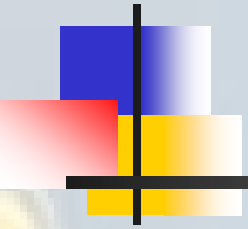
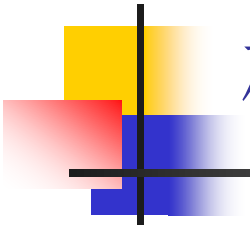
区块链基础及应用



Chapter 6 比特币和匿名性

苏 明



概览

- 6.1 匿名的基础知识
- 6.2 如何对比特币去匿名化
- 6.3 混币
- 6.4 分布式混币
- 6.5 零币和零钞

6.1 匿名的基础知识

匿名（Anonymity）：无关联性的化名

- 比特币系统中，使用者不需要使用真实的姓名
- 需要使用公钥哈希值作为交易标识
- 一个用户可以随机创建出任意多个比特币地址

6.1 匿名的基础知识

- 比特币具有化名性，但是***不能达到绝对隐私***

- 使用数字货币（如比特币）支付时，在真实的物理世界里容易暴露身份，进而关联到地址，以及其他所有的交易

6.1 匿名的基础知识

无关联性

- 同一个用户的不同地址应该不易关联
- 同一个用户的不同交易应该不易关联
- 一个交易的交易双方应该不易关联

6.1 匿名的基础知识

- 区块链货币中，所有交易都记录在一个公开账本上，也就是说相关交易信息可以*永久追踪*

- ✓ 希望**能够达到传统银行能够达到的隐私保护级别**，降低公共区块链带来的信息暴露风险
- ✓ 超越传统银行给我们的隐私保护级别

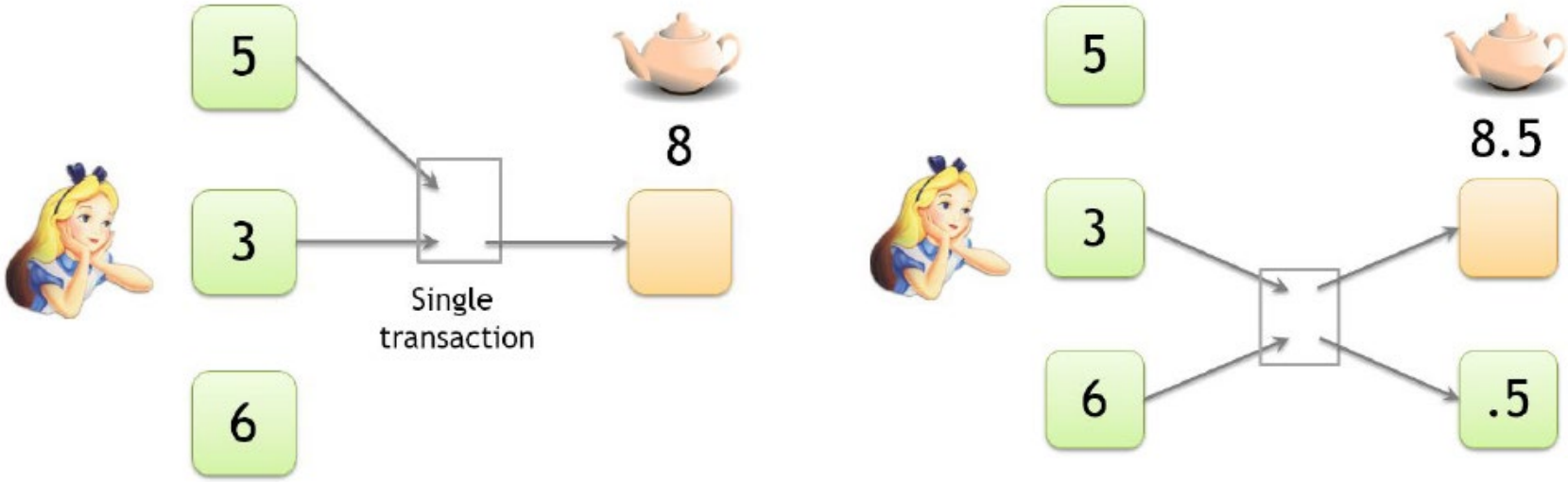
6.1 匿名的基础知识

匿名化和去中心化

- Chaum的电子现金系统，采用了*盲签名*技术，但还需一个*中央权威机构*
- Zerocoin， Zerocash：匿名化&去中心化的加密数字货币系统

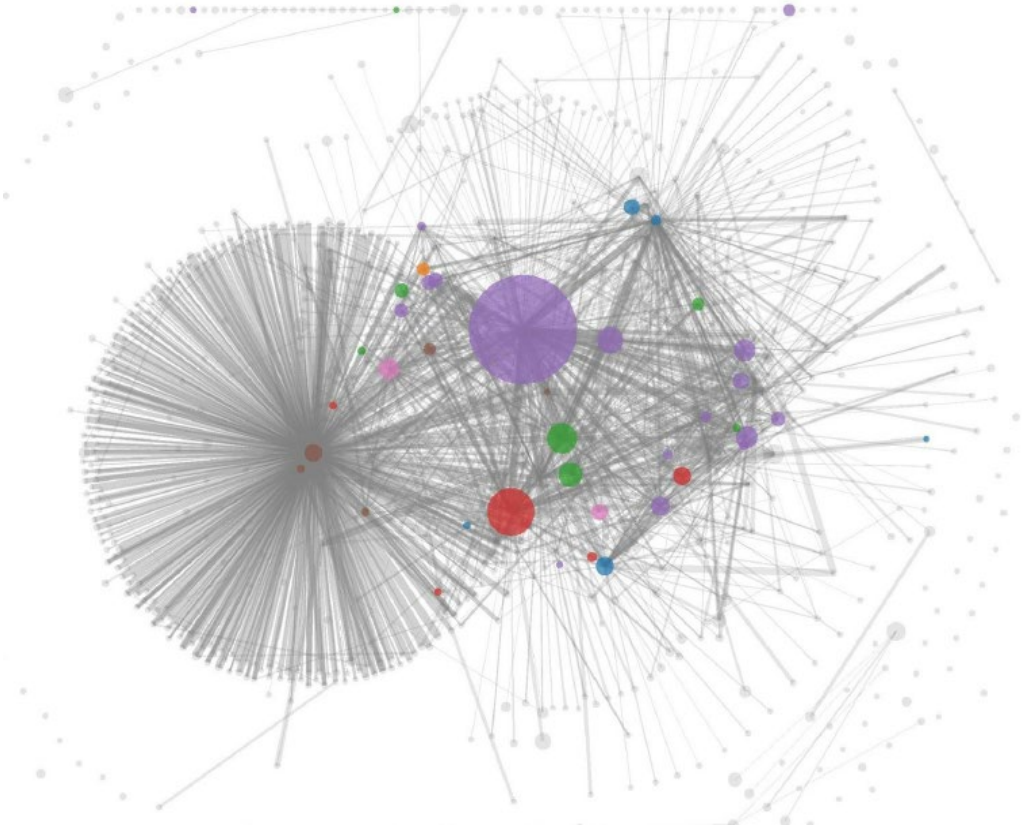
6.2 如何对比特币去匿名化

- 关联性



容易暴露零钱地址

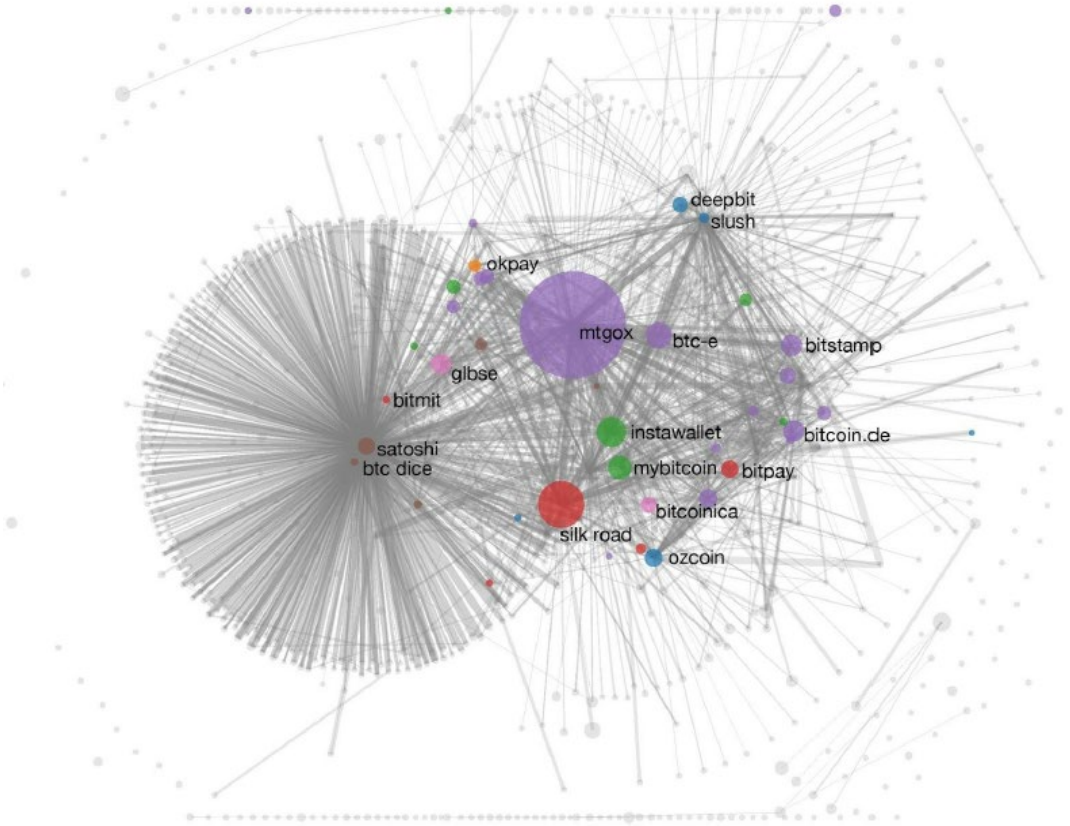
6.2 如何对比特币去匿名化



Clustering of addresses： *Characterizing Payments Among Men with No Names*

6.2 如何对比特币去匿名化

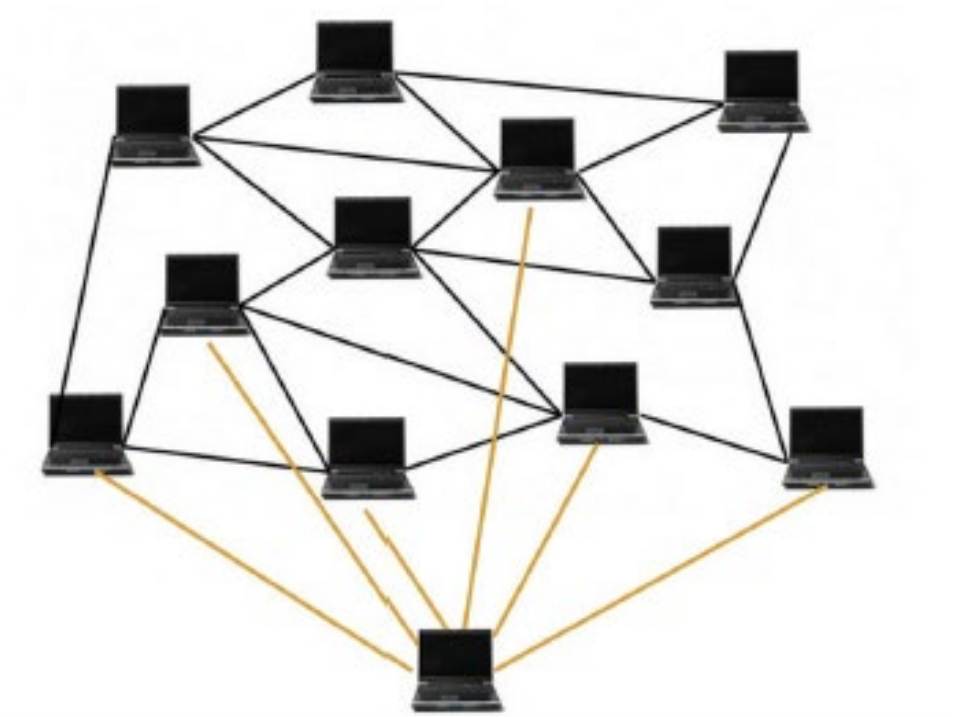
- 利用交易进行标记



交易图谱分析

6.2 如何对比特币去匿名化

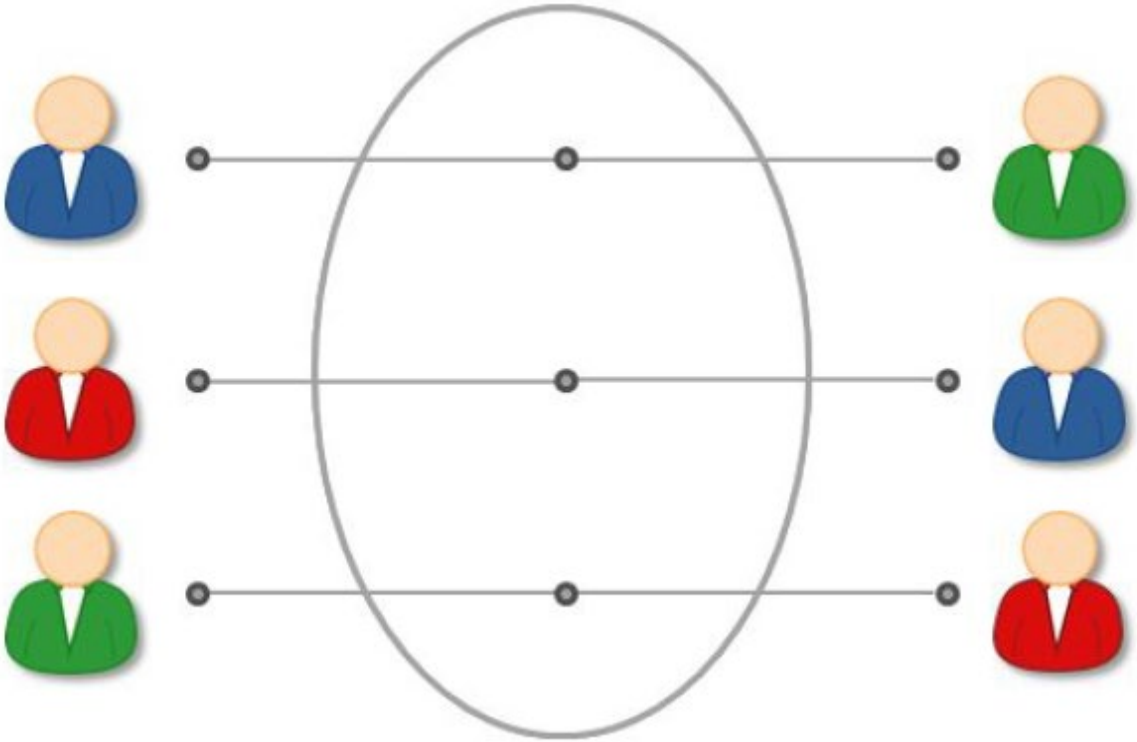
- 网络层的去匿名化



“the first node to inform you of a transaction is probably the source of it.”

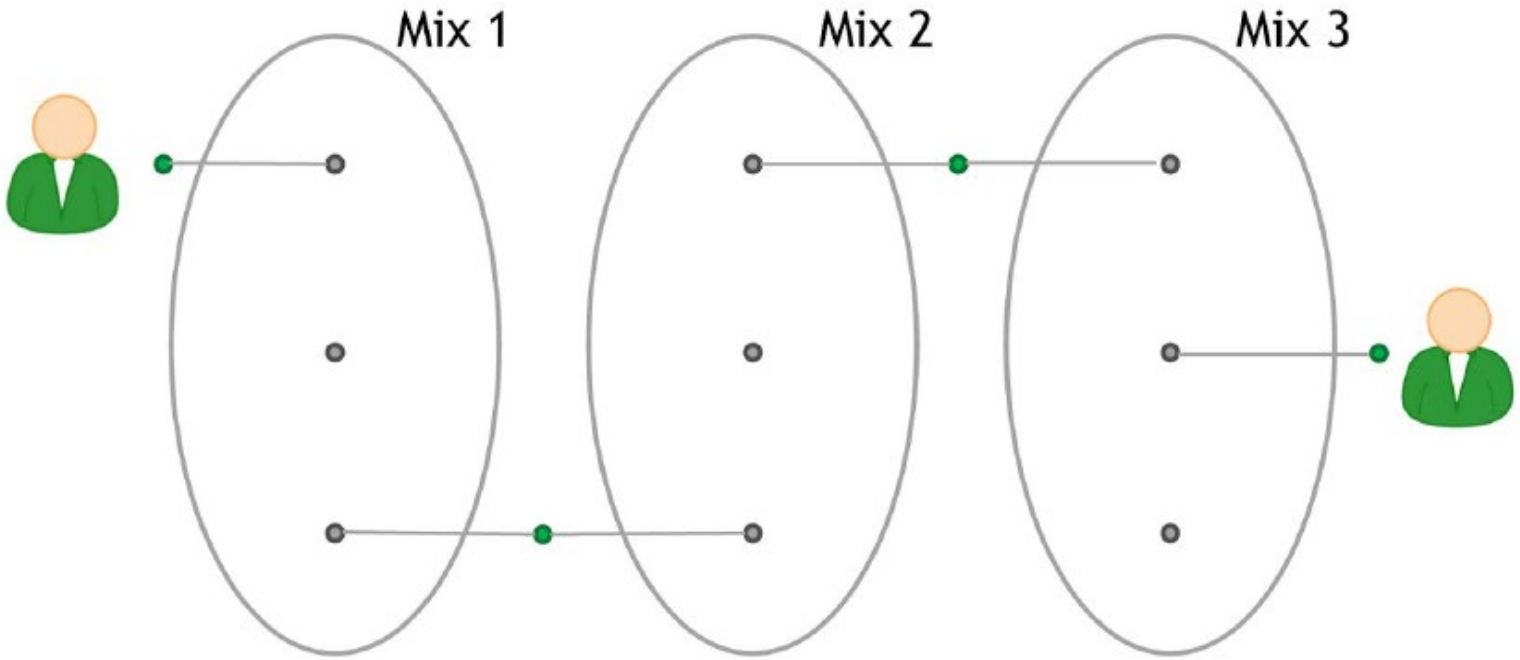
6.3 混币

- 想要匿名化，使用一个中介媒体



6.3 混币

- 多重混币



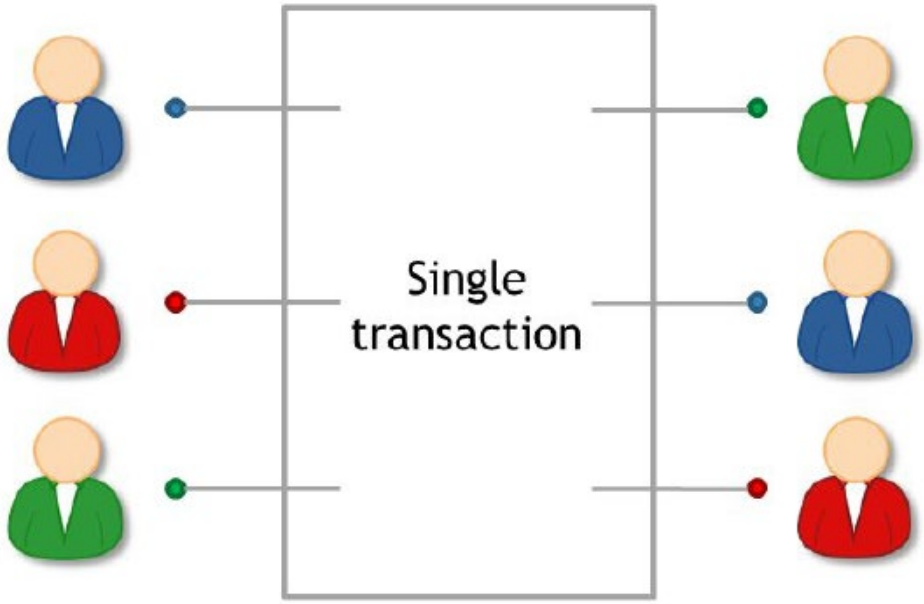
6.4 分布式混币

- 分布式混币(Decentralized Mixing)

- 采用一种用户之间的**点对点**模式实现混币交易的协议

6.4 分布式混币

攻击者无法建立输入和输出的匹配关系



A Coinjoin transaction

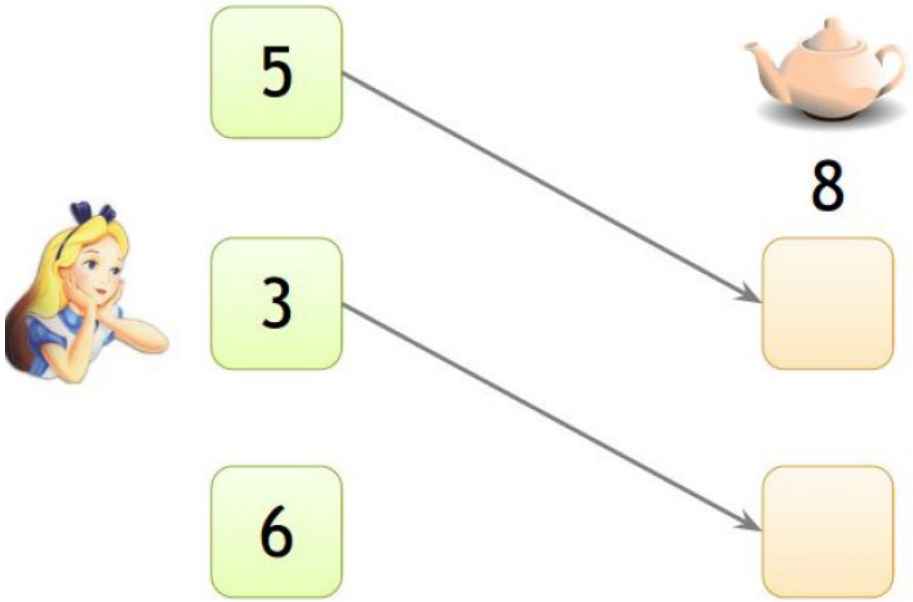
6.4 分布式混币

高交易风险流

- 为了完成一笔支付，用户通常会组合所拥有的数字货币，这样便有足够数额可以支付到**单一**接收地址

- 规避：所有输入地址被关联在一起

6.4 分布式混币

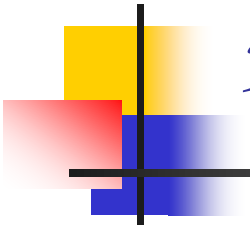


Merge avoidance

零知识证明

Zero Knowledge Proof：证明者(Prover)要让验证者(Verifier)相信自己拥有某种知识，但又不泄漏它

- 很多场景中有着广泛的应用，比如金融交易中，保护支付方、接收方、交易金额的**隐私**



零知识证明

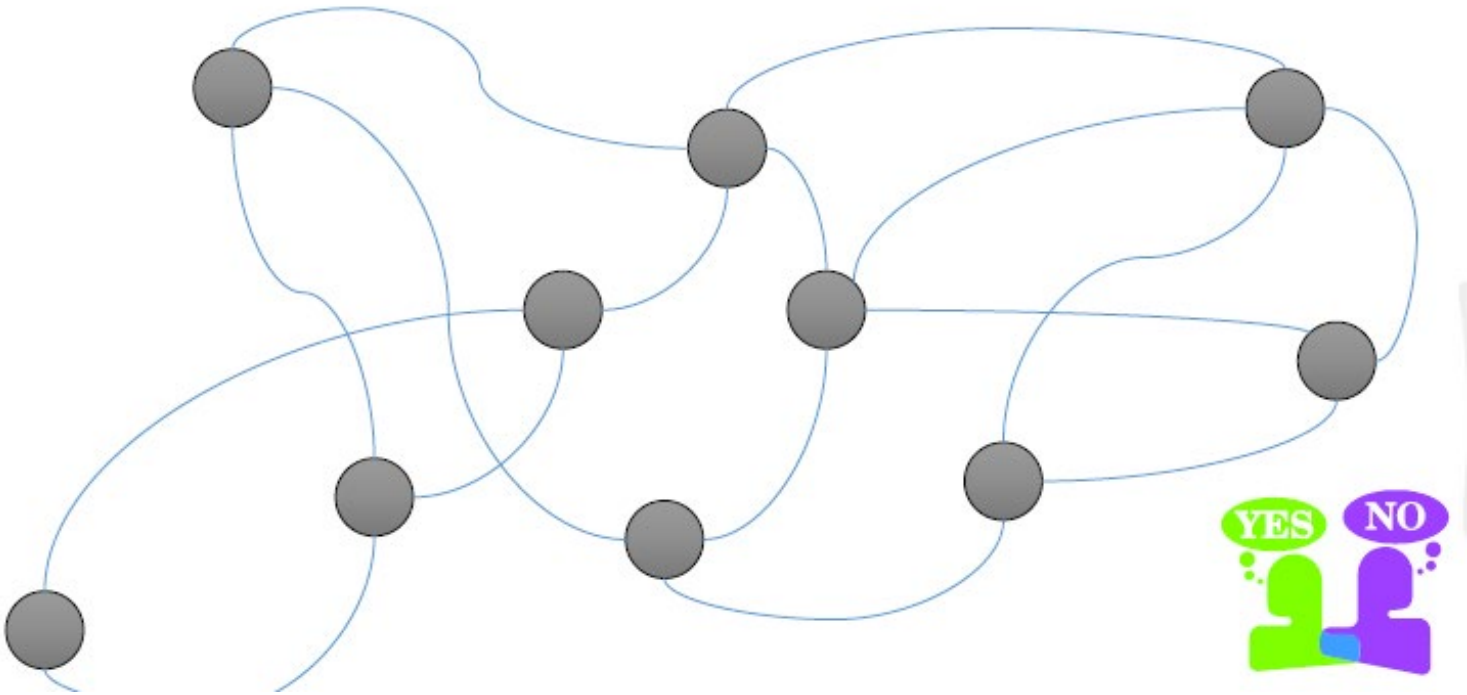
- Example 1. A Key to a Door
- Example 2. Coloring Problem

Example 1

Ali Baba cave

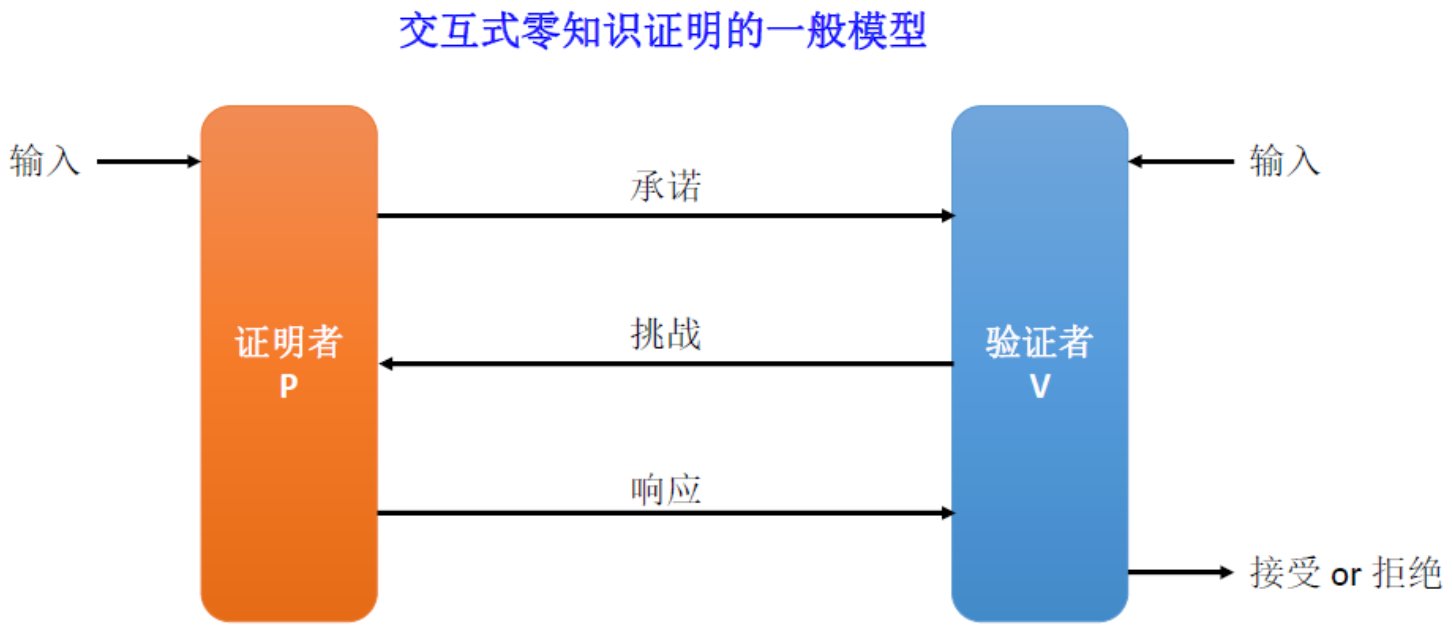
Example 2

Can we label this graph with {r, g, b}?



三色问题

交互式零知识证明的一般模型



- 证明者和验证者共享一个公共输入，证明者可能拥有某个秘密输入。
- 如果验证者认可证明者的响应，则输入接收（Accept）；否则，输出拒绝（Reject）。

Sigma-Protocol

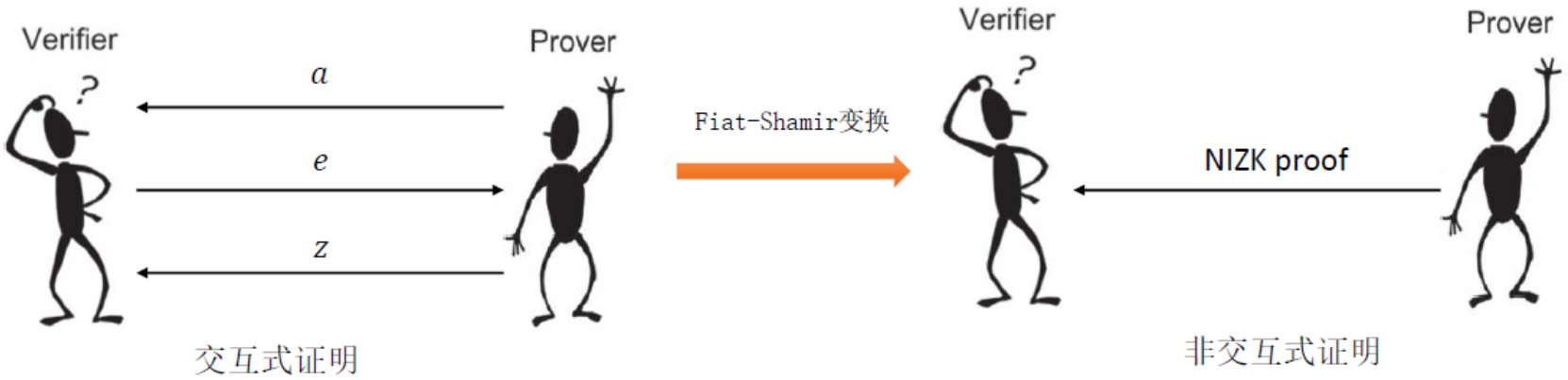
Sigma-protocols

- P sends V a message *a*
- V sends P a random t-bit string *e*
- P sends a reply *z*, and V decides to accept or reject based solely on the data it has seen; i.e., based only on the values *(x, a, e, z)*.

非交互式零知识证明

Fiat-Shamir变换是一种可以将Sigma协议变成非交互证明的技术。它能够让证明者Prover可以通过给验证者Verifier发送一个证明信息即可完成证明(无需交互，无需返回挑战)。

而且，它能把任何一个Simga协议变成一个数字签名，签名的含义就是“知道这个Sigma协议的秘密的人已经签署了这个消息”。Prover能够创造一个证明，然后分发给很多个验证者，验证者可以不必联系Prover即可验证证明有效性。同时零知识也变得容易了，因为验证者或者其他敌手不能做任何事情。



一个密码学安全的 Hash 函数可以近似地模拟传说中的「随机预言机」

6.5 Zerocoin & Zerocash

- Zerocoin:

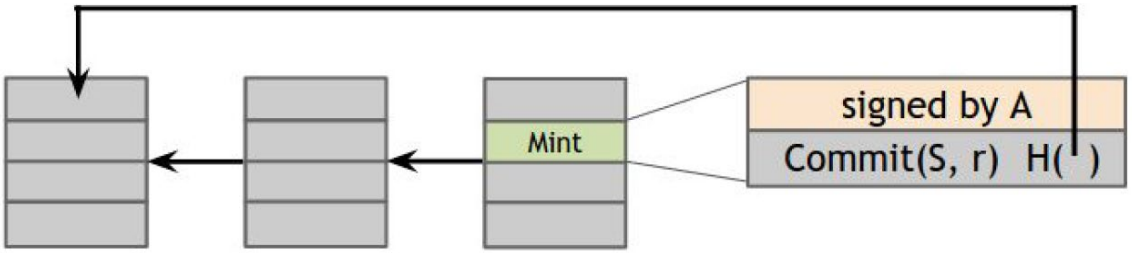
I know x such that H(x || ⟨other known inputs⟩) < ⟨target⟩ .

"I know x such that H(x) belongs to the following set: {...}".
The proof **would reveal nothing** about x

6.5 Zerocoin & Zerocash

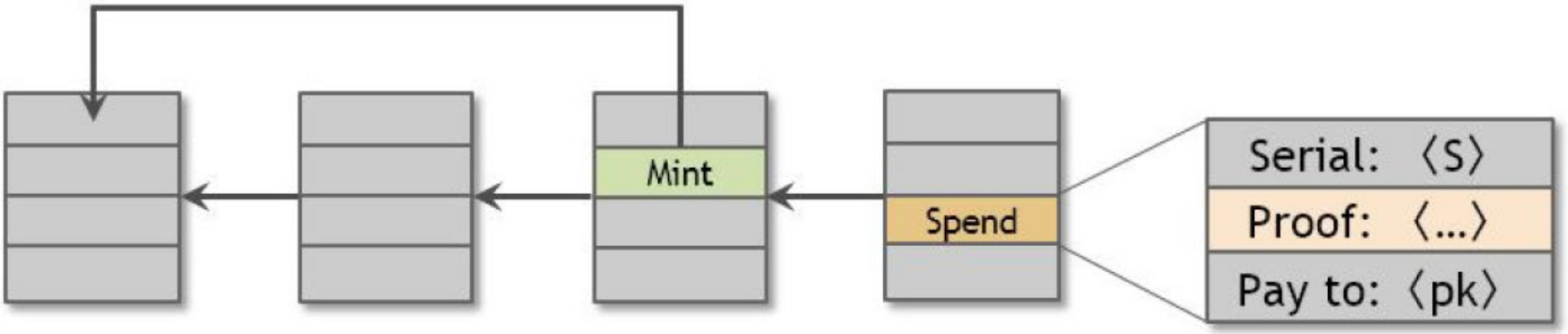
- Zerocoin

Committing to a serial number



Putting a zerocoin on the block chain

6.5 Zerocoin & Zerocash



Spending a zerocoin

6.5 Zerocoin & Zerocash

Spending a zerocoin with serial number S to redeem a new basecoin

- Create a special "spend" transaction that contains S, along with a zero-knowledge proof of the statement:

  "I know *r* such that *Commit(S, r)* is in the set $\{c_1, c_2, \ldots, c_n\}$".
- Miners will verify your zero-knowledge proof which establishes your *ability* to open one of the zerocoin commitments on the block chain, without actually opening it.
- Miners will also check that the serial number S has never been used in any previous spend transaction (since that would be a double-spend).
- The output of your spend transaction will now act as a new basecoin. For the output address, you should use an address that you own.

6.5 Zerocoin & Zerocash

Zerocoin：匿名性

- 铸币交易或者花费交易中没有展示过r
- 无人知道序列号对应哪一个具体的零币

6.5 Zerocoin & Zerocash

Zerocash

- zk-SNARK (Zeroknowledge Succinct Non-interactive Arguments of Knowledge)
- **DAP** (Decentralized Anonymous Payment Scheme)
- *Hiding user identities, transaction amounts, and account balances from public view*

Summary

System	Type	Anonymity attacks	Deployability
Bitcoin	pseudonymous	transaction graph analysis	default
Manual mixing	mix	transaction graph analysis, bad mixes/peers	usable today
Chain of mixes or coinjoins	mix	side channels, bad mixes/peers	bitcoin-compatible
Zerocoin	cryptographic mix	side channels (possibly)	altcoin, trusted setup
Zerocash	untraceable	none known	altcoin, trusted setup

A comparison of the anonymity technologies