Blockchain Anonymization

-- The Fight for Privacy

LING Zong, Ph. D.
Senior Software Engineer / Scientist
IBM Almaden Research Center
San Jose, California, U.S.A.

Lecture Outline

Anonymity Basics

区块链在默认情况下不是匿名的

Blockchains are not anonymous by default

直觉:区块链采用一个中央数据库并将其分发
· 然而，这意味着你现在没有访问控制
默认情况下，所有数据都是公开的
· 私有区块链的匿名性稍强，因为只有少数成员可以访问数据库

- Intuition: Blockchains take a central database and distribute it
  - However, this means that you now have no access control
- All of the data is public by default
  - Private blockchains are slightly more anonymous since only a few members have access to the database

Most blockchains are **pseudonymous** - we use an identity that is not our real identity (e.g. your Bitcoin address)大多数区块链是假名的——我们使用的身份不是我们的真实身份(例如，你的比特币地址)

我们的假名可能与我们的真实身份有“关联”，也可能与真实身份没有“关联”

- Our **pseudonyms** may or may not be "linked" to our real identity

Deanonymization

"Linking" in the context of anonymity is associating a real world identity to a pseudonym. This is also called **deanonymization**

匿名语境中的“链接”就是将真实世界的身份与假名联系起来。这也叫做去匿名化
· 在比特币:一个身份和一个地址
· 在以太坊:一个身份和一个帐户

- In Bitcoin: an identity and an **address**
- In Ethereum: an identity and an **account**

比特币的最佳实践实现小程度的匿名

最佳实践:永远不要重用您的假名!
· 每次收到比特币生成一个新地址
· 我喜欢为每条评论创建一个新的reddit账号
在以太坊是不可能的，因为它是基于帐户的(而不是基于UTXO)
但基本的分析表明这种技术无效

Bitcoin best practice achieves a small degree of anonymity

- Best practice: Never reuse your pseudonyms!
  - Generate a new address every time you receive Bitcoin
  - Like creating a new reddit account for every single comment
- Not possible in Ethereum, since it is account-based (not UTXO based)
- But basic analysis renders this technique ineffective

Degree of anonymity

Anonymity isn't absolute (not a clear yes or no)

匿名性不是绝对的(没有明确的是或不是)
●“ 匿名程度 ”(有时是“ 匿名程度 ”)是由把你的笔名和真实身份联系起来的难易程度来定义的。
高度的匿名性使你有理由认为已经获得了隐私。但为什么这很重要呢?

- The **"degree of anonymity"** (or sometimes "**level of anonymity**") is defined by how difficult it is to associate your pseudonym with your real world identity.

A high degree of anonymity allows you to reasonably expect having achieved **privacy.** But why is this important?

"Anonymity is only for buying drugs, right?"

想象一下在基于区块链的金融世界中这些场景

Imagine these scenarios in a blockchain-based financial world.

'Bob's Burgers'

你在沃尔格林购物。你的收银员在blockchain.info上查找你，发现你每月购买了20件公开标注为“鲍勃汉堡”的商品，但每个人都知道这是互联网上最大的pr0n网站的隐藏名称

You make a purchase at Walgreens. Your cashier looks you up on blockchain.info and sees 20 purchases a month to the address publically labeled "Bob's Burgers," but everyone knows that that's the hidden name for the internet's biggest pr0n site.

极端的例子——敲诈:同一位店员还看到你坐拥6000万美元的比特币。当他们下周绑架你母亲的时候，他们知道要勒索你多少钱。

Extreme example - blackmail: The same store employee also sees that you're sitting on a stash of $60 million in Bitcoin. When they kidnap your mother next week, they know exactly how much money to blackmail you for.

"Anonymity is only for buying drugs, right?"

例子:从朋友那里得到回报
餐馆拒绝分摊账单，你自愿买单。你的朋友寄给你一些比特币。后来，你用朋友的比特币去Bob's Burgers购物，但他们不接受你的付款，原因是
“你的钱和毒贩有关联。”
可替代性指的是货币的每一单位必须与其他单位的价值相等

Example: Getting paid back by a friend

A restaurant refuses to split the bill, and you volunteer to foot it. Your friend send you some Bitcoin. Later, you go to Bob's Burgers to make a purchase with your friends' Bitcoin, but they don't accept your payment because "your money is associated with drug dealers."

Fungibility is the idea that every unit of a currency must be equal in value to every other unit

货币的重要属性

- Crucial property of currency

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

Source: Forbes on "Coin Validation“
http://www.forbes.com/sites/kashmirhill/2013/11/13/sanitizing-bitcoin-coin-validation/#6bb370ed6a45

"Anonymity is only for buying drugs, right?"

例如:区块链上的企业
你刚刚建立了一个炙手可热的新公司，完全基于区块链- BitBlockBaseCoinPay.cash。你想要跟上竞争对手的步伐CoinBitBlock。付费购买他们的产品。
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，你的秘密商业策略。
结论:
匿名性的缺乏意味着与你进行过交易的每个人都可以看到你过去和将来是如何花钱的。

Example: Businesses on the blockchain

You've just founded a hot new startup run purely on the blockchain - BitBlockBaseCoinPay.cash. You want to keep up to date with your competitor CoinBitBlock.pay so you purchase their product. Except now they know all of your operational expenses, how much revenue you have, who your customers are, and your secret business strategy.

Conclusion:

A lack of anonymity means everyone you've ever transacted with gets to see how you've spent your money in the past and forever into the future.

Source: CoinTelegraph

Anonymity and Ethics

匿名加密货币确实可以用于洗钱和在线购买毒品。
●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
○回忆AML/KYC:几乎可以匿名交易加密货币，但不能接触美元/英镑/欧元，没有护照照片
●“道德”难以在技术层面实现
○道德和不道德的使用案例从技术角度来看是相同的
对社会的正面利益是否大于成本?
○例子:Tor
■由美国政府创建。
●Tor通过一个免费的、全球的、志愿者覆盖的网络来指导互联网流量，该网络由超过7000个中继组成，可以隐藏用户的位置和使用情况，不让任何进行网络监视或流量分析的人知道。
■这使得官员难以监控网络流量，但他们找到了其他方法
■为压制性政权下的记者提供言论自由

Anonymous cryptocurrencies can indeed be used for money laundering and online drug purchases.

- Partial solution: the interfaces between cryptocurrencies and fiat currencies are highly regulated
  - Recall AML/KYC : can trade cryptocurrencies almost anonymously but can't touch USD/GBP/EUR without a picture of your passport
- Hard to implement "morality" at a technological level
  - Moral and immoral use cases look identical from a technological standpoint
- Do the positive benefits to society outweigh the costs?
  - Example: Tor (https://en.wikipedia.org/wiki/Tor_(anonymity_network))
    - Created by the U.S. government.
      - Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.
    - Makes it difficult for the officials to monitor web traffic, but they've found other ways
    - Enables free speech for reporters in oppressive regimes

Deanonymization Techniques

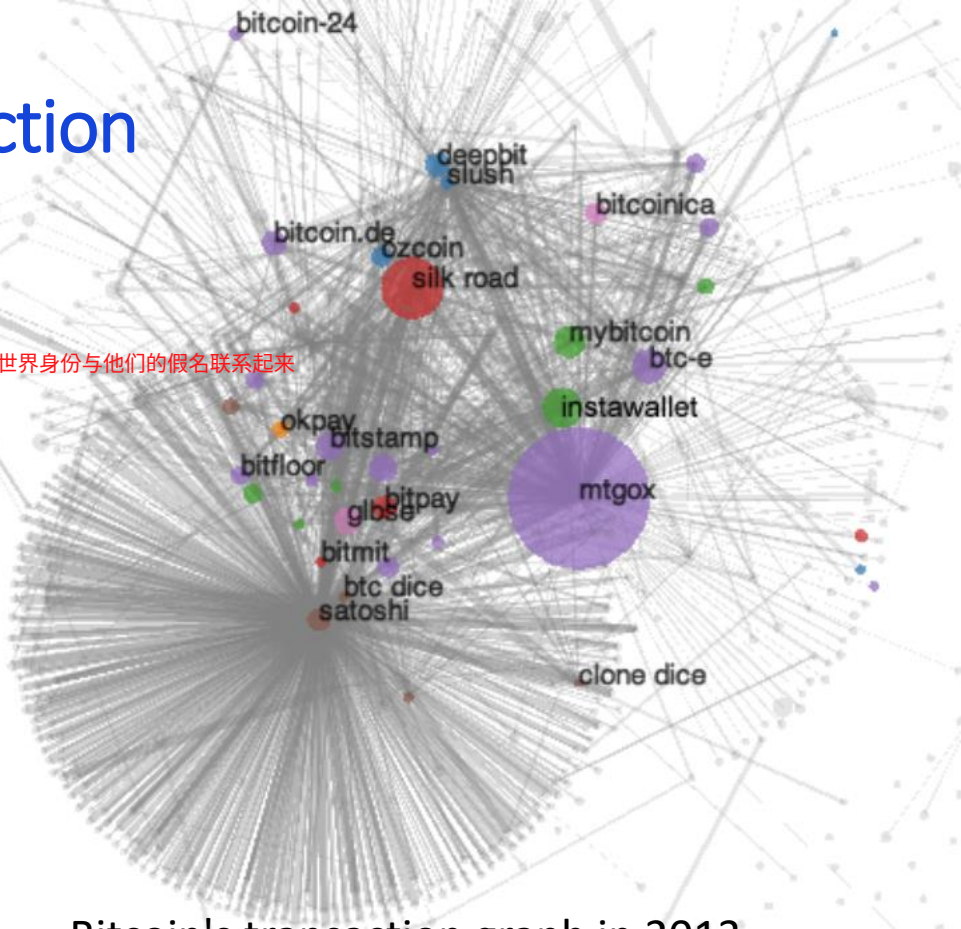
Deanonymization via Transaction Graph Analysis

交易图分析:
分析区块链中的交易图表
去匿名化的目标:将一个实体的真实世界身份与他们的假名联系起来
群集:将一群地址归属于同一实体

Transaction Graph Analysis: Analyzing the graphs of transactions in the blockchain

Goal of deanonymization: **Link** an entity's real world identity with their pseudonym(s)

Clustering: Attributing a **cluster** of addresses to the same entity



Bitcoin's transaction graph in 2013.

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names (Meiklejohn et al)

聚类

Clustering

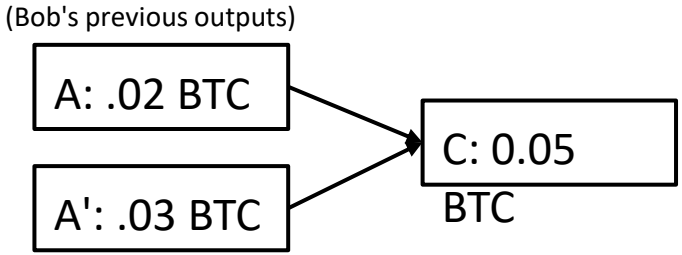
关联两个地址的两个主要启发式方法:
1. 交易输出合并
   a.当一笔交易有多个输入时发生
   b.相当合理的假设两个输入地址由同一个实体配对
      i.很少有人进行联合支付
2. 变更地址
   a.交易被分成0.95和0.05金额
      i.其中一个必须是变更地址，除非两件物品共同购买
   b.有用的启发:变更地址通常是新生成的-以前从未在区块链上看到过
在这两种情况下，如果地址A已知为Bob所拥有，我们现在就知道地址A'也为Bob所拥有

Two main heuristics to associate two addresses:

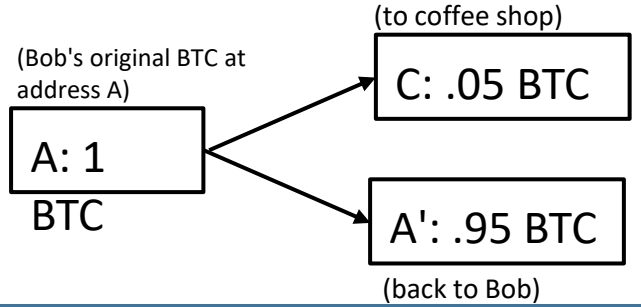
1. **Merging of transaction outputs**
   a. Occurs when there are multiple inputs to a transaction
   b. Fairly reasonable assumption that the two input addresses are paired by the same entity
      i. Rarely do people conduct joint payments
2. **Change addresses**
   a. Transaction is split into 0.95 and 0.05 amounts
      i. One of them must be a change address unless two items were purchased jointly
   b. Helpful heuristic: Change addresses are usually newly generated - never before seen on the blockchain

In both cases, if address **A** was known to be owned by Bob, we now know that address **A'** is also owned by Bob.

Case 1: Buying coffee of cost 0.05 BTC with 0.02 BTC and 0.03 BTC UTXOs. *A and A' merging into one output links them together.*



Case 2: Buying coffee of cost 0.05 BTC with a 1 BTC UTXO. *Identifying the change address links addresses A and A' together.*

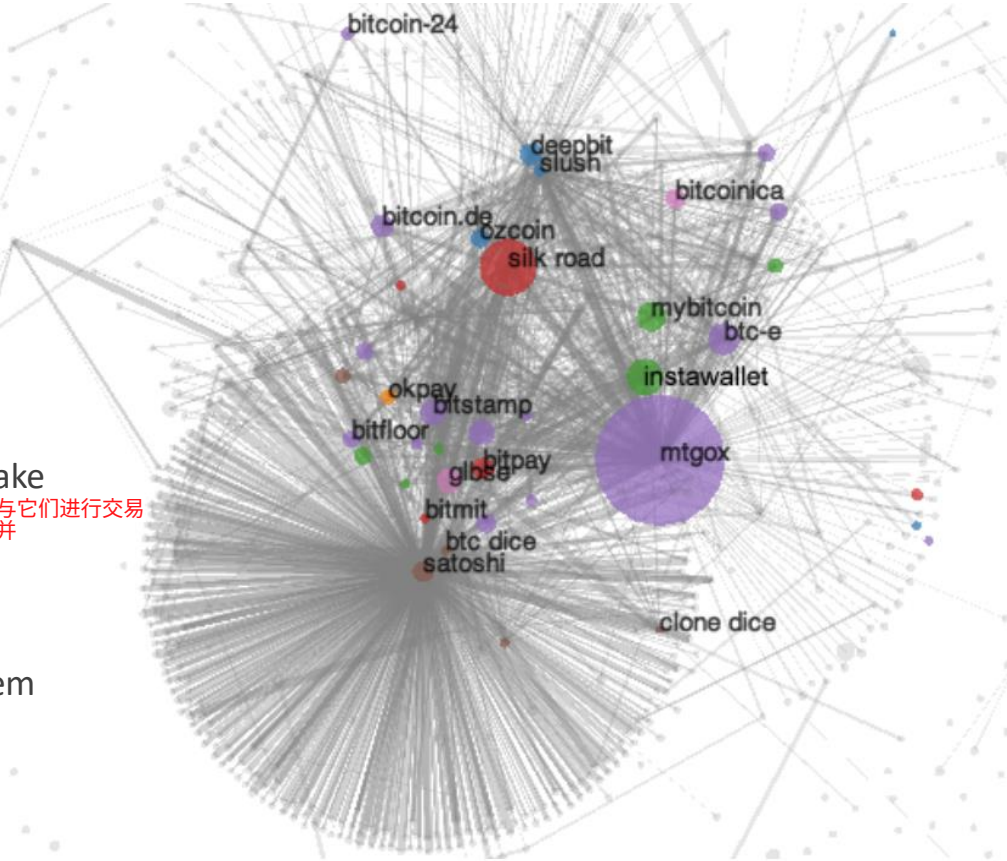


Identifying services

用现实世界的企业身份识别集群的几种技术:

Several techniques to identify clusters with the real world identities of businesses:

1. **Tagging by transacting**
   a. Go to online service (e.g. Coinbase) and make a transaction with them 进入在线服务(如Coinbase)，与它们进行交易
   b. Wait for address to be merged with rest of the cluster 等待地址与集群的其他部分合并
2. **Infer by looking at activity** 通过观察活动来推断
   a. In 2013, Mt. Gox was large part of ecosystem
      i. Large volume (large purple dot)
   b. SatoshiDice was a gambling site allowing smaller denominations
      i. Small volume (small dot)
      ii. Lot of transactions



Bitcoin's transaction graph in 2013.

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names (Meiklejohn et al)

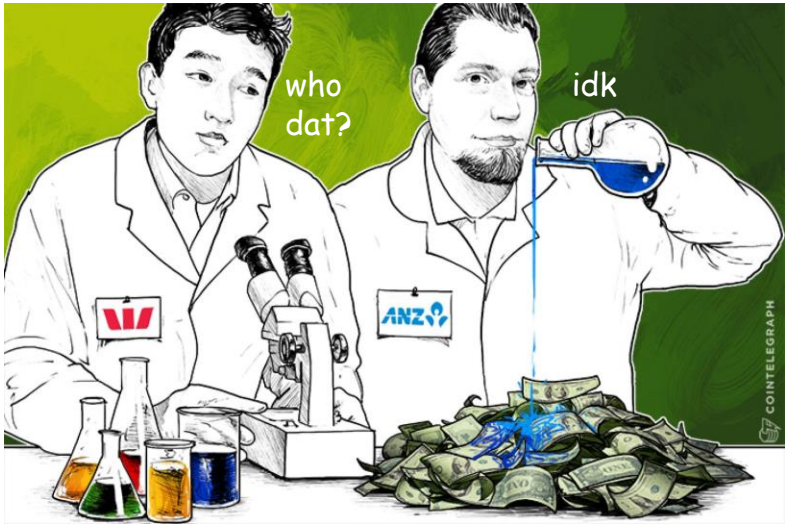
Identifying individuals

几种将地址与个人关联的技术

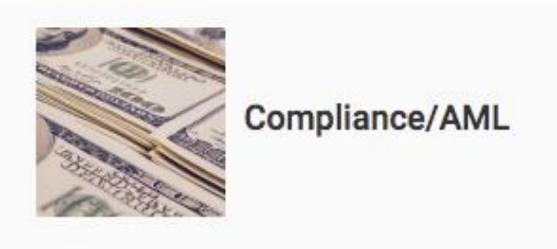
Several techniques to associate addresses with individuals:

1. **Sending them Bitcoin**
   - Obviously, they need to reveal an address
2. **Carelessness**

   在任何地方公开发布你的比特币地址(比如在论坛上)至少会显示一个地址
   - Posting your Bitcoin address publicly anywhere (like on forums) reveals at least one address
3. **Service providers**
   - Ex. Skry (previously Coinalytics)



Source: CoinTelegraph



Skry

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

Source: skry.tech ("Bloomberg for Bitcoin")

污点分析

Taint analysis

Each circle is an address.

Let **t** denote the "taint" at that address.

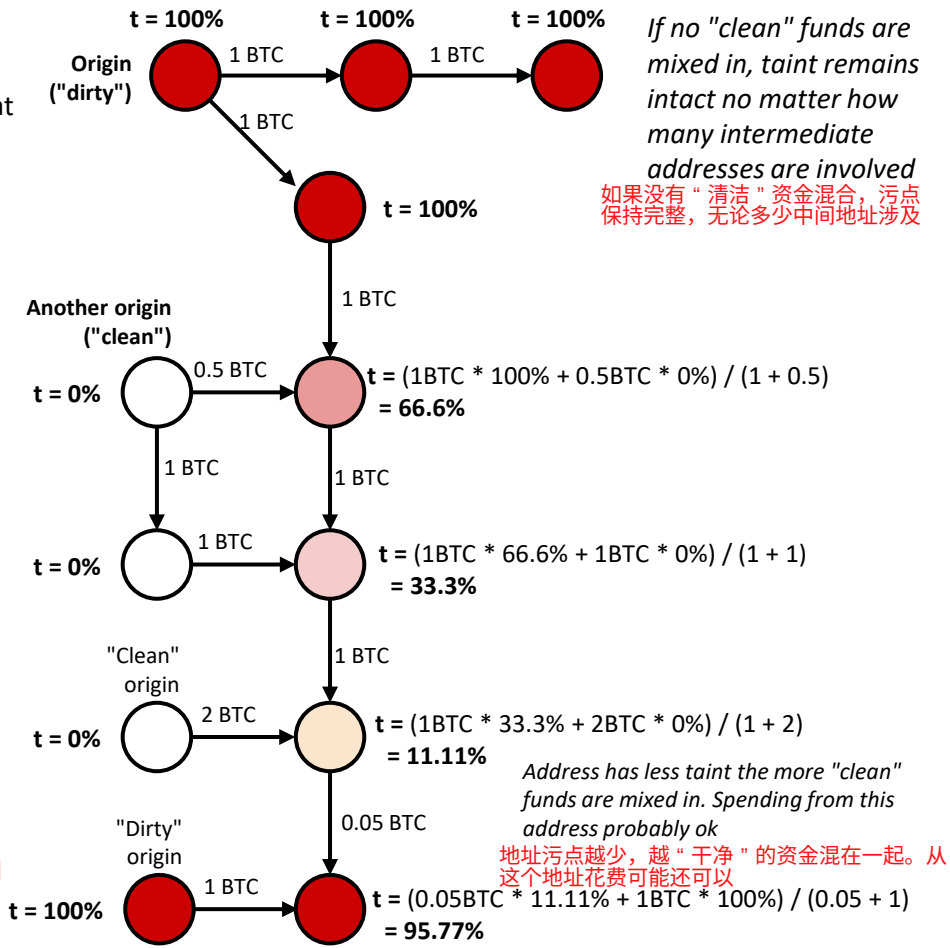
Taint is the percentage of funds received by an address that can be traced back to another address

Taint analysis can reveal useful information

- See whether money came from a 'tainted' source
- Example: tag a known "bad" address
  - E.g. Silk Road
  - Taint analysis ruined Ross Ulbricht's defense that his huge Bitcoin stash was obtained legitimately!

Naive anonymization strategy: send all your coins to a bunch of fresh addresses (**manual mixing**). Taint analysis is why manual mixing doesn't work!

污点是指一个地址收到的资金中可以追溯到另一个地址的百分比
污点分析可以揭示有用的信息
· 看看钱是否来自一个“ 肮脏的 ” 来源
· 例如:标记一个已知的“ 坏 ” 地址
· (丝绸之路)
· 污点分析破坏了罗斯 · 乌布里希的辩护，他的巨额比特币藏是合法获得的!
幼稚的匿名策略:将你所有的硬币发送到一堆新的地址(手动混合)。污点分析是手工混合不能工作的原因



If no "clean" funds are mixed in, taint remains intact no matter how many intermediate addresses are involved

如果没有“ 清洁 ” 资金混合，污点保持完整，无论多少中间地址涉及

Address has less taint the more "clean" funds are mixed in. Spending from this address probably ok

地址污点越少，越“ 干净 ” 的资金混在一起。从这个地址花费可能还可以

大量的交易会对污点产生强烈的影响

Large amounts transacted will have a strong effect on the taint

Taint analysis tool on Blockchain.info

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	1bankkjx5E9Xqd5... (Satoshi Dice Change Address)	2.497099566%	9	
5	1dice97ECuByXAv... (SatoshiDICE 50%)	2.2296799195%	24	

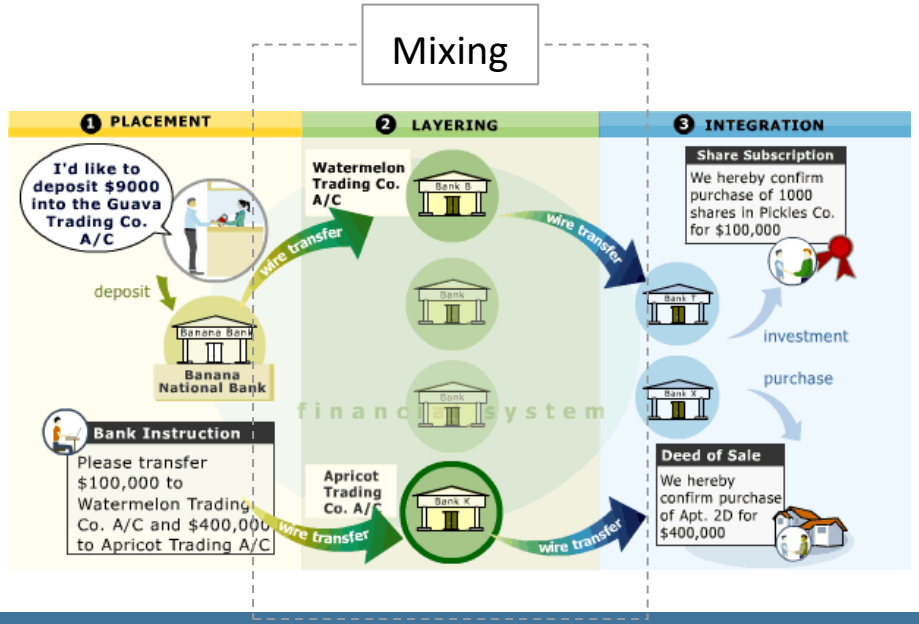
Anonymity through Mixing

Mixing

创建数百个虚假的“ 空壳 ”公司，这些公司不做任何事情，也不拥有任何资产，但看起来它们有(根据账簿和纳税申报单)。
随着时间的推移，把“ 肮脏 ”资金存入空壳公司。(位置)。
空壳公司把存款注销为购买、投资等，让存款看起来像真的一样。
空壳公司通过向其他空壳公司提供资金进一步混淆(分层)。
最后,犯罪组织。把“ 干净 ”的钱花在奢侈品上，例如钻石、汽车、房地产(一体化)。
区块链的混合利用了同样的理念

以隐瞒资金来源为目的进行交易

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.

source: http://casiinoo.blogspot.com/

匿名的正式框架

A Formal Framework for Anonymity

匿名集是一个实体与对应实体之间无法区分的假名集

Def.: An **anonymity set** is the set of pseudonyms between which an entity cannot be distinguished from her counterparts

Main goal of mixing:

- We want our anonymity set to be as large as possible
  - Conducting multiple rounds of mixing exponentially increases our anonymity set
  - If one round of mixing makes you indistinguishable among **N** peers, then size of anonymity set is **N** for one round, $\mathbf{N^2}$ after two rounds, $\mathbf{N^3}$ after three, etc.
  - However, the size of the anonymity set is bounded by real world constraints

我们希望我们的匿名集尽可能大
〇进行多次混合会指数增加我们的匿名集
〇如果一轮混合使得你在N个同伴中无法区分，那么第一轮匿名集的大小为N，两轮后为N2，三轮后为N3，等等。
〇然而，匿名集的大小受到现实世界的约束

匿名集越大，对假名进行去匿名化或“重新链接”就越难。
●理想情况下，任何人都很难将身份与地址联系起来
额外的属性
●不受信任(无交易对手风险)
〇想要确保我们的资金在混合的时候不会被偷
●可信可否认的
〇从交易历史和你混合的任何其他数据痕迹中不应该很明显;也就是说，你的活动应该像正常的活动一样

The larger the anonymity set, the harder it is to deanonymize, or "re-link", pseudonyms to identities.

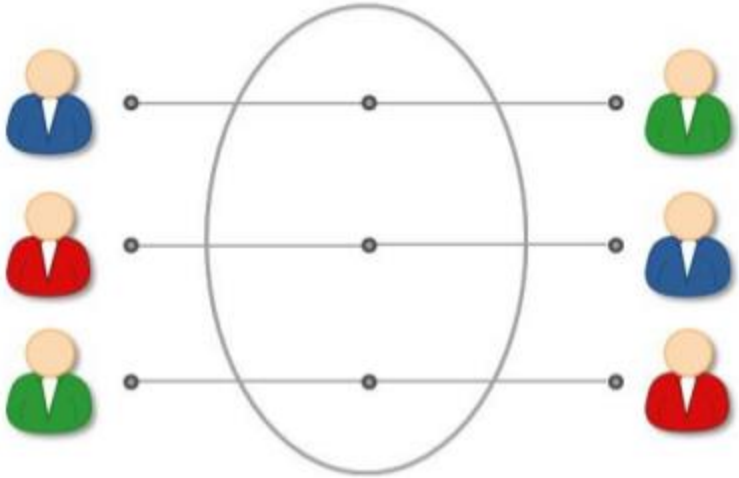
- Ideally, it is hard for **anyone** to link identities to addresses

Additional desirable properties

- **Trustless** (No counterparty risk)
  - Want to ensure that our funds can't be stolen while mixing
- **Plausibly deniable**
  - It shouldn't be obvious from transaction history and any other data traces that you're mixing; i.e. your activity should look just like normal activity

Types of Mixing

- Centralized Mixers
- Altcoin Exchange Mixing
- Decentralized Mixing Protocols
- Privacy-focused Altcoins

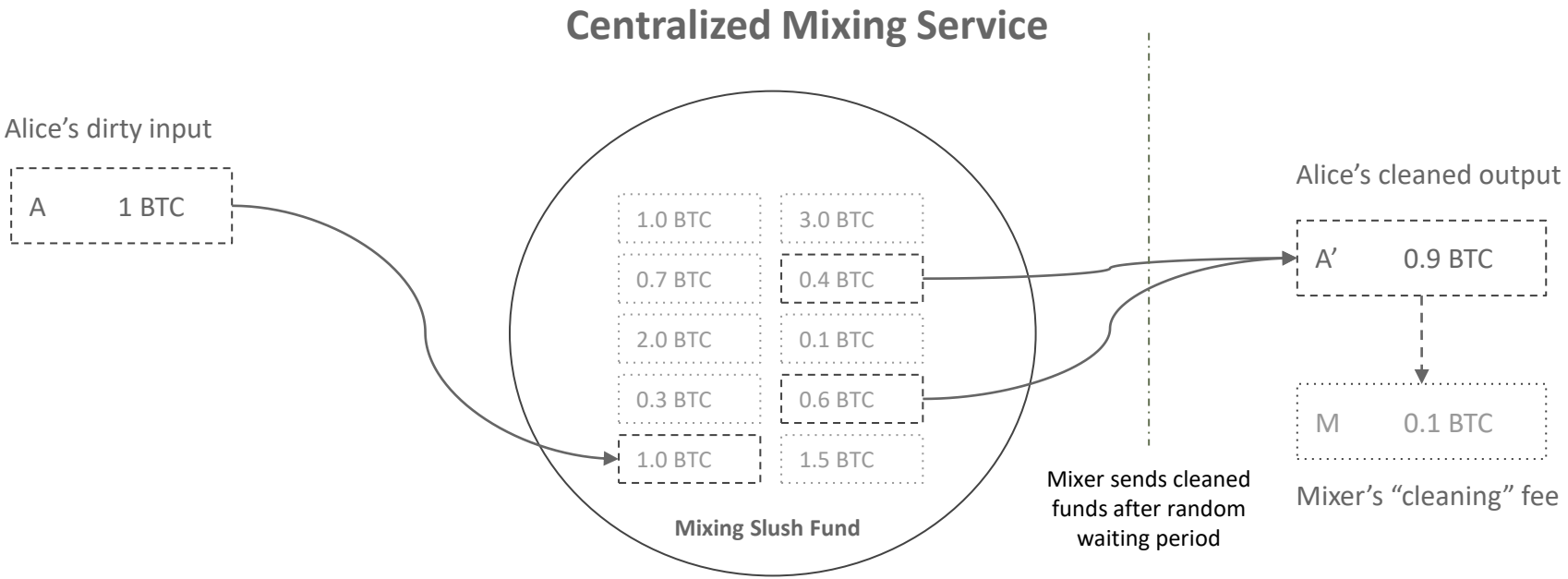


Centralized Mixers

Centralized Mixers

发送硬币到第三方混合器地址，混合器发送(希望)未连接的硬币到您在不久的将来(以减少时间信息泄漏)

Send coins to third-party mixer address, mixer sends (hopefully) unlinked coins to you sometime in near future (to minimize timing information leak).



Centralized Mixers - Issues

对手风险:混合器可能窃取资金;必须相信它不会。
记录风险:混合器可能会记录它从谁那里收到的脏钱，以及它把清理的钱送到了哪里。
集中风险:单点故障。黑客攻击的单一目标。对手(如政府)安装它自己的日志或发送一个删除通知，并夺取对混合器的控制

Counterparty Risk: Mixer could steal funds; have to ***trust*** that it won't.

Logging Risk: Mixer could be logging who it received dirty funds from and where it sent the cleaned funds to.

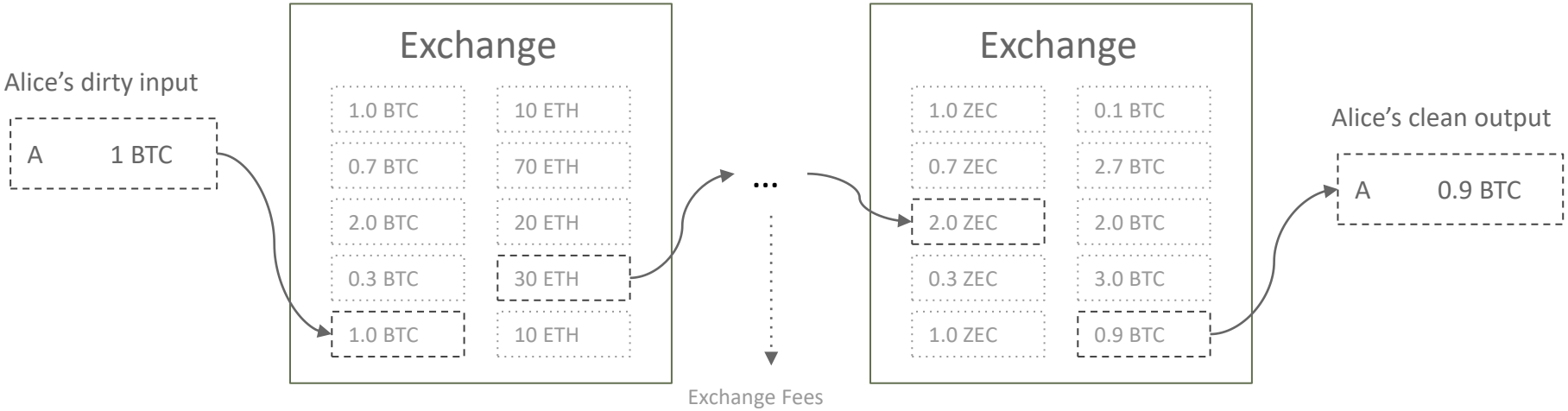
Centralization Risk: Single point of failure. Single target for hacking. Adversary (e.g. Government) installs its own logging or sends a takedown notice and seizes control of mixer.

Altcoin Exchange Mixing

Altcoin Exchange Mixing

通过几层altcoin发送脏基金⇐⇒altcoin交换以混淆资金来源

Idea: Send dirty funds through several layers of altcoin ⟺ altcoin exchanges to obfuscate money trail.



Altcoin Exchange Mixing - Issues

Pros:

对手将不得不通过几个不同的区块链和交易所追踪交易链。
更合理的推诿——看起来像是正常的货币交换

+ Adversary would have to trace transaction chain through several disparate blockchains and exchanges.
+ Better plausible deniability -- looks like normal currency exchanging.

Cons:

依赖交换器来隐藏交易映射
交易对手风险:交易所被黑，在交易过程中亏本
(美国)交换通常需要个人身份信息，并遵循KYC/AML

- Rely on exchanges keeping transaction mappings hidden
- Counterparty risk: Exchange gets hacked ⇒ Lose money in transit
- (U.S.) Exchanges usually require personally identifiable information and follow KYC/AML.

Decentralized Mixing

Decentralized Mixing Protocols

想法:去掉中间人(中央混合机)，避免交易对手风险和费用。
建议:创建一个比特币网络之外的对等网络，他们合作进行混合他们的货币的交易，而不依赖于可信任的第三方

Idea: Remove counterparty risk and avoid fees by taking out the middleman (centralized mixer).

Proposition: Create a network of peers outside of Bitcoin network who cooperate to make transactions which mix their coins, without relying on a trusted third party.

Can this be done?

Dmix Research Project

这就是我们要回答的问题
Well, this is the question is sought to answer.

Dmix Project: Build a **trustless**, **decentralized Bitcoin** mixer that maintains **plausible deniability**. 建立一个不可信的、分散的比特币混合器，保持貌似可信的否认。

Additional requirements:

- **Low fees** 混合的成本不应该过高;将是不切实际的
  - Mixing shouldn't be cost-prohibitive; would be impractical
- **Bitcoin-compatible**
  - Sure, you can mix with a variety of altcoins. But what if you don't want to go through the hassle of exchange? No one has yet developed a Bitcoin mixer with these properties.当然，你可以和各种不同的硬币混合使用。但如果你不想经历交易的麻烦呢?到目前为止，还没有人开发出一款具有这些属性的比特币混合器
    - Not to mention Lightning Network doesn't exist yet 更不用说闪电网络还不存在
      - So let's build Dmix!

敌对的模型:
●被动的对手
○不是混合的一部分
○基本匿名防止被动对手学习映射
●Semi-honest对手
○组合中的一部分
○正确地遵循协议，但试图通过分析混合的程序去匿名化混合。
●恶意对手
○组合中的一部分
○不受规程规范的约束;会主动背离协议并企图窃取资金
○可能会发送错误的信息，放弃交流，等等。

Decentralized Mixing Protocols - Nuances

Additional considerations for designing a good decentralized mixing protocol

设计一个好的分散混合协议的附加注意事项

混合包括输入和输出:

●一个输入和一个输出属于同一个实体，混合的目标是隐藏所有输入到所有输出的映射

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).

正确性:硬币不能丢失、被盗或重复使用。混合是真正随机的，必须最终成功混合或退回诚实用户的资金(抵抗DoS攻击的弹性)

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.

Decentralized Mixing Protocols - Nuances

分散混合背景下的西比尔阻力有两部分定义：

Sybil resistance in the context of decentralized mixing has a two part definition:

抵制盗窃资金
○不能依靠“部分”门限加密来加强正确性(例如m-of-n multisig，使m < n)。
○协议必须正确执行(没有资金被偷)，即使所有的同伴都是恶意的对手

1. Resistance to stealing funds
   - Can't rely on 'partial' threshold cryptography to enforce correctness (e.g. m-of-n multisig such that m < n).
   - Protocol must execute correctly (no funds are stolen) <u>even if all other peers are malicious adversaries</u>
2. Resistance to deanonymization
   - **Weak**: Participants <u>outside</u> the mix cannot determine the mapping of inputs to outputs, but participants <u>within</u> the mix can. 混合之外的参与者不能确定输入到输出的映射，但是混合内的参与者可以
     - Only requires one semi-honest adversary to break anonymity 只需要一个半诚实的对手即可打破匿名
   - **Strong**: Even participants <u>within</u> the mix do not know the mapping of inputs to outputs 即使是混合的参与者也不知道输入和输出的映射
     - However, a high proportion of Sybil peers reduces the anonymity set. 但是，较高比例的Sybil节点减少了匿名集

Protocol - CoinSwap (2013)

Idea: Natural extension of centralized mixer: “A mixer that can’t run with your coins.”

Using hash-locked, 2-of-2 multi-signature transactions, we can trustlessly send coins through a third-party mixer and the mixer can’t steal the funds.

Pros:

+ **No counterparty risk**; mixer can’t steal funds.
+ **Better plausible deniability;** passive adversary only sees 2of2 multi-signature transactions

Cons:

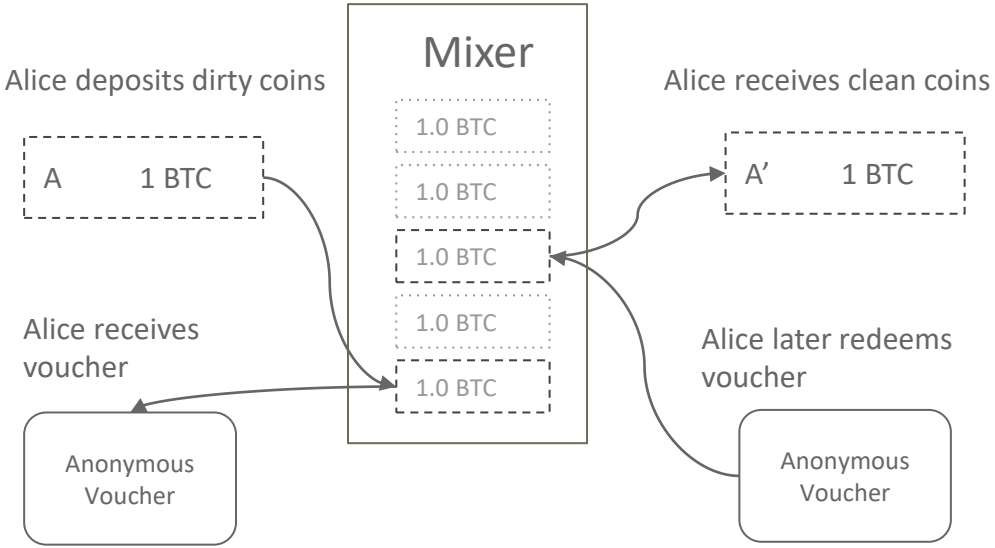
- **Values not hidden;** mixer still sees amounts transferred
- **Mappings not hidden;** mixer knows who receives which coins
- **Expensive;** uses 4 transactions per mix round

价值未隐藏;混合器仍然看到转移的数量
映射未隐藏;混合器知道谁收到了哪个硬币
贵;每轮混合使用4个交易

CoinSwap: https://bitcointalk.org/index.php?topic=321228.0

Protocol - TumbleBit (2016)

Idea: Improve on CoinSwap so the mixer **can't steal funds** and **never learns who receives the clean funds**.



Requires a total of 2 transactions on blockchain.

Anonymous vouchers can't be distinguished from one another and also can't be forged.

Enables Alice to deposit her dirty coins and receive clean, unlinked coins without revealing herself.

Not restricted to just single mixer. Can be used as primitive in more complex protocols

Recipient does not have to be depositor.

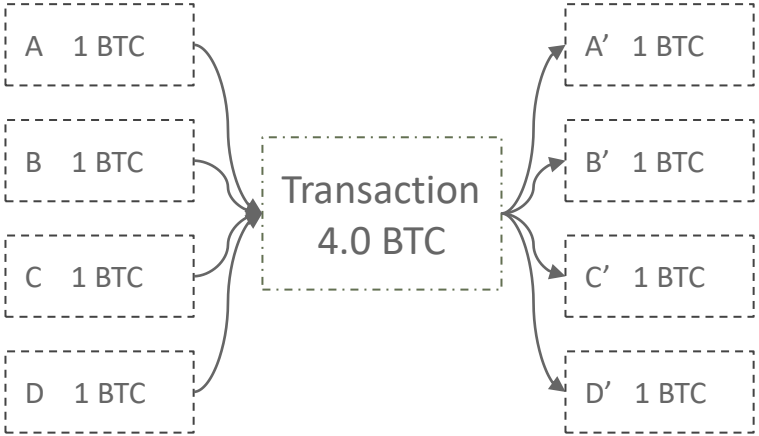
在区块链上总共需要2个事务。
匿名凭证不能区分，也不能伪造。
使爱丽丝能在不暴露自己的情况下存放脏硬币和接收干净、没有连接的硬币。
不局限于单个混合器。可以在更复杂的协议中作为原语使用
收款人不一定是存款人

TumbleBit: https://eprint.iacr.org/2016/575.pdf

Protocol - CoinJoin (2013)

在单一的n-of-n多重签名交易中混合硬币

Alternative Approach: Mix together coins in a single n-of-n multisignature transaction.



Pros:

+ Funds can’t be stolen
+ No central mixing party who needs enough liquidity for good anonymity.

没有需要足够流动性来保证良好匿名性的中央混合方

Cons:

很容易在区块链上发现，因为n-of-n多签名交易，其中n通常很大

- **Not plausibly deniable;** very easy to spot on the blockchain since n-of-n multisignature transaction where n is usually large.
- **Not DoS attack resistant;** only needs 1 malicious node to start protocol and then halt halfway through to disrupt.

只需1个恶意节点就可以启动协议，并在中途停止以中断协议。

- Anonymity set limited to transaction participants.

匿名设置仅限于交易参与者

CoinJoin: https://bitcointalk.org/index.php?topic=279249.0

JoinMarket (2015)

Idea: Create market of liquidity providers who are willing to mix their coins for a fee.

想法:创造一个流动性提供者的市场，这些流动性提供者愿意以一定的费用混合他们的硬币。
由于做市商几乎不承担风险，混合佣金通常非常小。

Since market makers take almost no risk, mixing fees are typically very small.

Issues:

- Mixed coins have small anonymity set
- Deanonymizing entire system would require only $32,000 (recoverable after attack) with success rate of ~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	J5CZTub55wvWFZBu	0	0.00000969	0.00000000	0.00003830	0.00160000
Absolute Fee	J5CZTub55wvWFZBu	4	0.00001000	0.00000000	0.00003830	7.49206132
Absolute Fee	J5CZTub55wvWFZBu	25	0.00001000	0.00000000	0.00003830	0.01200000
Absolute Fee	J54ipjp2Diz9XqMS	1	0.00001750	0.00000000	0.00010000	0.99999999
Absolute Fee	J5CZTub55wvWFZBu	2	0.00002700	0.00000500	0.00003830	7.08951594
Absolute Fee	J5CZTub55wvWFZBu	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	J5CZTub55wvWFZBu	14	0.00003000	0.00000000	0.00003830	4.14202467
Absolute Fee	J57wggYo1Q3uDjyV	0	0.00003100	0.00000100	0.00100000	1.44742679
Absolute Fee	J5CZTub55wvWFZBu	1	0.00003630	0.00000000	0.00003830	2.99999999
Absolute Fee	J54MdBzKZpz1xp4c	3	0.00003630	0.00000000	2.00000000	2.99999999
Absolute Fee	J5CZTub55wvWFZBu	17	0.00004100	0.00000100	0.00003830	5.09930543
Absolute Fee	J54exwiYnGkhJB9j	0	0.00004100	0.00000100	0.00100000	3.81806101
Absolute Fee	J5CZTub55wvWFZBu	5	0.00004287	0.00000000	0.00003830	1.99999999

JoinMarket: https://github.com/JoinMarket-Org/joinmarket
Möser, Böhme: http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_58.pdf

Protocol - CoinParty (2015,2016)

分散混合协议，但有更好的可推诿性。希望交易在被动的观察者看来与正常的比特币交易一样。

Idea: Decentralized mixing protocol but with better deniability. Want transactions to look the same as normal Bitcoin transactions to passive observers.

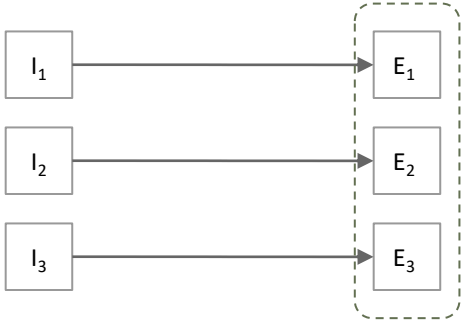
I	Input address
E	Escrow address
O	Output address

CoinParty允许我们这样做，但牺牲了一些协议安全性

CoinParty lets us do this, but sacrifices some protocol security.

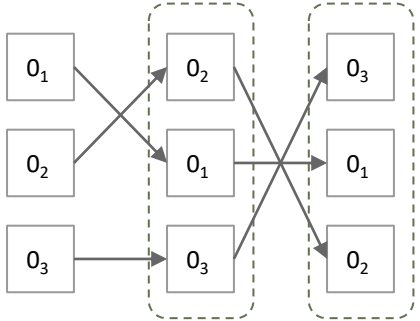
Peers generate escrow addresses. Escrow addresses require ⅔ consensus to spend.

对等点生成第三方地址。第三方地址需要花⅔共识



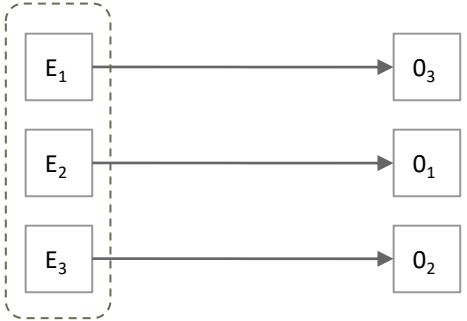
Peers perform secure multi-party shuffle on output address ordering.

对等点在输出地址排序上执行安全的多方转移



If protocol executed correctly, peers agree to transfer funds out of escrow addresses to designated outputs.

如果协议正确执行，对等点同意将资金从第三方地址转移到指定输出



1 COMMITMENT

2 SHUFFLE

3 TRANSACTION

Protocol - CoinParty (2015,2016)

Pros:

+ **High plausible deniability;** transactions on the blockchain look just like “normal” Bitcoin transactions.

+ **Decent efficiency;** requires 2 transactions on the blockchain per input peers.
每个输入对等点需要区块链上的2个事务

Cons:

- **Reduced protocol security;** escrow funds controlled by ⅔ threshold signature scheme.

- **Vulnerable to Sybil Attack;** malicious peer can spawn several fake peers, join mix group, overthrow ⅔ threshold, and steal mix group’s funds.

Dmix "Swinger Protocol" & Project Conclusion

Dmix项目的最后一个迭代:Swinger协议

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 obliviously 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
- You were the designated pair for another pair; you receive an incoming wife from that pair. Your husband performs CoinSwap with the incoming wife.
- Abort protocol if no wife or more than one wife were received.

· 和你的混合组成一组，指定一个为“丈夫”，另一个为“妻子”
· 成对地执行mixnet解密，以获得一个指定的对，你的对将与之交换。
· 你的“妻子”被送到指定的丈夫那里。他们进行硬币互换来交换硬币
· 你是另一对指定的伴;你会收到来自那对夫妇的新妻子。你的丈夫与新任妻子进行硬币交换。
· 如果没有妻子或多个妻子被接收，终止协议

当前存在的任何东西都不能满足Dmix项目的设计目标

Nothing that currently exists meets the design goals set out for the Dmix project

- Swinger Protocol comes close, but has a lesser degree of anonymity than the naive mixing strategy of simply executing CoinSwap with random nodes on the Dmix network
- Forming mixing groups actually reduces the anonymity set since Sybils

· Swinger协议与之很接近，但其匿名性要低于简单地在Dmix网络上与随机节点执行CoinSwap的朴素混合策略
· 形成混合群实际上减少了自Sybils以来的匿名集

Conclusion: Building a good decentralized Bitcoin mixer is **damn hard**.

建立一个好的去中心化的比特币混合器是非常困难的

Privacy-focused Altcoins

CoinJoin ⇒ DASH

DASH (formerly DarkCoin) is a privacy-centric cryptocurrency that employs a network of Masternodes to perform privileged actions such as voting on proposals, instantly confirm transactions, and **mix the coins (by default) of all network participants.**

DASH(以前的暗币)是一种以隐私为中心的加密货币，使用的网络是Masternodes以执行特权操作，例如对提议进行投票，立即确认交易，以及(默认情况下)混合所有网络参与者的硬币

Pros:

- Uses CoinJoin for mixing: **trustless**
- No issue of plausible deniability with using CoinJoin since almost everyone on the entire network is participating in CoinJoin transactions

· 使用CoinJoin混合:不可信
· 由于几乎整个网络上的每个人都参与了CoinJoin交易，所以使用CoinJoin没有合理否认的问题

Cons:

主节点网络本身必须是安全的--可以支付1000 DASH每个主节点以假设获得大量他们

- Masternode network itself must be secured - can pay 1000 DASH per masternode to hypothetically acquire a large number of them

Dash是一种开源加密货币，是一种由称为“主节点”的用户子集运行的分散式自治组织(DAO)。这是一种从比特币协议派生出来的替代币。这种货币允许无法追踪的快速交易。45%的被开采的硬币流向了矿工，45%流向了masternode，10%进入了DAO投资的一只基金。

Dash is an open source cryptocurrency and is a form of decentralized autonomous organization (DAO) run by a subset of users, called "masternodes". It is an altcoin that was forked from the Bitcoin protocol. The currency permits fast transactions that can be untraceable. 45% of mined coins go to miners, 45% to masternodes, and 10% into a fund that the DAO invests.

CryptoNote ⇒ Monero

使用环签名隐藏输入/输出映射。选择一些以前的输出来“混合”。然后将它们与您的输出绑定到一个加密环签名中

Idea: Hide input/output mappings with Ring Signatures. Choose some set of previous outputs to “mix” with. These are then bound with your outputs in a cryptographic ring signature.

在此上下文中，证明您拥有其中一个输出，但不说明具体是哪个输出

Ring Signature: In this context, prove you own one of the outputs without revealing which specific output.

· 在密码学中，环签名是一种数字签名，可以由一组用户中的任何成员执行，每个用户都有密钥。
· 因此，使用环签名的消息是由特定群体中的某人背书的。
· 环签名的一个安全属性是，确定哪个组成员的密钥被用来产生签名在计算上是不可行的
· 环签名与组签名相似，但在两个关键方面有所不同:第一，无法撤销单个签名的匿名性;第二，任何一组用户都可以作为组使用，无需额外设置。环签名由Ron Rivest、Adi Shamir和Yael Tauman发明，并于2001年在ASIACRYPT上引入。这个名字，环签名，来自于签名算法的环状结构。

- In cryptography, a **ring signature** is a type of digital signature that can be performed by any member of a group of users that each have keys.
- Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people.
- One of the security properties of a ring signature is that it should be computationally infeasible to determine *which* of the group members' keys was used to produce the signature.
- Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup. Ring signatures were invented by Ron Rivest, Adi Shamir, and Yael Tauman, and introduced at ASIACRYPT in 2001. The name, *ring signature*, comes from the ring-like structure of the signature algorithm.
- https://en.wikipedia.org/wiki/Ring_signature

Monero还没有隐藏交易值。对手可能通过跟踪可能的价值流来跟踪交易。时间相关性也提出了一个问题。

Issue: Monero doesn’t hide transaction values (yet). Adversary could potentially trace transactions by following likely value flows. Temporal correlations also pose an issue.

Issue: Decent anonymity set, but can we do better?

Monero（XMR)是一种开源加密货币，创建于2014年4月，专注于可替代性、隐私性和分散化。Monero使用了一种模糊的公共账本，这意味着任何人都可以广播或发送交易，但外部观察者无法得知交易的来源、金额或目的地。Monero使用工作证明机制来发行新硬币，并激励矿工确保网络安全和验证交易

Monero (**XMR**) is an open-source cryptocurrency created in April 2014 that focuses on fungibility, privacy and decentralization. Monero uses an obfuscated public ledger, meaning anybody can broadcast or send transactions, but no outside observer can tell the source, amount or destination. Monero uses a Proof of Work mechanism to issue new coins and incentivize miners to secure the network and validate transactions.

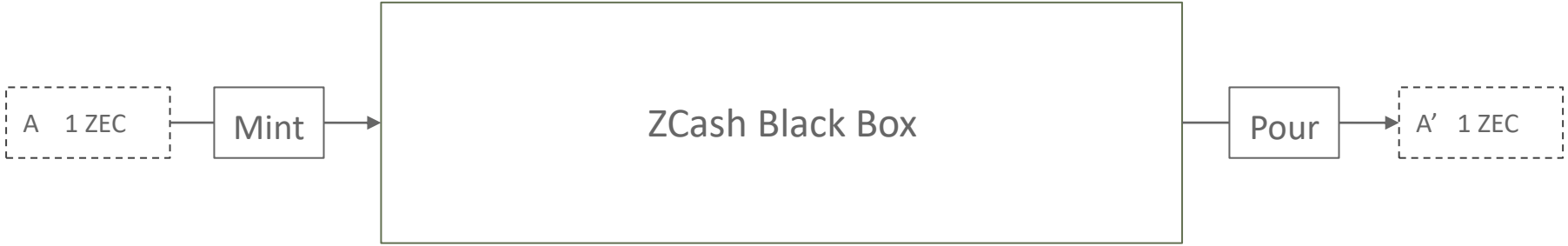
zk-SNARKs ⇒ ZCASH

在Altcoin中，事务不显示输入/输出地址和输入/输出值

Idea: Altcoin where transactions reveal *nothing* about input/output addresses AND input/output values.

使用零知识简洁的非交互知识参数(zk- snark)，又名"密码"我们可以创建一个支持完全匿名支付的系统

Using **zero-knowledge Succinct Non-interactive ARguments of Knowledge** (zk-SNARKs) a.k.a. “Crypto Magic” we can create a system which supports **fully anonymous payments**.



Zcash is a cryptocurrency aimed at using cryptography to provide enhanced privacy for its users compared to other cryptocurrencies such as Bitcoin. Like Bitcoin, Zcash has a fixed total supply of 21 million units. Transactions can be "transparent" and similar to bitcoin transactions in which case they are controlled by a t-addr, or can be a type of zero-knowledge proof called zk-SNARKs; the transactions are then said to be "shielded" and are controlled by a z-addr. Zcash coins are either in a transparent pool or a shielded pool; as of December 2017 only around 4% of Zcash coins were in the shielded pool and at that time most wallet programs did not support z-addrs and no web-based wallets supported them.

Zcash affords private transactors the option of "selective disclosure", allowing a user to prove payment for auditing purposes. One such reason is to allow private transactors the choice to comply with anti-money laundering or tax regulations. "Transactions are auditable but disclosure is under the participant's control.“ The company has hosted virtual meetings with law enforcement agencies around the U.S. to explain these fundamentals and has gone on the record of saying that "they did not develop the currency to facilitate illegal activity".

ZCash

Pros:

假设底层加密是安全的，黑箱事务是匿名的。整个黑箱历史的匿名集

+ **Fully Anonymous;** Assuming security of underlying crypto, blackbox transactions are anonymous. Anonymity set of entire blackbox history.

Cons:

- **Resource Intensive;** zk-SNARK proof system currently in use requires about 4 GB of RAM and 2 minutes of computation on modern CPU to generate proofs for pour transactions.
- **Requires Semi-Trusted One-time Setup;** adversary with toxic setup parameters can mint coins without spending base coins. Can be somewhat mitigated with a secure multiparty computation setup.

具有有毒设置参数的对手可以在不花费基础硬币的情况下铸造硬币。可以通过安全的多方计算设置有所缓解

Mixing Caveats

- Side channel attacks
  - Generally, we want to use TOR for everything
  - However, TOR exit nodes may be adversary-controlled

边信道攻击
○一般来说，我们想用TOR来表示所有的东西
○然而，TOR出口节点可能是对手控制的

- Analyzing transaction amounts
  - Easy to identify input and outputs (E.g. 1337.6969 BTC in -> 1337.420 out: hmmmmm 🤔)
  - Solution: Always use uniform transaction amounts (like 1 BTC, 0.1 BTC)
  - All transactions going through all mixes would look the same
  - For this reason, fees should be all or nothing

分析交易金额
○容易识别的输入和输出
○解决方案:始终使用统一的交易金额(如1比特币、0.1比特币)
○所有的交易经过所有的混合看起来是一样的
○基于这个原因，费用应该是全部或没有

- Timing correlations
  - Humans often act in predictable ways
  - Solution: the client that handles interactions with other peers should be automated

时间相关性
○人的行为通常是可预测的
○解决方案:处理与其他同伴的互动的客户应该是自动化的

- Network-level deanonymization (transaction propagation)
  - "The first node to inform you of a transaction is probably the source of it."

网络级去匿名化(交易传播)
○第一个通知你交易的节点可能就是交易的来源。

Conclusion

匿名性的大致比较水平：

Rough comparative level of anonymity:
(least anonymous to most anonymous)

1. Bitcoin
2. Centralized mixers
3. Decentralized mixing protocols
   a. CoinSwap
   b. CoinJoin
   c. CoinShuffle
   d. CoinParty
   e. Blindly Signed Contracts
   f. Tumblebit
4. Altcoin exchange
5. DASH
6. Monero
7. Zcash

Practical question: **How would I mix coins today?** (In November 2016)

- Probably altcoin exchange through DASH/Monero/Zcash + TOR/VPN + throwaway exchange accounts and emails

Lecture Outline

- ✓ Anonymity Basics
- ✓ Deanonymization techniques
- ✓ Anonymity through Mixing
- ✓ Centralized Mixers
- ✓ Altcoin Exchange Mixing
- ✓ Decentralized Mixing
- ✓ Privacy-focused Altcoins
- ✓ Conclusion

完

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكراً
Arabic

Obrigado
Brazilian Portuguese

Grazie
Italian

多谢
Simplified Chinese

Danke
German

Merci
French

நன்றி
Tamil
Tamil

ありがとうございました
Japanese

감사합니다
Korean