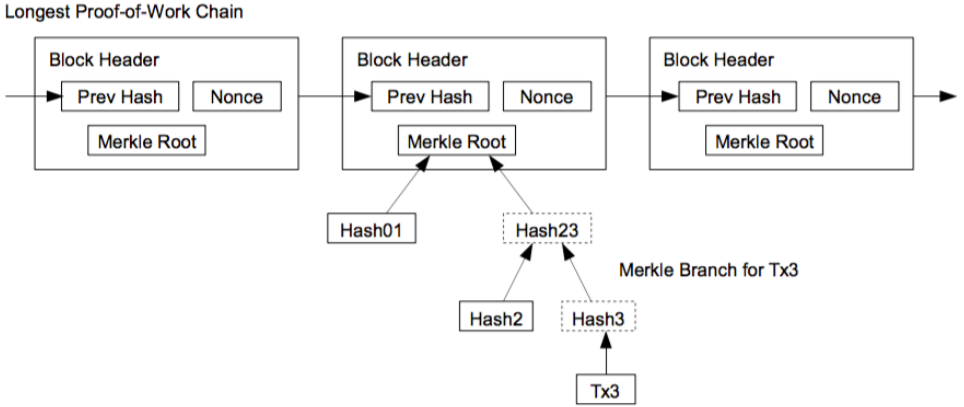
比特币采矿素描-寻找块

- **找到 "找到" 一个方块;可以添加块到区块链**
  - 发现块的矿工添加 "**造币交易记录**"
    - 包含采矿奖励 (目前为 12.5 btc)
  - 矿工广播块
  - 其他节点验证, 然后添加到自己的区块链副本
- **时间线 + 统计信息**
  - 这种情况大约每10分钟发生一次
    - 问题的难度每2周调整一次
  - 轮款奖励每4年减半 (最近于7月9日减半)
    - 比特币的供应有限----到 2140, 有 2 100万枚比特币
      - 通缩
  - 目前流通的比特币为15.2 枚
  - ~ 96亿美元的市值
  - 目前价格约为每比特币600美元

比特币采矿素描-采矿问题

将组件拼接在一起:

- **默克根**
  - 块中的交易记录的 "摘要"
- **上一个块的哈希**
- **Nonce**
  - sha-256 的随机性在这里是有用的!



正式:

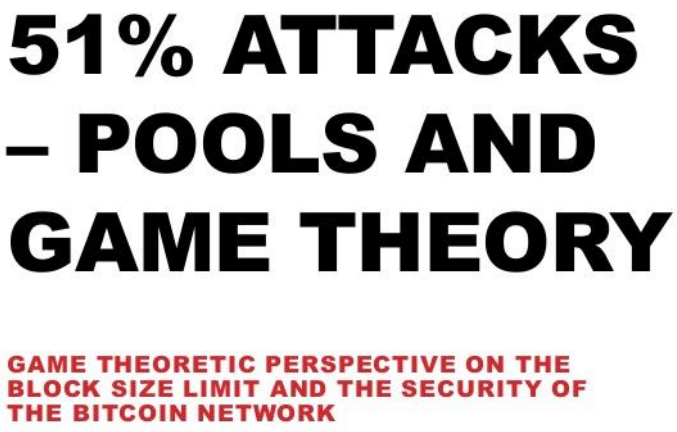
- **输出 = sha-256(Merkle 根 + sha-256(PreviousBlock) + nonce)**
- **解决方案 (工作证明): 包含所需数量的前导0位的输出**
  - 0位的数量是中。**困难**
  - 每个2016年块 * 都有困难调整, 以调节块创建
    - * 技术上每2015块

比特币采矿素描-51% 的攻击

比特币的主要假设:

- 不超过 5 1% 的网络不诚实
- 诚实的大多数人将永远构成最长的工作证明链

51% 攻击: 试图压倒网络的挖掘能力



资料来源: martin koppelmann 在 sf 比特币 devs 上介绍。

比特币采矿素描. 摘要

功能如下:

- 一种确保硬币以公平的方式分配的铸造机制
- 激励人们帮助保护网络安全
- 使您能够以分散货币达成共识的关键组件

概述

- 比特币概念
- 建立共识
- 挖掘概述
- 加密货币开采

加密货币开采

--工作证明共识

什么是利润

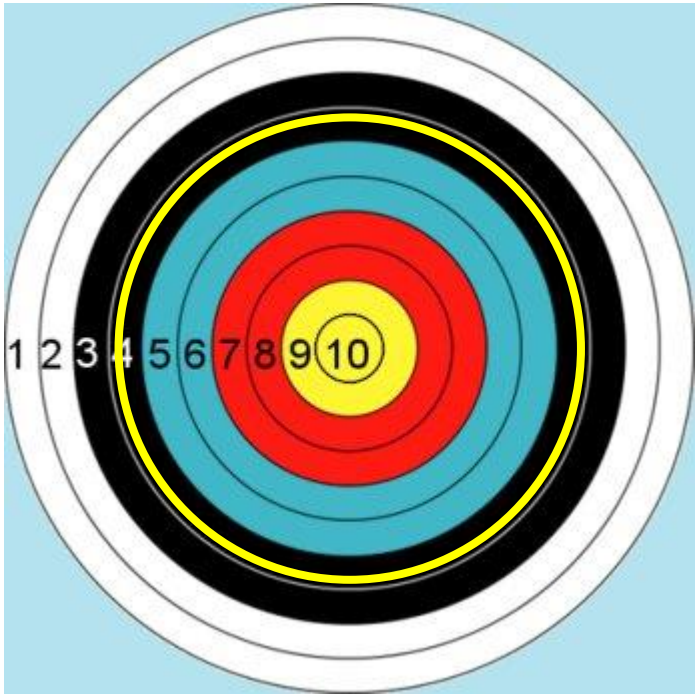
如果
奖励 > 成本
然后是 $ $

利润 = 奖励-成本

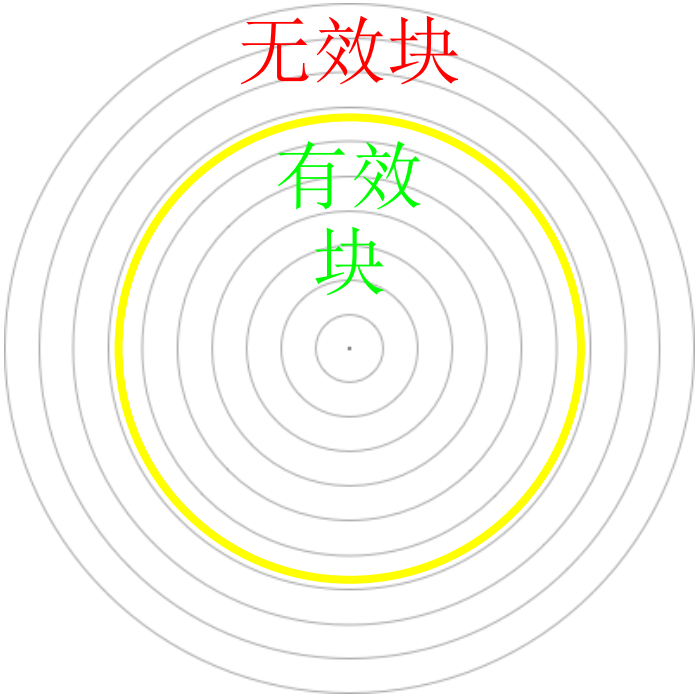
采矿成本

如果
采矿奖励 > 采矿成本
然后矿工的利润
在哪里
采矿奖励 = 块奖励 + tx 费用
采矿成本 = 硬件成本 + 运营成本 (电力、制冷等)

块奖励:: 难度调整



块奖励:: 难度调整

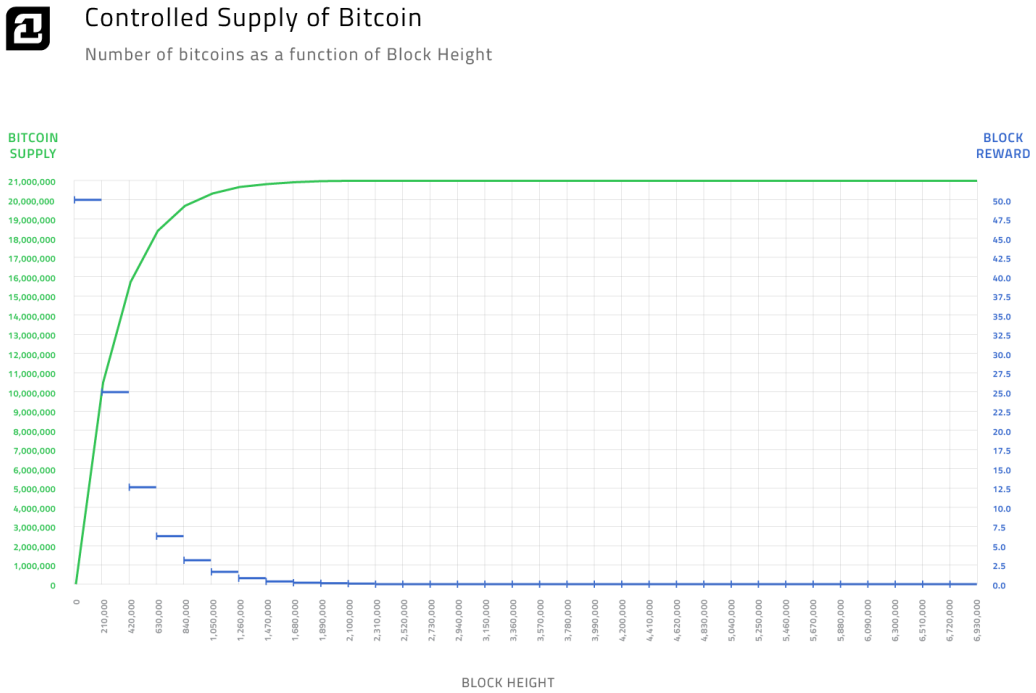


H(*Nonce*||*昨日_散 列*||*Tx*||*Tx*||... ||*Tx*) < *目标*

- 同样有可能击中环 1, 2, 3,..。
- 矿工 = 更多点击次数/秒
- 目标: 黄色戒指内
- 继续减小黄环的大小..。
- 2016年每个区块的采矿难度调整
- 难度调整为

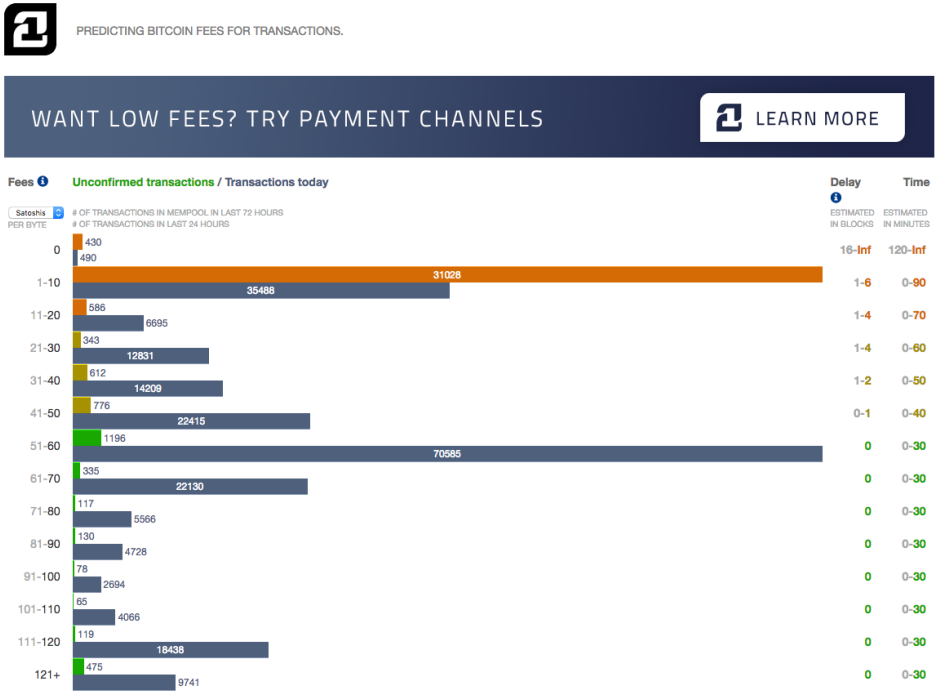
下一个 _ 难度 = 以前的难度 * (2周)/(最后2016年区块的开采时间)

块奖励:: 比特币半



- 节点创建块包括一个特殊的 tx 到自己
- 当前块奖励: 12.5 btc
- 诚实行为的货币激励
- 每21万块将一半
  - 通货紧缩的货币!
- 几何金额: 结束在21e6
- 那接下来呢？

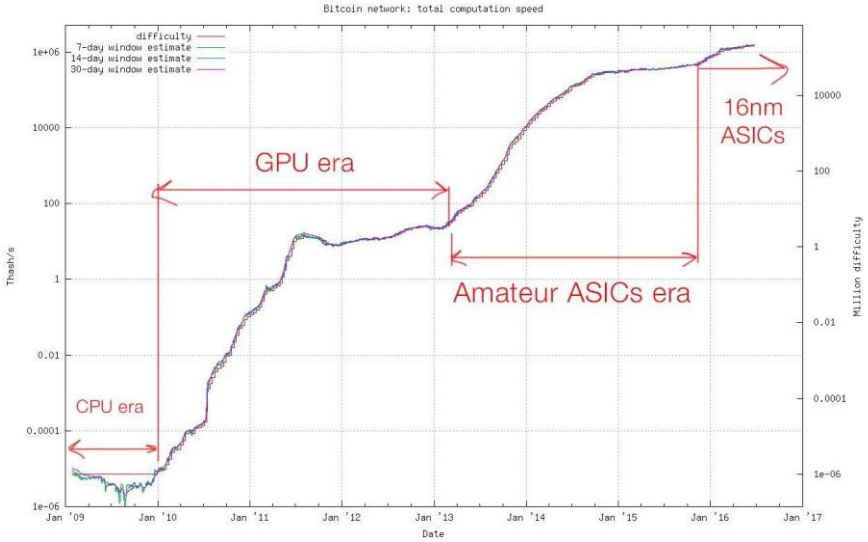
交易费用



- 交易费用是可选的
- 矿工倾向于使用交易费用较高的交易
  - 激励将您的交易包括在他们正在挖掘的下一个块中
- 21世纪以后矿工的主要收入来源6

硬件成本

	哈希/秒	要阻止的时间
Cpu	2000万	30万年
Gpu	2亿	3万年
Fpga	10亿	600年
Asic	10万亿	22天



cpu 挖掘

	哈希/秒	要阻止的时间
Cpu	2000万	30万年
Gpu	2亿	3万年
Fpga	10亿	600年
Asic	10万亿	22天

- 对于每一个 **nonce**
  - 运行 sha256
  - 检查结果是否为有效块
- **慢**
- **佐藤用什么**
- **你的婚礼!**

gpu 采矿

	哈希/秒	要阻止的时间
Cpu	2000万	30万年
Gpu	2亿	3万年
Fpga	10亿	600年
Asic	10万亿	22天

- 专为并行计算而设计
- 数量级比 cpu 快
- 消耗大量的能量, 产生大量的热量
- 446.66 为 r9 290 早在当天

又名。麦克斯和我在高中的时候是什么?

fpga 采矿

	哈希/秒	要阻止的时间
Cpu	2000万	30万年
Gpu	2亿	3万年
Fpga	10亿	600年
Asic	10万亿	22天

- F费尔德P罗格拉普西G吃a 个rrays
  - 获取更多特定于应用程序的信息
- asic 与通用之间的权衡

asic 采矿

	哈希/秒	要阻止的时间
Cpu	2000万	30万年
Gpu	2亿	3万年
Fpga	10亿	600年
Asic	10万亿	22天

- **a 个pplication-pplication-pplication-ppls特异性我恩格拉德Circuits。**
  - 专门为进行比特币开采而设计的电路(sha256)
  - 非常昂贵
- **最快的矿工周围**
- **~ 1600**

运营成本

- **比特币中的能量**
  - 体现能量
  - 电力
  - 冷却
- **兰道尔原理的热力极限**
  - kt 2 (k = 玻尔兹曼常数)/位
- **比特币网络能耗 (当前)**
  - 14, 000 ghs:1, 375w
  - 1, 820 429 066 ghs:178, 72, 140 w
  - 占大型燃煤电厂能源的10%
- **电加热器, 让你赚钱**

创新的工作证明理念

工作难题要求的证明

基本谜题要求:

1. **快速验证**
2. **获胜拼图的机会应与计算能力成比例**
3. **无记忆或 "无进展"**
    a. 解决难题的可能性必须与你已经花了多少精力去解决它无关
    b. 一般情况下, 基于试验和错误

比特币的拼图是一个 "部分哈希前图像拼图"

- **查找部分指定的哈希输出的预映像**

抗 asic

参数为:

- 如果没有 asic 的抗性, 生态系统中的大多数个体在采矿过程中没有任何作用
- 更加民主和分散----"一 cpu 一票"

反对:

- **sha-256 asic 仅适用于比特币的开采**
  - 因此, 拥有51% 大麻力的矿工投资于比特币的安全
- **崩溃的汇率 = > 攻击者在无用的硬件上浪费了一堆钱**
  - 否则, 攻击者可以租用一般计算资源, 如 amazon ec2, 并且在受到攻击后不会产生任何后果

抗逆性: 记忆硬算法

内存难: 需要大量内存来计算, 而不是计算时间

内存绑定: 内存量控制总计算时间

为什么这些有助于抗 asic?

- **计算现代哈希函数所需的逻辑操作只是 cpu 功能的一小部分**
  - cpu 是广义的;使 asic 能够基于这一事实进行优化
- **内存性能的增加比计算能力慢很多**
  - 解决这个难题的成本会降低得更慢

示例: scc虫

sc虫是一个哈希函数。挖掘拼图是相同的部分哈希前图像拼图。

设计注意事项:

- 用于哈希密码
- 难以擦伤

由 lececoin、dogecoin 使用

抗日药: 斯凯特

在不使用内存的情况下, 必须动态计算 v [j]。只需选择 n, 这样使用内存的速度就会更快

两个主要步骤:

1. **填充缓冲区**
   相互依赖的数据
2. **中访问此数据。**
   伪随机方式

缺点: (1) 需要
同样多的内存
验证, (2) 已 asic

Figure 8.1: Scrypt pseudocode

```
1 def scrypt(N, seed):
2     V = [0] * N  // initialize memory buffer of length N

  // Fill up memory buffer with pseudorandom data
3   V[0] = seed
4   for i = 1 to N:
5       V[i] = SHA-256(V[i-1])

  // Access memory buffer in a pseudorandom order
6   X = SHA-256(V[N-1])
7   for i = 1 to N:
8       j = X % N  // Choose a random index based on X
9       X = SHA-256(X ^ V[j]) // Update X based on this index

10  return X
```

抗 asic: 其他方法

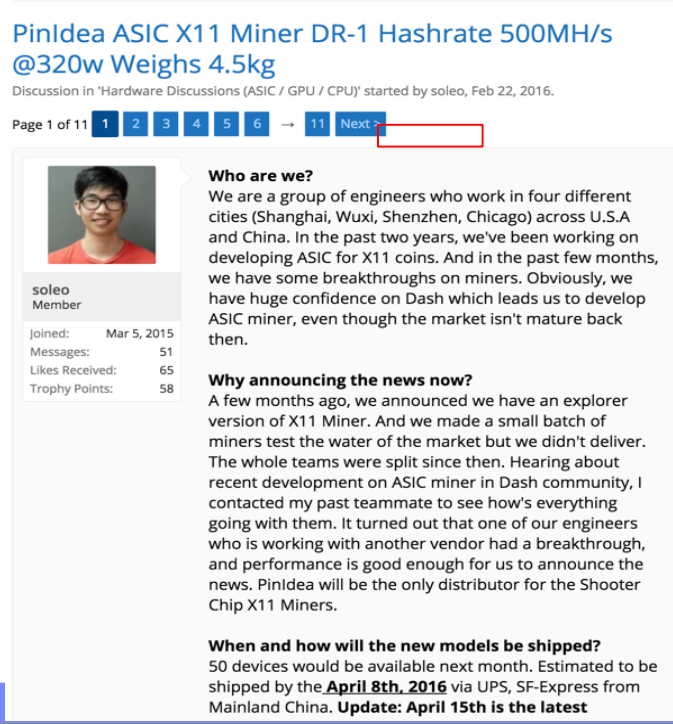
x11 或 x11: 链 11/13个不同的哈希函数在一起 (由 dash 使用)

- 使设计变得更加困难 asic
- ...但已经做完了

定期更改挖掘难题

- 例如, 在 sha-1、sha-3 之间切换, sc虫每人6个月
- 易于工作;未执行

迈克·赫恩: "真的没有这样的事情 抗 asic 算法。



PinIdea ASIC X11 Miner DR-1 Hashrate 500MH/s @320w Weighs 4.5kg

Discussion in 'Hardware Discussions (ASIC / GPU / CPU)' started by soleo, Feb 22, 2016.

Page 1 of 11 1 2 3 4 5 6 → 11 Next >

soleo
Member

Joined: Mar 5, 2015
Messages: 51
Likes Received: 65
Trophy Points: 58

Who are we?
We are a group of engineers who work in four different cities (Shanghai, Wuxi, Shenzhen, Chicago) across U.S.A and China. In the past two years, we've been working on developing ASIC for X11 coins. And in the past few months, we have some breakthroughs on miners. Obviously, we have huge confidence on Dash which leads us to develop ASIC miner, even though the market isn't mature back then.

Why announcing the news now?
A few months ago, we announced we have an explorer version of X11 Miner. And we made a small batch of miners test the water of the market but we didn't deliver. The whole teams were split since then. Hearing about recent development on ASIC miner in Dash community, I contacted my past teammate to see how's everything going with them. It turned out that one of our engineers who is working with another vendor had a breakthrough, and performance is good enough for us to announce the news. PinIdea will be the only distributor for the Shooter Chip X11 Miners.

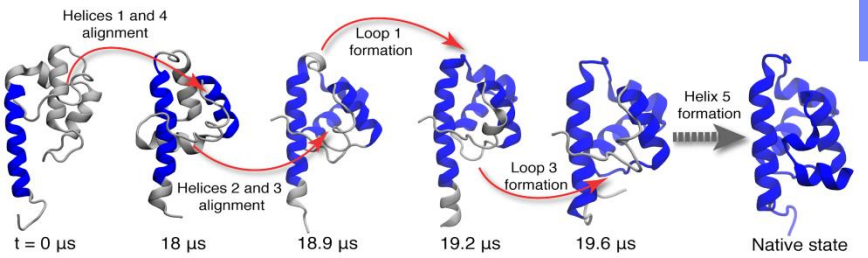
When and how will the new models be shipped?
50 devices would be available next month. Estimated to be shipped by the **April 8th, 2016** via UPS, SF-Express from Mainland China. **Update: April 15th is the latest**

有用的工作证明

总思路: "回收" 计算能力;
重新定位它的东西有用的

例子:

- 搜索大型优质的
- 寻找外星人
- 蛋白质折叠法研究疾病的原子级模拟
- 创建预测气候模型
- solarcoin: 分发给发电的人



Project	Founded	Goal	Impact
Great Internet Mersenne Prime Search	1996	Finding large Mersenne primes	Found the new "largest prime number" twelve straight times, including $2^{57885161} - 1$
distributed.net	1997	Cryptographic brute-force demos	First successful public brute-force of a 64-bit cryptographic key
SETI@home	1999	Identifying signs of extraterrestrial life	Largest project to date with over 5 million participants
Folding@home	2000	Atomic-level simulations of protein folding	Greatest computing capacity of any volunteer computing project. More than 118 scientific papers.

普林斯顿教科书表8。3

有用的工作证明: 挑战

大多数分布式计算问题都不适合证明工作

- **固定数量的数据**
  - seti @ home 可能会耗尽原始数据来计算
  - 缺少一个**取之不尽、用之不竭的拼图空间**
- **潜在的解决办法并非都是同样有可能的**
  - 缺少一个**等可能的溶液空间**
- **不能依赖中央实体来委派任务**
  - 拼图必须能够是**算法生成的**

示例: seti @ home (搜索外星人)

- **某些段可能更有可能包含异常**

- 所有矿工都会先搜查这些地区
- 更快的矿工有更高的可能性来解决这个难题
- 因此, 它不会是无记忆的, 大矿工有优势

存储证明

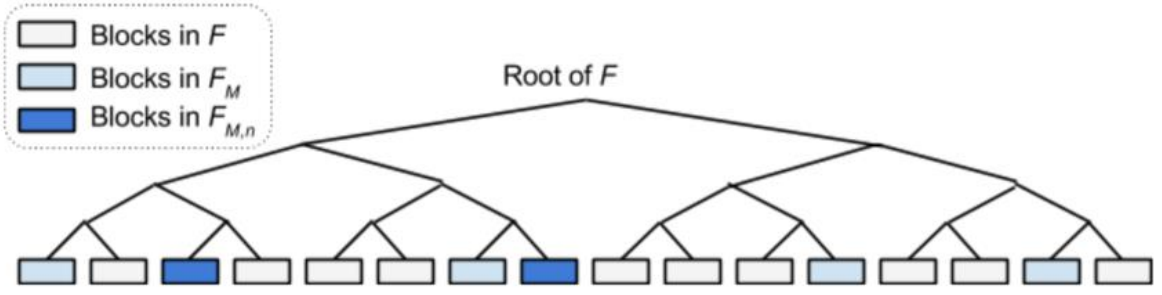


Figure 8.4: Choosing random blocks in a file in Permacoin.
In this example k_1=6 and k_2=2. In a real implementation these parameters would be much larger.

普林斯顿教科书, permacoin

佩尔马科因

- **查找一些大文件**
  - 重要的、公开的和需要复制的
  - 没有人可以储存的东西
  - 大型强子对撞机的实验数据为几百 pb
- **将文件存储在块中, 存储在一个 merkle 树中**
  - 网络在默克根上达成一致
- **矿工存储的 t 块的子集, 基于他们的公钥**
  - 连续使用 nonce 来在其存储的子集中选取块来哈希共识信息
  - 将选取的方块绑在一起, 必须低于某个目标值
  - 确保存储, 因为每一次增加查询网络的效率极低
- **缺点: 很难找到大文件, 改变困难, 修改文件**

合并采矿

当启动一个 altcoin, 你需要哈希电源来保护您的网络

- **默认情况下, 挖掘是独占的; 默认情况下, 挖掘是独占的。不能同时解决两个问题**
- **采矿 altcoin = > 失去其他连锁店的利润**
  - 对马力的争夺
- **容易受到来自较大硬币的攻击**

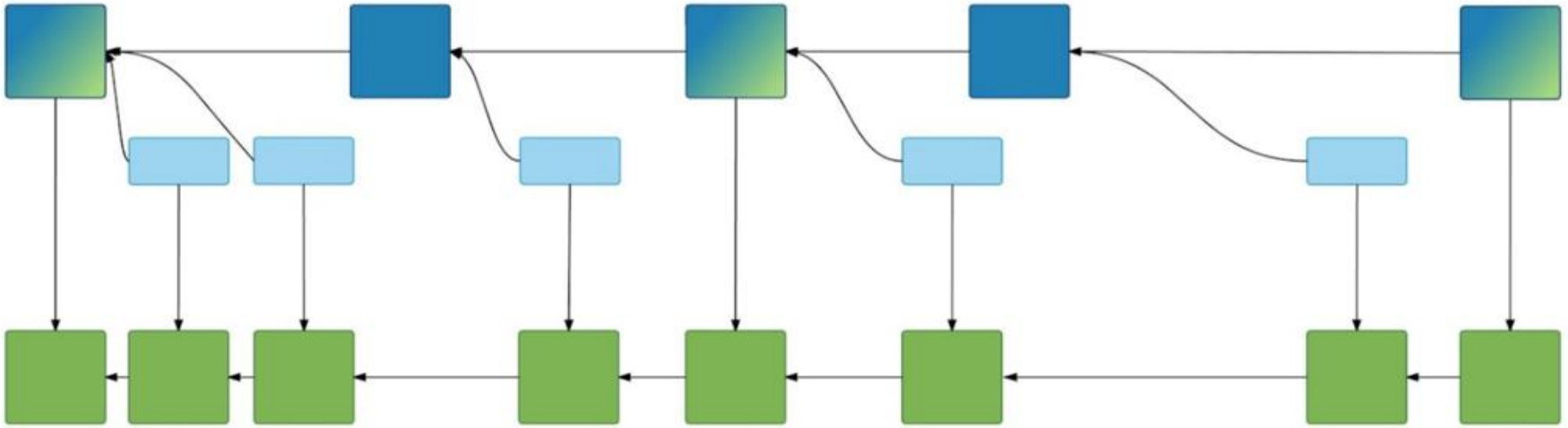
"杀死艾尔特币的婴儿"

- **个人比特币矿物池哈希 > 整个 altcoin 哈希利率**
- **2012年: eligius 矿池运营商袭击 CoiledCoin**
  - 已反转多日的交易记录
  - 空块的长链

合并采矿

合并挖掘

- **创建具有比特币和 altcoin 交易的块**
  - 分享哈希力量
- **实现**
  - 容易为祭坛硬币-免费建立你的硬币, 无论你喜欢
  - 但如何将 altcoin 交易包括在比特币中呢?
- **解决方案: 在比特币的硬币基础参数中包含 altcoin 交易的摘要**
  - 摘要可以是 altcoin 交易的 merkle 根
  - 其他比特币客户并不关心
- **altcoin 将尝试挖掘比特币块**
  - 两个平行链



Altcoin blocks

Bitcoin blocks mined by altcoin merge-miners

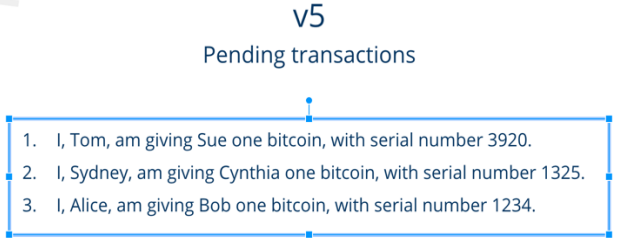
Bitcoin blocks mined by non-altcoin miners

Attempted Bitcoin blocks found by altcoin merge-miners that met the altcoin's difficulty target but not Bitcoin's target

把这一切结合起来--回到交易中

- **我想把钱寄给桑尼**
  - 签署交易记录
  - 向网络广播
- **矿工收到交易, 添加到 "零 conf 池"**
  - 验证交易记录: 即签名匹配, 足够的资金,
- **矿工发现 pow, 广播块**
  - 块传播;其他验证
- **矿工们在研究下一个问题**

Slide by Viget



结束！

धन्यवाद
Hindi印地语

多謝
繁体中文

ขอบคุณ
泰语

Спасибо
俄语

谢谢
西班牙语

谢谢
英语

شكرا
阿拉伯语

奥布里加多
巴西葡萄牙语

多谢
简体中文

丹克
德语

格拉齐
意大利语

谢谢
法语

நன்றி
Tamil
泰米尔语

ありがとうございました
日语

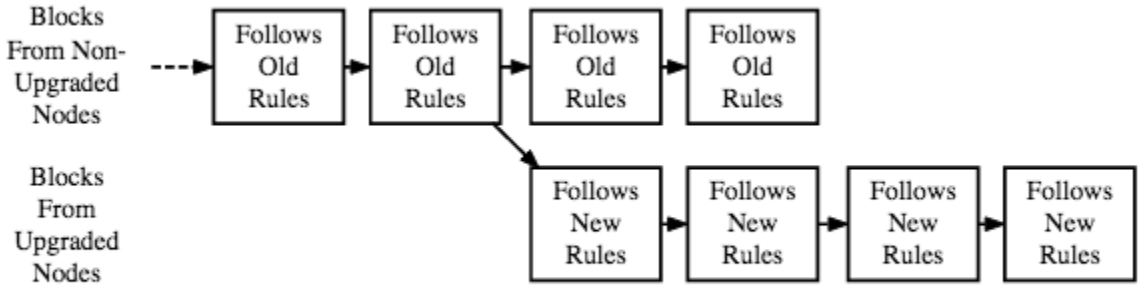
감사합니다
朝鲜语

读数

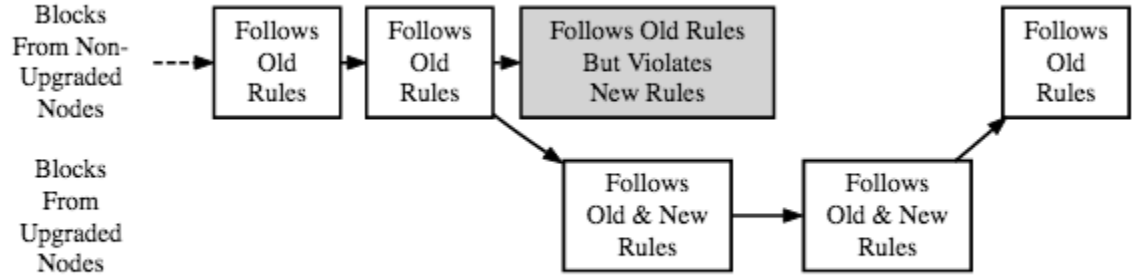
- "比特币钱包解释"
  - http://cryptorials.io/bitcoin-wallets-explained-how-to-choose-the-best-wallet-for-you/
- "比特币多西钱包: 比特币的未来"
  - https://bitcoinmagazine.com/articles/multisig-future-bitcoin-1394686504
- "什么是比特币硬件钱包？"
  - https://www.cryptocompare.com/wallets/guides/what-is-a-bitcoin-hardware-wallet/
- (可选)虚荣比特币地址:
  - https://www.cryptocoinsnews.com/get-custom-bitcoin-address/

来源: bitcone. org 开发者指南

奖金: 分叉 + 共识更新

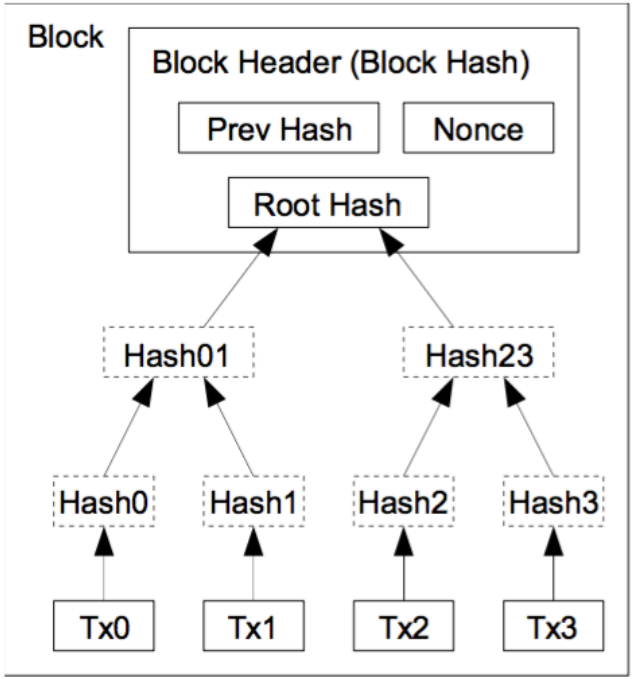


A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

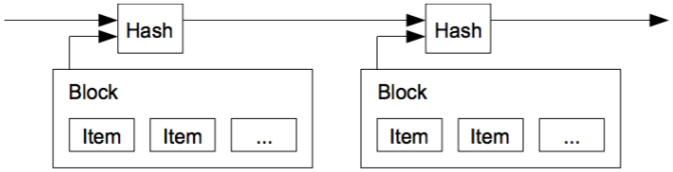


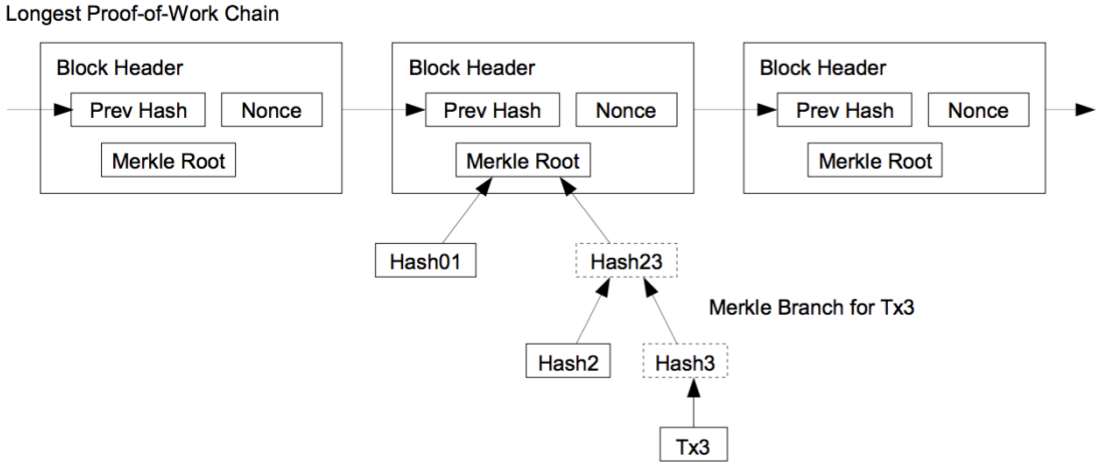
A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

奖金: 汞树



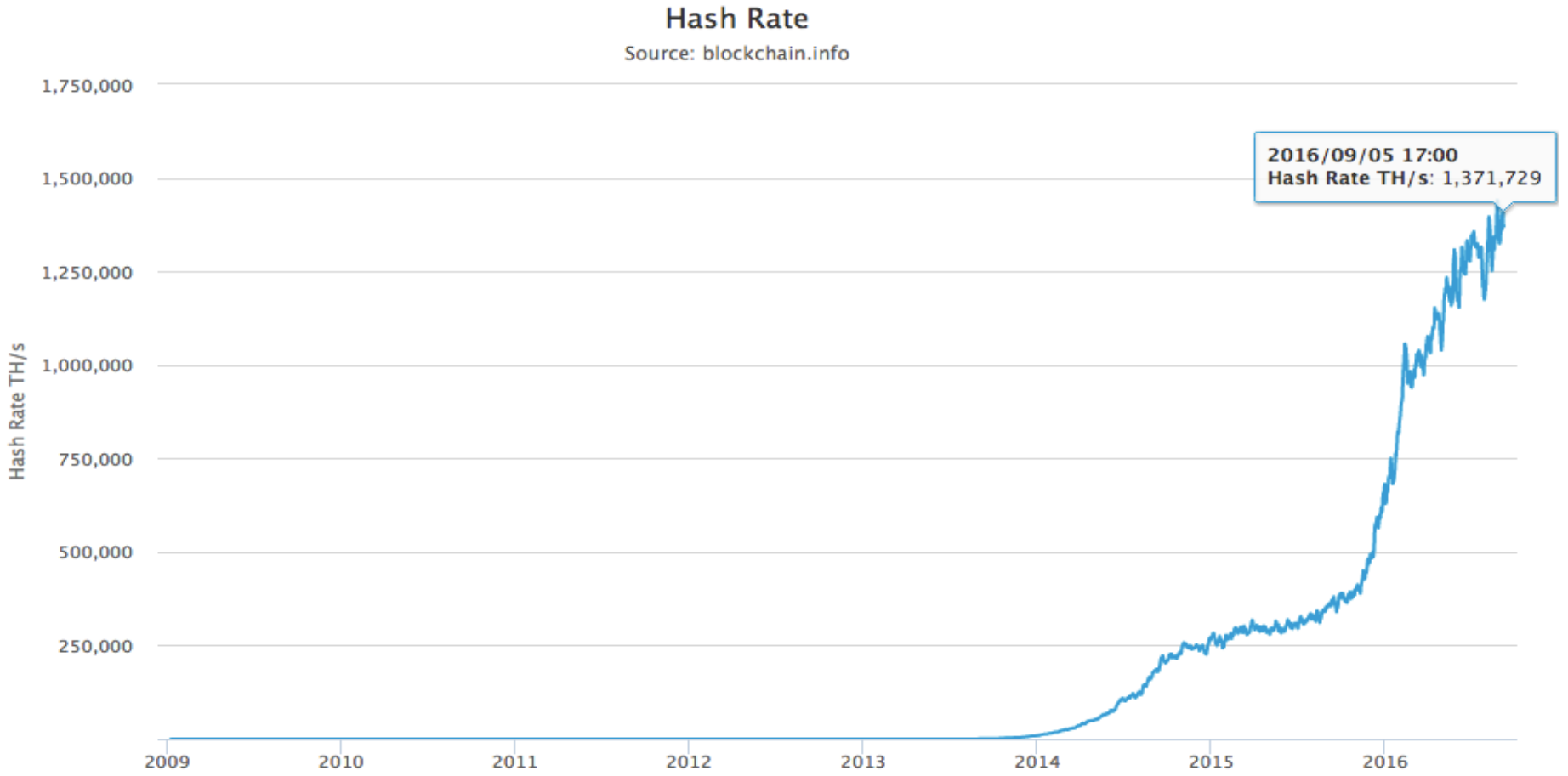
Transactions Hashed in a Merkle Tree





- 使事务历史记录不可变
- 添加链的 pow

资料来源: 中本2009


Hash Rate
Source: blockchain.info
1,750,000
1,500,000
1,250,000
1,000,000
750,000
500,000
250,000
Hash Rate TH/s
2016/09/05 17:00
Hash Rate TH/s: 1,371,729
2009
2010
2011
2012
2013
2014
2015
2016