ANONYMITY MIXING AND ALTCOINS

Brian Ho
Gillian Chu

BLOCKCHAIN
AT BERKELEY

LECTURE OVERVIEW

1. ANONYMITY BASICS
2. INTRO TO DEANONYMIZATION
3. ANONYMITY THROUGH MIXING
4. ANONYMITY THROUGH ALTCOINS
5. MIMBLEWIMBLE

1

ANONYMITY BASICS

ANONYMITY BASICS

BLOCKCHAIN FUNDAMENTALS

“Is anonymity in Bitcoin only good for buying drugs?”

IS ANONYMITY ONLY FOR DRUGS?

BLOCKCHAIN FUNDAMENTALS

Imagine these scenarios in a blockchain-based financial world.

'Bob's Burgers'

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 porn site.

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 BASICS

BLOCKCHAIN FUNDAMENTALS

Blockchains are not anonymous by default.

- 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)

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

ANONYMITY BASICS

LINKING

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

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

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
  - But basic analysis renders this technique ineffective
- Not possible in Ethereum, since it is account-based (not UTXO based)

ANONYMITY BASICS

LEVELS OF ANONYMITY

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

- 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?

IS ANONYMITY ONLY FOR DRUGS?

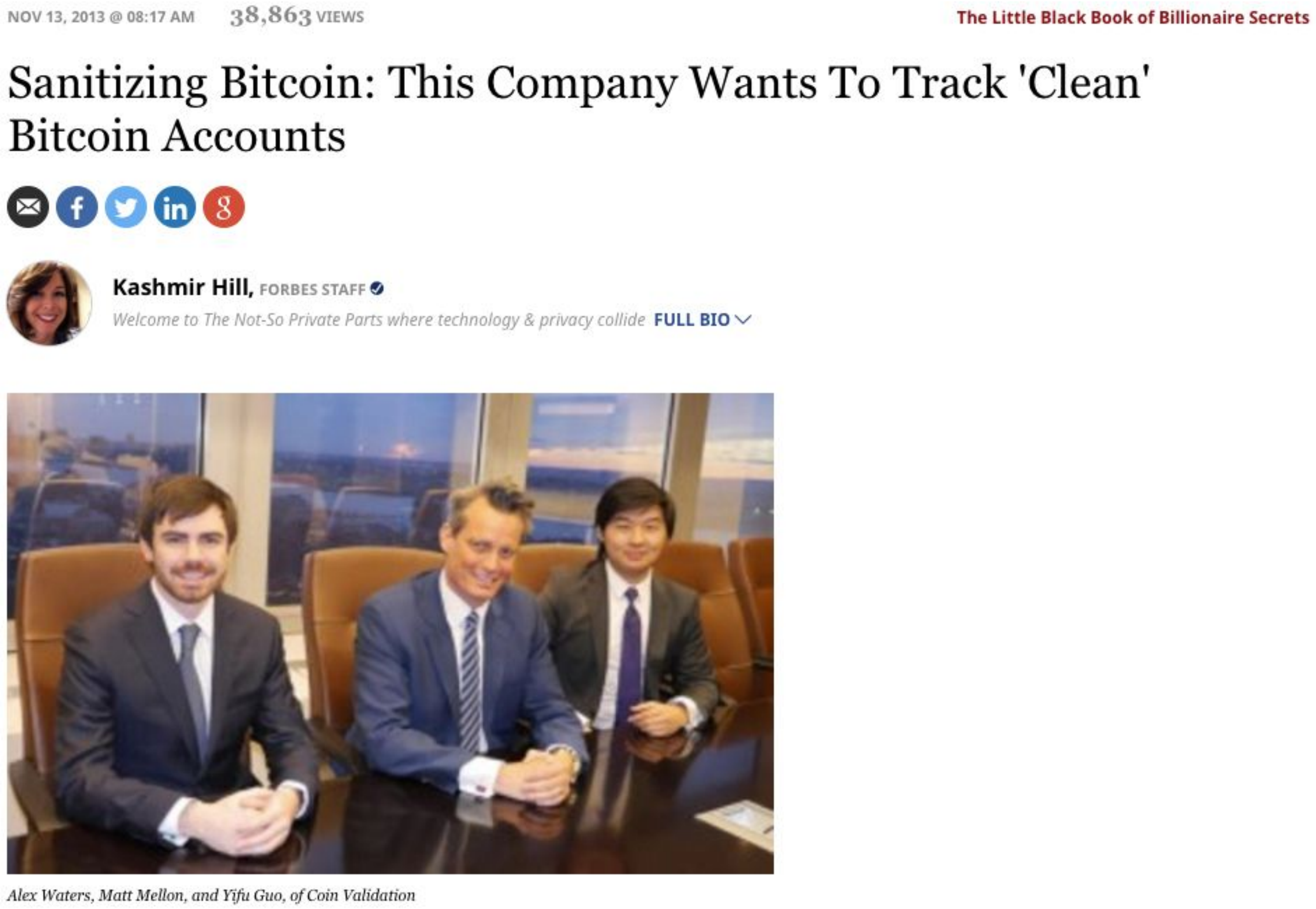
BLOCKCHAIN FUNDAMENTALS

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

- 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

IS ANONYMITY ONLY FOR DRUGS?

BLOCKCHAIN FUNDAMENTALS

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 & ETHICS

WHY ANONYMITY?

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 from last lecture: 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 from Princeton Textbook: Tor
        - Created by the U.S. government. Makes it difficult for the officials to monitor web traffic, but they've found other ways
        - Enables free speech for reporters in oppressive regimes

2 INTRO TO DEANONYMIZATION

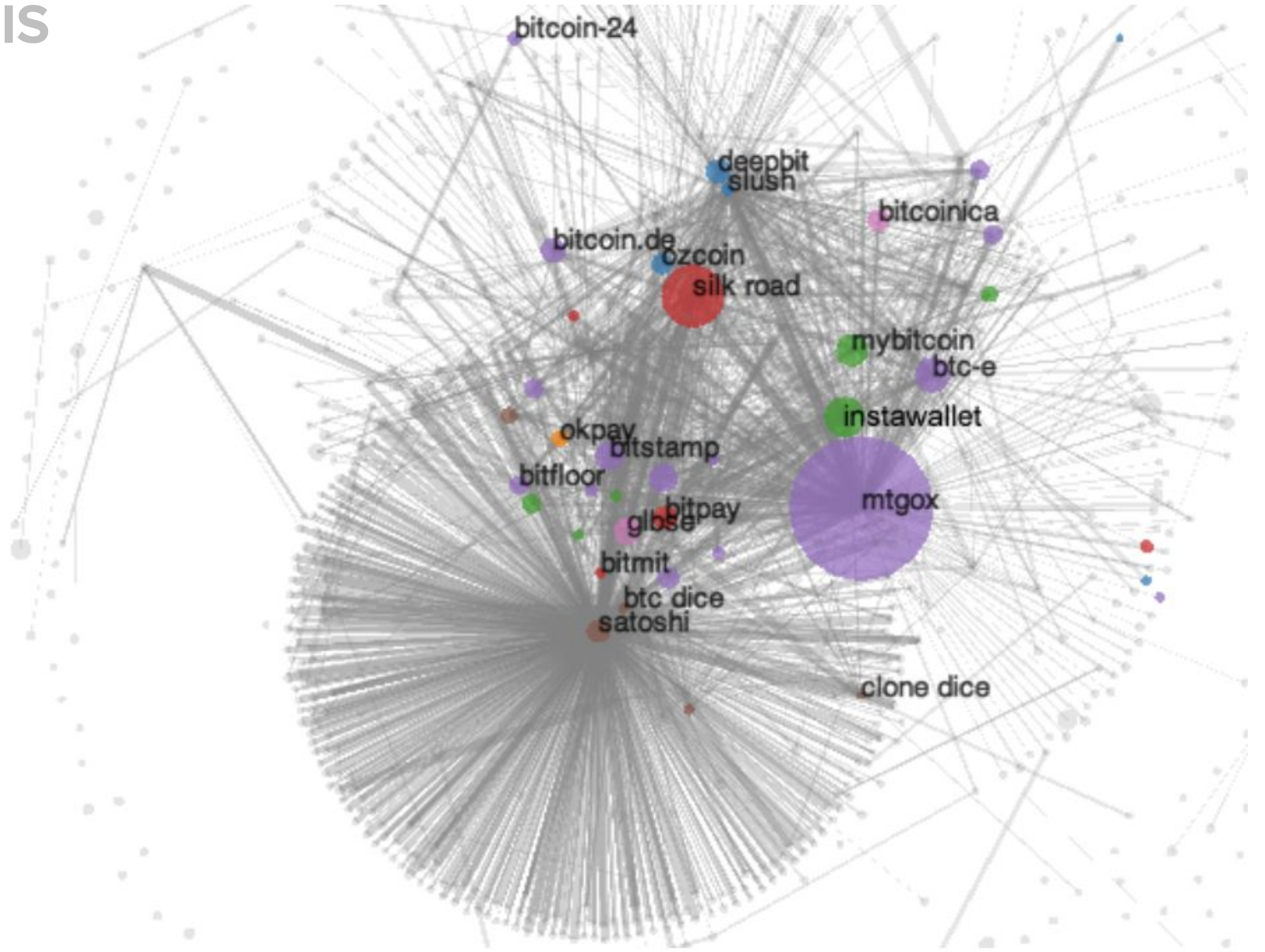
DEANONYMIZATION

TRANSACTION GRAPH ANALYSIS

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

Transaction Graph Analysis: Inspecting blockchain history to derive useful information

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)]

CLUSTERING

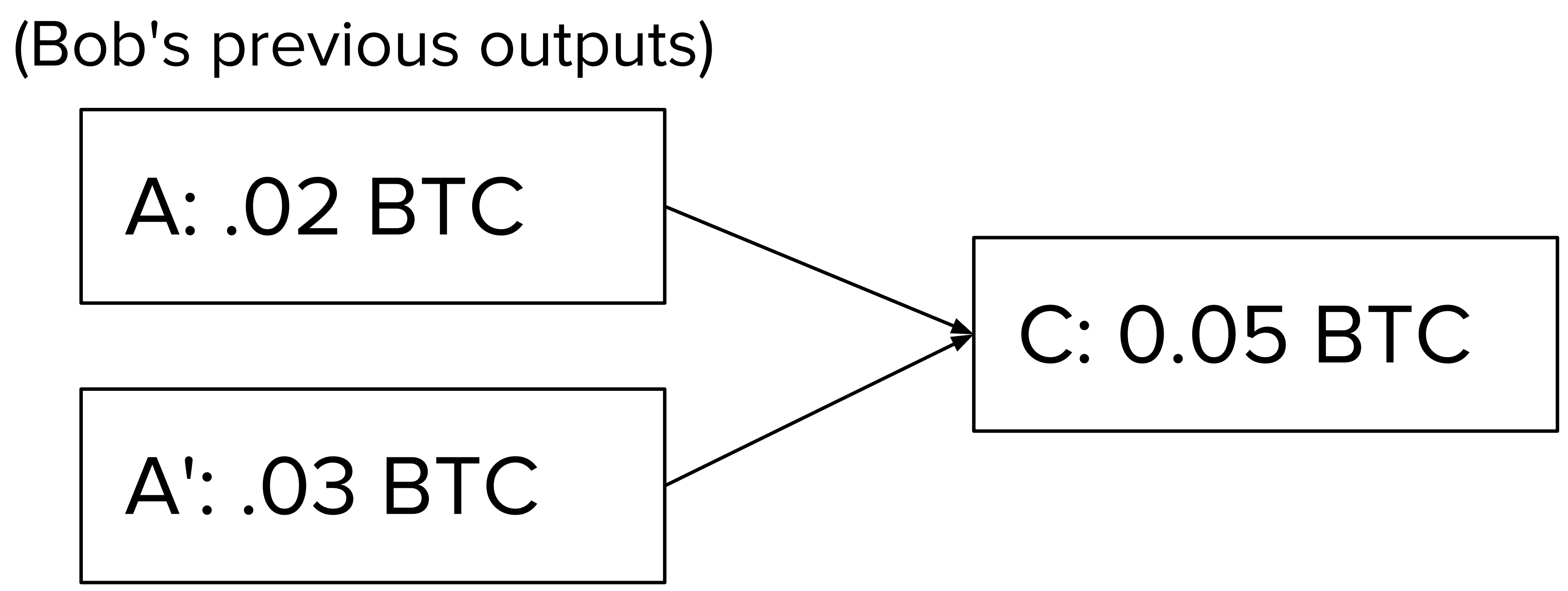
BLOCKCHAIN FUNDAMENTALS

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.*



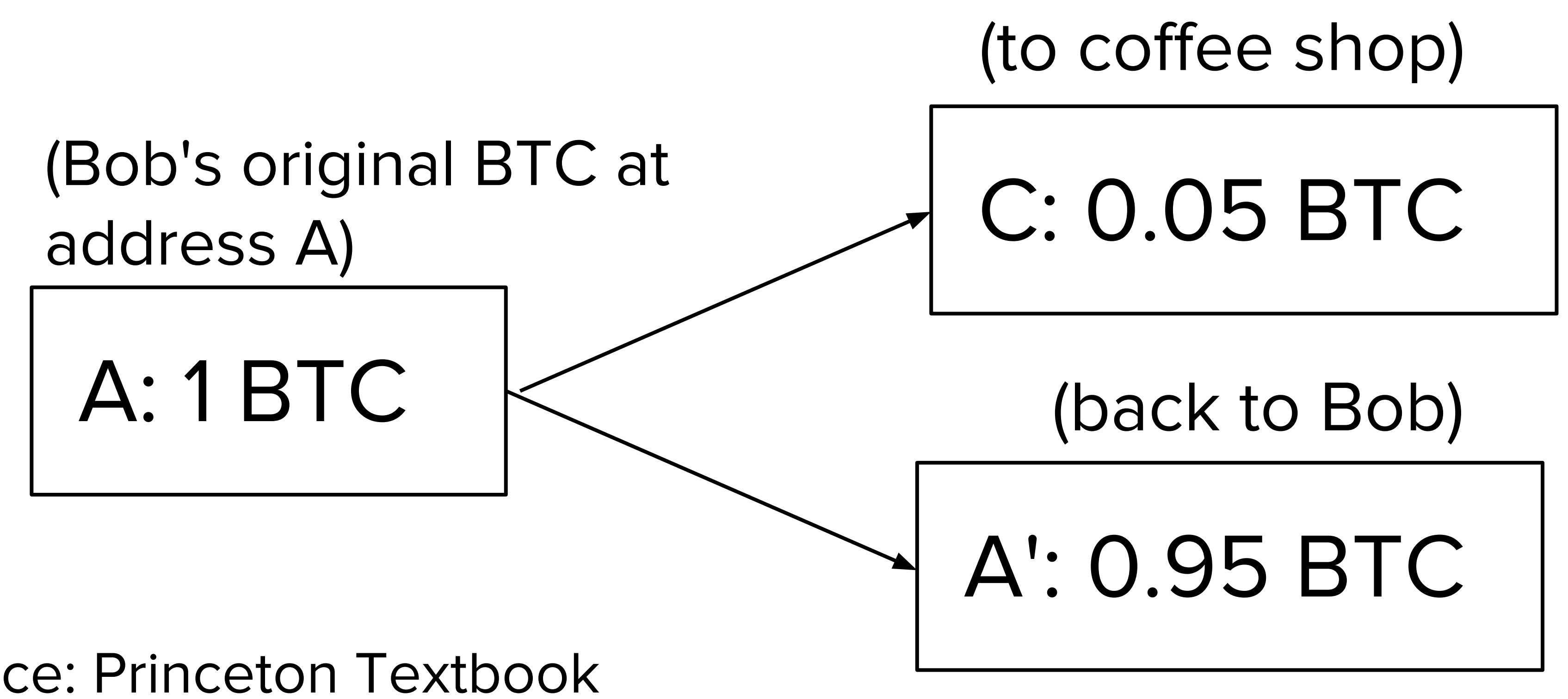
(Bob's previous outputs)

A: .02 BTC

A': .03 BTC

C: 0.05 BTC

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



(to coffee shop)

(Bob's original BTC at address A)

C: 0.05 BTC

A: 1 BTC

(back to Bob)

A': 0.95 BTC

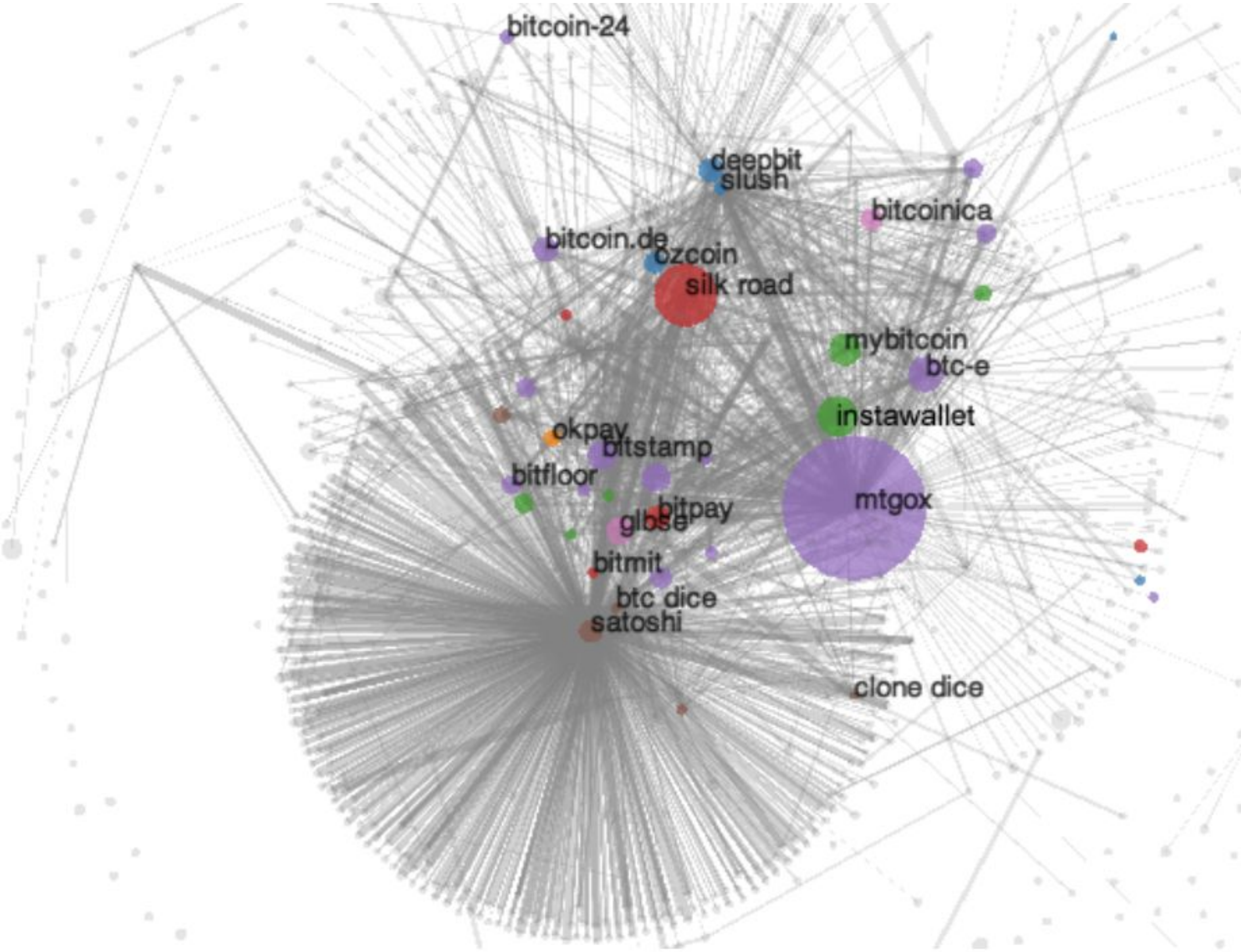
Source: Princeton Textbook

IDENTIFYING SERVICES

BLOCKCHAIN FUNDAMENTALS

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
   b. Wait for address to be merged with rest of the cluster
2. **Infer by looking at activity**
   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)

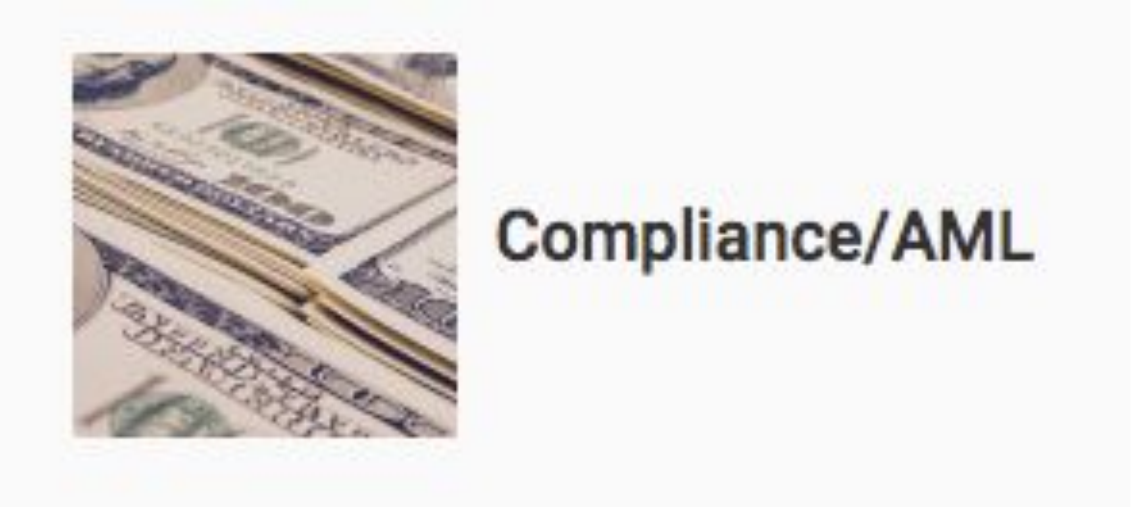
Source: Princeton Textbook

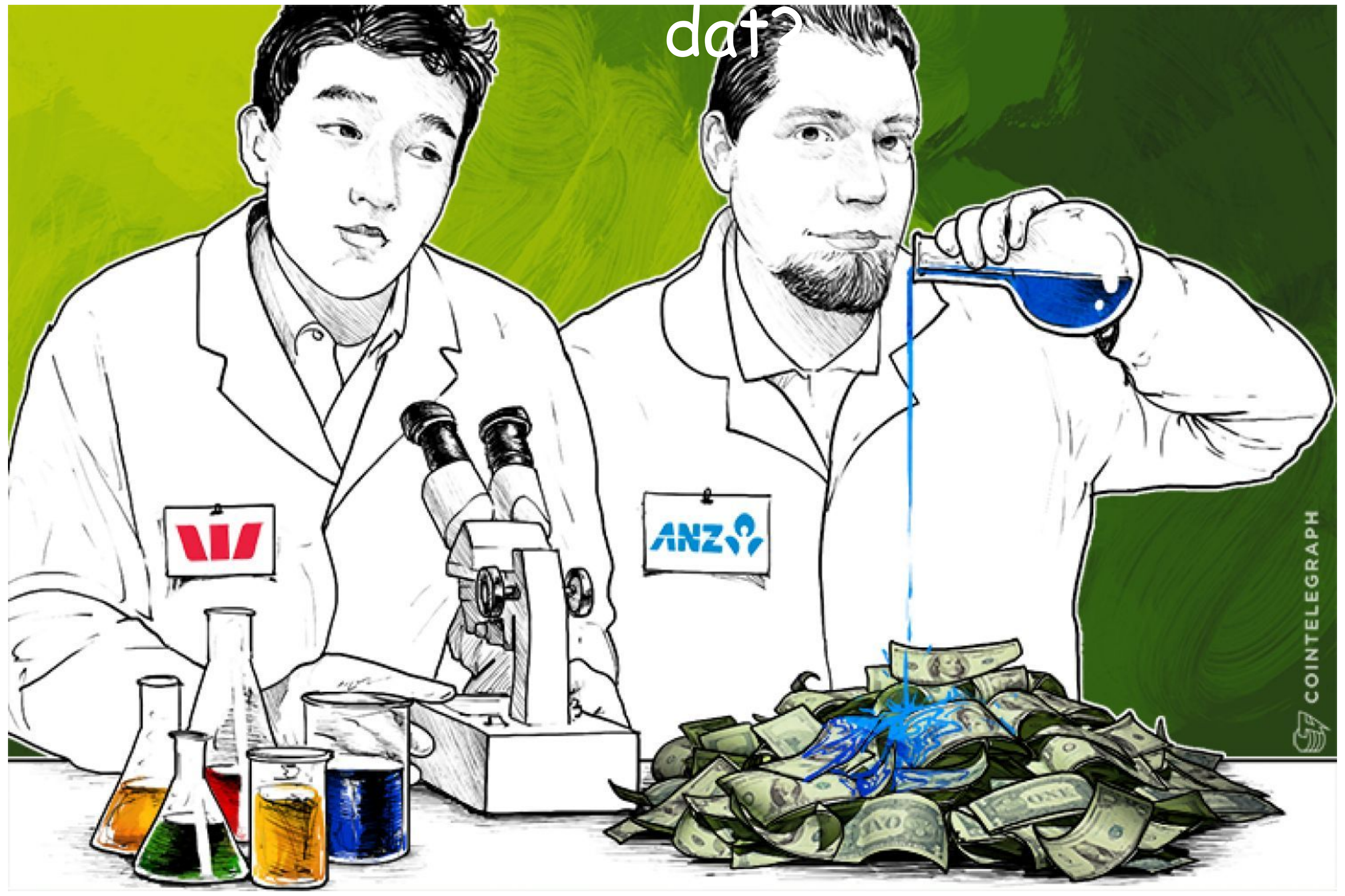
IDENTIFYING INDIVIDUALS

BLOCKCHAIN FUNDAMENTALS

Several techniques to associate addresses with individuals:

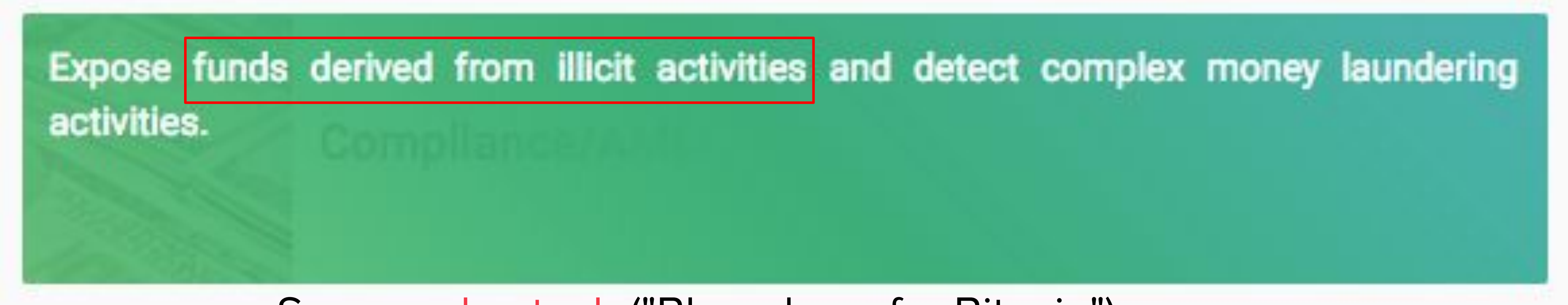
1. **Sending them Bitcoin**
    a. Obviously, they need to reveal an address
2. **Carelessness**
    a. Posting your Bitcoin address publicly anywhere (like on forums) reveals at least one address
3. **Service providers**
    a. Ex. Skry (previously Coinalytics)


Compliance/AML



Source: CoinTelegraph

Skry


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

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

TAINT ANALYSIS

BLOCKCHAIN FUNDAMENTALS

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

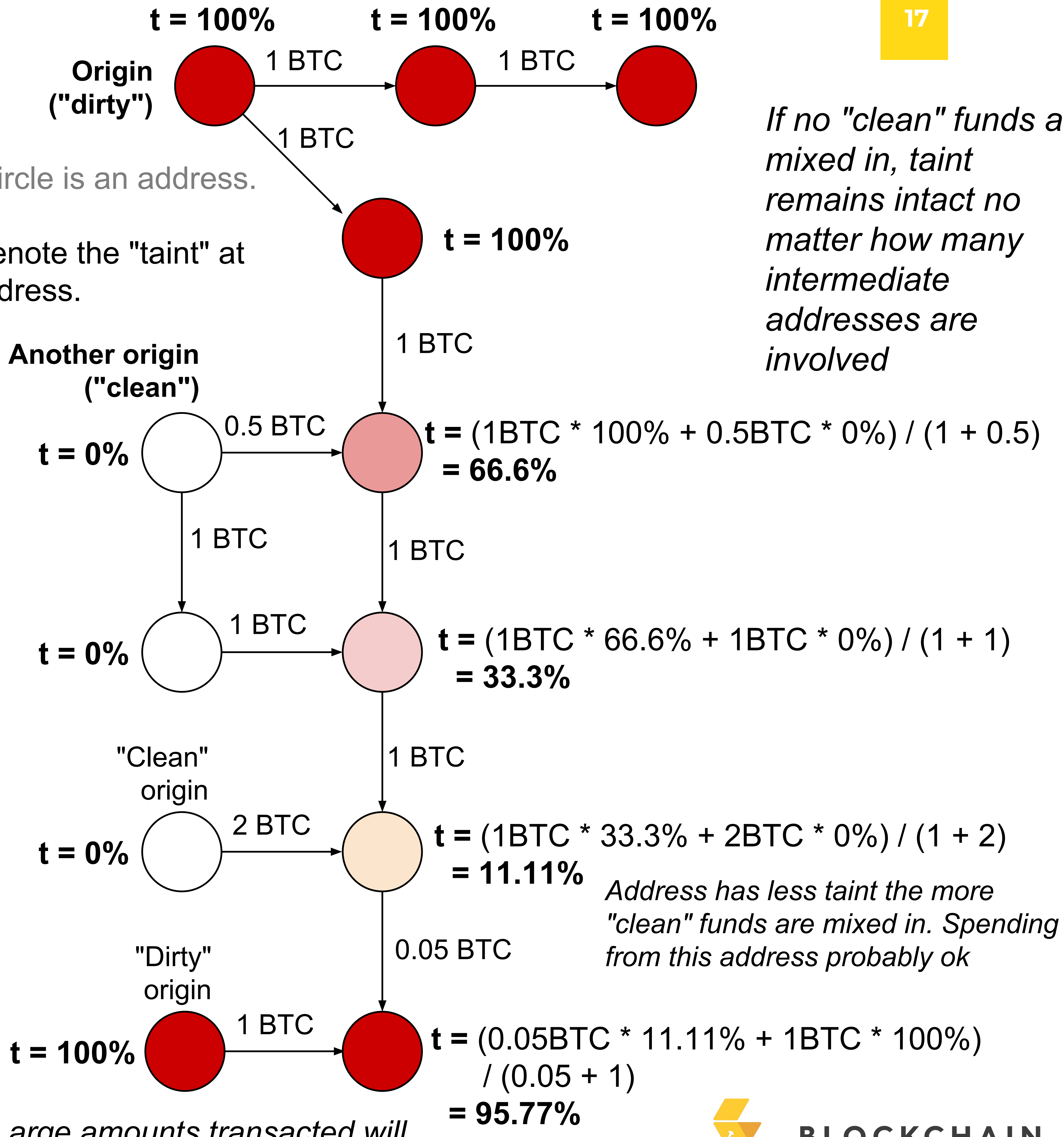
Taint analysis can reveal useful information

- 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!

Each circle is an address.

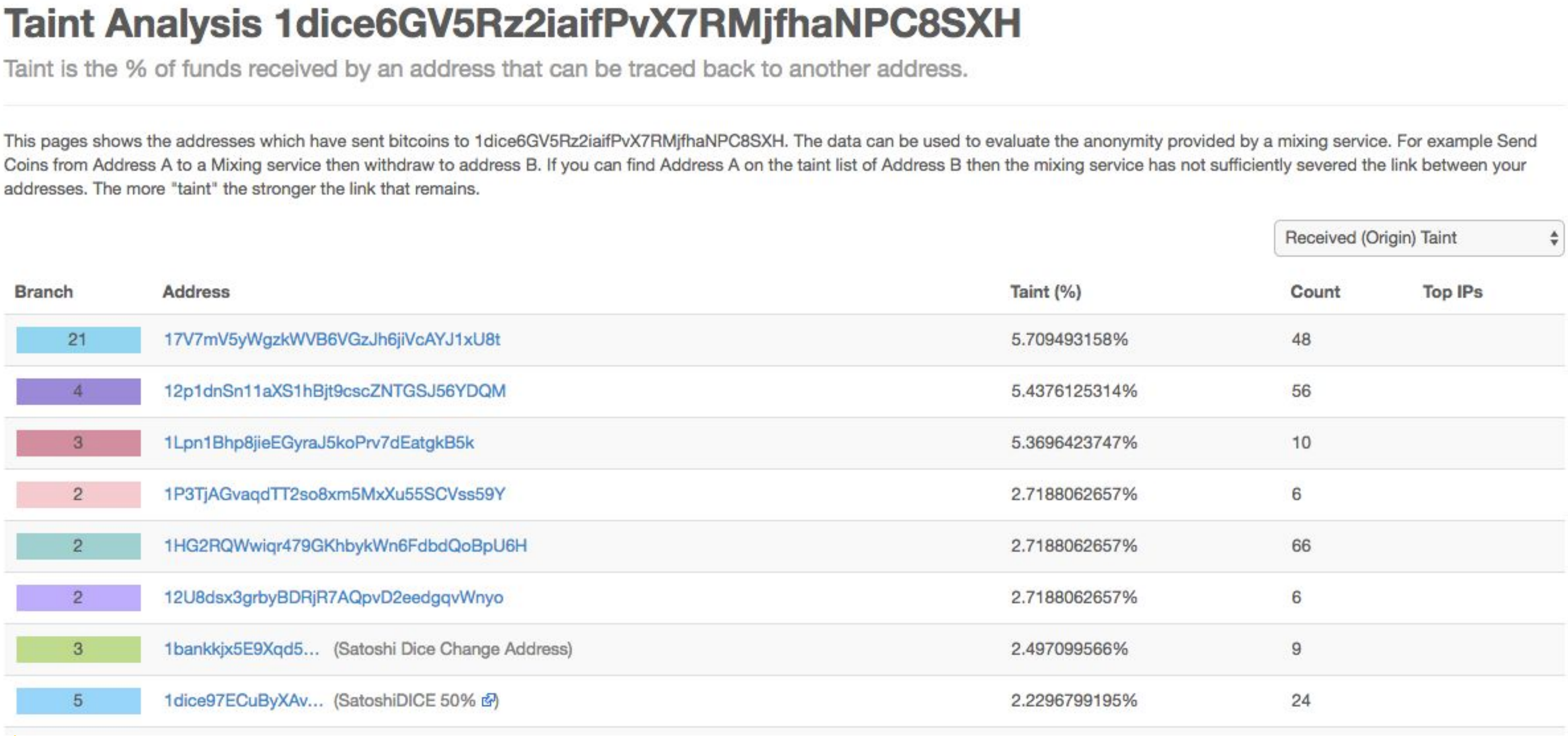
Let **t** denote the "taint" at that address.



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

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

Large amounts transacted will have a strong effect on the taint



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.

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	

Taint analysis tool on Blockchain.info

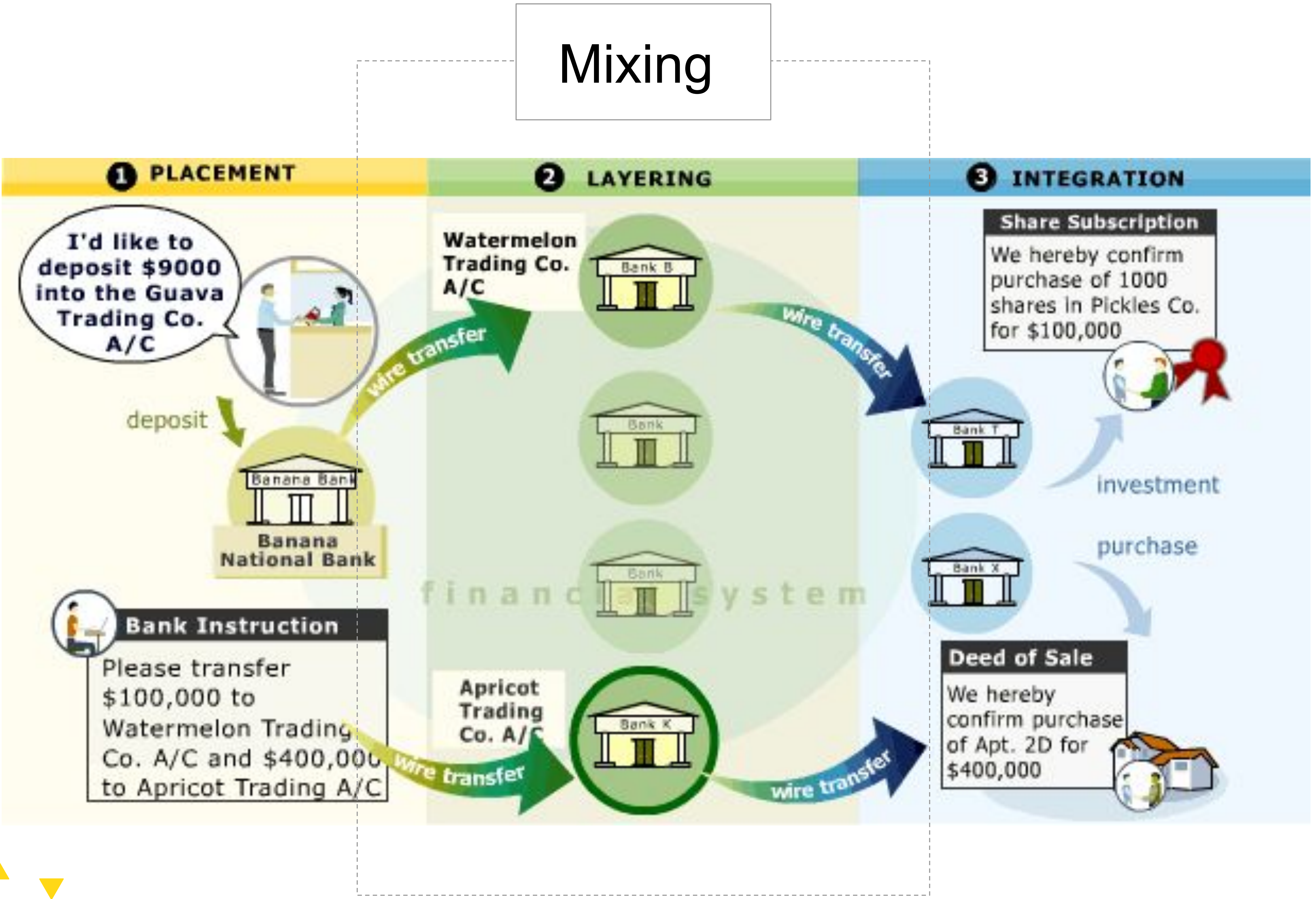
BREAK SECTION

BLOCKCHAIN AT BERKELEY

3 ANONYMITY THROUGH MIXING

MIXING

MONEY LAUNDERING BASICS



Bank Instruction

Please transfer $100,000 to Watermelon Trading Co. A/C and $400,000 to Apricot Trading A/C

Share Subscription

We hereby confirm purchase of 1000 shares in Pickles Co. for $100,000

Deed of Sale

We hereby confirm purchase of Apt. 2D for $400,000

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

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.

FORMAL ANONYMITY

GOALS OF MIXING

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
  - 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.
  - Real world constraints

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 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

BLOCKCHAIN FUNDAMENTALS

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

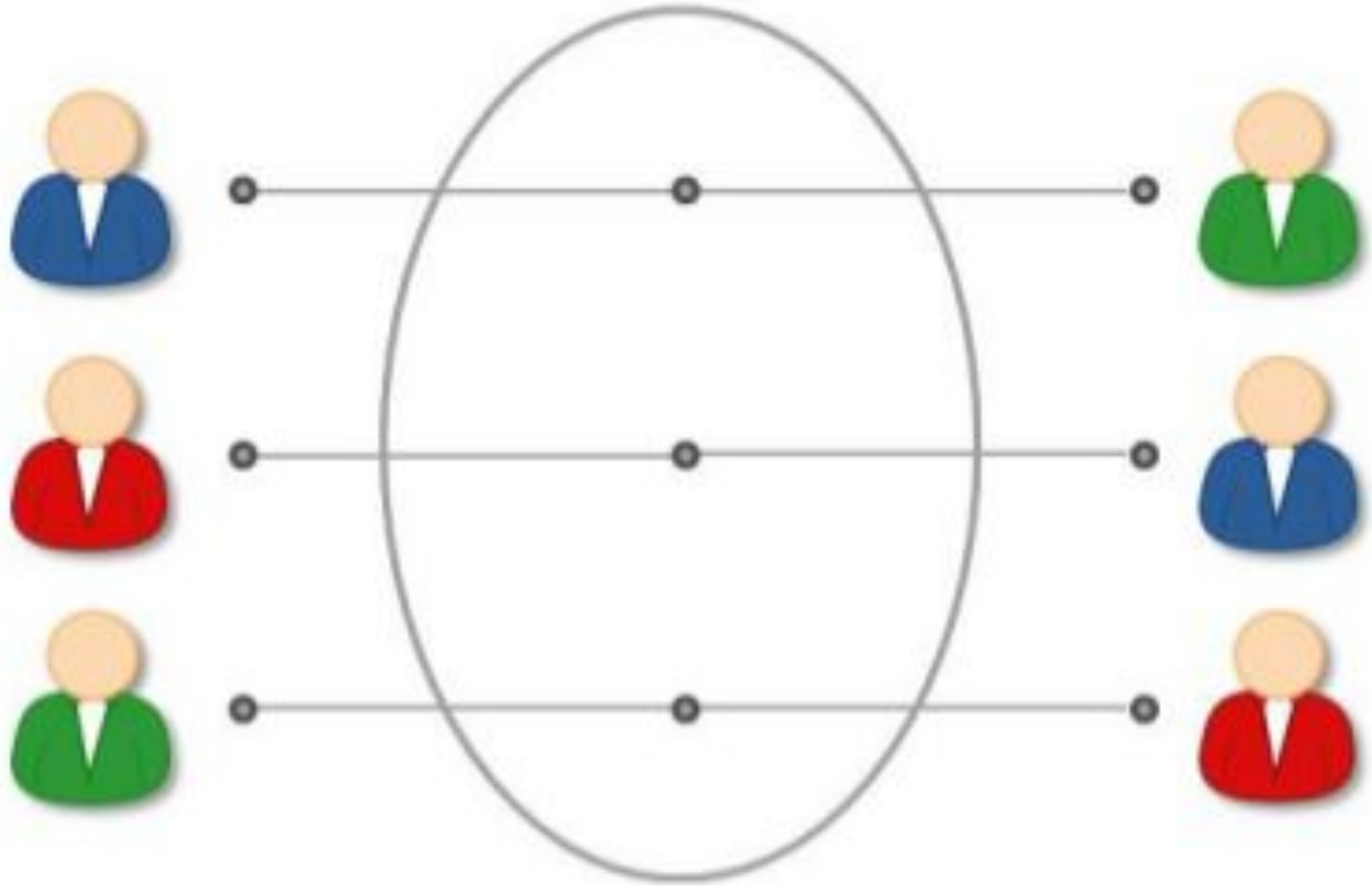
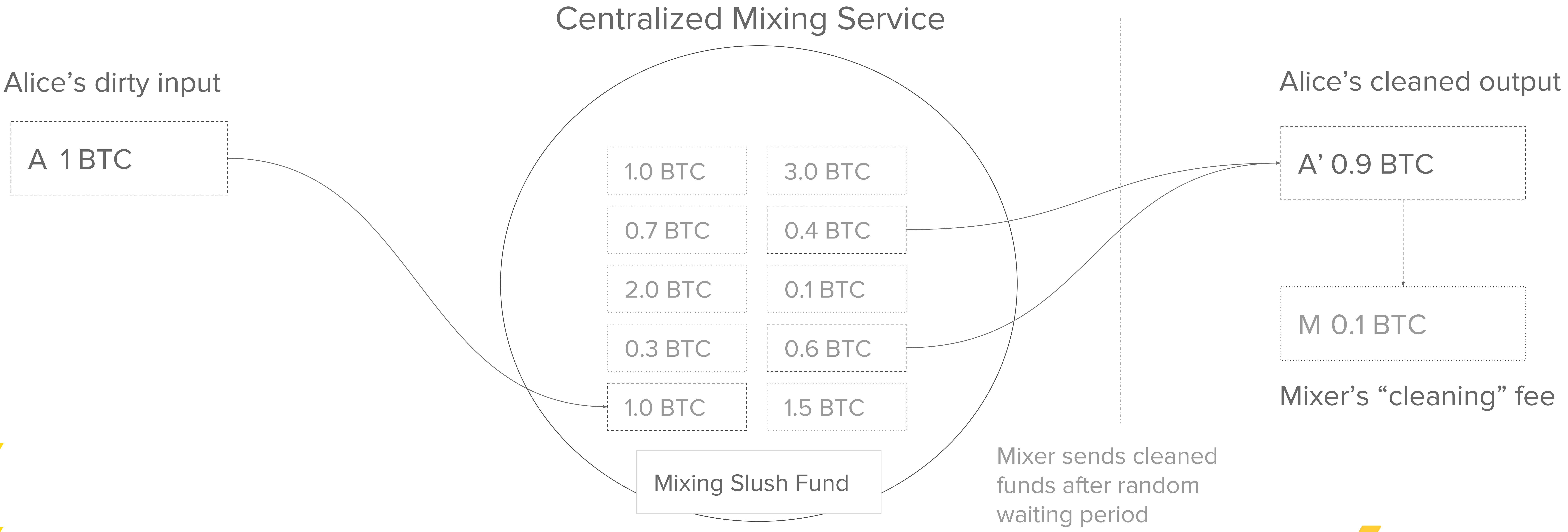


Image source: Princeton Textbook

CENTRALIZED MIXERS

BLOCKCHAIN FUNDAMENTALS

Third Party (TTP), TTP sends (hopefully) unlinked coins to you sometime in the near future.



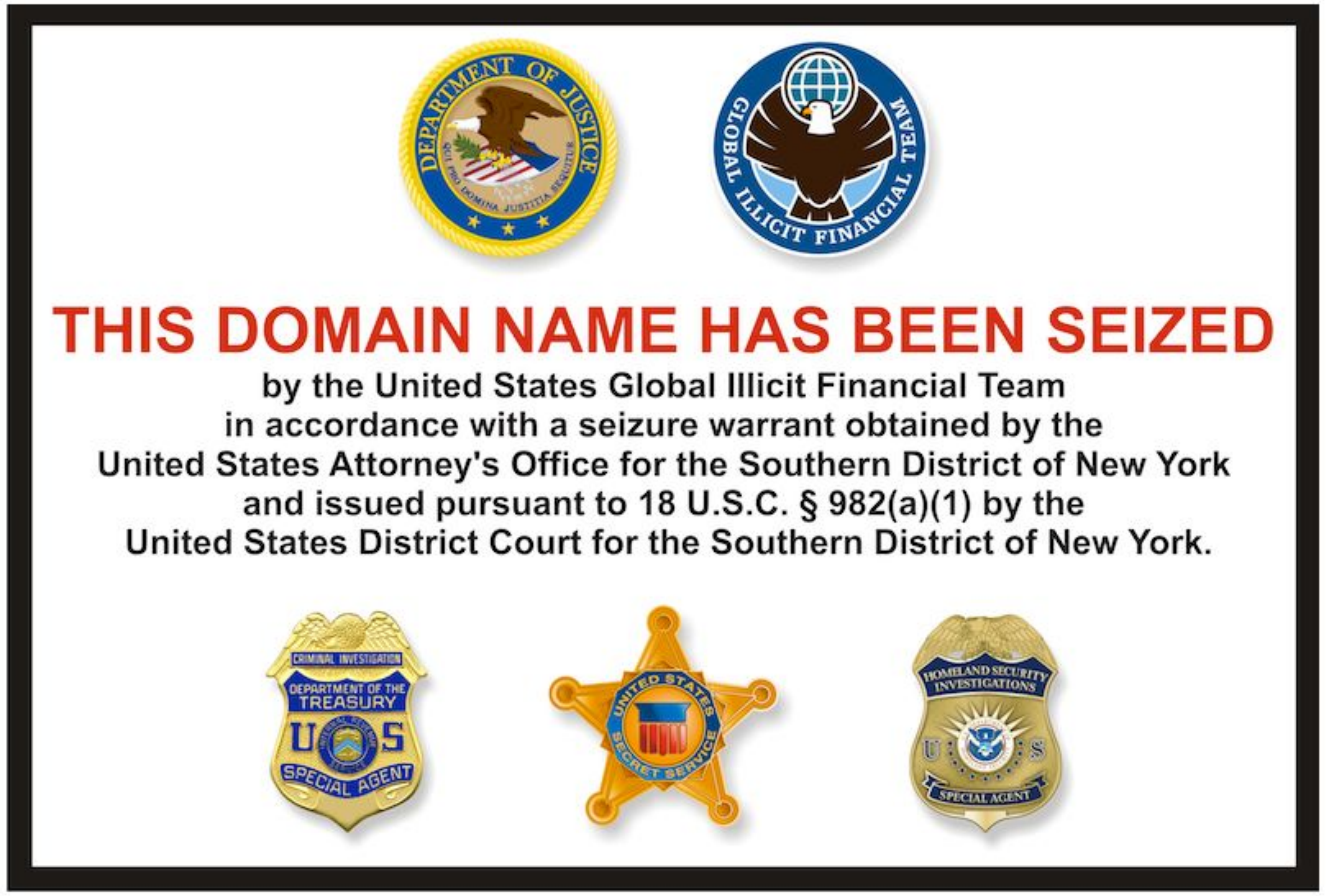
CENTRALIZED MIXERS

CONCLUSIONS

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.



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.

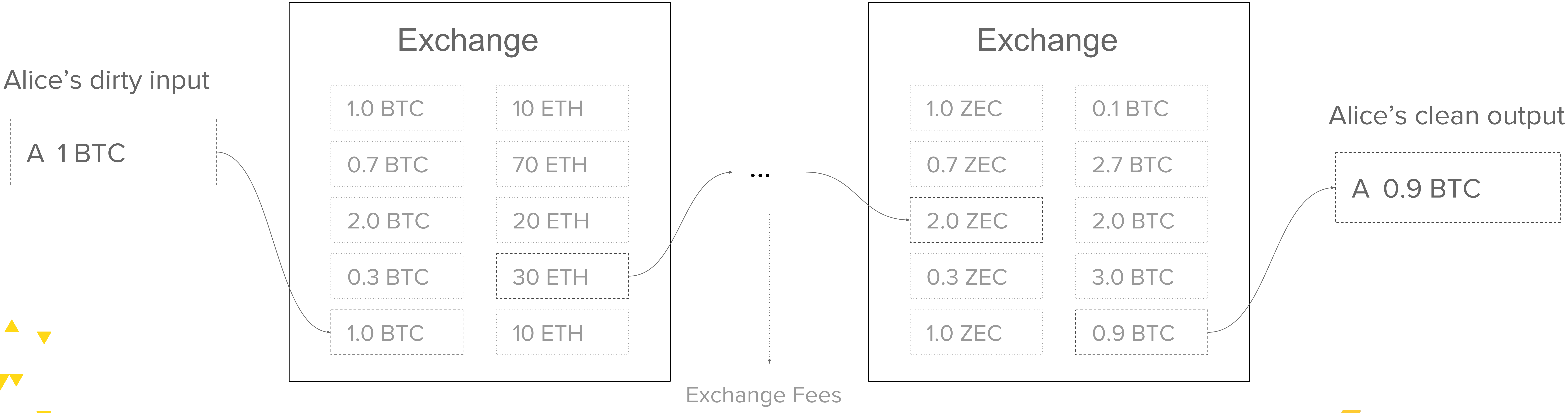
Examples of centralized mixing protocols

- **Mixcoin**
  - Relies on the TTP accountable
- **Blindcoin**
  - Same as Mixcoin, but TTP is blind - cannot infer the permutation of mixes

ALTCOIN EXCHANGE MIXING

BLOCKCHAIN FUNDAMENTALS

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



ALTCOIN EXCHANGE MIXING

CONCLUSIONS

Pros:

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

Cons:

- 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 PROTOCOLS

THE BRAND NEW IDEA YOU DEFINITELY DIDN'T SEE COMING

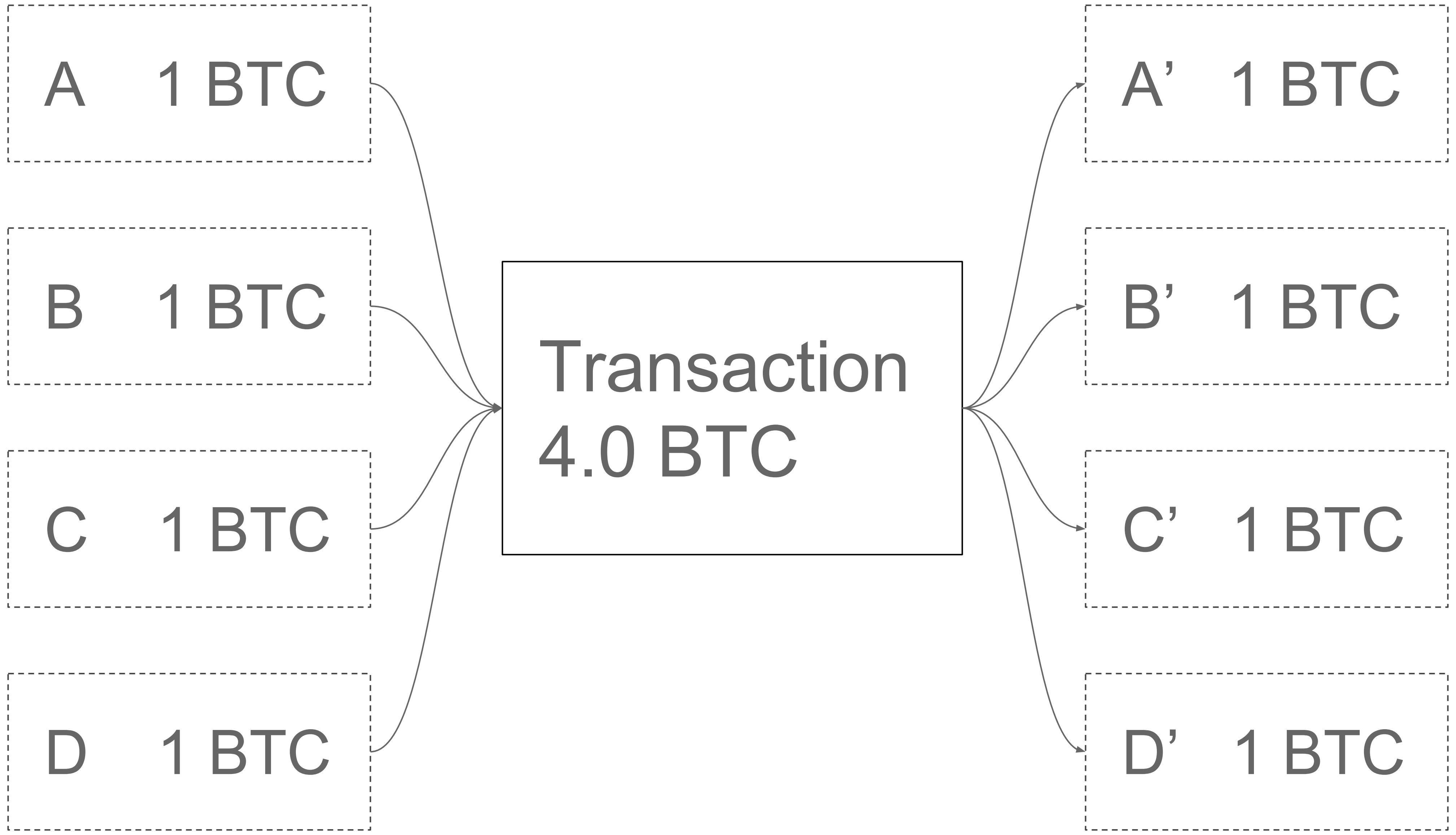
Idea: Remove counterparty risk and avoid fees by taking out the middleman (centralized mixer).

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?

PROTOCOL - COINJOIN (2011)

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



A 1 BTC

B 1 BTC

C 1 BTC

D 1 BTC

Transaction 4.0 BTC

A’ 1 BTC

B’ 1 BTC

C’ 1 BTC

D’ 1 BTC

Pros:

+ **Trustless:** Funds can’t be stolen, since all users must agree on the CoinJoin transaction.

Cons:

- **Anonymity not secure against passive adversary (mix facilitator)**
  Best existing implementation for executing the protocol is via a **centralized server**; assumes private and anonymous communication channels for submitting output addresses. E.g. vulnerable to **traffic analysis**
- **Not plausibly deniable;**
  very easy to spot on the blockchain since n-of-n multisignature transaction where n is usually large. (Can be fixed with Schnorr sigs)
- **Not DoS attack resistant;**
  only needs 1 malicious node to start protocol and then halt halfway through to disrupt.

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

DECENTRALIZED MIXING PROTOCOLS

CONCLUSIONS

Pros:

+ No central point of failure (coin shuffle)
+ Anonymity against mix facilitator

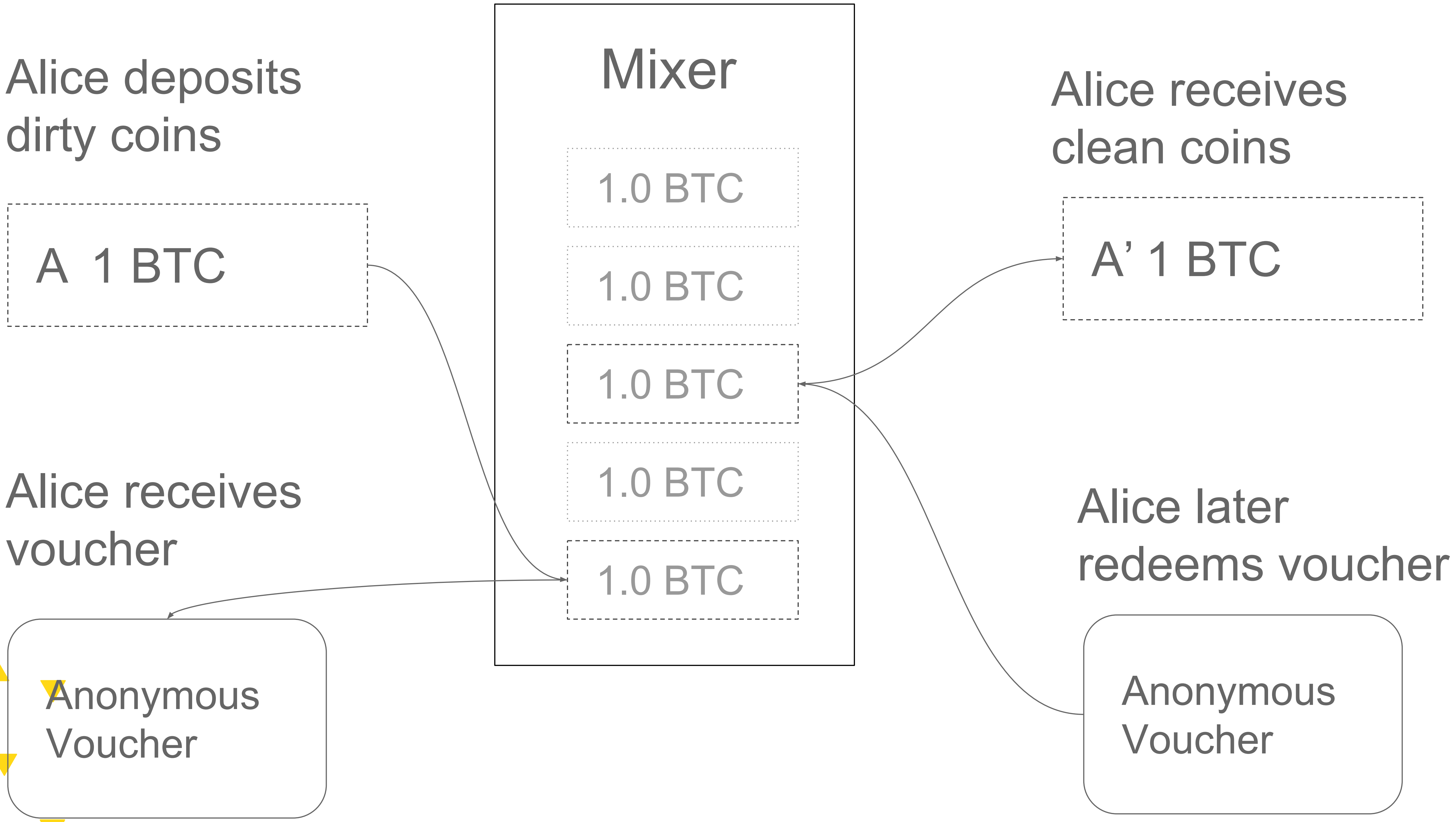
Cons:

- Deanonymization via Sybil attacks.
- Tradeoff between centralized server(coin join) and anonymity to mixing protocol (coin shuffle)
- Trade off between plausible deniability and security.

FAIR EXCHANGE MIXERS

BLOCKCHAIN FUNDAMENTALS

- Build upon traditional **Fair-exchange** protocol to no longer require a trusted third party
- "Fair-exchange mixer": model of A paying B through an untrusted intermediary T



Recipient does not have to be depositor, i.e., A could be B.

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

Relies on the assumption that if **enough transactions pass through the mixer at the same time, the mixer cannot tell which inputs map to which outputs**

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

FAIR EXCHANGE MIXERS

CONCLUSIONS

Pros:

- + Trustless, don't have to trust intermediary
- + Some are even DOS/Sybil attack resistant

Cons:

- Pretty hard to build
  - ○ TumbleBit: works if sufficient liquidity
  - ○ Xim: Few hours of computation
  - ○ BSC : Bitcoin scripting

4 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**.

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.

Cons:

- Masternode network must be secure. You can run a masternode if you place a 1000 DASH bond that also earns you interest.
- To acquire **4125 nodes to 51% attack** the masternode network, you would need 4125 * 1000 DASH * $60/DASH = **$250 million**. (as of 2017-04-12)

CRYPTONOTE ⇒ MONERO

Fork of Cryptonote - based currency Bytecoin
Idea: Provides untraceability and unlinkability of transactions

- **Untraceability**: For each incoming transactions, all possible senders are equiprobable.
  - Hide input 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.
  - **Ring Signature:** In this context, prove you own one of the outputs without revealing which specific output.
    - Anonymity set is the set of outputs you're signing from
  - Better plausible deniability since mixing enabled by default
- **Unlinkable:** For any two outgoing transactions, it is impossible to prove they went to the same person.
  - Create multiple one-time payment addresses

MONERO

HOW DOES MONERO WORK?

Untraceability through ring signatures

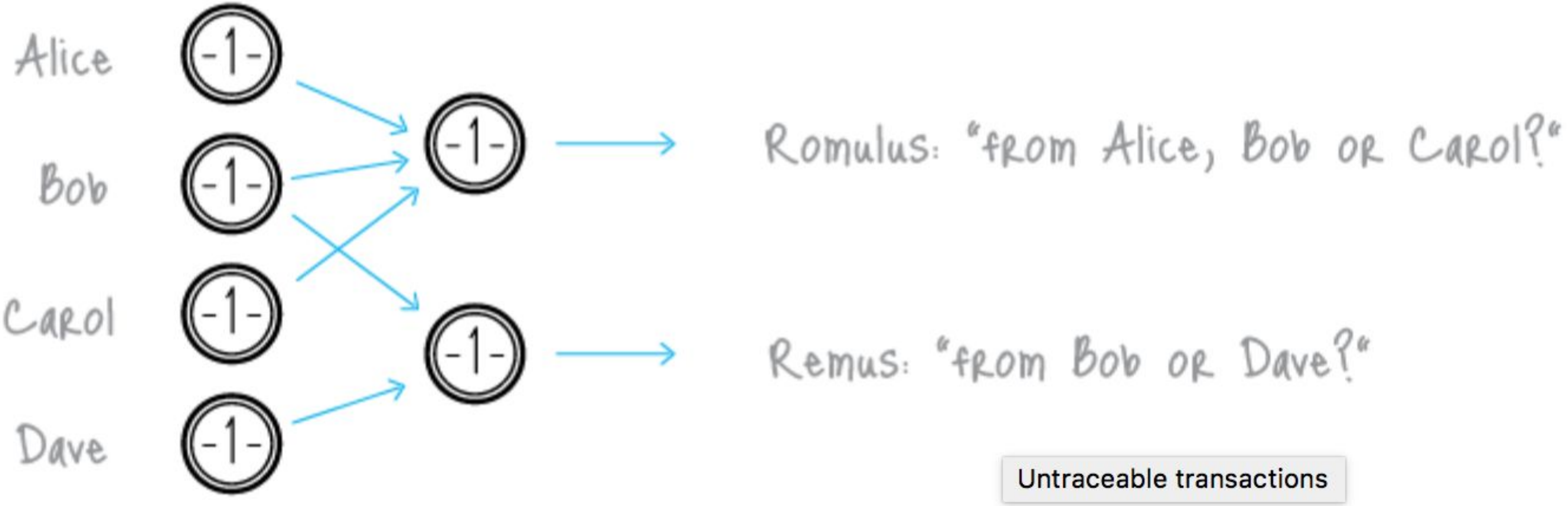
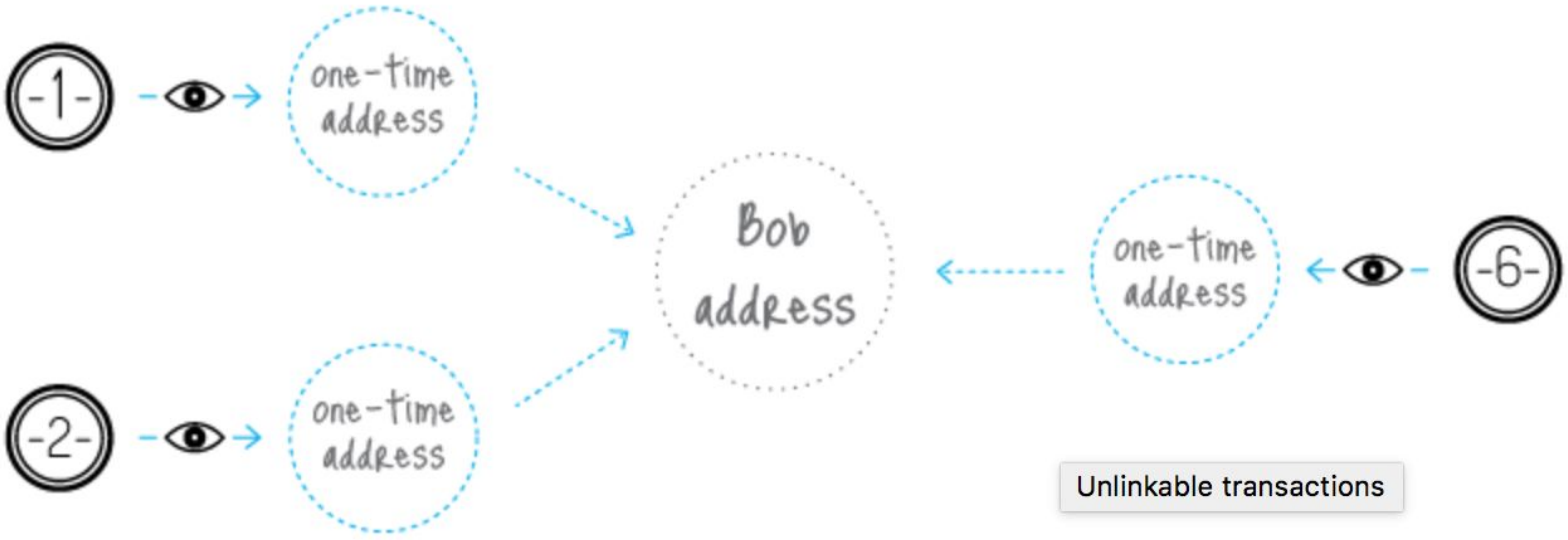

Alice
Bob
Carol
Dave
-1-
-1-
-1-
-1-
-1-
-1-
Romulus: "from Alice, Bob or Carol?"
Remus: "from Bob or Dave?"
Untraceable transactions

Image source: https://cryptonote.org/inside

MONERO

HOW DOES MONERO WORK?

Unlinkability through one time address



Unlinkable transactions

Image source: https://cryptonote.org/inside

MONERO

CONCLUSIONS

Pros:

- No other coin has the proven anonymity behind their product! (Zcash comes close)
- New block released every minute

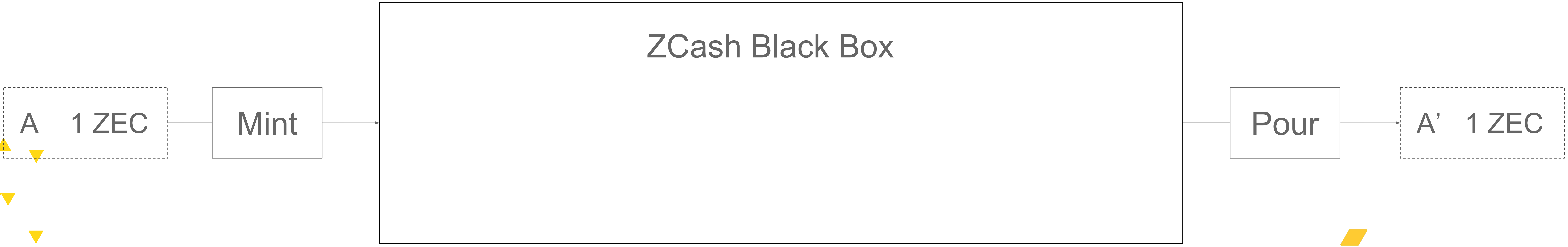
Cons:

- Monero doesn't hide **transaction values** (yet). Adversary could potentially trace transactions by following likely value flows. **Temporal correlations** also pose an issue.
- Decent anonymity set, but can we do better?

zk-SNARKs ⇒ ZCASH

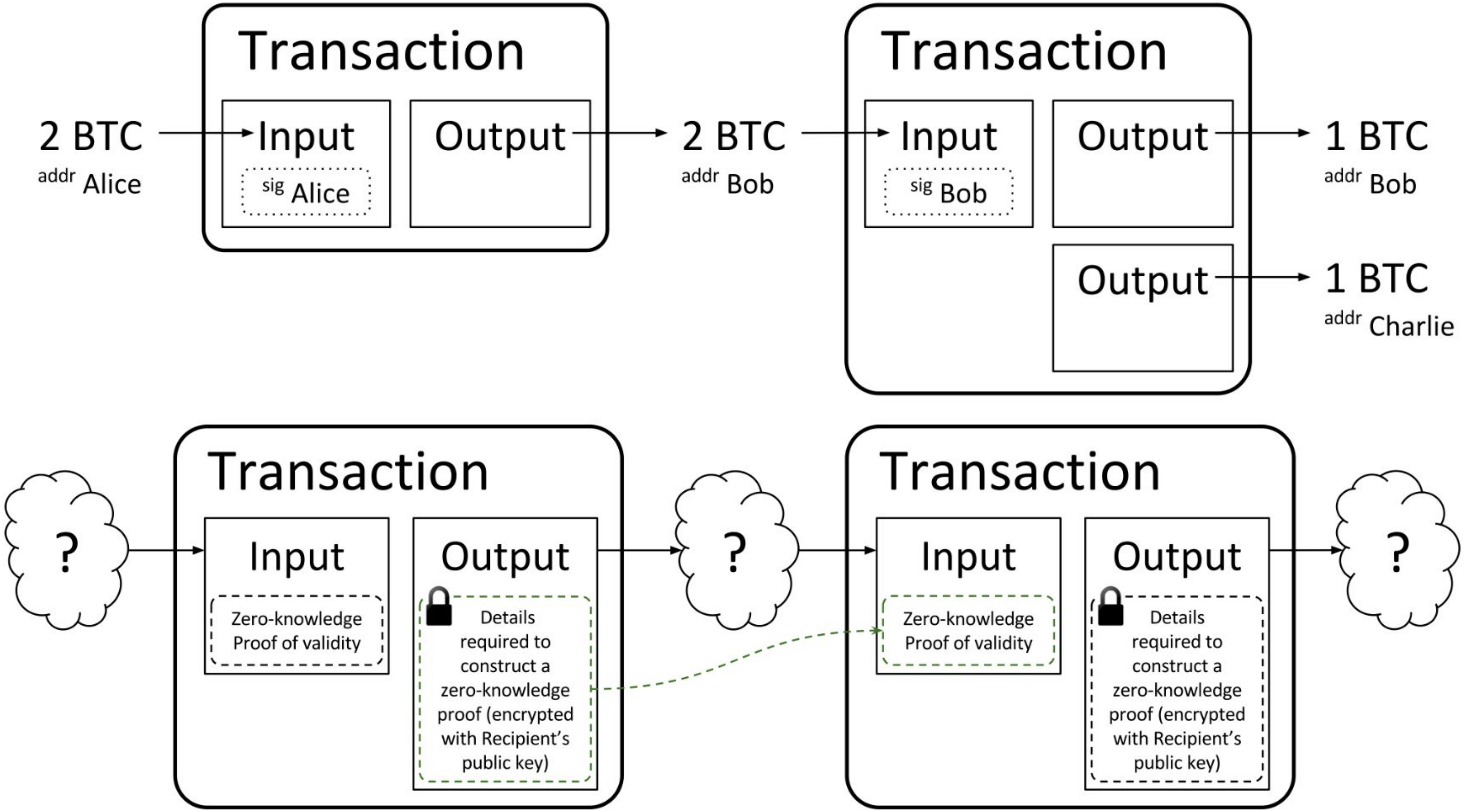
Idea: Altcoin where transactions reveal *nothing* about input/output addresses AND input/output values.

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**.



zk-SNARKs ⇒ ZCASH

HOW DOES ZCASH WORK?

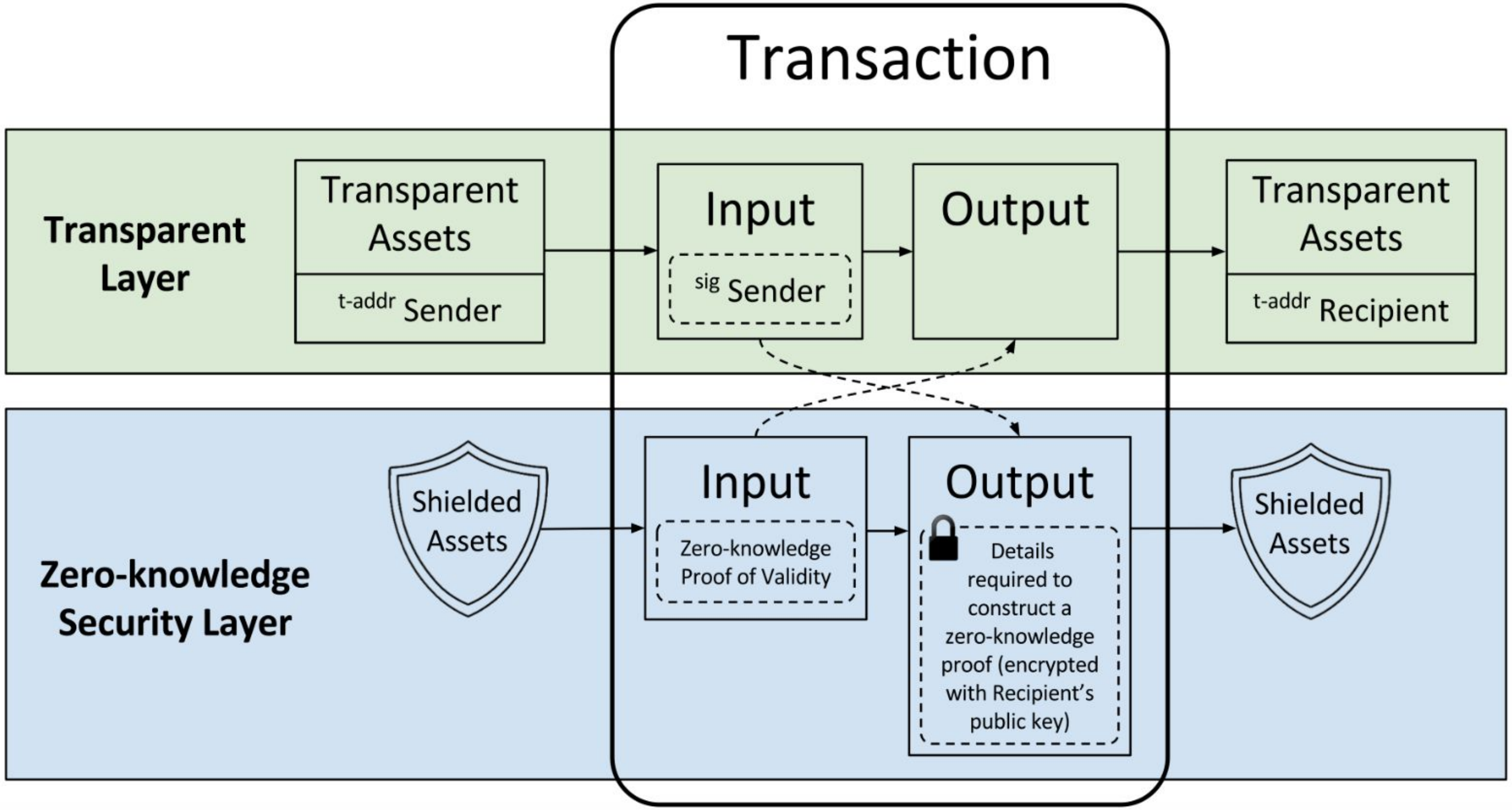

2 BTC
addr Alice
Transaction
Input
sig Alice
Output
2 BTC
addr Bob
Transaction
Input
sig Bob
Output
1 BTC
addr Bob
Output
1 BTC
addr Charlie
?
Transaction
Input
Zero-knowledge Proof of validity
Output
Details required to construct a zero-knowledge proof (encrypted with Recipient's public key)
?
Transaction
Input
Zero-knowledge Proof of validity
Output
Details required to construct a zero-knowledge proof (encrypted with Recipient's public key)
?

Bitcoin vs. Zcash

Image source:
https://z.cash/blog/zsl.html

zk-SNARKs ⇒ ZCASH

HOW DOES ZCASH WORK?



Zcash is an implementation of Zero Knowledge Security Layer, using a fork of the Bitcoin codebase to enable transparent transactions

Image source: https://z.cash/blog/zsl.html

ZCASH

A PEEK BEHIND THE BLACK BOX

Homomorphic Hiding - A function which has the following properties

- If we are given the output, it is hard to find the input
- Different inputs lead to different outputs
- If we know the outputs of two different input values, we can find the output of the function on some arithmetic combination (addition, multiplication etc.) of the two inputs, without knowing the input values.

    - Alice has 2 numbers x and y such that x + y = 7
    - Alice doesn’t want Bob to know x,y
    - Alice sends F(x), F(y) to Bob
    - Bob can find F(x + y) from F(x) and F(y)
    - Bob then checks if F(x + y) = F(7)

ZCASH

CONCLUSIONS

Pros:

+ **Fully Anonymous;** Assuming security of underlying crypto, blackbox transactions are anonymous. Anonymity set of entire blackbox history.
+ **Can be integrated with any consensus mechanism**

Cons:

- **Resource Intensive;** zk-SNARK proof system currently in use requires about 4 GB of RAM and 40 seconds 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.
- **Assumes security at network Level**

CONCLUSIONS

BLOCKCHAIN FUNDAMENTALS

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

1. Bitcoin
2. Centralized mixers
3. Decentralized mixing protocols
4. Altcoin exchange
5. DASH
6. Monero
7. Zcash

Practical question: **How would I mix coins today?** (In March 2017)

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

Not covered in this lecture:

- Lightning Network and Onion Routing
- Confidential Transactions by Greg Maxwell

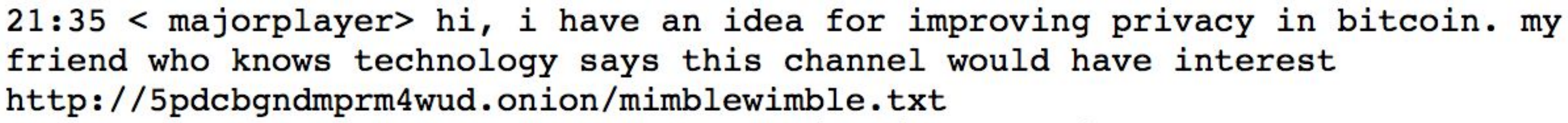
5 MIMBLEWIMBLE

MIMBLEWIMBLE

BITCOIN AND ITS HARRY POTTER REFERENCES

History of Mimblewimble

- Originated in #bitcoin-wizards IRC channel
- Aug 1st, 2016: Random user dropped a link to a .onion link hosting a textfile and left
- Written by a pseudonymous author “Tom Elvis Jedusor” (Voldemort’s real name in the French edition of the Harry Potter novels)
- Mimblewimble was a spell in Harry Potter that binds the target's tongue to keep him or her from talking about a specific subject



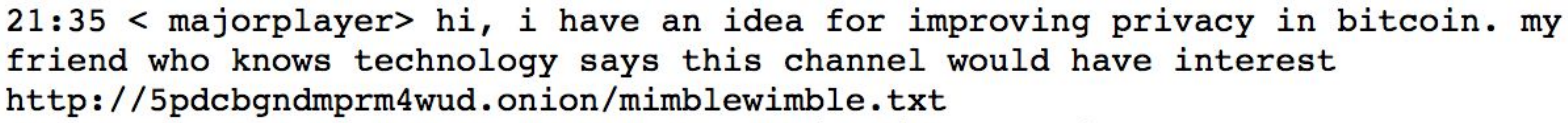
```
21:35 < majorplayer> hi, i have an idea for improving privacy in bitcoin. my
friend who knows technology says this channel would have interest
http://5pdcbgndmprm4wud.onion/mimblewimble.txt
```

MIMBLEWIMBLE

BITCOIN AND ITS HARRY POTTER REFERENCES

Mimblewimble Proposal

- Design for a blockchain-based ledger
- Cryptographic protocol to make Bitcoin more scalable and private
- Alternate blockchain (sidechain/altcoin) that supports a different type of transaction than what Bitcoin uses currently
- Meant as a low-functionality, high-scalability, high-privacy system for simpler transactions



```
21:35 < majorplayer> hi, i have an idea for improving privacy in bitcoin. my
friend who knows technology says this channel would have interest
http://5pdcbgndmprm4wud.onion/mimblewimble.txt
```

MIMBLEWIMBLE

BITCOIN AND ITS HARRY POTTER REFERENCES

Mimblewimble Privacy

- Supports Confidential Transactions, where all values in a transaction are encrypted with “blinding factors”
- Uses fancy math to generate “dummy outputs” which enable receivers to spend valid UTXOs
- Bundle many transactions into a larger transaction to scramble inputs and outputs (obfuscate origin/destination of Bitcoins)

Mimblewimble Scalability

- Simplifies the current Bitcoin transaction model to account for transactions that don’t need extra fancy functionality
- Changes verification process from having to rely on previous transactions
- Reduces the need to maintain entire blockchain history (since genesis block)