

# 课程摘要

--由区块驱动的未来



**灵宗, 博士**

高级软件工程师/科学家  
**ibm almaden** 研究中心  
美国加利福尼亚州圣何塞

# Course Plan

**Unit1: Course Introduction, BlockChain Basics**

**Unit2: IT Infrastructures, IOT**

**Unit3: Bitcoin Basics, Bitcoin History**

**Unit4: Ethereum, Enterprise Blockchain**

**Unit5: BlockChain Foundation for Developers**

**Unit6: Blockchain Anonymization, Cryptography**

**Unit7: Bitcoin Scalability, ICO**

**Unit8: Zero-Knowledge Proof, Course Summary**

# 课程目标 (作为讲师)



## 帮助观众

- 熟悉基本**概念**的区块链;
- 有能力识别**挑战**处理可扩展解决方案的应用程序所面临的问题;
- 了解如何区块链**影响**商业智能、科学发现和日常生活。



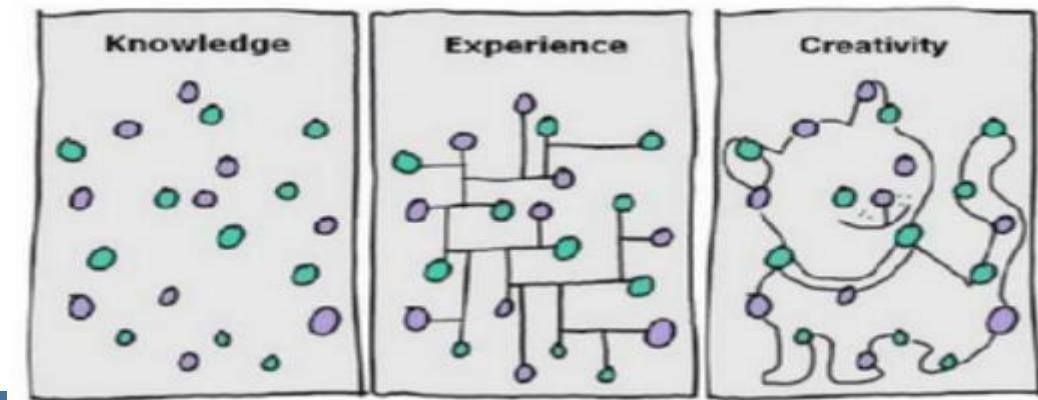
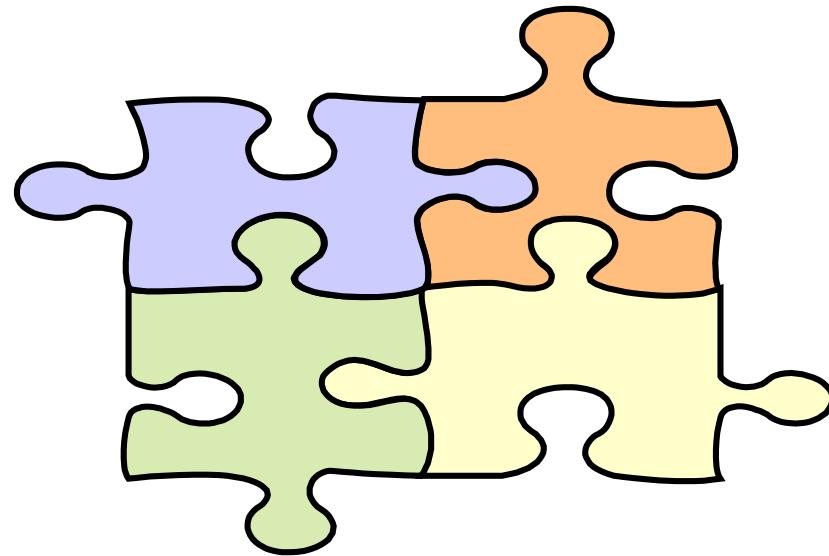
# 课程优势 (作为受众)

- 广阔的视野
- 参与体验
- 扩展自我关注
- 提高生活质量



# 课程内容

- 知识
- 经验
- 方法
- 实践



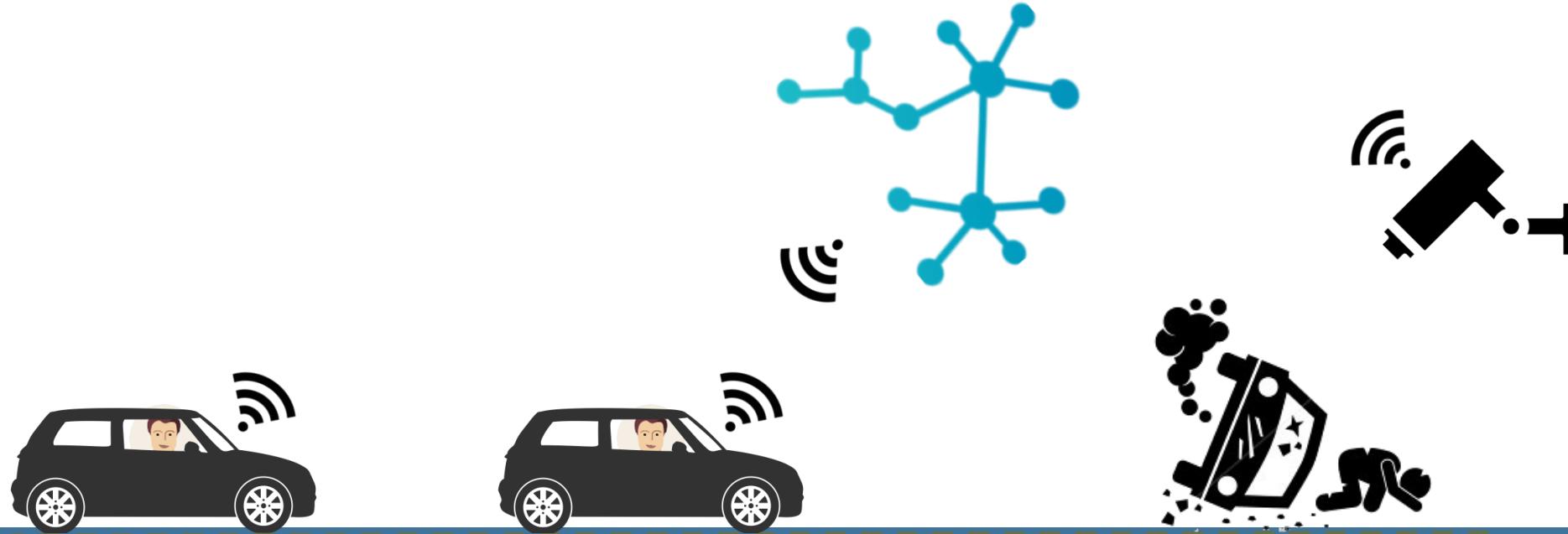
# 封锁乌托邦中的一天

# 乌托邦区块链世界



# 乌托邦区块链世界

保险智能合同



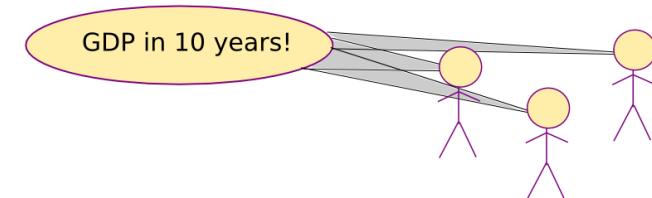
# 乌托邦区块链世界

道

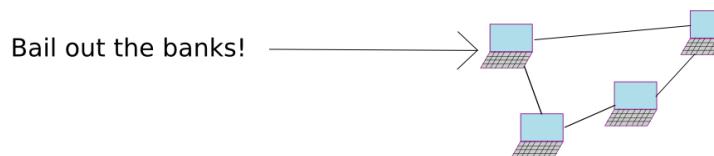


# 乌托邦区块链世界

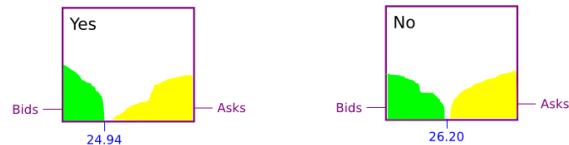
Step 0: choose a success metric and maturity duration



Step 1: create and publish proposal



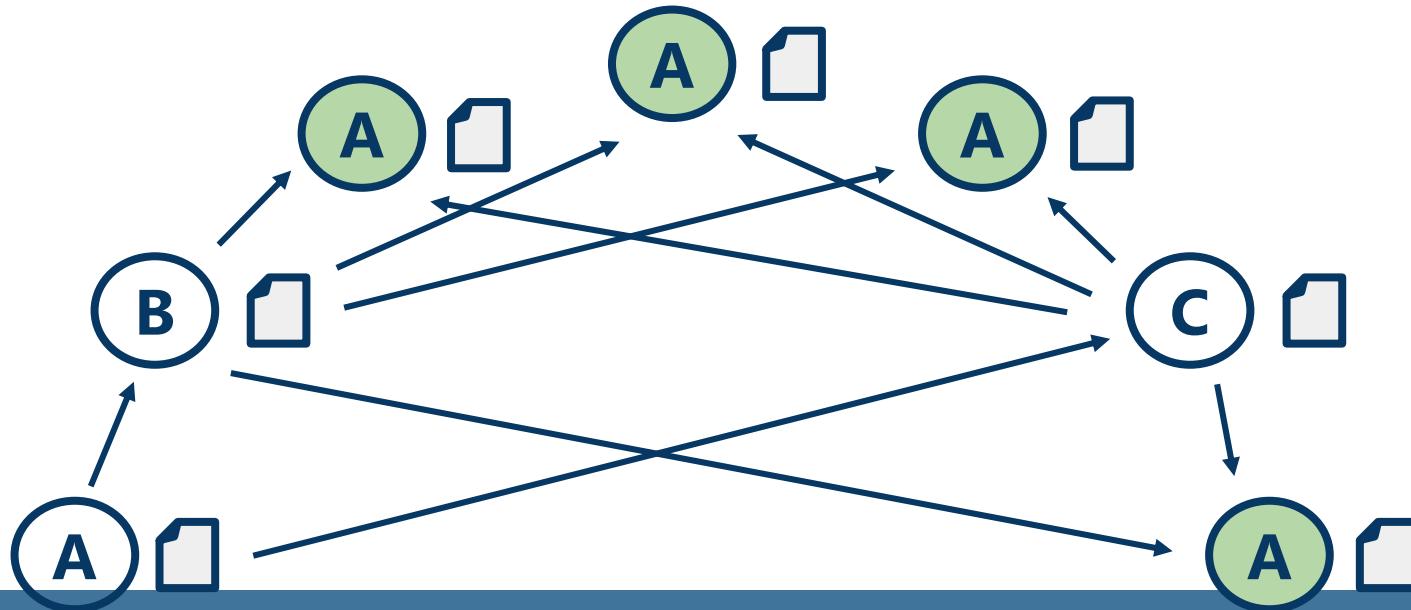
Step 2: set up prediction markets for "yes" and "no"



Note the average price of both over some period

v4

Alice double spends with her multiple identities



# Wallet Options: Choose Your Level of Control & Responsibility



**GreenAddress**



## Case Wallet

2 / 3 Signatures

Device, Case service,  
& separate backup  
company

## Green Address

2 / 2 Signatures

2-factor

Authorization

Spending Limits

## Coinbase Wallet

They hold  
private keys

Can call if you  
forget password

## Mycelium & Electrum

You alone hold  
private keys

No recourse if lost

# 简单的哈希承诺计划-作弊

鲍勃怎么能骗爱丽丝？

- 1) 当鲍勃收到 $C=H(B||R)$ , 如果他能计算  $h^{-1}(C) = B||R$ , 鲍勃可以恢复爱丽丝的猜测, 并给她相反的结果!

如果我们的哈希函数 $H$ 是抗预映像, 这不应该是可能的。

爱丽丝怎么能骗鲍勃？

- 1) 爱丽丝把她的承诺寄给鲍勃 $C=H(B||R)$ , 但揭示了相反的猜测,  $(!B, r')$ . 爱丽丝赢了, 如果她能挑 $r'$ s. t.  $c' = H(!B||r') = C$ .

如果我们的哈希函数, 这将失败, $H$ 是第二预映像电阻!

# 椭圆曲线

赛文256k1: $y^2 = x^3 + 7$   
比特币的椭圆曲线

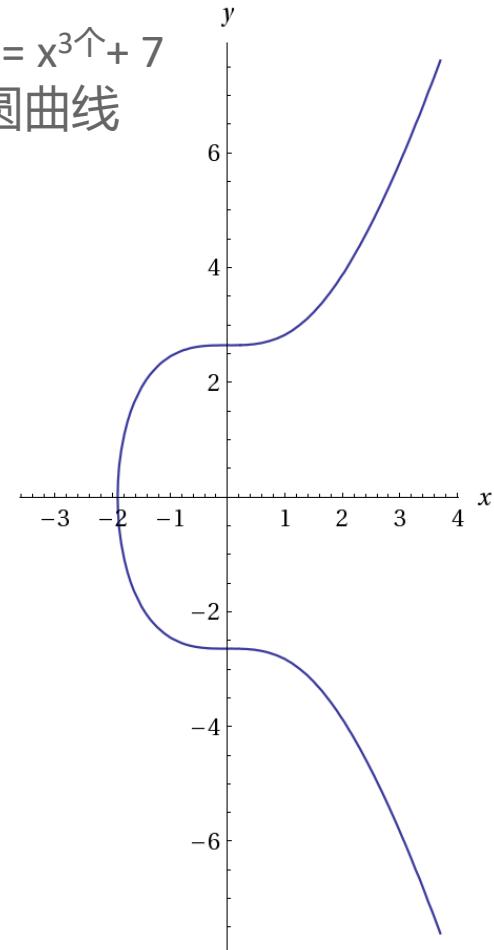
椭圆曲线由以下仿射长的 weierstrass 形式定义：

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

我们通常考虑短的 weierstrass 形式：

$$E : Y^2 = X^3 + aX + b$$

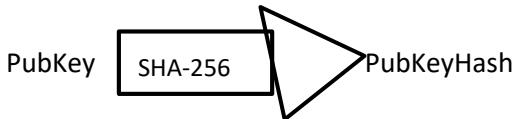
在大多数情况下，您需要了解的椭圆曲线是它们提供了另一个具有某些所需属性的有限阿贝尔群。



# ecdsa

在比特币中使用 ecdsa 签名来证明交易输出的所有权!

# Bitcoin Scripting



The Main Parts Of  
Transaction 0

Version	Inputs	Outputs	Locktime
---------	--------	---------	----------

The Main Parts Of  
Transaction 1

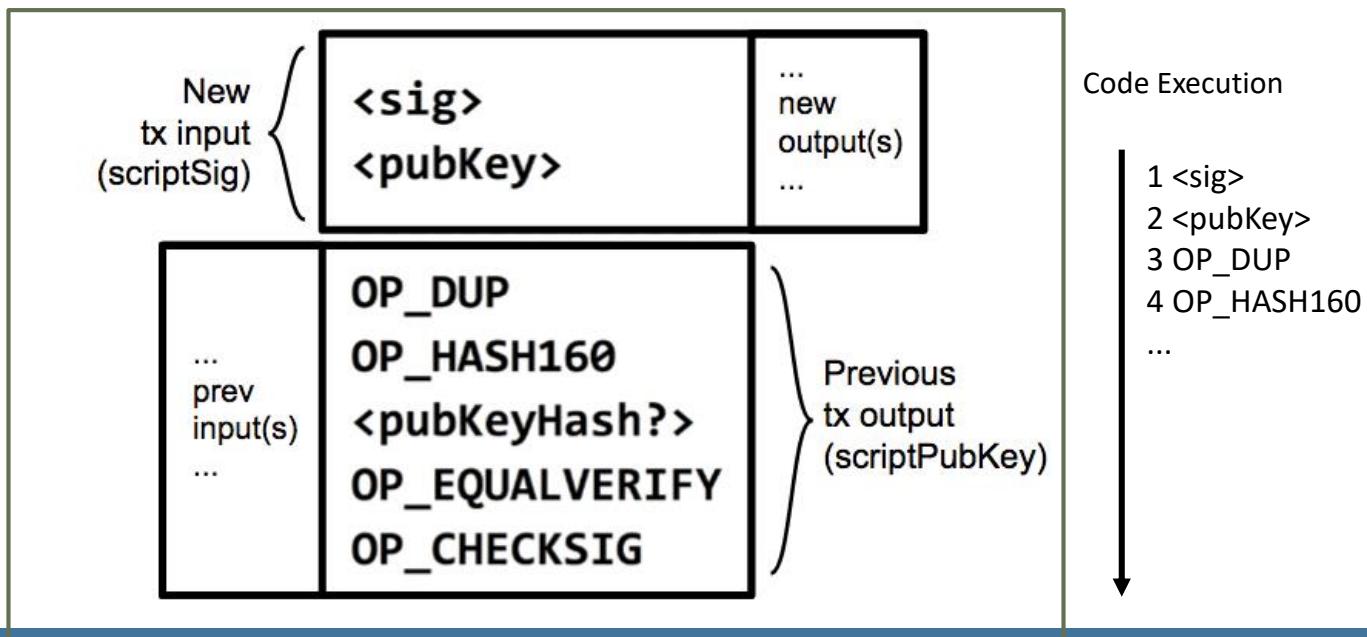
Version	Inputs	Outputs	Locktime
---------	--------	---------	----------

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

Remember: Hash(PubKey) == Address == "PubKeyHash"

## Figure:

Two transactions  
along with their  
input and output  
scripts

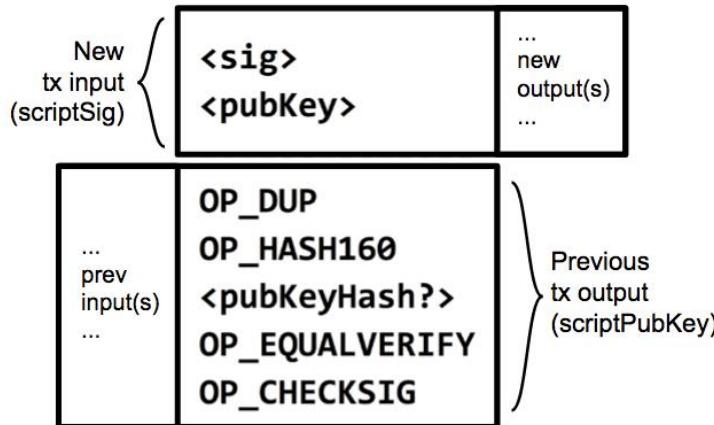


Each input spends a previous output

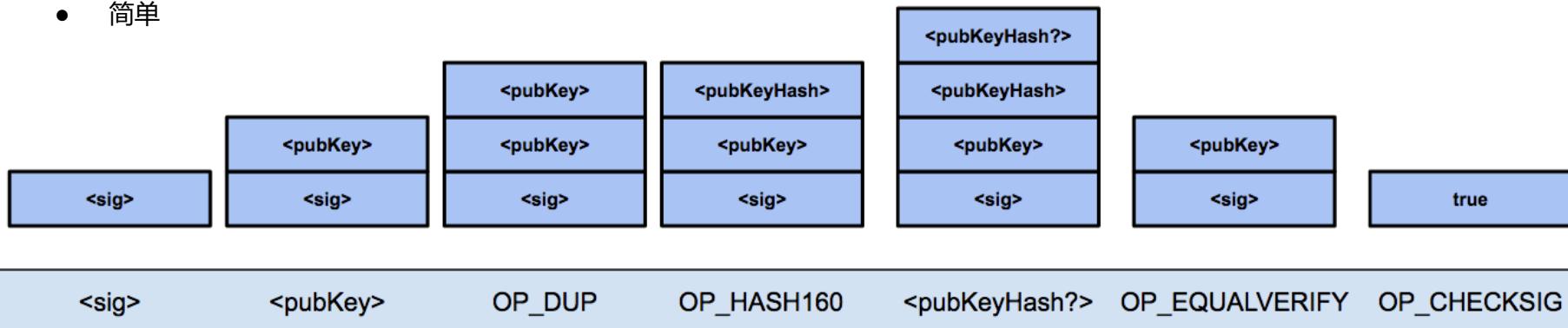
# 比特币 脚本

专门为比特币构建的名为 "脚本" 或 "比特币脚本语言" 的语言

- 基于堆栈
- 对密码学的本机支持
- 简单



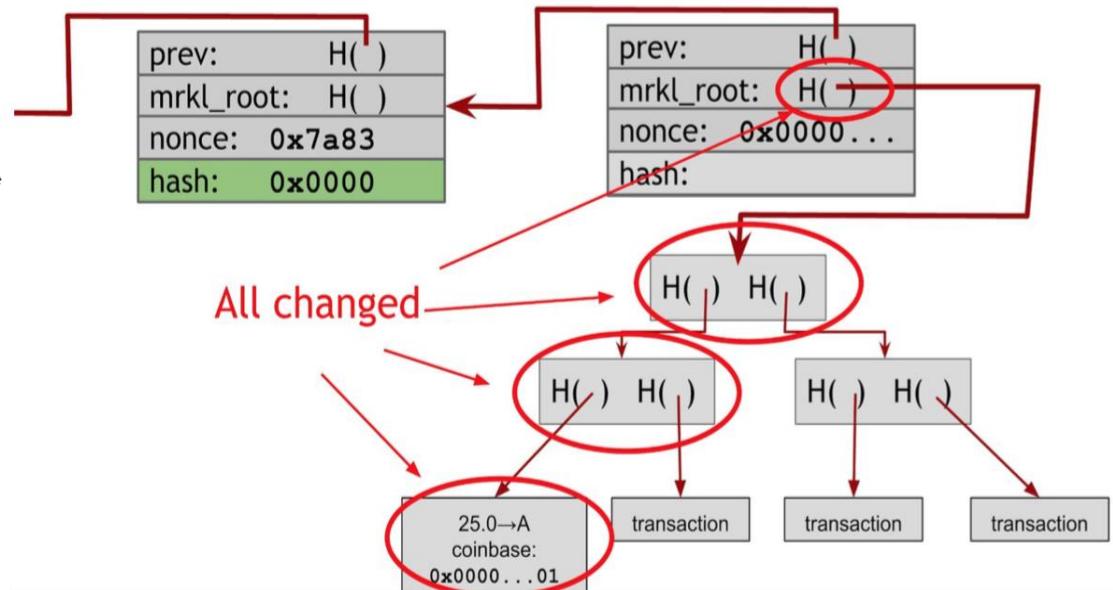
输出显示: "此金额可由  
1)<pubKey>哈希来解决<  
pubkeyhash? >  
2) 加上一个<sig>从业主的  
<pubKey>  
这将使这个脚本评估到真."



# 默克树-比特币建设

如果没有解决办法呢?

- 块标头 nonce 为32位
  - 尝试所有组合需要多长时间?
  - $2^{32}/14\,000,000,000,000,000 = 0.00031$ 秒
  - 消耗 3260次/秒
- 因此, 必须更改默克根
  - 增量硬币开始, 然后再次运行块标头
  - 增加硬币基础的效率降低, 因为它必须传播到树上

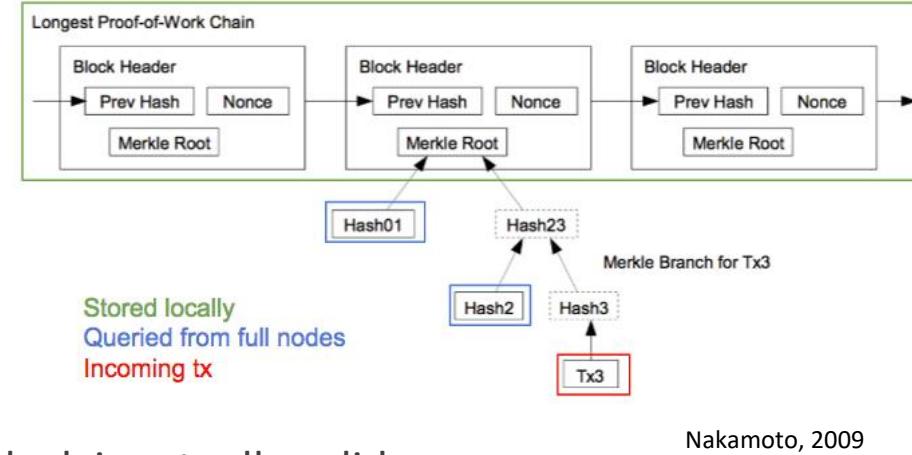


普林斯顿教科书

# SPV - Security Analysis

SPV nodes:

- Don't have full tx history, don't know UTXO set
- Don't have same level of security of full nodes
  - Can't check if every tx included in a block is actually valid

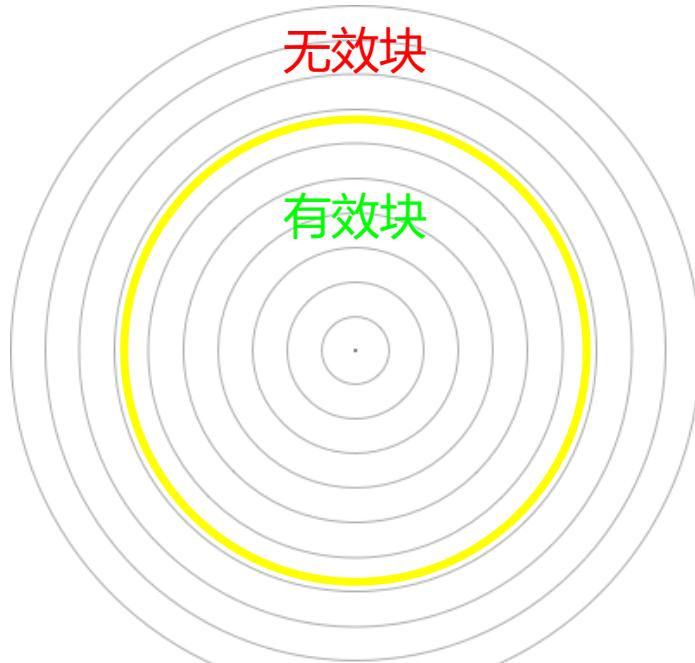


Nakamoto, 2009

SPV nodes assume:

- ...that incoming block headers aren't a false chain
  - Very expensive for attacks (or anyone) to create blocks
  - Not sustainable over the long term
- ...that there ARE full nodes out there validating all transactions
  - There are efficiency benefits and incentives to doing so
- ...that miners ensure that the transactions they include in their blocks are valid
  - Otherwise their blocks would be rejected by full nodes (very expensive mistake!)

# 块奖励:: 难度调整



$H(\text{Nonce} || \text{昨日散列} || \text{Tx} || \text{Tx} || \dots || \text{Tx}) < \text{目标}$

- 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)

# 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

# 抗日药: 斯凯特

斯库尔特是一个哈希函数。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 leecoin、dogecoin 使用

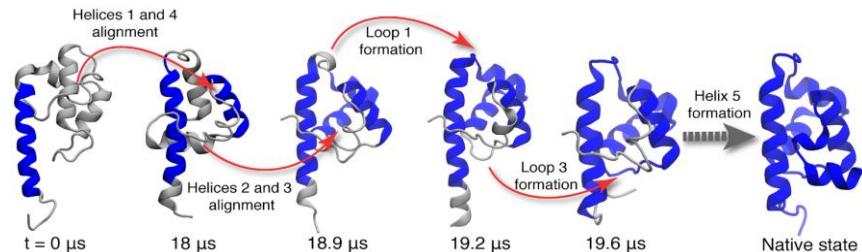


# 有用的工作证明

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
- 原子级模拟
- 蛋白质折叠研究
- 疾病
- 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



# Proof of Storage

## Permacoin

- Find some large file
  - Important, public, and in need of replication
  - Something that not any individual can store
  - Ex. Experimental data from Large Hadron Collider is several hundred Petabytes
- Store file in blocks, in a Merkle tree
  - Network agrees on the Merkle Root
- Miner stores a subset of blocks of T, based off of their public key
  - Continuously hash consensus information with nonce to pick blocks in their stored subset
  - Hash the picked blocks together, must be below some target value
  - Ensures storage, since querying network at every nonce increment is extremely inefficient
- Drawbacks: Hard to find large file, to change difficulty, to modify file

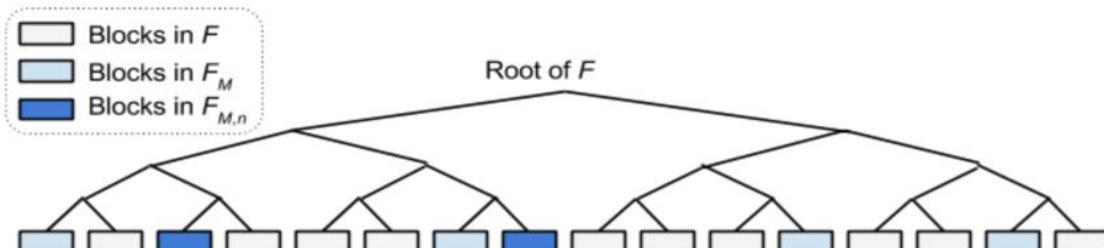
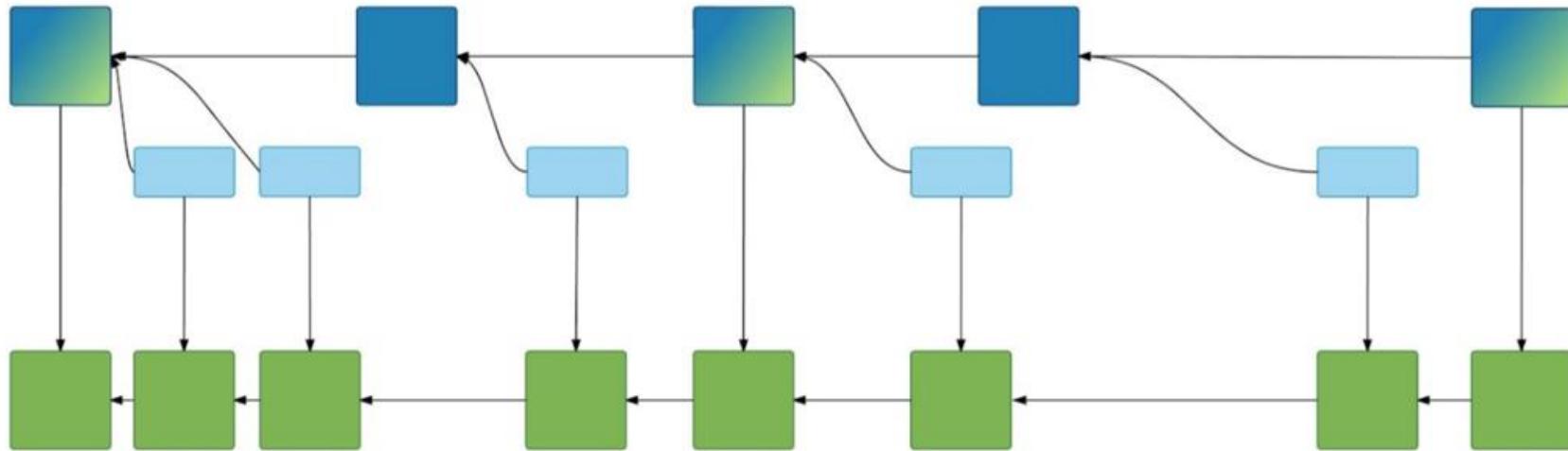


Figure 8.4: Choosing random blocks in a file in Permacoin.  
In this example  $k_1=6$  and  $k_2=2$ . In a real implementation these parameters would be much larger.

Princeton Textbook, Permacoin



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

# 备选共识

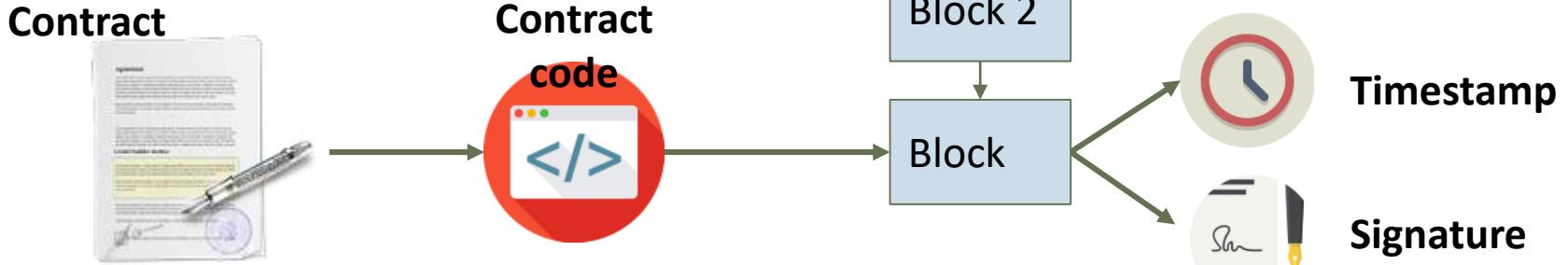
## 活动证明 (poa)

- pos 和 pow 之间的混合。使用 pow 机制作为块创建的检查点。
- 块是通过 pow 方法生成的, 具有 pos 类型的签名来验证块。
- 只是个理论, 一点发展。

# Smart Contracts & Property

*“Smart contracts as **smart contract code**”*

- (a) Expressing Business logic as a computer program
- (b) Representing the events which trigger that logic as message to program
- (c) Using digital signatures to prove who sent the message
- (d) putting all above on the Blockchain



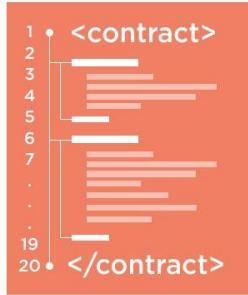
**Blockchain**



Block 1

Block 2

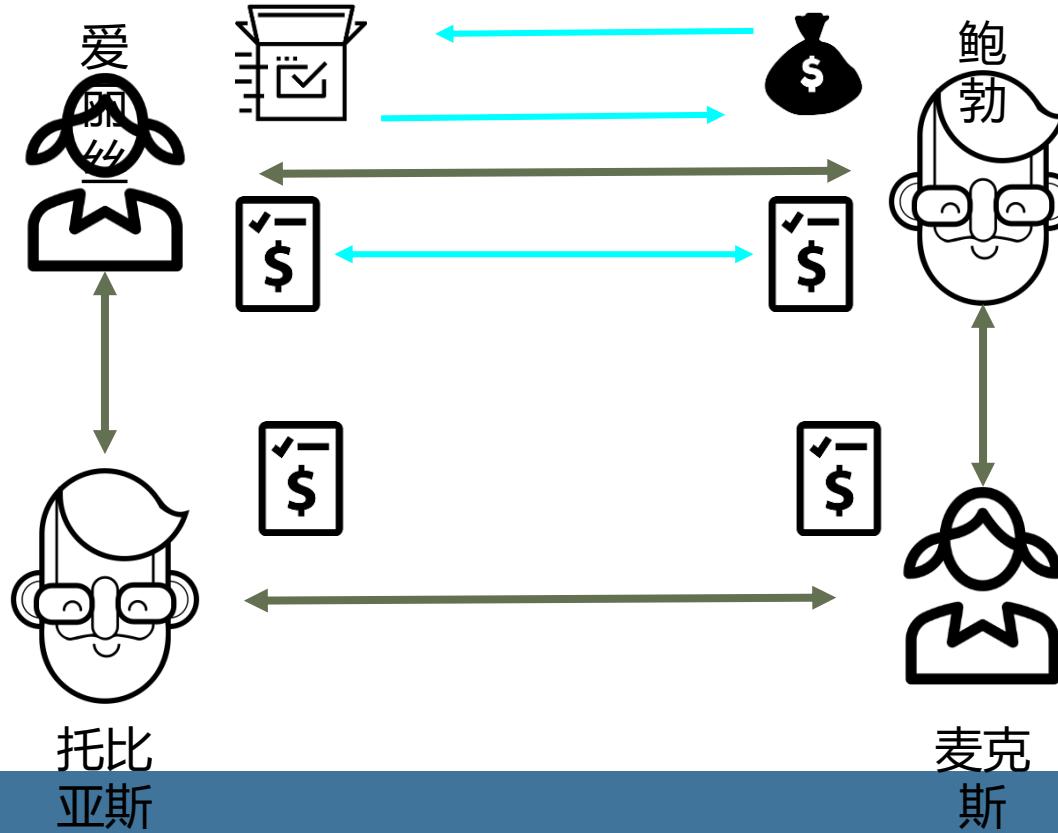
Block



**Timestamp**

**Signature**

# 智能联系人-示例



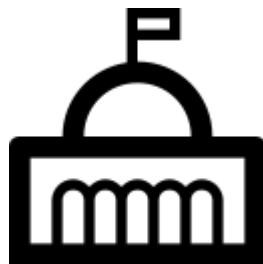
# 应用

我们所说的企业封锁是什么意思？



## 医疗

- 患者注册
- 假药
- 医学研究数据



## 政府

- 身份证注册
- 纳税



## 金融和投资

- 交易
- 债券
- 商品交易
- 内部交易记录

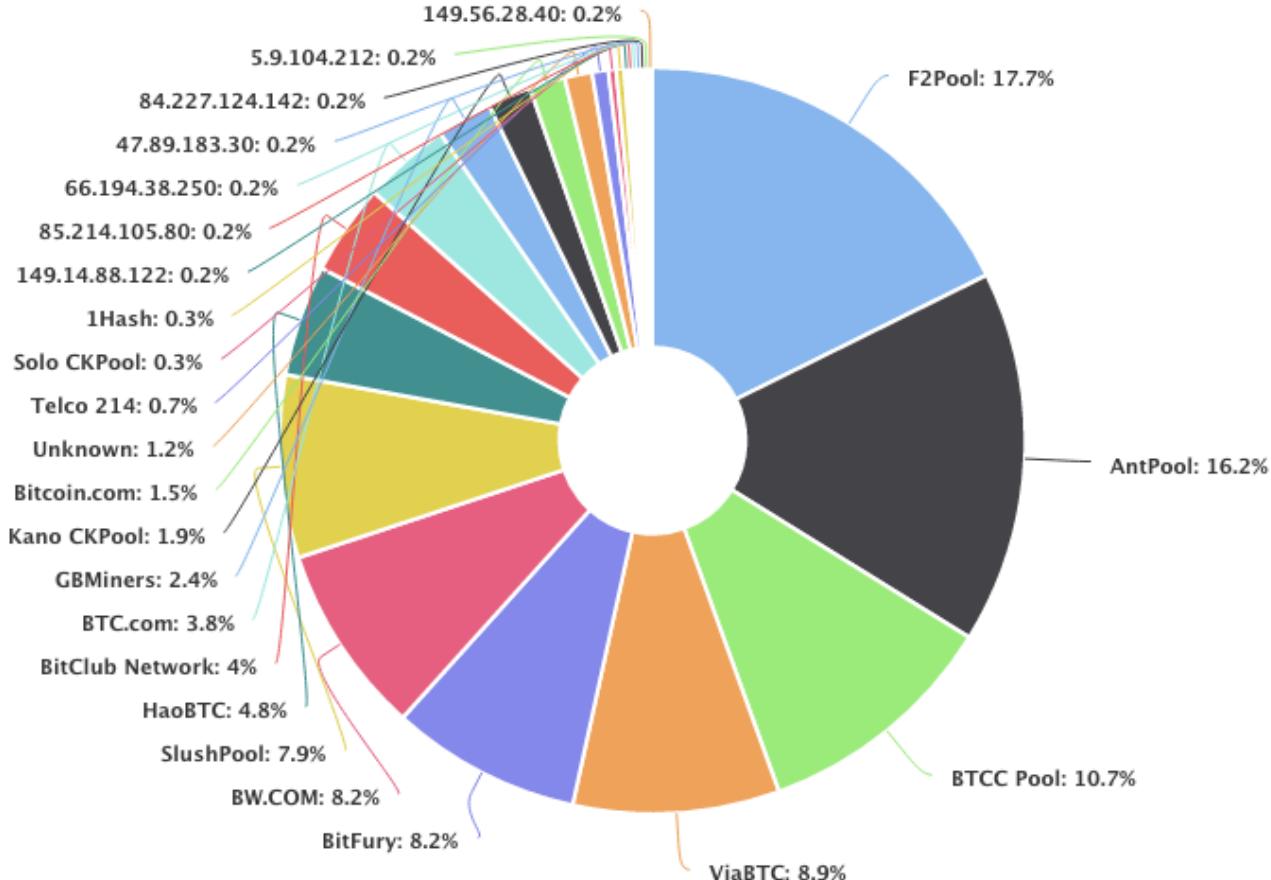
# 挖掘池哈希率分布

社区对大型采矿池表现出强烈不满

- 例如: 2014年的 ghashh. io

单个实体可能参与了多个池

- 所谓的 "清洗清洗"
- 采矿硬件控制的实际集中度是未知的

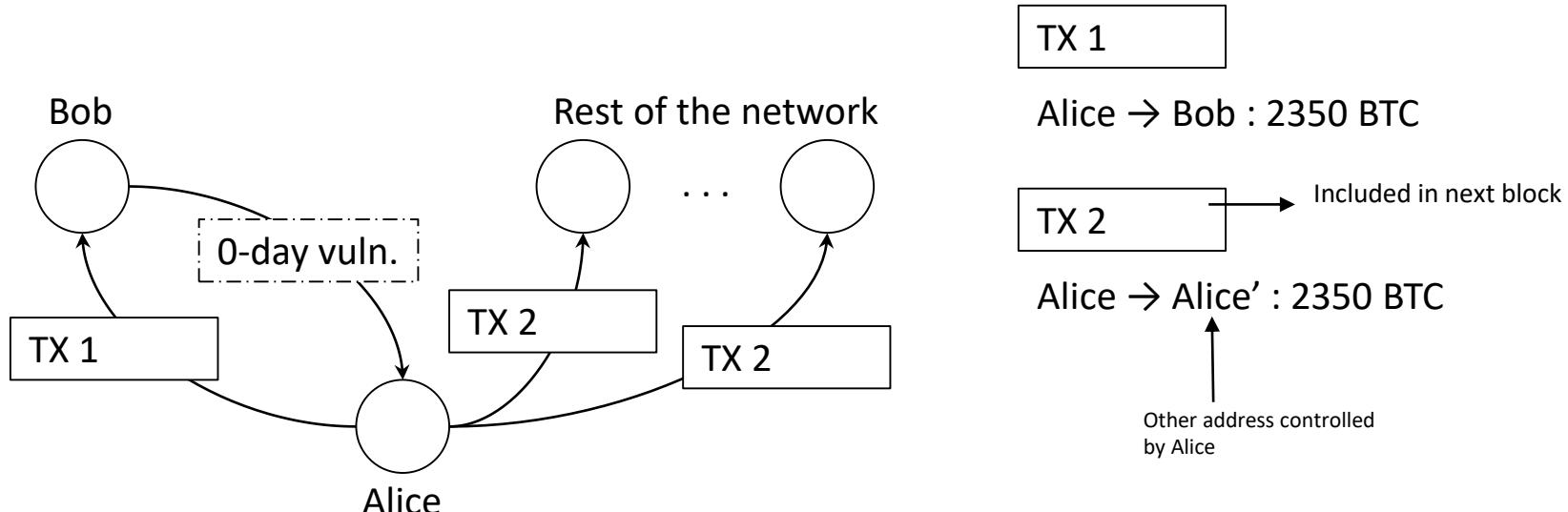


Name	Location	Size <sup>[1]</sup>	Merged Mining <sup>[2]</sup>	Reward Type	Transaction fees	PPS Fee	Other Fee	Stratum	GBT	Launched	Variance	Forum	Website
AntPool	China	Large	No	PPLNS & PPS	kept by pool	2.5%	0%	Yes	No	?	?	<a href="#">link ↗</a>	<a href="#">link ↗</a>
BTC.com Pool	China	Medium	Yes	PPS	kept by pool	1.5%	0%	Yes	No	2016-09-13	?	?	<a href="#">link ↗</a>
BCMonster.com		Small	No	PPLNS	shared		0.5%	Yes	No	2016-01-13	Dynamic	<a href="#">link ↗</a>	<a href="#">link ↗</a>
BitcoinAffiliateNetwork		?	NMC, DOGE	?	kept by pool	?	?	Yes		2014-07-15	User/Dynamic	<a href="#">link ↗</a>	<a href="#">link ↗</a>
Slush's pool (mining.bitcoin.cz)	Global	Medium	No	Score	shared		2%	Yes	No	2010-11-27	User <sup>[3]</sup>	<a href="#">link ↗</a>	<a href="#">link ↗</a>
BitMinter		Small	NMC	PPLNSG	shared		1%	Yes	No	2011-06-26	User <sup>[3]</sup> /Dynamic	<a href="#">link ↗</a>	<a href="#">link ↗</a>
BTCC Pool	China, Japan	Large	NMC	PPS	kept by pool	2.0%	0%	Yes	Yes	2014-10-21	Dynamic	?	<a href="#">link ↗</a>
BTCDig		Small	No	DGM	kept by pool		0%	Yes		2013-07-04	User <sup>[3]</sup> /Dynamic 20SPM	<a href="#">link ↗</a>	<a href="#">link ↗</a>
btcmp.com		Small	No	PPS	kept by pool	4%		Yes		2011-06-28	Diff 1		<a href="#">link ↗</a>
BW Mining	China	Medium	?	PPLNS & PPS	?	?	?	Yes		?	?	?	<a href="#">link ↗</a>
CKPool		Medium	No	PPLNSG	shared		0.9%	Yes	No	2014-09-20	User <sup>[3]</sup> /Dynamic 18SPM	<a href="#">link ↗</a>	<a href="#">link ↗</a>
Eclipse Mining Consortium	Global	Small	No	DGM & PPS	kept by pool	5%	0%	Yes	Yes	2011-06-14	User <sup>[3]</sup> /Dynamic	<a href="#">link ↗</a>	<a href="#">link ↗</a>
Eligius		Small	NMC	CPPSRB	shared		0%	Yes	Yes	2011-04-27	Dynamic: 32 shares/m	<a href="#">link ↗</a>	<a href="#">link ↗</a>
F2Pool		Large	NMC, DOGE, HUC	PPS	kept by pool	3%		Yes	No	2013-05-05	Dynamic	<a href="#">link ↗</a>	<a href="#">link ↗</a>
GHash.IO		Small	NMC, IXC, Devcoin	PPLNS	shared		0%	Yes	No	2013-07-01	User <sup>[3]</sup>	<a href="#">link ↗</a>	<a href="#">link ↗</a>
Give Me COINS		Small	NMC	PPLNS	shared		0%	Yes	Yes	2013-08-12	Dynamic	<a href="#">link ↗</a>	<a href="#">link ↗</a>
Merge Mining Pool		Small	NMC, IXC, Devcoin	DGM	shared		1.5%	Yes	No	2012-01-08	User <sup>[3]</sup>	<a href="#">link ↗</a>	<a href="#">link ↗</a>
Multipool		Small	NMC	Score	shared		1.5%	Yes	No	2012-03-15	User	<a href="#">link ↗</a>	<a href="#">link ↗</a>
P2Pool	Global (p2p)	Small	Solo <sup>[4]</sup>	PPLNS	shared		0%	Yes	No	2011-06-17	User <sup>[3]</sup>	<a href="#">link ↗</a>	
PolMine		Small	NMC	SMPPS	shared		0%	Yes	Yes	2011-06-13	Dynamic/User	<a href="#">link ↗</a>	<a href="#">link ↗</a>

# Double Spend - (0)-confirmations Bob

Suppose Bob doesn't wait for **any** confirmations on Alice's transaction. He simply checks that the transaction is valid and **immediately** sends Alice the exploit.

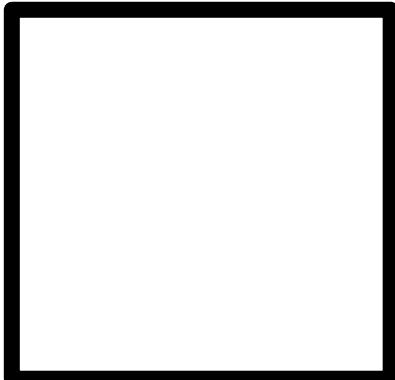
Bob is vulnerable to a **Race Attack!**



# 通过惩罚性伪造列入黑名单

你是一个对采矿池拥有管辖权的政府, 比如说中国。

**目的:** 例如, 检查某些人拥有的比特币地址加里·约翰逊, 并防止他们花他们的比特币



普通方块



中国矿工开采的区块



包含加里·约翰逊交易的块

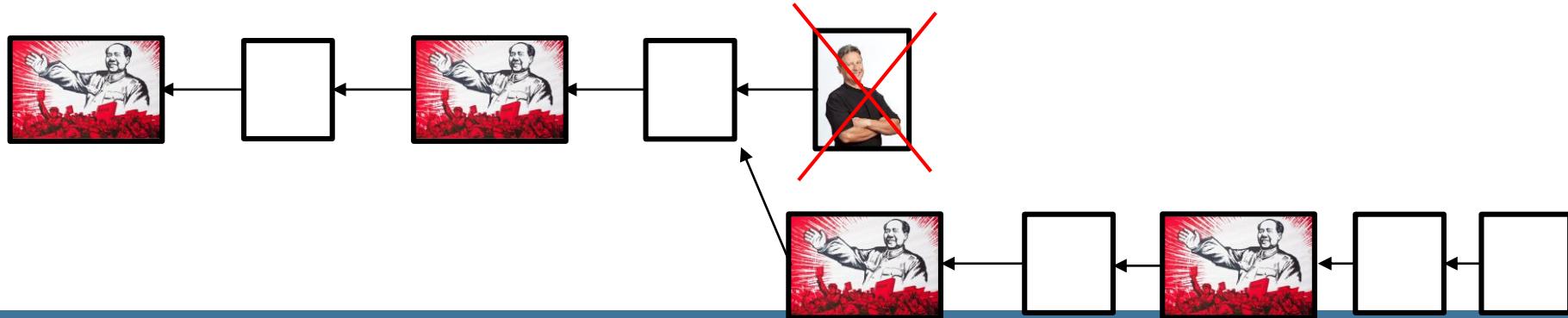
# 通过羽毛锻造列入黑名单

$ev(\text{包括}) = (1-\alpha^2) * \text{阻塞奖励} + \text{约翰逊的 tx 费用}$

$ev(\text{不包括}) = \text{阻塞奖励}$

因此,除非加里·约翰逊支付 $\alpha^2$ \*在他的交易费用奖励,其他矿工将矿山恶意链

- $4\% * 12.5 \text{ btc} = 0.5 \text{ btc} = \text{约翰逊必须支付\$31 \$31最小/交易}$



# 结合莱姆斯

外稃：

- lemma 1: 采矿奖励 = 采矿成本
- lemma 2: 收购51% 的成本 < 采矿成本
- lemma 3: 51% 攻击值 > 采矿奖励

**因此, 51% 攻击的价值 > 获取51% 的成本**

如果数学是正确的, 博弈论说51% 的人攻击比特币是有利可图的

(原由马丁·科佩尔曼在 sf 比特币开发公司研讨会上介绍)

# 所有帐户 == 网络状态

所有帐户的状态是 ethereum 网络的状态, 即整个网络在当前的平衡、存储状态、合同代码等方面是一致的。的每个账户.

网络状态将随每个块一起更新。您可以将块视为状态转换函数;它采用以前的状态并产生一个新的网络状态, 每个节点都必须同意。

帐户通过交易记录与网络、其他帐户、其他合同和合同状态交互。

# 智能合同

## 用例和分析

消毒处理

合同

主要担保合同

博客

自动共享经济

AD HOC MESH 网络

智能传感器

# 分散的预测市场



预测市场利用群众的智慧预测未来

- 做市商创造活动
  - 例如: "谁将赢得2016年美国总统选举"
  - 事件必须是公开的, 并且易于验证, 并设定了截止日期。
- 参与者购买股票特朗普或希拉里, 并支付少量费用
- 在选举日, 随机神谕在网络上投票谁赢了。
  - 与多数人投票的神谕收取一定的费用, 否则将受到处罚
- 正确投票的股东兑现了他们的赌注

每个市场的股价准确地代表了最好的事件发生的预测概率

- 某人有额外的信息 => 套利机会



# 分散共享经济

**斯特洛克。** : 可以通过支付直接打开的锁

- 所有者设置存款 + 价格
- renter 支付存款 + 价格到锁连接到 ethereum 节点
- 锁定检测付款并解锁自身

用例 (s解锁. it):

- 全自动空中客车公司公寓
  - 不需要满足业主的关键
- 按需租用无线网络路由器
- 全自动商店
  - 通过将商品的价格发送给持有货物的锁购买商品
- 自动自行车租赁服务



# Decentralized IoT

## Filament

- "Blockchain-based decentralized Internet of Things"
- "Ad hoc mesh networks of smart sensors"
- Intended for industrial IoT applications

## Product

- Sensors with 10 mile range
- battery lasts years
- no internet connection needed - uses mesh networking



## FILAMENT

### Technologies used:

- **Telehash** - end-to-end message encryption
- **TMesh** - self-forming radio mesh networks
- **Blockname** - private device discovery
  - Uses Bitcoin blockchain + public notaries to verify authenticity of name/address bindings
- **Blocklet** - smart contracts and microtransactions



### Exchange

Value can be exchanged between devices in the form of data, network access, currencies such as Bitcoin, compute cycles, contracts for ongoing service, trusted introductions to other devices, and more.

Filament is a great application of decentralized tech especially because of its emphasis on **resilience** and **dependability**.

# 智能合同与区块链技术的局限性

## 没有不可信赖的方式访问外部数据

- 必须依靠**神谕**从区块链外部提供信息
  - 问题。。。神谕必须得到信任
- 潜在的解决方案:**久经考验的执行(不受信任的神谕)**
  - 它有一个劣质的实现
    - tIsararary-修改 tIs 协议, 以提供接收页的加密证明
- 潜在的解决方案:**甲骨文网络对信息的投票**
  - 缺陷: 在协商一致议定书的基础上达成共识议定书
  - 难以协调激励/声誉

## 无法强制实施连锁支付

- 无法实施贷款和债券等金融产品
  - 资金必须存放在区块链上, 以确保付款
- 直觉: 部分由于违约风险, 我们支付贷款利息

## 合同无法操作机密数据

- 机密数据不能在其他人的计算机上组装
- 非常有限的访问控制功能
- 只能存储加密的数据并在本地解密
- 潜在解决方案: 同态加密

# 社区、政治和法规

---

# 社区

- 社区在哪里存在?
- 雷德特: r/bitcoin
- 像 bitcointalk.org 这样的论坛
- 比特币会议和会议



# 方块辩论

- 问题: 2015年, 比特币块开始填满
- 无法再处理事务量
- 在解决问题上存在巨大分歧
- 分散与集中



# Segregated Witness

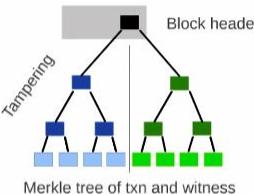
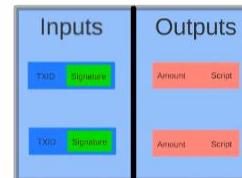
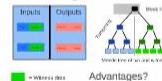
- Takes the signature out of the transaction, thus providing more room in the block
- Politics
- Bitcoin Unlimited and ViaBTC

## Segregated Witness redesign Bitcoin

Signatures are part of the hash

For now, just refers to the scriptSig in inputs  
Not part of a transaction's effect, only proving it  
was authorized.  
Multiple possible, but we just care that one exists.  
Such an example is called a witness.

Assume we can redesign Bitcoin from scratch?



Advantages?

Drop signatures from relay  
Prune old signatures

# 比特币 xt vs. 比特币核心

- 比特币 xt vs. 比特币核心
- 迈克·赫恩: "一个失败的项目"
- 红衣争议: 比特币审查 xt
- 不同的理念



# 反洗钱-反洗钱

反洗钱政策的目标是防止大量资金越过边界或在地下经济和合法经济之间流动,而不被发现。

目前正在遵守反洗钱规定:

位图-<https://www.bitstamp.net/aml-policy/>

bitfinex-<https://www.bitfinex.com/pages/tos>

cavirtex-[https://www.cavirtex.com/why\\_virtex#proactively\\_working](https://www.cavirtex.com/why_virtex#proactively_working)

硬币基地-<https://coinbase.com/legal/privacy>

克拉肯-<https://www.kraken.com/legal/aml>

加密-<https://cryptonit.net/regulations>

# 风险与 风险



Table 1.A: National risk assessment on money laundering

Thematic area	National risk assessment on money laundering					
	Total vulnerabilities score	Total likelihood score	Structural risk	Structural risk level	Risk with mitigation grading	Overall risk level
Banks	34	6	211	High	158	High
Accountancy service providers	14	9	120	High	90	High
Legal service providers	17	7	112	High	84	High
Money service businesses	18	7	119	High	71	Medium
Trust or company service providers	11	6	64	Medium	64	Medium
Estate agents	11	7	77	Medium	58	Medium
High value dealers	10	6	56	Low	42	Low
Retail betting (unregulated gambling)	10	5	48	Low	36	Low
Casinos (regulated gambling)	10	3	32	Low	24	Low
Cash	21	7	147	High	88	High
New payment methods (e-money)	10	6	60	Medium	45	Medium
Digital currencies	5	3	15	Low	11	Low

<http://www.coindesk.com/uk-treasury-digital-currencies-low-money-laundering-risk/>

# 争取隐私: 匿名技术、协议和阿尔特币

---

# "匿名只是用来买毒品的, 对吧? "

## 示例: 区块链上的企业

你刚刚在区块链上建立了一个热销的新创业公司--bitblockecinpayp。你想跟上你的竞争对手硬币。除了现在他们知道你所有的运营费用, 你有多少收入, 你的客户是谁, 以及你的秘密业务策略。

结论: 缺乏匿名性意味着和你交往过的每个人都能看到你过去和未来是如何花掉你的钱的。



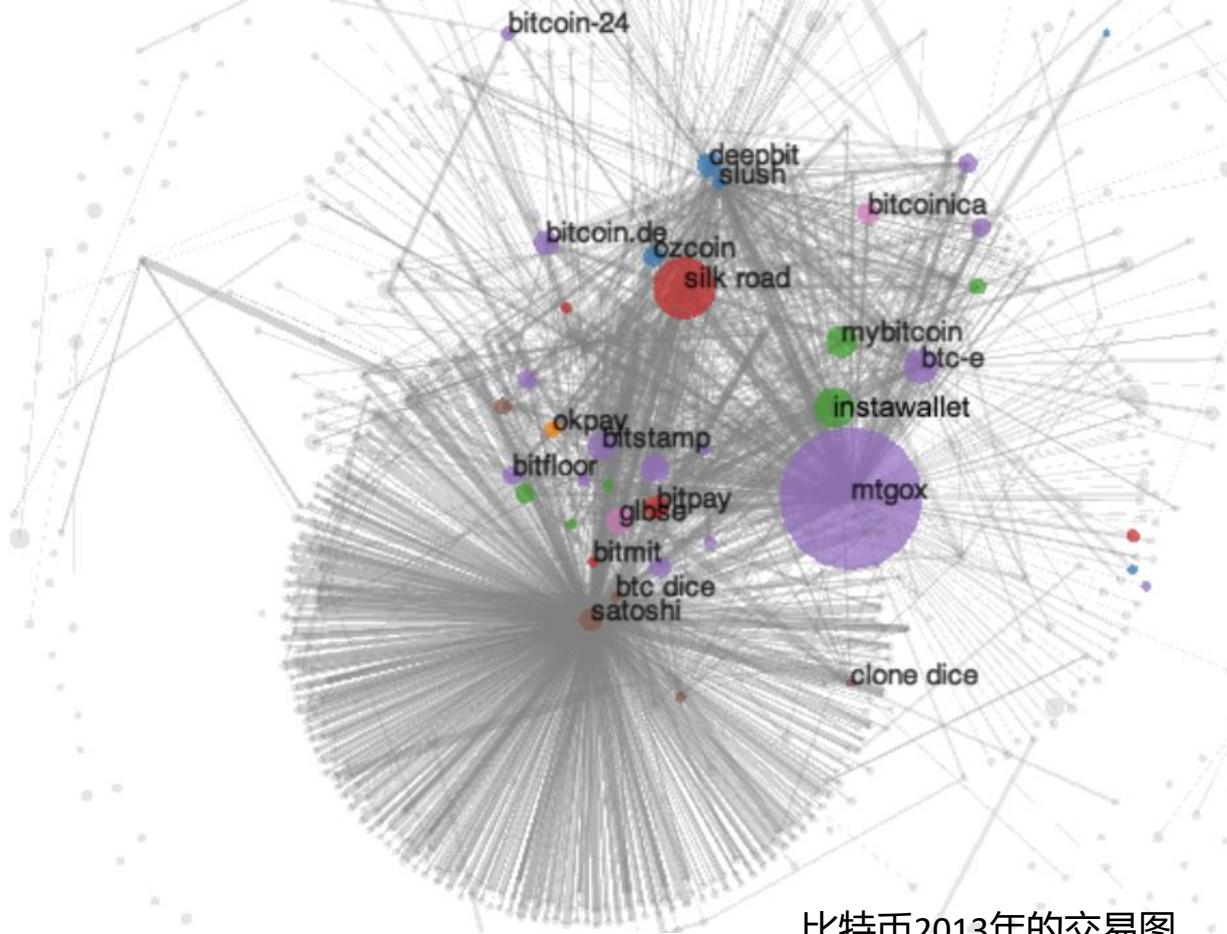
资料来源: 《科因电讯报》。

# 通过事务图分析进行匿名化

**交易图分析:** 分析区块链中的交易图表

匿名化的目标: **链接**一个实体的真实世界的身份与他们的化名

**聚类:** 属性集群到同一实体的地址



比特币2013年的交易图。

比特币: 无名字男子的报酬特征 (Meiklejohn 等人)

# 古色古香分析

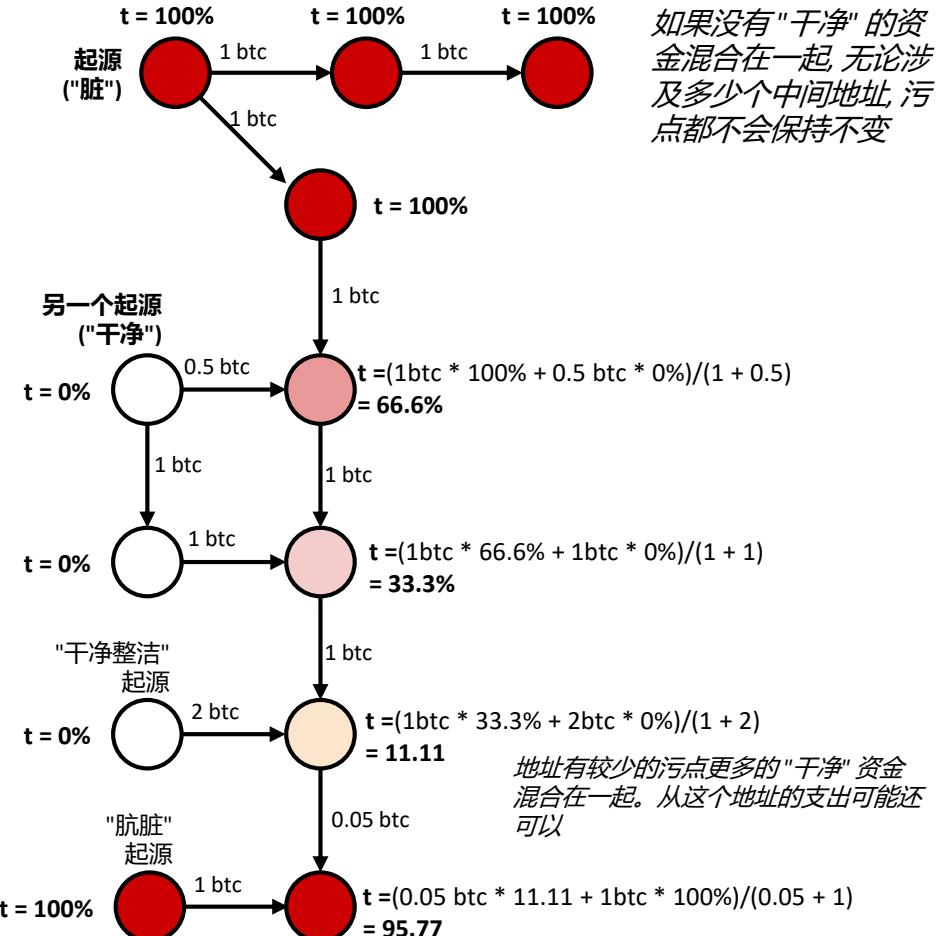
每个圆圈都是一个地址。  
让 $t$ 表示该地址的 "污点"。

污点是一个地址收到的资金的百分比, 可以追溯到另一个地址

古色古香分析可以揭示有用的信息

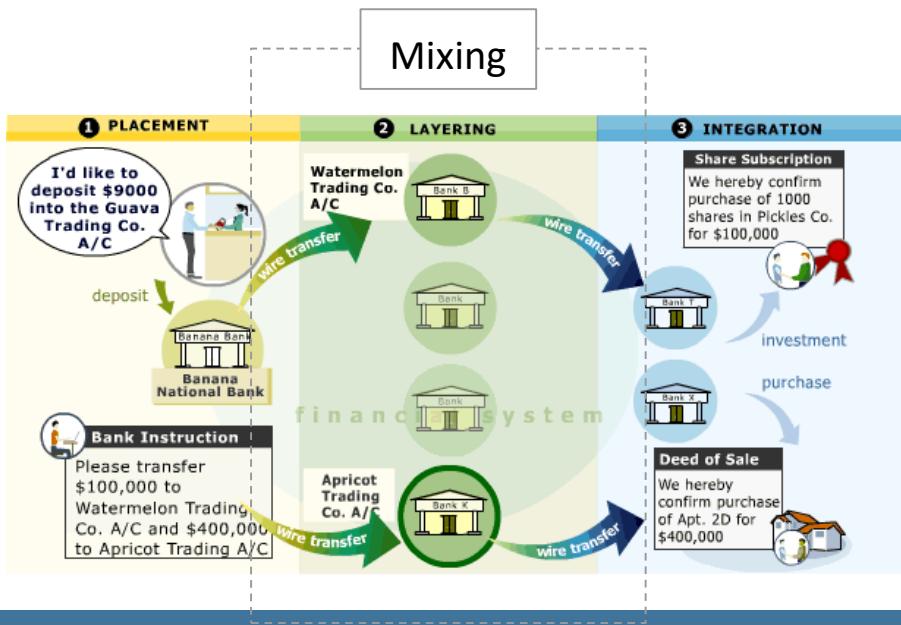
- 看看钱是否来自 "被污染" 的来源
- 示例: 标记已知的 "坏" 地址
  - 例如丝绸之路
  - 古色古香的分析毁了罗斯·乌尔布里希特的辩护, 他巨大的比特币藏品是合法获得的!

天真的匿名策略: 将您所有的硬币发送到一堆新鲜的地址 (**手动混合**). 张力分析是为什么手动混合不工作!



# Mixing

**Mixing:** Making transactions with the intention of concealing the origins of your funds.



## Traditional Mixing / Money Laundering:

Create hundreds of fake “shell” companies, which don’t do anything or own any assets, but *look* like they do (according to the accounting books and tax returns).

Over time, deposit “dirty” funds into shell corps. (Placement).

Shell corps. write off deposits as purchases, investment, etc... to make deposits look real.

Shell corps. further obfuscate by sending funds to *other* shell corps (Layering).

Finally, criminal org. spends “clean” money on luxury goods, e.g., diamonds, cars, real estate (Integration).

**Mixing on blockchains harness the same idea.**

# 匿名的正式框架

Def。一个**匿名集**是一组假名, 其中一个实体不能与她的对应

**混合的主要目标:**

- 我们希望我们的匿名性尽可能大
  - 进行多轮混合呈指数级增加我们的匿名集
  - 如果一轮的混合使你之间无法区分 $n$ 对等, 则匿名集的大小是 $n$ 一轮,  $n^2$ 两轮后 $n^3$ 个三之后, 等等。
  - 但是, 匿名集的大小受现实世界约束的限制

匿名集越大, 就越难将假名或 "重新链接" 到身份。

- 理想情况下, 这是很难**任何人**将标识链接到地址

**其他所需属性**

- **无信(无交易对手风险)**
  - 希望确保我们的资金不能在混合过程中被盗
- **可合理否认**
  - 从事务历史记录和您混合的任何其他数据跟踪中, 不应该很明显; 即你的活动应该看起来像正常的活动

# 集中式混合器

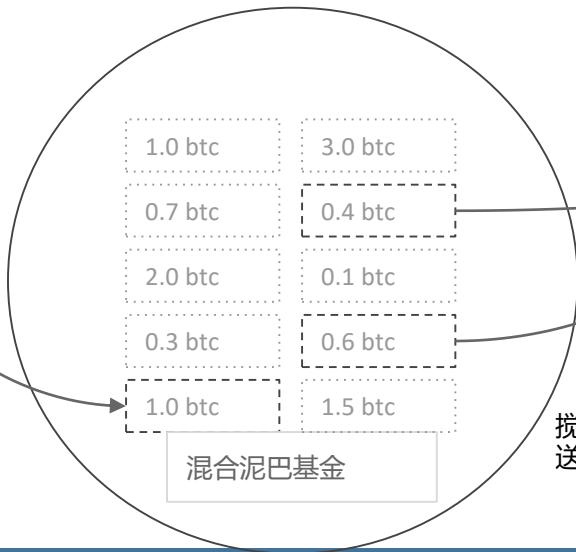
发送硬币到第三方混频器地址, 混频器发送(希望)未链接的硬币给你在不久的将来的某个时候(以尽量减少计时信息泄漏)。

集中混合服务

爱丽丝肮脏的输入

入

a 1 btc



搅拌机在随机等待后发送清洁资金

爱丽丝的清洁输出

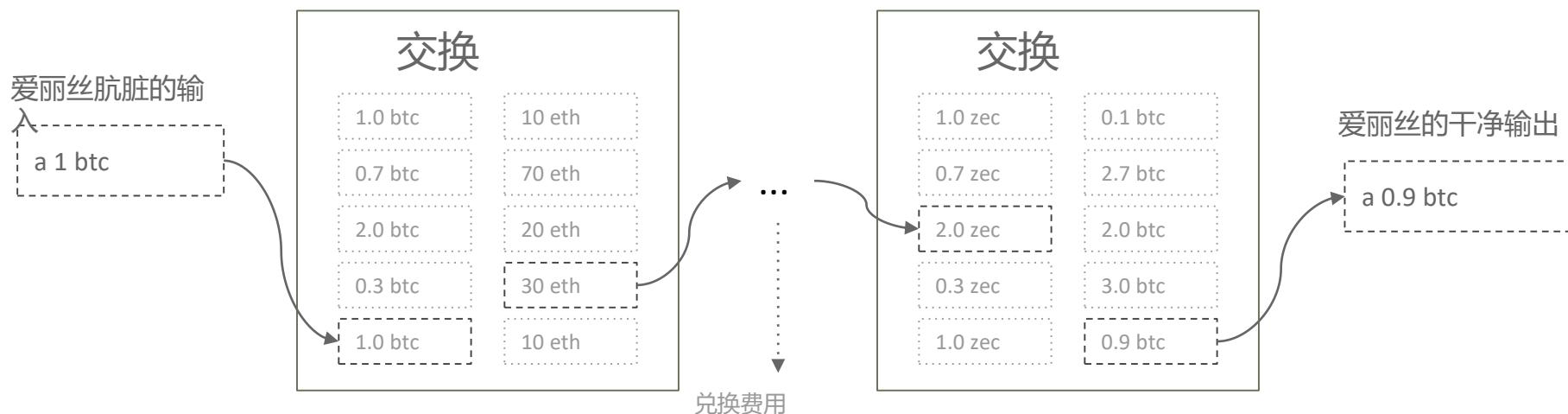
0.9 btc

m 0.1 btc

搅拌机的 "清洁" 费

# altcoin 交换混合

想法：通过几层祭坛硬币发送脏钱 altcoin 交换来混淆资金跟踪。



# zk-snark zcash

想法：交易显示的 altcoin 什么输出地址和输出值。

使用零知识简洁非互动的知识积累(zk-snark). a. a. "加密魔术", 我们可以创建一个系统, 支持完全匿名付款.



# Decentralized Mixing Protocols - Nuances

Additional considerations for designing a good decentralized mixing protocol

A mix is comprised of inputs and outputs:

- One input and one output are owned by the same entity, and the goal of the mix is to hide the **mapping** from all inputs to all outputs.

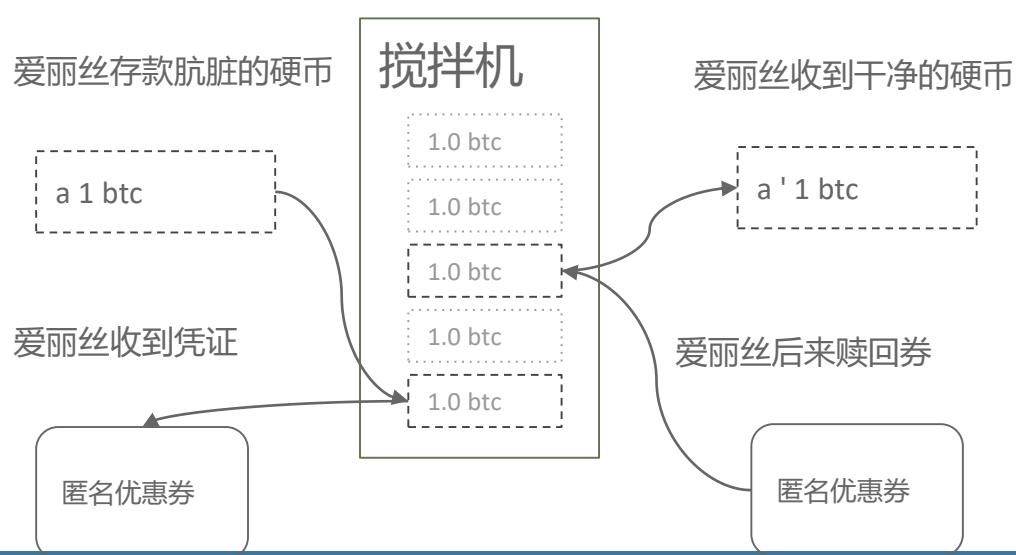
**Def. Correctness:** Coins must not be lost, stolen, or double-spent. The mixing is truly random and must eventually succeed in mixing or returning the funds of honest users (resilient against DoS attacks).

**Adversarial models:**

- **Passive adversary**
  - Not a part of the mix
  - Basic anonymity prevents passive adversaries from learning the mapping
- **Semi-honest adversary**
  - Part of the mix
  - Correctly follows the protocol but attempts to deanonymize the mix by analyzing the procedures of the mix.
- **Malicious adversary**
  - Part of the mix
  - Not bound by the protocol specifications; may actively deviate from the protocol and attempt to steal funds
  - May send false messages, abstain communications, etc.

# 协议-tumblebit (2016年)

想法：改进硬币交换，使混频器不能偷资金和永远不知道谁接受干净的资金。



区块链上总共需要2个交易记录。

匿名凭证不能区分开来，也不能伪造。

使爱丽丝存款她的脏硬币，并收到干净的，未链接的硬币，而不透露自己。

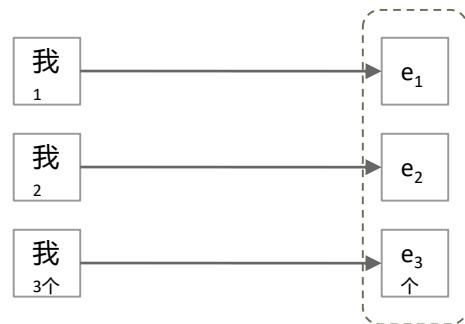
不只限于单混频器。可在更复杂的协议中用作基元

收款人不必是存款人。

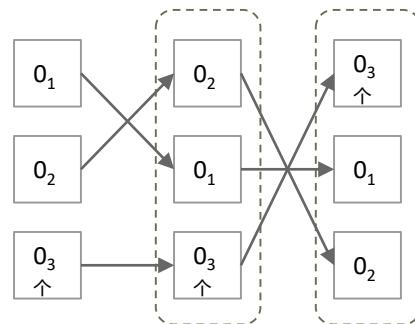
# 议定书----缔约方(2015年、2016年)

我	输入地址
e	托管地址
0	输出地址

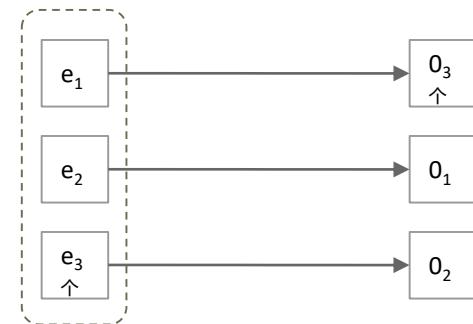
对等方生成托管地址。托管地址需要 2/共识才能使用。



对等方对输出地址排序执行安全的多方洗牌。  
。



如果协议执行正确, 同行同意将资金从托管地址转移到指定的输出。



1 承诺

2 洗牌

3个 交易

# Dmix "Swinger Protocol" & Project Conclusion

The last iteration of Dmix project: **Swinger Protocol**

- Form pairs with your mixing group, designate one as the "husband" and the other as the "wife"
- Execute a decryption mixnet pairwise to obviously obtain a designated pair that your pair shall swap with.
- Your "wife" is sent over to the designated husband. They perform CoinSwap to trustless exchange coins
- 你是另一对的指定一对;你会收到那对的新妻子  
你丈夫和即将上任的妻子一起表演硬币交换。
- 如果没有收到妻子或一个以上的妻子, 则中止协议。

当前存在的任何内容都不符合为 dmix 项目  
设计的设计目标

- 与简单地使用 dmix 网络上的随机节点执行硬币交换的天真混合策略相比, swinger 协议接近, 但匿名度较低
- 实际上形成混合基团减少自 sybils 以来设置的匿名

结论: 构建一个良好的分散比特币混频器是  
**该死的硬**.

# 缩放比特币： 面向大众的加密货币

---

# 隔离证人

**想法：**每个事务的数字签名在每个块中占用了大量空间。他们没有理由需要在那里。让我们删除它们。

**如何：**

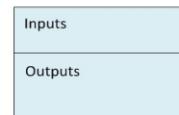
Segwit P2W\*

For Old Nodes:

ScriptPubKey: 0 e4873ef43eac347471dd94bc899c51b395a509a5

ScriptSig: Empty

Result: **Valid**



Segwit P2W\*

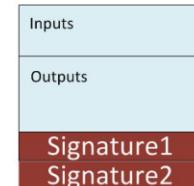
For New Nodes:

ScriptPubKey: 0 e4873ef43eac347471dd94bc899c51b395a509a5

ScriptSig: Empty

WitScript: **Signature1**

Result: **Valid**



# 施诺尔多签名

**想法：**不要要求每个成员的签名，而是将它们组合在一起，只有一个签名

**优点：**

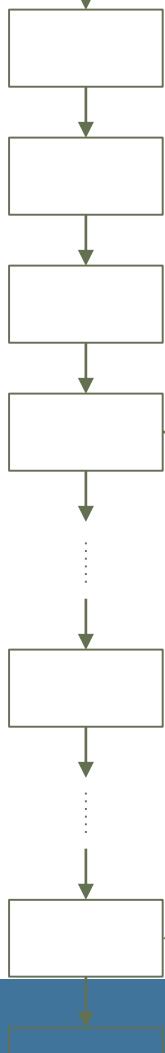
- 可使用软叉或硬叉（硬叉清洗剂）实现
- 多 sig 事务将明显变小
- 更快的验证
- 对参与者的可诉否认

**为什么它没有被实施？**

当比特币刚出来的时候，ecdsa 是最受欢迎的，因为 schnorrs 仍然受到专利保护。已经不是了各方面都好多了。只是需要有人来实现它。

额外的人信用吗？

# 布洛克链



爱丽丝和鲍勃只做一笔交易在区块链上  
当他们想解决他们的私人余额。

爱丽丝和鲍勃打开私人资产负债表

爱丽丝和鲍勃的资产负债表

爱丽丝	鲍勃
10 btc	0 btc

爱丽丝和鲍勃做了几个私人的 txns。

爱丽丝和鲍勃的资产负债表

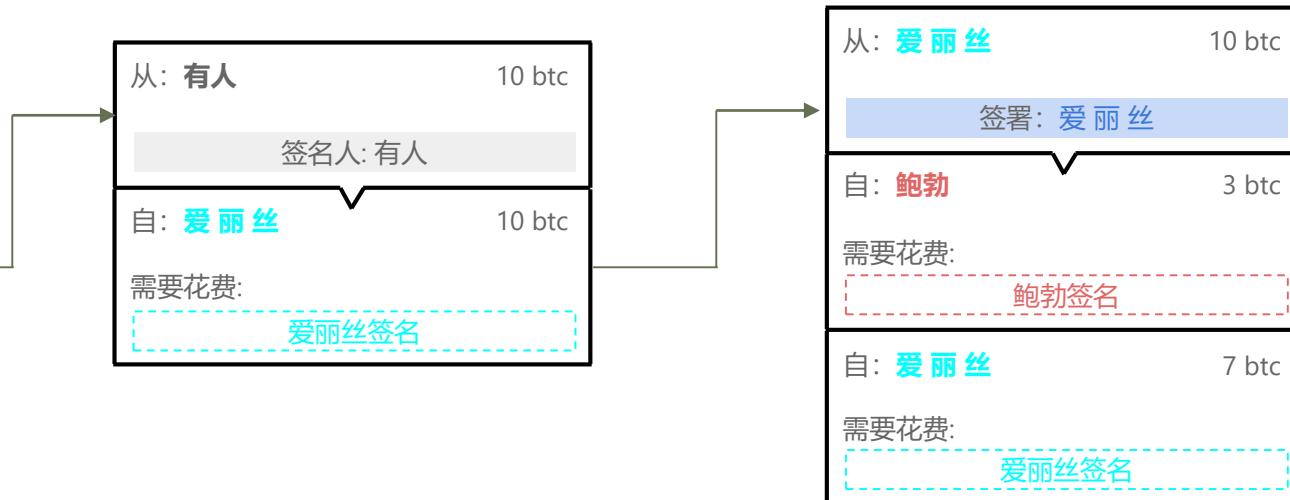
爱丽丝	鲍勃
3 btc	7 btc

爱丽丝和鲍勃后来关闭了资产负债表

# 哈希时锁定双向支付渠道

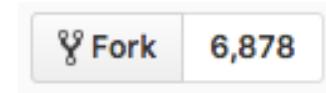
简单地说，一些符号：

- + alice 花费了 10 btc txn 的输出
- + 爱丽丝发送 3 btc 鲍勃和 7 btc 回到自己。



# "开发加密货币"

- 答: 转到[githubi.com/bitco/bitcoin](https://githubi.com/bitco/bitcoin)并按下
  - 接下来, 旋转一些节点。瞧!
  - "比特币和建筑公司之间的差异可以显示在一张幻灯片上"



"z-arcash mpc 安全协议"

"我认为我们应该专注于非区块链分散技术"

# 分散声誉

最终方法:信任网络模型

- 只接受你信任的人的评价
  - **买方自愿披露他们的 guid 而不是使用假名**
- 定义一个学位网络n, 这就是你的信任网。
  - 朋友 (n意思 1)? 朋友的朋友 (n= 2)?

三种主要变体:

1. "zindros":创建 guid 的刻录证明
2. **信用额度**:信托以提供给该用户的信贷额度衡量
  - 用户可以随时取款



- **信任网模型是:**
  - 适用于检测所有被认为信誉良好的可疑用户群
  - 但仍然无法区分真实和虚假的收视率。仍然不抵抗西比尔

## 结论

要么假名不是匿名的, 要么分散的声誉是毫无意义的。

openbazaar: "说白了, 没有一个声誉系统能抵制供应商购买自己的商品, 做出虚假的肯定评级。

# ipfs

请求：“我认为我们应该专注于非区块链分散技术”

## ipfs:我恩特P拉内特F伊莱s系统

- 每个文件都由其哈希唯一标识
  - 文件查找: 查找哈希到的文件H
- 删除网络上的重复
- 跟踪每个文件的版本历史记录
- 网络节点仅存储它感兴趣的内容

## 分布式技术的基础

- 分布式哈希表 (dhts), 有效维护有关对等方的元数据
- bittorrent: 协调不信任的对等方 (群人), 以合作向彼此分发文件
- git: 文件的版本控制
  - 构建在 merkle dag 数据结构之上: 不需要平衡, 非叶节点包含数据
- 自认证文件系统 (sfs):
  - "分布式信任链"
  - "平等共享的全球命名空间"
  - 基本上分散的 dns
    - 但可能过于简化

# 锌参数生成

## 锌参数生成仪式

- 6 "证人" (与会者)
  - 其中3人在仪式开始时就知道了
  - 其中1人仍不知道
- 整个过程的录音记录
- 仪式细节保密, 直到仪式已经完成

记得只有一个参与者需要成功地销毁他们的私钥,  
以确保参数生成的安全

## "计算节点": 用于生成随机数的计算机

- 专为仪式购买
  - 仪式结束后, 通过丙烷火炬被摧毁
- 计算节点是气隙
  - 所有的计算机都是身体无法进行网络连接
  - wifi 和蓝牙组件在打开之前从计算机上剥离
- 删除了任何可能的攻击通过网络
  - ...但如何与互联网沟通呢?

# fut高中

## 设置和房地

- 区分幸福的富裕国家和不幸的贫穷国家并不难
- 民主国家在很大程度上未能通过汇总现有信息而失败
  - 贫穷的民主国家往往采取愚蠢的政策来伤害每一个人
  - 但这并不是说没有聪明的人不赞成这些愚蠢的政策
  - 相关专家只是被忽略了
- 不能只是让相关专家上台
  - 因为那时他们开始为自己的利益行事, 将不再是相关专家"

建议的解决办法:fut高中

fut高中是经济哲学家罗宾·汉森提出的一种政府形式

- 利用民主就经济目标和目的达成一致
  - 但要利用预测市场来确定哪些政策要实际实施
  - "投票价值观, 投注信念"
- 预测市场是最著名的聚合信息方式
- 在政策上有发言权需要财政承诺
  - "把你的钱放在嘴边"
  - 用汉森的话说: "知道自己什么都不知道的专家闭嘴, 不知道自己什么都没丢, 然后闭嘴"

目前尚不清楚未来政府能否通过封锁实施

# 机密价值

**想法：**修改比特币交易以隐藏输入和输出值，以便只有交易发送方和接收方知道这些值。

检查区块链的每个人都可以验证正确性，但不学习值。

不隐藏发送方和接收方的假名！

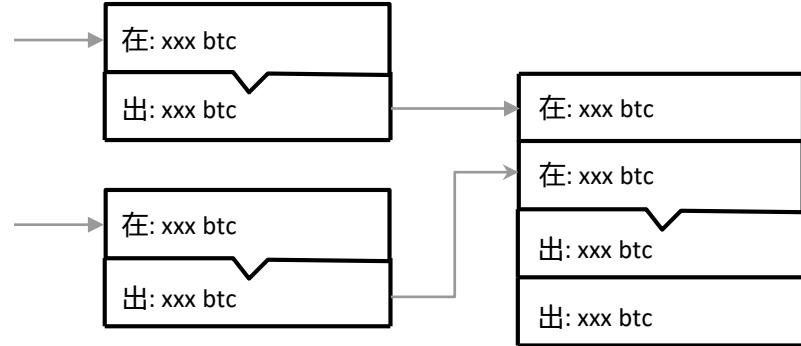


图1:输入和输出值隐藏给其他用户。

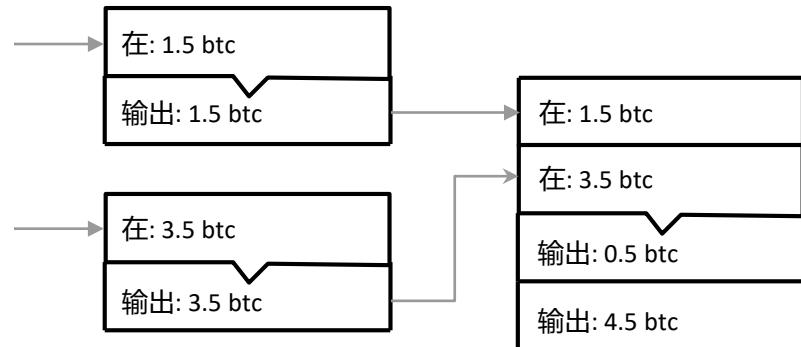


图2:输入和输出值仅向事务发件人和收件人显示。

# 彼得森承诺

彼得森承诺是如何工作的? --他们使用椭圆曲线密码学!

假设一些公共生成点,  $g, h$ , 主要订单等..。

$$c(x, r) = x * g + r * h$$

$$C(x_1, r_1) + C(x_2, r_1) = (x_1 \cdot G + r_1 \cdot H) + (x_2 \cdot G + r_2 \cdot H)$$

$$= (x_1 \cdot G + x_2 \cdot G) + (r_1 \cdot H + r_2 \cdot H)$$

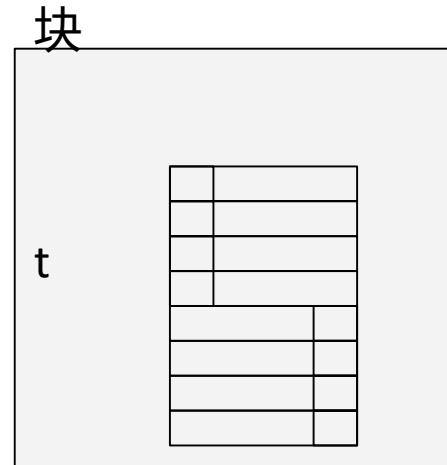
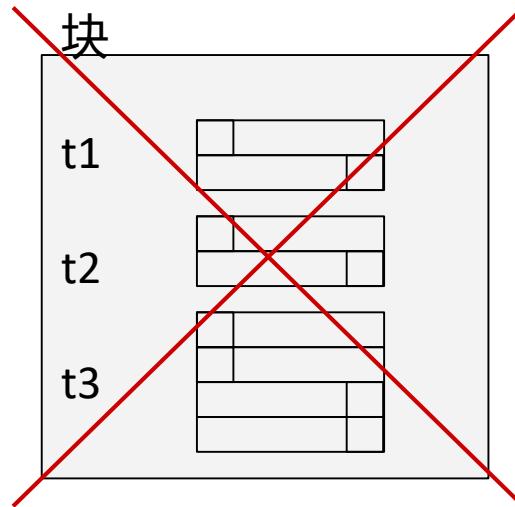
$$= (x_1 + x_2) \cdot G + (r_1 + r_2) \cdot H$$

$$= C(x_1 + x_2, r_1 + r_1)$$

# 毫米波

**酷理念:**一旦一个承诺被花掉了,它是无用的。我们也不再需要地址了。我们能通过利用这些信息来节省大量空间吗?

- + mimblewimble 提出了一个叫做“块合并”
- + 如果我们把一个块看作是一个事务的集合,而是一个单个交易记录,有大量的输入和输出?
- + 就像一个非交互式的硬币加入跨一个块中的所有事务!



# 概率支付

比特币目前不支持小额支付

- \$1 = 135000 萨托西
- 小额支付为  $\$10^{-6} = 0.135$  satoshi
  - 比特币区块链上不能有子 satoshi 金额
  - 因此比特币在技术上不支持小额支付
    - 得到雷克特
- "我不能付你一半的钱"
  - "但我可以付给你一个概率0.5 的佐藤"
  - 随着时间的推移平均输出

## 概率支付草图

- 两个党无爱的蛋糕切割问题
  - 一个人把蛋糕分开, 另一个人选择拿哪一块
- 分频器选择哈希预映像的长度
- 将哈希发送到选择器
- 选择器根据哈希猜测前图像长度
- 选择器猜测错=> 得到 satoshi
  - 否则什么都得不到

进一步探索:视频:闪电网络作为定向图单基金信道网络 topology.mp4

# 闪电网络洋葱路由

基本理念: 使用闪电网络的方式, 可以匿名您的付款

- 假设从 a 点路由付款
- 中间节点 b 和 c 不知道源或目标

基本理念:

- 使用  $\text{pubkey}_D$ ,  $\text{pubkey}_C$ ,  $\text{pubkey}_B$ , 发送到 b
  - b 解密, 看到消息应该去 c
  - c 解密, 看到消息应该去 d (但不知道它是目的地)
  - d 解密并接收付款

结论：

由区块驱动的未来

---

# 链式近视中的一天

## ● 分散的声誉

- 在这个世界上,一切都在封锁上..... 包括地球上每个人的全球声誉得分。有人对你好,你可以上投票他们的声誉。如果他们是一个家伙给你,你可以下投票他们,鼓励一个社会充满善良和富有同情心的人喜欢自己。不幸的是,邪恶的夏娃嫉妒你可以轻松地在谷歌获得实习,帕兰蒂奥尔和科因基地因为你的高声誉得分。夏娃意识到分散的声誉并没有抵御西比尔,并对你发起诽谤攻击。在你的余生里,你接触过的每一个人都会立即被告知你是性犯罪者,你的余生都找不到工作。

## ● 身份盗窃

- 至少你从那些实习中赚了很多钱,对吧? 你有你的普遍基本收入启动-啊,你还记得你这个月还没有收到你的付款。当你打开支付门户时,你会发现你的钱不见了!哦不!一定是有人泄露了你的私钥尽管你使用多西格与bitgo.不知何故,可疑的活动没有被抓到-它看起来像是因为bitgo自动签署一切 (btw, 这实际上发生与bitfinex).不用担心,既然所有的汇款都在封锁上,你可以检查是谁偷的..... 除了那些讨厌的东西混合人们最终实现了他们的摇摆协议,并建立了一个全球混合网络,所以现在区块链上的所有交易都是完全匿名的。
- 沮丧之下,你回家去挖掘你的积蓄zcash这些年你积累的东西至少这个私钥是安全的-为什么不花钱一点打开电视,在想办法的时候放松一下呢? 随着电视的打开,你的厨房电器突然开始站在机器人腿上走了出去。你的洗衣机和冰箱也是如此。困惑,你看着电视,看到屏幕上的紧急报告-1337年前,彼得·托德和每个人在zcash参数生成仪式串通,他们的机器人后代现在有能力打印无限数量的钱。作为自主的、自主的代理,您的设备会礼貌地通知您,他们将退出合同,为您寻求更好的未来收入zcash而不是比特币当你闭上眼睛的时候,你周围的空气充满了物联网连接设备的声音,这些设备来回移动,将自己融入到zcash资助的大规模杀伤性机器人,以带来彼得·托德的新世界秩序

# Tying it all together

Crypto/blockchain is a field that must be approached carefully

- Huge upsides...
- but many ways it can go wrong.

One of the most valuable instincts you can bring to the industry is a clear mindset for determining what blockchain is good for, and what it isn't.

# 区块链杀手应用程序的基本属性

dapp 可以被认为是客户端软件-没有中央经理

需要共识或协调的无信任环境(例如, 智能电网、能源市场)

以优先为中心的系统(例如社交网络?)

- 虽然数据不应该存储在区块链本身

可编程货币与开放集成

- 物联网,m2m付款, (例如 ibm adept)
- 易于发送和接收资金-无需个人信息
- 小额支付可能的 (例如勇敢的)

容错、有弹性的系统(例如长丝)

- 自主网络和设备

创建激励措施的新闻方法(例如, 灵知)

新的治理模式(例如 dao, futarchy)

非中介, 耐审查

对数学和代码的信任, 而不是机构

与集中化的对比:

深度集成, 有凝聚力的用户体验

- 效率-区块链一般都很慢
- 完全控制在数据和读写权限上

总是问: 为什么使用区块链比使用中央数据库更好?

# 课程考试

- 2小时
- 50个问题需要通过多种选择来回答
- 剪贴簿
  - 否用于携带 ppt 和其他读数
  - 英语是以中文词典可能是允许的
- 2019-1-11, 14:00-16:00



# 另一个示例：

使用闪电网络的方式，可以 \_ 您的付款

- a. 匿名
- b. 完成
- c. 控制
- d. 加密



# 考试前

- **通读课程资料**

- ppt, 注释, \*. doc

- **策略:**

- 自上而下, 分解...。

- **深入思考**

- 识别概念之间的差异

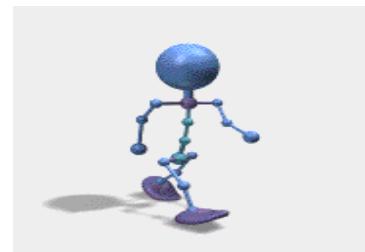
---

- **睡得好**

- 考试前不要过夜!

- **吃得好**

- 不要错过早餐午餐!



# *During the exam*

## --参加考试的策略

- **仔细阅读问题**

注意 "不"、"排除" 和 "除了" 等词

- **阅读所有答案**

一种方法是先阅读 "d"

- **Eliminate wrong choices**

Cross out choices that look incorrect

If you're still uncertain, circle the question and come back to it after you completed a first pass through the exam  
– don't waste time.

- **Use “Common Sense” and “Logical Thinking”**

There is NO magic puzzle

- **Choose the best answer**

More than one answer may be technically correct



# 考试后

- **记录仍然令人困惑的问题**

写下问题 id 和**关键词**

---

- **自我验证**

使用**关键词**

- **相互验证**

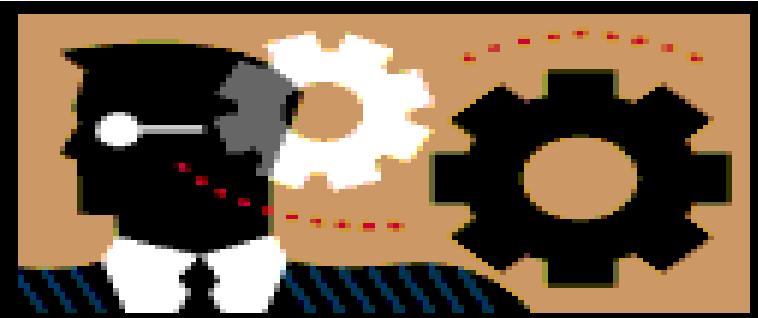
四处寻找正确的答案

- **进一步查询**

向教师发送带有问题索引号的电子邮件



# 祝你好运！



完

धन्यवाद

Hindi

Спасибо

Russian

شُكْرًا

Arabic

Grazie

Italian

நன்றி

Tamil

Tamil

多謝

Traditional Chinese

Thank You

English

多謝

Simplified Chinese

ありがとうございました

Japanese

Gracias

Spanish

Obrigado

Brazilian Portuguese

Danke

German

Merci

French

감사합니다

Korean