

# B锁链 匿名化

—争取隐私



# 讲座大纲

匿名基础知识

匿名化技术

通过混合匿名

分散混合

匿名 Altcoins

结论

# 匿名基础知识

# 默认情况下, 区块链不是匿名的

- 直觉: 区块链获取中央数据库并将其分发
  - 但是, 这意味着您现在没有访问控制
- 默认情况下, 所有数据都是公共的
  - 私有区块链略显匿名, 因为只有少数成员可以访问数据库

大多数区块链都是**假名**-我们使用的身份不是我们的真实身份 (例如您的比特币地址)

- 我们**假名**可能与我们的真实身份 "相关", 也可能不与我们的真实身份 "相关"

# 匿名化

"**链接**"在匿名的背景下, 将真实世界的身份与假名联系起来。这也称为**匿名化**

- 在比特币: 一个身份和一个**地址**
- 在以太: 一个身份和一个**帐户**

比特币最佳实践实现了一定程度的匿名性

- 最佳实践: 切勿重复使用您的假名!
  - 每次收到比特币时生成新地址
  - 就像为每一个评论创建一个新的红字账户
- 不可能在以太, 因为它是基于帐户的 (而不是基于 utxo 的)
- 但基本分析使这种技术无效

# 匿名程度

匿名不是绝对的 (不是是或不是)

- 中。"匿名程度"(或有时"匿名级别")的定义是, 将你的化名与你的现实世界身份联系起来有多困难。

高度的匿名性使您能够合理地预期已经实现了**隐私**。但为什么这很重要呢？

# "匿名只是用来买毒品的, 对吧? "

想象一下, 在一个基于区块链的金融世界中, 这些场景。

## "鲍勃的汉堡"

你在沃尔格林买东西。您的收银员在区块链上查找您, 每月看到20笔购买, 网址是 "bob ' s burers", 但每个人都知道, 这是互联网上最大的 pr0n 网站的隐藏名称。

**极端的例子-勒索:**同一个商店的员工也看到你坐在一个藏有 6, 000万美元的比特币上。当他们下周绑架你母亲的时候, 他们很清楚有多少钱可以敲诈你。

# "匿名只是用来买毒品的, 对吧?"

## 示例: 由朋友支付

一家餐馆拒绝平分账单, 你自愿付帐。你的朋友给你寄了一些比特币。后来, 你去鲍勃的汉堡和你朋友的比特币一起购买, 但他们不接受你的付款, 因为 "你的钱和毒贩有关"。

**可替代性**是一种想法, 即货币的每一个单位的价值必须等于每一个其他单位

- 货币的关键属性

NOV 13, 2013 @ 08:17 AM 38,863 VIEWS

The Little Black Book of Billionaire Secrets

## Sanitizing Bitcoin: This Company Wants To Track 'Clean' Bitcoin Accounts



Kashmir Hill, FORBES STAFF

Welcome to The Not-So Private Parts where technology & privacy collide [FULL BIO](#)



Alex Waters, Matt Mellon, and Yifu Guo, of Coin Validation

来源:《福布斯》关于 "硬币验证" 的报道。

<http://www.forbes.com/sites/kashmirhill/2013/11/13/sanitizing-bitcoin-coin-validation/>



# "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:

缺乏匿名性意味着你曾经与之打交道的每一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》。

# 匿名与伦理

匿名加密货币确实可以用于洗钱和网上购买毒品。

- 部分解决方案: 加密货币和法定货币之间的接口受到高度监管
  - 召回 aml/kyc: 几乎可以匿名交易加密货币, 但不能在没有护照图片的情况下接触 usdbbpeur
- 在技术层面难以实施 "道德"
  - 从技术角度来看, 道德和不道德的使用案例看起来是相同的
- 对社会的积极好处是否大于代价?
  - 示例: tor ([http://en.wikipedia.org/wiki/Tor\\_\(anonymous\\_nets\)](http://en.wikipedia.org/wiki/Tor_(anonymous_nets)))
    - 由美国政府创建。官员们很难监控网络流量, 但他们已经找到了其他方法
    - 为压迫政权中的记者提供言论自由

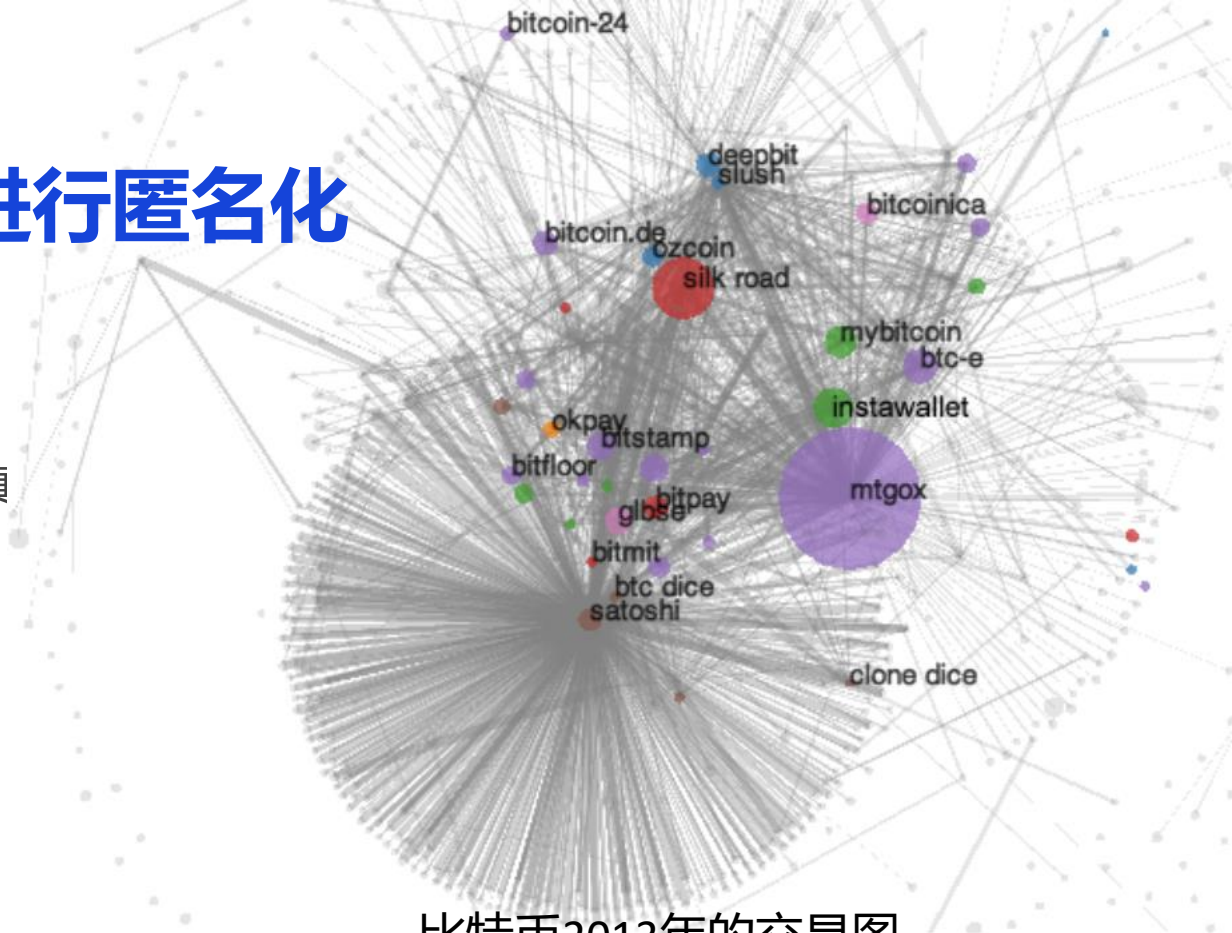
# 基本的匿名化技术

# 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 \(Meiklejohn 等人\)](#)

# 聚类

关联两个地址的两个主要启发式方法:

## 1. 事务输出的合并

- a. 当事务有多个输入时发生
- b. 相当合理的假设两个输入地址由同一实体配对
  - i. 很少有人进行联合支付

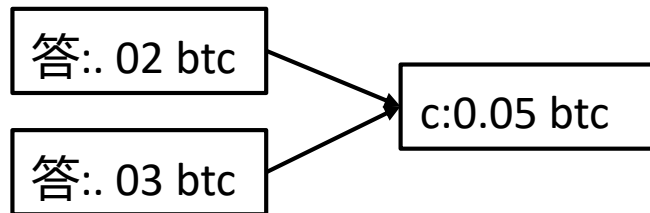
## 2. 更改地址

- a. 交易分为0.95 和0.05额
  - i. 其中一个必须是变更地址, 除非有两个项目是共同购买的
- b. 有用的启发式: 更改地址通常是新生成的--以前从未在区块链上看到过

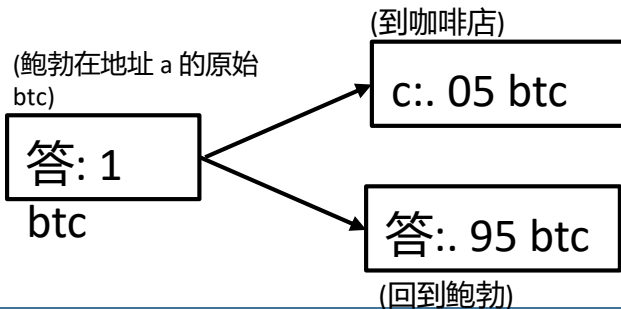
在这两种情况下, 如果地址 $a$ 个已知是鲍勃所有, 我们现在知道, 地址 $a'$ 也是鲍勃所有。

**案例1:** 用 0.02 btc 和 0.02 btc utxo 购买成本 0.05 btc 的咖啡。 $a$  和  $a'$  合并为一个输出将它们链接在一起。

(鲍勃以前的输出)



**案例2:** 使用 1 btc utxo 购买成本为 0.05 btc 的咖啡。标识更改地址链接地址  $a$  和  $a'$  一起。



# 识别服务

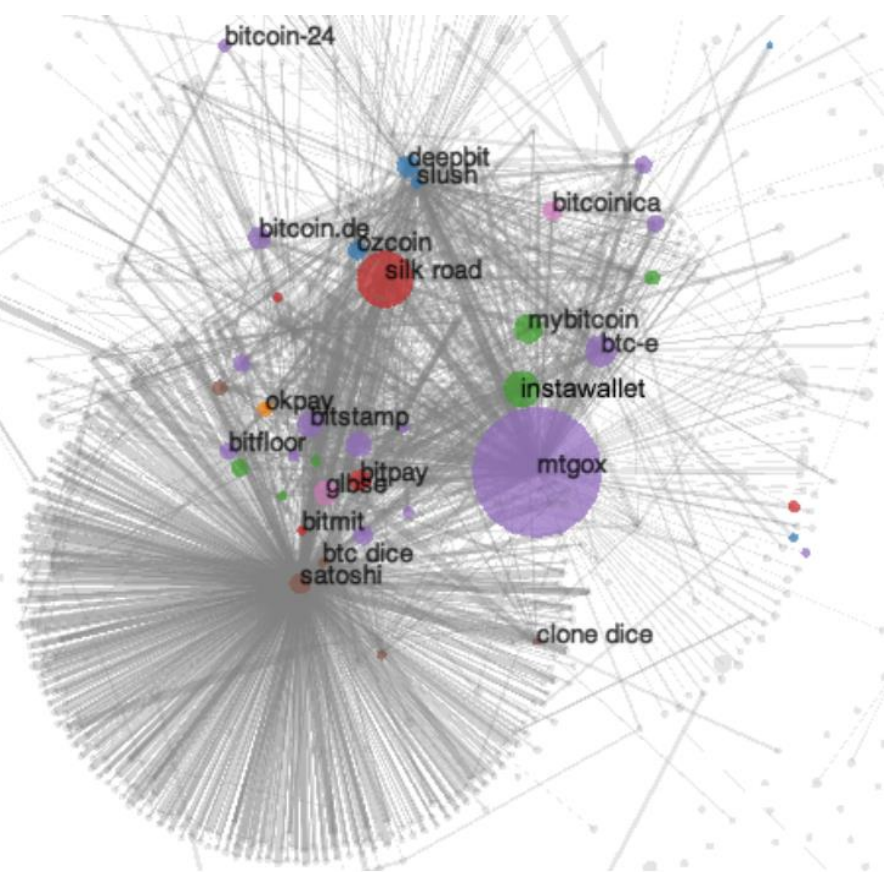
识别具有企业真实世界标识的集群的几种技术:

## 1. 通过交易标记

- a. 转到在线服务 (例如, 代码库) 并与他们进行交易
- b. 等待地址与群集的其余部分合并

## 2. 通过查看活动来输入

- a. 2013年, 戈克斯山是生态系统的重要组成部分
  - i. 大体积 (大紫色圆点)
- b. satoshidice 是一个赌博场所, 允许较小的面值
  - i. 小体积 (小点)
  - ii. 大量交易



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)

# 识别个人

将地址与个人关联的几种技术:

1. 送他们比特币

- a. 显然, 他们需要透露一个地址

2. 粗心大意

- a. 在任何地方 (如论坛上) 公开发布您的比特币地址会显示至少一个地址

3. 服务提供方

- a. 例如: 天空 (以前的共药)



资料来源:《科因电讯报》



Compliance/AML

Expose funds derived from illicit activities and detect complex money laundering activities.

Compliance/AML



# 古色古香分析

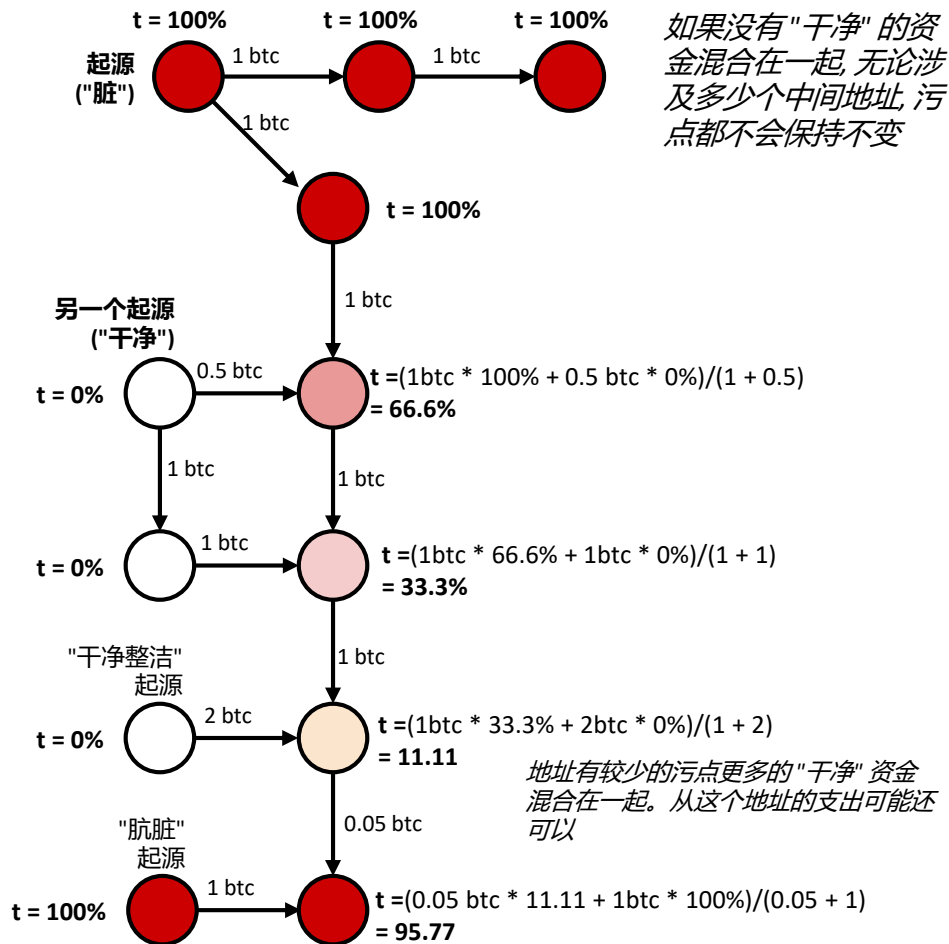
每个圆圈都是一个地址。  
让t表示该地址的"污点"。

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!



大量的交易会对污渍产生强烈的影响




# 区块链上的张力分析工具。



## Taint Analysis 1dice6GV5Rz2iaifPvX7RMjfhaNPC8SXH

Taint is the % of funds received by an address that can be traced back to another address.

This pages shows the addresses which have sent bitcoins to 1dice6GV5Rz2iaifPvX7RMjfhaNPC8SXH. The data can be used to evaluate the anonymity provided by a mixing service. For example Send Coins from Address A to a Mixing service then withdraw to address B. If you can find Address A on the taint list of Address B then the mixing service has not sufficiently severed the link between your addresses. The more "taint" the stronger the link that remains.

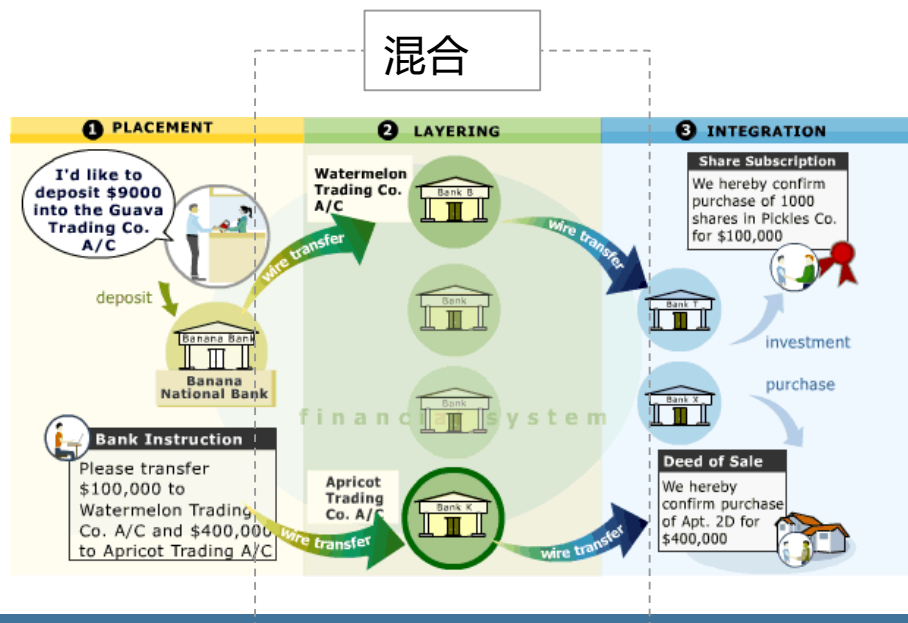
Received (Origin) Taint 				
Branch	Address	Taint (%)	Count	Top IPs
21	17V7mV5yWgzkWVB6VGzJh6jiVcAYJ1xU8t	5.709493158%	48	
4	12p1dnSn11aXS1hBjt9cscZNTGSJ56YDQM	5.4376125314%	56	
3	1Lpn1Bhp8jieEGyraJ5koPrv7dEatgkB5k	5.3696423747%	10	
2	1P3TjAGvaqdTT2so8xm5MxXu55SCVss59Y	2.7188062657%	6	
2	1HG2RQWwiqr479GKhbykWn6FdbdQoBpU6H	2.7188062657%	66	
2	12U8dsx3grbyBDRjR7AQpvD2eedgqvWnyo	2.7188062657%	6	
3	1bankkx5E9Xqd5... (Satoshi Dice Change Address)	2.497099566%	9	
5	1dice97ECuByXAv... (SatoshiDICE 50% <a href="#">🔗</a> )	2.2296799195%	24	

# 通过混合匿名

# 混合

**混合：**进行交易的目的是隐瞒你的资金来源

。



## 传统的混合/洗钱:

创建数以百计的假 "壳" 公司, 不做任何事情或拥有任何资产, 但**看**就像他们一样 (根据会计账簿和纳税申报单)。

随着时间的推移, 将 "脏" 资金存入空壳军团。(位置)。

壳牌军团。注销存款作为购买、投资等..... 让存款看起来真实。

壳牌军团。通过将资金汇给**其他**壳军团 (分层)。

最后, 犯罪组织将 "干净" 的钱花在奢侈品上, 如钻石、汽车、房地产 (集成)。

**在区块链上混合使用同样的想法。**

# 匿名的正式框架

def.: a**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。

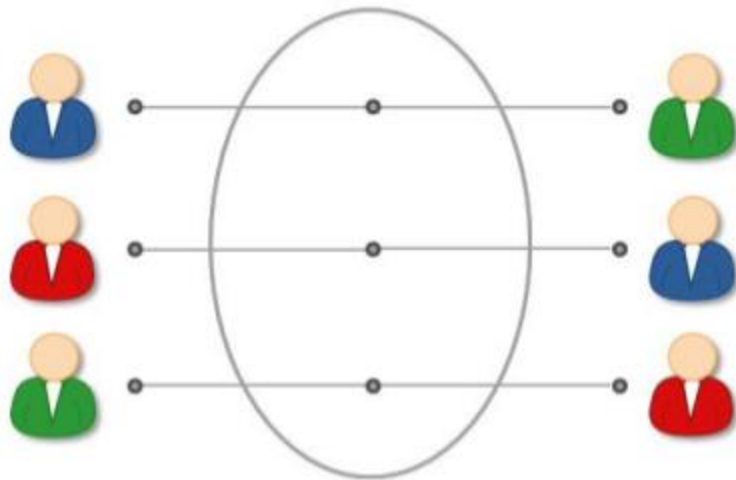
- 理想情况下, 这是很难**任何人**将标识链接到地址

## 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

# 混合的类型

- 集中式混合器
- altcoin 交换混合
- 分散混合协议
- 以普锐斯为重点的阿尔特币

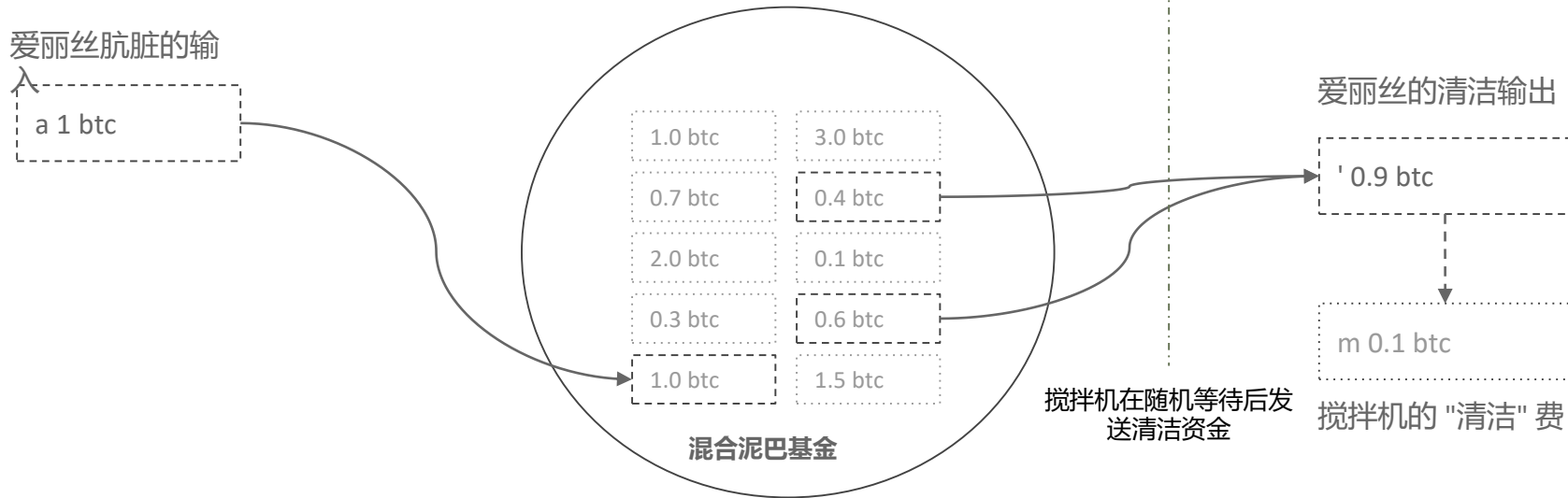


# 集中式混合器

# 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



# 集中式混合器-问题

**交易对手风险:**搅拌机可以窃取资金;必须信任它不会。

**日志记录风险:**混频器可能是伐木谁收到了肮脏的资金, 从哪里送去了清理过的资金。

**集中化风险:**单点故障。黑客攻击的单一目标。对手 (如政府) 安装自己的日志记录或发送删除通知, 并夺取混频器的控制权。



**THIS DOMAIN NAME HAS BEEN SEIZED**

by the United States Global Illicit Financial Team  
in accordance with a seizure warrant obtained by the  
United States Attorney's Office for the Southern District of New York  
and issued pursuant to 18 U.S.C. § 982(a)(1) by the  
United States District Court for the Southern District of New York.

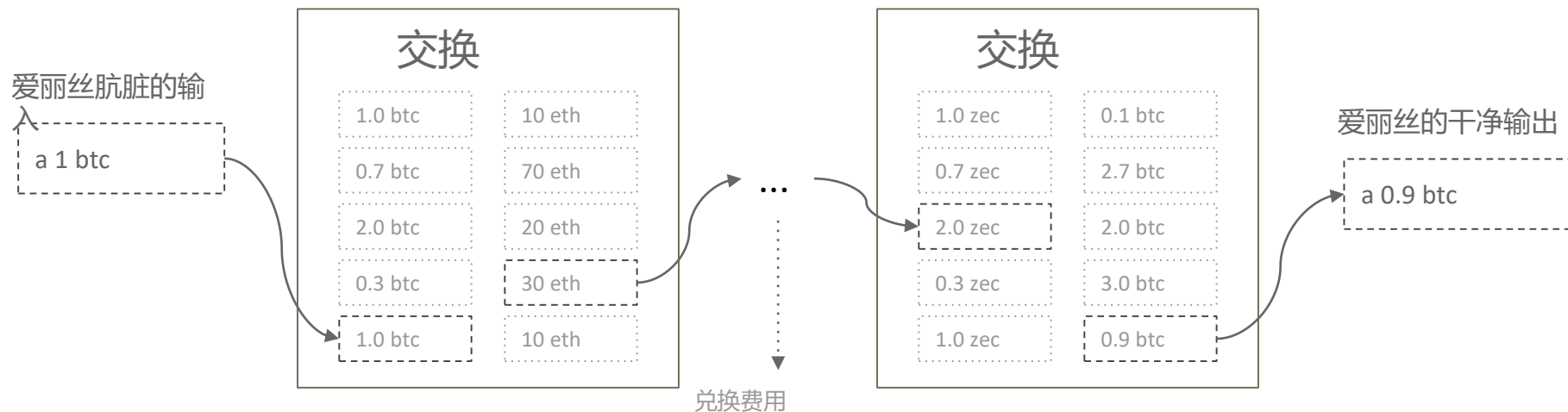




altcoin 交换混合

# 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。



# altcoin 交换混合-问题

## 优点:

- + 对手必须通过几个不同的区块链和交易所追踪交易链。
- + 更好的似是而非的否认--看起来像正常的货币兑换。

## 缺点:

- 依赖于隐藏事务映射的交换
- 交易对手风险: 交易所在运输途中被黑客攻击
- (美国)交易所通常需要个人身份信息, 并遵循 kyc/aml。

# 分散混合协议

# 分散混合协议

**想法：**通过取出中间人 (集中混频器) 来消除交易对手风险并避免收费。

**命题：**在比特币网络之外创建一个对等方网络, 他们合作进行混合硬币的交易, 而不依赖受信任的第三方。

**这可以做到吗？**

# 混合研究项目

嗯, 这就是我们 (讲师) 要回答的问题。

**混合项目:**构建一个**不信任,分散 比特币**混频器, 维护**似是而非的否认**.

其他要求:

- **低廉的费用**
  - 混合不应该是成本过高的;将是不切实际的
- **比特币配合**
  - 当然, 你可以混合各种阿尔特币。但如果你不想经历交流的麻烦呢? 目前还没有人开发出具有这些特性的比特币混合器。
    - 更不用说闪电网络还不存在
      - 所以, 让我们建立 dmix!

# 分散混合协议-nu省长

设计良好的分散混合协议的其他注意事项

一个组合由输入和输出组成:

- 一个输入和一个输出由同一实体拥有, 混合的目标是隐藏**映射**从所有输入到所有输出。

**Def. 正确性:** 硬币不得丢失、被盗或双倍使用。混合是真正的随机, 必须**最终成功地**混合或返还诚实用户的资金 (抵御 dos 攻击)。

## 对抗性模型:

- **被动对手**
  - 不是组合的一部分
  - 基本匿名性可防止被动对手学习映射
- **半诚实的对手**
  - 混合的一部分
  - 正确地遵循协议, 但**尝试去匿名的混合**通过分析混合的程序。
- **恶意对手**
  - 混合的一部分
  - 不受协议规范的约束; 可能**积极偏离协议并试图偷资金**
  - 可能会发送虚假信息、放弃通信等。

# 分散混合协议-nu省长

**抗战**在分散混合的情况下有一个两部分定义:

## 1. 抵制盗窃资金

- 不能依赖 "部分" 阈值加密来强制正确性 (例如,  $m < n$  这样的  $m$  多 sig)。
- 协议必须正确执行 (没有资金被盗)即使所有其他对等方都是恶意对手

## 2. 对匿名化的抵制

- **弱**: 参会人员外面混合不能确定输入到输出的映射, 但参与者在混合可以。
  - 只需要一个半诚实的对手来打破匿名
- **强**: 即使是参与者在混合不知道输入到输出的映射
  - 然而, 很大比例的 sybil 同行降低了匿名设置。



# 协议-硬币交换 (2013)

**想法：**集中式搅拌机的自然延伸："一个不能与你的硬币运行的搅拌机。

使用哈希锁定, 2比2多签名交易, 我们可以通过第三方混频器可靠地发送硬币, 混频器不能窃取资金。

**优点:**

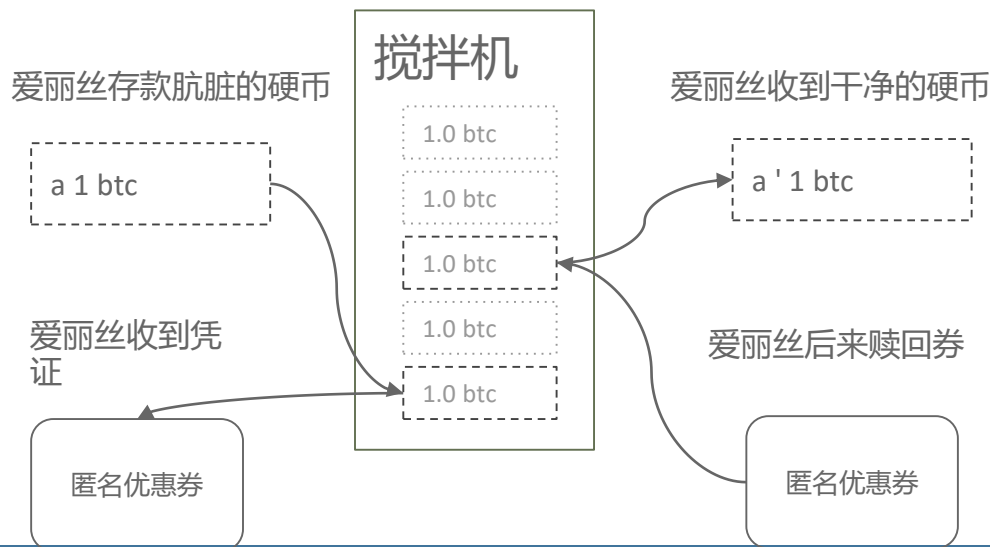
- + **无交易对手风险**;混频器不能偷资金。
- + **更好的似是而非的否认**;被动对手只看到22个多签名交易

**缺点:**

- **未隐藏的值**;混频器仍然看到金额转移
- **映射未隐藏**;混频器知道谁收到哪些硬币
- **价格昂贵**;每轮使用4个交易记录

# 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。

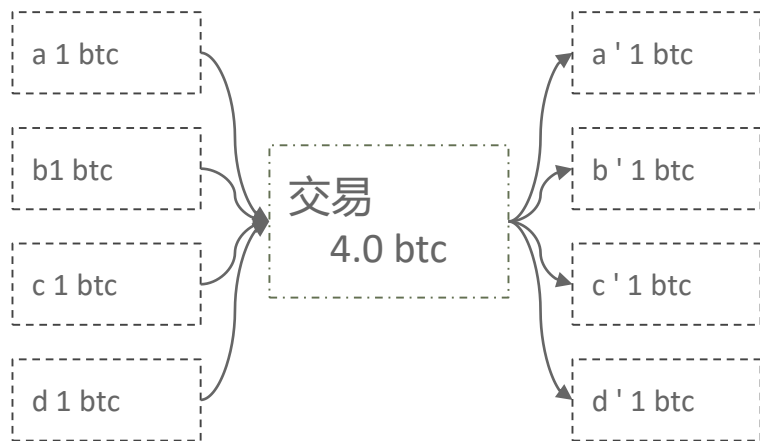
使爱丽丝存款她的脏硬币, 并收到干净的, 未链接的硬币, 而不透露自己。

不只限于单混频器。可在更复杂的协议中用作基元

收款人不必要是存款人。

# 协议-硬币加入 (2013年)

**替代方法:**在一个  $n$  的多签名交易中混合硬币。



## 优点:

- + 资金不能被偷
- + 没有一个中央混合党谁需要足够的流动性, 良好的匿名性。

## 缺点:

- **不可合理的否认; 不可信的否认**很容易在区块链上发现, 因为  $n$  的多签名交易通常是大的。
- **不需要攻击的攻击;**只需要1个恶意节点启动协议, 然后中途停止中断。
- 匿名设置仅限于交易参与者。

# 联合市场 (2015)

**想法：** 创建流动性提供商的市场, 他们愿意混合他们的硬币收费。

由于做市商几乎不承担任何风险, 混合费用通常很小。

**问题：**

- 混合硬币有小的匿名设置
- 取消整个系统只需要 32, 000 美元 (攻击后可恢复), 成功率约为 90% (möser, böhme)

## JoinMarket Orderbook

142 orders found by 66 counterparties

Type	Counterparty	Order ID	Fee	Miner Fee Contribution / BTC	Minimum Size / BTC	Maximum Size / BTC
Absolute Fee	J5CZTub55wwWFZBu	0	0.0000969	0.0000000	0.00003830	0.00160000
Absolute Fee	J5CZTub55wwWFZBu	4	0.00001000	0.00000000	0.00003830	7.49206132
Absolute Fee	J5CZTub55wwWFZBu	25	0.00001000	0.00000000	0.00003830	0.01200000
Absolute Fee	J54ipjp2Diz9XqMS	1	0.00001750	0.00000000	0.00010000	0.99999999
Absolute Fee	J5CZTub55wwWFZBu	2	0.00002700	0.00000500	0.00003830	7.08951594
Absolute Fee	J5CZTub55wwWFZBu	18	0.00002818	0.00000000	0.00003830	0.00971051
Absolute Fee	J54ipjp2Diz9XqMS	2	0.00002928	0.00000000	1.00000000	1.99999999
Absolute Fee	J523sac3EtDzLN8P	1	0.00002985	0.00000000	0.00002730	0.00976520
Absolute Fee	J5CZTub55wwWFZBu	14	0.00003000	0.00000000	0.00003830	4.14202467
Absolute Fee	J57wggY01Q3uDiYV	0	0.00003100	0.00000100	0.00100000	1.44742679
Absolute Fee	J5CZTub55wwWFZBu	1	0.00003630	0.00000000	0.00003830	2.99999999
Absolute Fee	J54MdBzKZp1xp4c	3	0.00003630	0.00000000	2.00000000	2.99999999
Absolute Fee	J5CZTub55wwWFZBu	17	0.00004100	0.00000100	0.00003830	5.09930543
Absolute Fee	J54exwIYnGkhJB9j	0	0.00004100	0.00000100	0.00100000	3.81806101
Absolute Fee	J5CZTub55wwWFZBu	5	0.00004287	0.00000000	0.00003830	1.99999999

联合市场:<https://github.com/JoinMarket-Org/joinmarket>

möser, böhme:[http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS\\_2016\\_paper\\_58.pdf](http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_58.pdf)

# 议定书---缔约方 (2015年、2016年)

**想法：**分散混合协议,但具有较好的否认性。希望交易与被动观察者的正常比特币交易看起来相同。

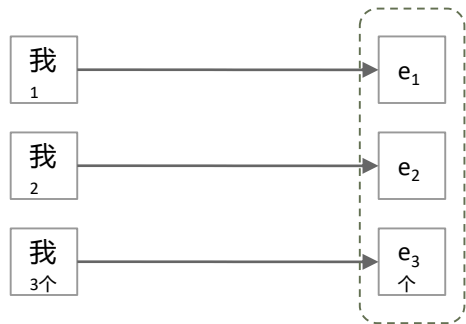
**这可能吗？**

硬币党让我们这样做,但牺牲了一些协议的安全性。

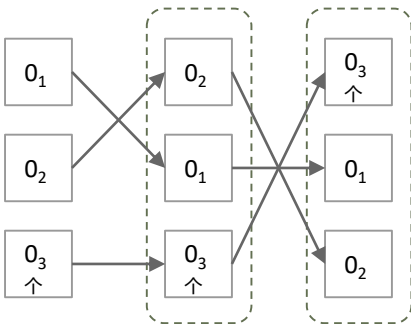
# 议定书---缔约方 (2015年、2016年)

我	输入地址
e	托管地址
o	输出地址

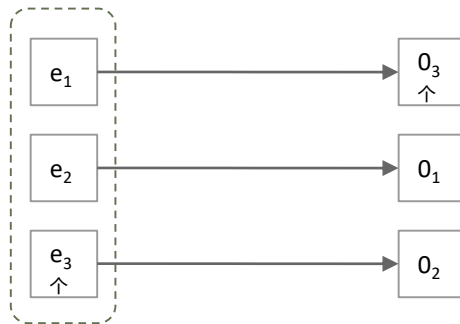
对等方生成托管地址。托管地址需要 2/共识才能使用。



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

# 议定书---缔约方 (2015年、2016年)

## 优点:

- + **高似是而非的否认**;区块链上的交易看起来就像 "正常" 的比特币交易。
- + **体面的效率**;每个输入对等方需要区块链上的2个事务。

## 缺点:

- **降低协议安全性**;由 "2" 阈值签名方案控制的托管资金。
- **易受西比尔攻击的伤害**;恶意同行可生成多个假同行, 加入混音组, 推翻2门槛, 窃取混音集团的资金。

# "交换协议" 和项目结论

## dmix 项目的最后一次迭代:交换协议

- 窗体与您的混合组对, 指定一个为 "丈夫", 另一个指定为 "妻子"
- 执行解密混合成对明显地获得一个指定对, 你的对应应该交换。
- 你的 "妻子" 被送到指定的丈夫身边。他们执行硬币交换到不可信任的交换硬币
- 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。

## 什么当前存在的满足为 dmix 项目设定的设计目标

- 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: 建立一个良好的分散比特币混频器是该死的硬.



# 以普锐斯为重点的阿尔特币



# 硬币连接



**破折号**(原 darkcoin) 是一种以隐私为中心的加密货币, 它使用主节点网络来执行特权操作, 如对建议进行投票、立即确认事务和**混合所有网络参与者的硬币 (默认情况下)**。

## 专业人员:

- 使用硬币联接进行混合:**不信任**
- 使用 coinjoin 没有合理的否认问题, 因为整个网络上几乎每个人都在参与硬币联接事务

## 缺点:

- 主节点网络本身必须是安全的-可以支付 1000 dash 每个主节点假设获取大量的主节点

**破折号**是一种开源加密货币, 是由用户子集 (称为 "主节点") 运行的分散自治组织 (dao) 的一种形式。这是一个从比特币协议分叉的 altcoin。货币允许可无法跟踪的快速交易记录。45% 的开采硬币流向矿工, 45% 提供给主节点, 10% 流向 dao 投资的基金。

# 加密注意莫内罗

**想法：**使用环签名隐藏输出映射。

选择一些以前的输出集与 "混合"。然后, 这些绑定与您的输出在加密环签名中。

**戒指签名:**在此上下文中, 证明您拥有其中一个输出, 而不显示哪个特定输出。

**问题：**monero 尚未隐藏事务值。对手可能会跟踪交易记录, 方法是跟踪可能的价值流。时间相关性也带来了一个问题。

**问题：**体面的匿名设置, 但我们能做得更好吗?

莫内罗(xmr) 是2014年4月创建的开源加密货币, 专注于可替代性、隐私和权力下放。monero 使用模糊的公共分类帐, 这意味着任何人都可以广播或发送事务, 但没有外部观察者可以告诉来源、金额或目的地。monero 使用工作证明机制发行新硬币, 并激励矿工确保网络安全并验证交易。

# 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**.



**zcash** 是一种加密货币, 旨在使用加密技术为用户提供增强的隐私, 而不是与比特币等其他加密货币相比。与比特币一样, **zcash** 的固定总供应量为 2,100 万台。交易可以是 "透明的", 类似于比特币交易, 在这种情况下, 它们是由阿德尔, 或可以是一种称为 **zk-snark** 的零知识证明; 然后, 这些交易被称为 "屏蔽", 并由 z 阿德尔. **zcash** 硬币要么在透明的池子里, 要么在屏蔽池里; 截至 2017 年 12 月, 只有约 4% 的 z-硬币在屏蔽池中, 当时大多数钱包程序不支持 z-阿德斯没有基于网络的钱包支持他们。**zcash** 为私人交易者提供了 "选择性披露" 的选择, 使用户能够证明为审计目的付款。其中一个原因是允许私人运输者选择遵守反洗钱或税务条例。"交易是可审计的, 但披露是由参与者控制的。该公司与美国各地的执法机构举行了虚拟会议, 以解释这些基本, 并公开表示 "他们没有开发货币来为非法活动提供便利"。

# 扎卡什

## 优点:

- + **完全匿名**;假设底层加密的安全性, 黑盒事务是匿名的。整个黑匣子历史的匿名集。

## 缺点:

- **资源密集型**;目前使用的 zk-snark 证明系统需要大约 4 gb 的 ram 和2分钟的计算在现代 cpu 上生成用于倾吐事务的证明。
- **需要半受信任的一次性设置**;对手与有毒的设置参数可以薄荷硬币, 而无需花费基本硬币。通过安全的多方计算设置, 可以稍微缓解一些问题。

# 混合注意事项

- 侧通道攻击
  - 通常情况下, 我们希望对所有事情都使用 tor
  - 但是, tor 退出节点可能是由对手控制的
- 分析交易记录金额
  - 易于识别输入和输出 (例如, 1337.69 btc in-> 1337.420 输出: hmmm)
  - 解决方案: 始终使用统一的交易记录金额(如 1 btc, 0.1 btc)
  - 所有正在进行的交易所有混音看起来是一样的
  - 由于这个原因, 费用应该是全部或全部
- 时间相关性
  - 人类的行为方式通常是可以预见的
  - 解决方案: 处理与其他对等方交互的客户端应实现自动化
- 网络级匿名化 (事务传播)
  - "通知您事务的第一个节点可能是它的来源。

# 结论

## 不匿名的粗糙比较级别: (大多数匿名者最少)

1. 比特币
2. 集中式搅拌机
3. 分散混合协议
  - a. 硬币交换
  - b. 硬币加入
  - c. 科因舒弗
  - d. 科宁方
  - e. 盲目签署合同
  - f. tumblebit
4. altcoin 交换
5. 破折号
6. 莫内罗
7. zcash

实际问题: **今天我将如何混合硬币?** (2016年11月)

- 可能 altcoin 交换 通过 dashi\ monero\ zcash + 托尔/VPN + 节流交换帐户和电子邮件

धन्यवाद

Hindi 印地语

Спасибо

俄语

شكراً

阿拉伯语

格拉齐

意大利语

நன்றி

Tamil

泰米尔语

以任何  
多謝  
努力

繁体中文

谢谢

英语

多谢

简体中文

ありがとうございました

日语

ขอบพระคุณ

泰语

谢谢

西班牙语

奥布里加  
多

葡萄牙语

丹克

德语

谢谢

法语

감사합니다

朝鲜语