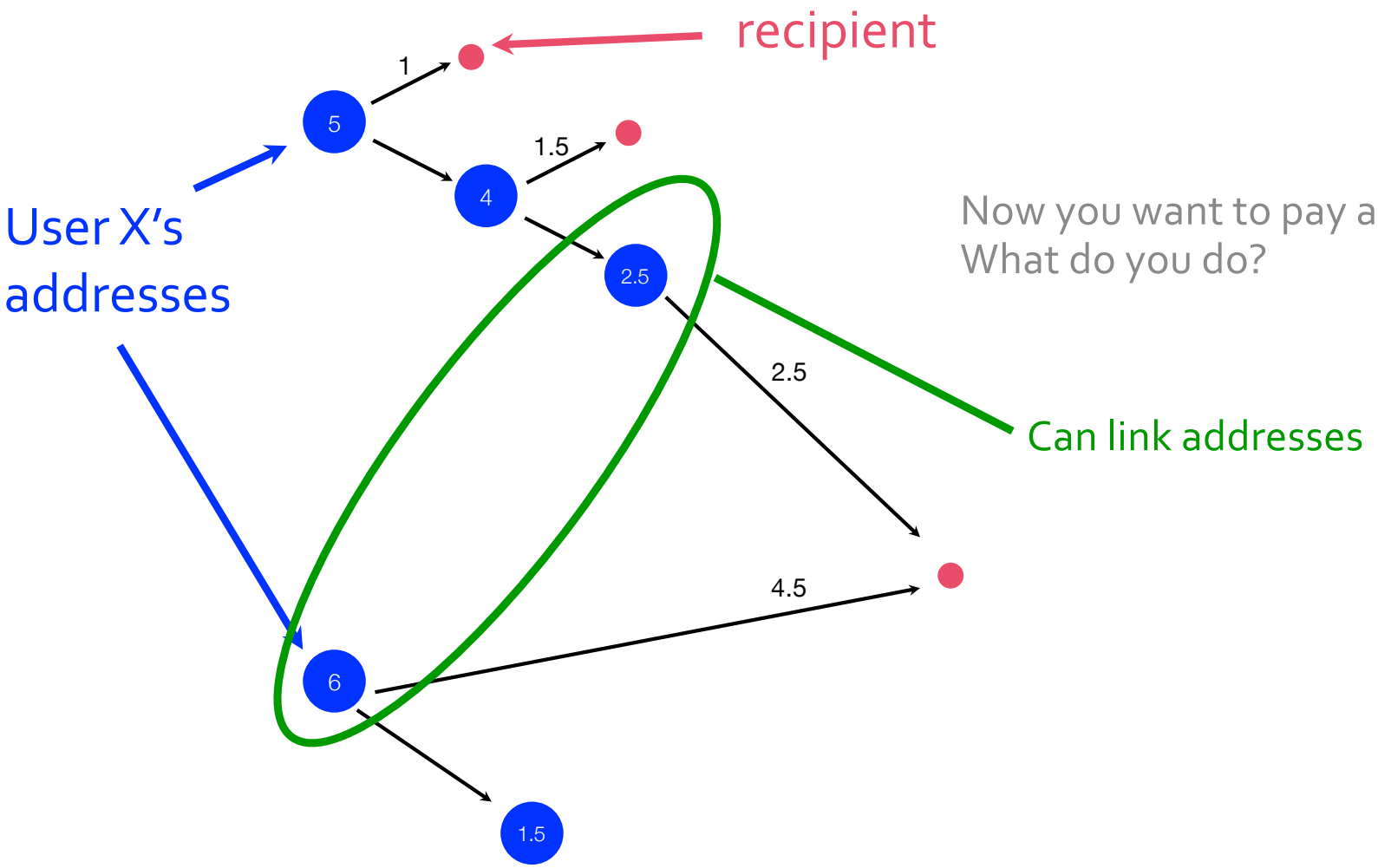
Cse291-J: Blockchain Security

Deian Stefan and Stefan Savage, Spring 2024

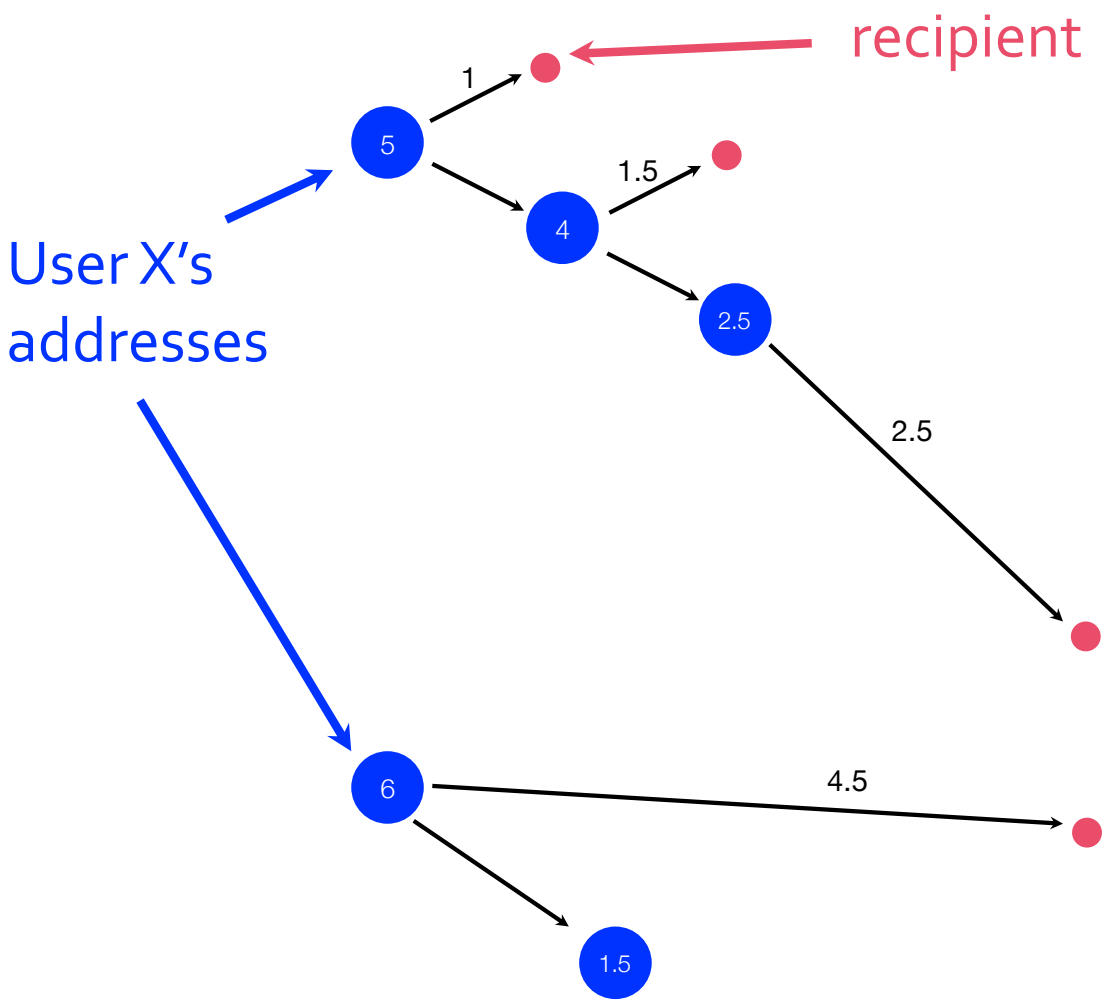
Blockchain antitracing: mixes, coinjoin, etc

First, lets look a a simple anonymity problem

Linking addresses caused by the need to aggregate when transaction value is greater than funds in any particular sender address



Now you want to pay a recipient 7 BTC
What do you do?



Alternative, recipient could create and offer multiple deposit addresses

Not clear that these transactions belong to same person

First, lets look a a simple anonymity problem

Linking addresses caused by the need to aggregate when transaction value is greater than funds in any particular sender address

Ok, so we can improve this situation if the recipient can offer multiple addresses to the sender

- This is a bit like a split transaction for credit card payment or venmo

But how? What is interface?

- UI to ask for how many addresses you want? A bit clunky
- Proposals to export hierarchical deterministic wallets (e.g., BIP32) from sellers (i.e., allow senders to generate as many recipient deposit address as they need)
- Basically not done in practice… why not?

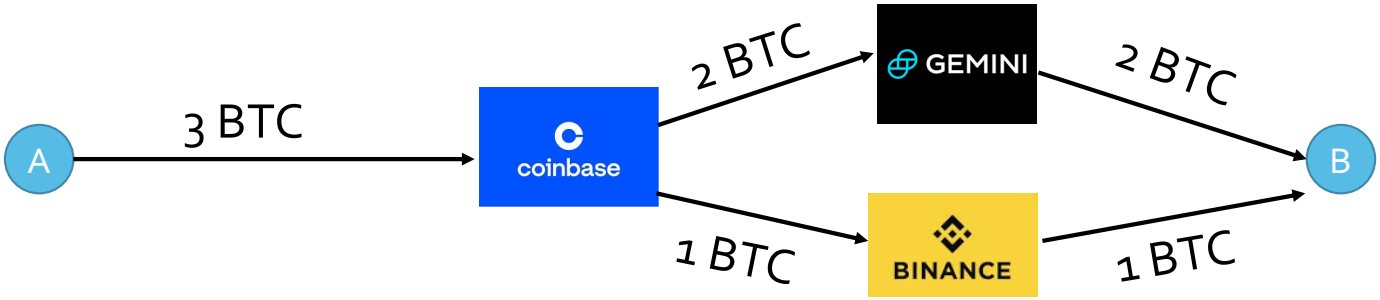
Just doesn't help that much…

- Key issue is linking inputs to outputs
- Lots of other ways to link inputs/inputs (i.e., how did it get funded?)
- Lots of external information (if know recipient is selling something for 7BTC, then two contemporaneous transactions that add to 7BTC might be a clue…)

What is the bigger problem?

Every individual transaction is visible which makes it easy to link inputs to outputs

Hmm… what if you route through exchanges?



Middlemen help, link not clear on Blockchain…
but can just subpoena each exchange (remember KYC)

But what if exchanges don't do the KYC, etc?

PRESS RELEASE

Binance and CEO Plead Guilty to Federal Charges in $4B Resolution

CRYPTO WORLD

Binance founder Changpeng Zhao sentenced to four months in prison after plea deal

PUBLISHED TUE, APR 30 2024•3:06 PM EDT

Binance Holdings Limited (Binance), the entity that operates the world's largest cryptocurrency exchange, Binance.com, pleaded guilty today and has agreed to pay over $4 billion to resolve the Justice Department's investigation into violations related to the Bank Secrecy Act (BSA), failure to register as a money transmitting business, and the International Emergency Economic Powers Act (IEEPA).

Binance's founder and chief executive officer (CEO), Changpeng Zhao, a Canadian national, also pleaded guilty to failing to maintain an effective anti-money laundering (AML) program, in

Two kinds of technical anonymity approaches

Build a privacy overlay on existing blockchain

- Mixers/tumblers

Build a new privacy-preserving blockchain

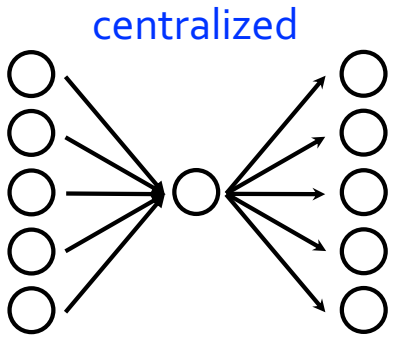
- Privacy coins

Mixers/Tumblers

Roughly speaking, three kinds of mixers

- Custodial/Centralized mixers (e.g., Bitcoin Fog, Blender.io, Helix)

  You send your inputs to them and they, in turn, send transactions to your intended outputs



- Non-custodial/decentralized mixers

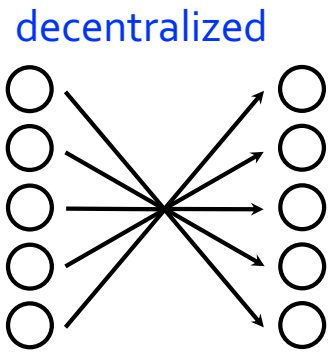
  CoinJoin-based (Bitcoin) (e.g., Wasabi Wallet, Samurai Wallet)

  - Service arranges to aggregate customer transactions into large multi-input, multi-output transactions

    No sharing of private keys, only signed statements

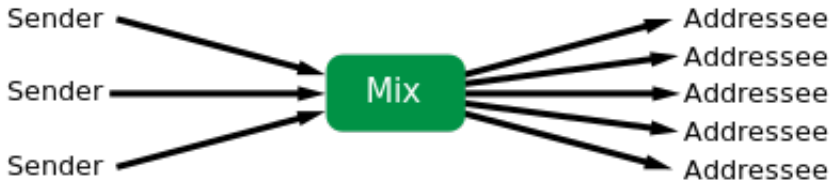
  Smart-contract based (non-Bitcoin) (e.g., Tornado Cash)

  - Smart contract arranges



Basic idea of mixing: Chaum '79

Basic idea: intermediate node breaks link between sender and recipient



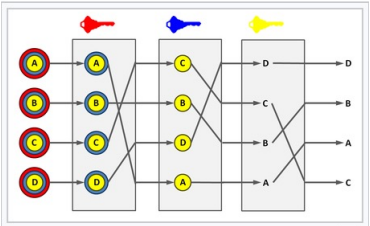
- Senders send message to Mix (address of recipient is encrypted so only Mix knows it)
- Mix takes in messages, forwards them in random order to recipients
- Makes it difficult for outside observer to link sender to receiver (k-anonymity)

Original conception: mixnet

- Messages sent through series of mixes
- Basis for ToR protocol

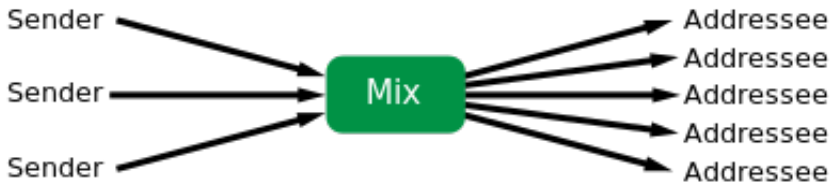
For Bitcoin

- Senders send to Mix address, Mix schedules payments to outputs
- Out-of-band protocol to specify outputs to Mix; Mix charges fee



Simple decryption mix net. Messages are encrypted under a sequence of public keys. Each mix node removes a layer of encryption using its own private key. The node shuffles the message order, and transmits the result to the next node.

What are weaknesses here for Bitcoin?



Side channels

- Size of payments aren't uniform
  - Can break payments into uniform chunks or random chunks (which is better?)
  - But some of this depends on user (i.e., if sum of outputs = input that may be distinct)
- Timing
  - Can delay payment of chunks
- Depends on sufficient "cover" traffic
  - Hard to launder $20M, if rest of users are moving just $1M
- Hard to offer clear proofs of unlinkability here…

Trust

What are we **trusting** centralized mixes to do?

Not just take our money (this has definitely happened)

- Maybe it hurts their reputation, but if they only rip off some people – how would you prove that you'd be ripped off and that you aren't just ripping them off?

Not to keep records about who sent what to whom

That their ad hoc protocols for addressing *traffic analysis* works

- In reality, they do all kinds of weird things – many of which just *seem* hard to trace

That their security is good
(i.e., that they won't get compromised; electronically or physically)

That they maintain online availability (its own potential side channel)

Mixcoin

Anonymity for Bitcoin with accountable mixes

Joseph Bonneau[1], Arvind Narayanan[1], Andrew Miller[2], Jeremy Clark[3], and Joshua A. Kroll[1] and Edward W. Felten[1]

[1] Princeton University
[2] University of Maryland
[3] Concordia University

Abstract. We propose Mixcoin, a protocol to facilitate anonymous payments in Bitcoin and similar cryptocurrencies. We build on the emergent phenomenon of currency mixes, adding an accountability mechanism to expose theft. We demonstrate that incentives of mixes and clients can be aligned to ensure that rational mixes will not steal. Our scheme is efficient and fully compatible with Bitcoin. Against a passive attacker, our scheme provides an anonymity set of *all* other users mixing coins contemporaneously. This is an interesting new property with no clear analog in better-studied communication mixes. Against active attackers our scheme offers similar anonymity to traditional communication mixes.

Key ideas here (never deployed in practice)

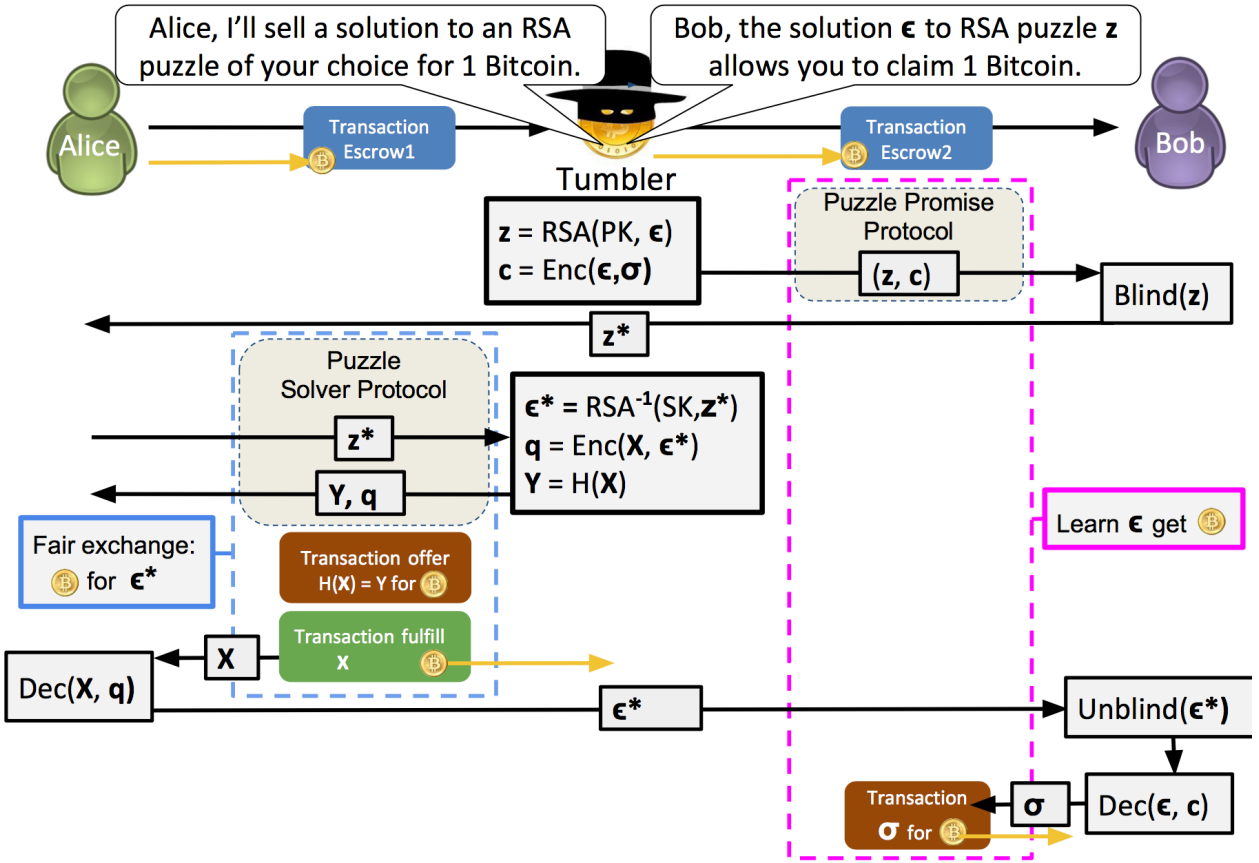
- Accountability via Warranty that MIX got your coin and was supposed to send it to out
- A bunch of thinking about how mixes should work (fees, tradeoffs, side channels)

  Much more influential for the latter than the former

Note, there are some more sophisticated protocols to try to deal with trust (e.g., tumblebit, HABSG16)

- Don't need to trust Mixer not to steal
- Don't need to trust tumbler not to track

- But not used
  - A bunch more messages out-of-band
  - 2x the on-chain transaction
  - Movement away from central mixes anyway?



(slides at: https://scalingbitcoin.org/milan2016/presentations/D1%20-%20TumbleBit%20-%20ForWebsite.pdf)

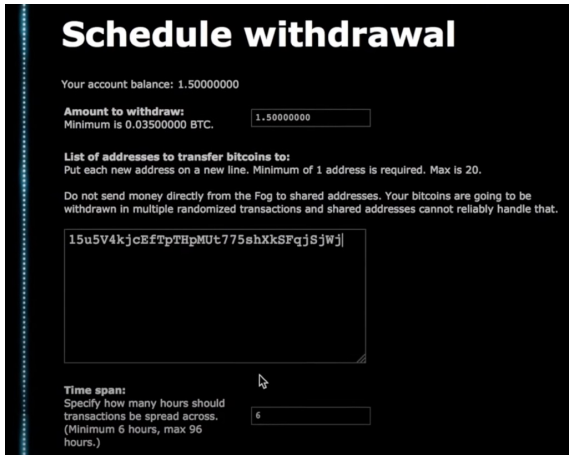
Real-world example: Bitcoin Fog

Only accessible as a ToR hidden service (common for centralized Mixes)

You open an account with Bitcoin fog and deposit your BTC with them

You request a "withdrawal" to the address(s) you want to send money to

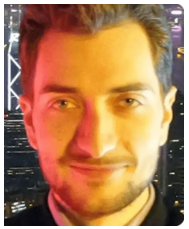
- Select timespan of payout (6-96 hours)
- Select delay before start (0-48 hours)



Efforts to obscure amount

- Withdrawal split into random number of payouts each of random size
- 1-3% fees assess randomly on each payout

What happened to Bitcoin Fog?



Reputedly run by Roman Sterlingov (Russian/Swedish) from 2011-2021

Sterlingov arrested in 2021 at LAX

- Charged with money laundering, money laundering conspiracy, operating an unlicensed money transmitting business, and money transmission without a license in the District of Columbia
- Claim that Fog had laundered > 1.2M BTC
- IRS investigator had corresponded undercover with Bitcoin Fog asking if it would be good service for laundering the proceeds of their illegal drug sales

Defense focused on tracing analysis

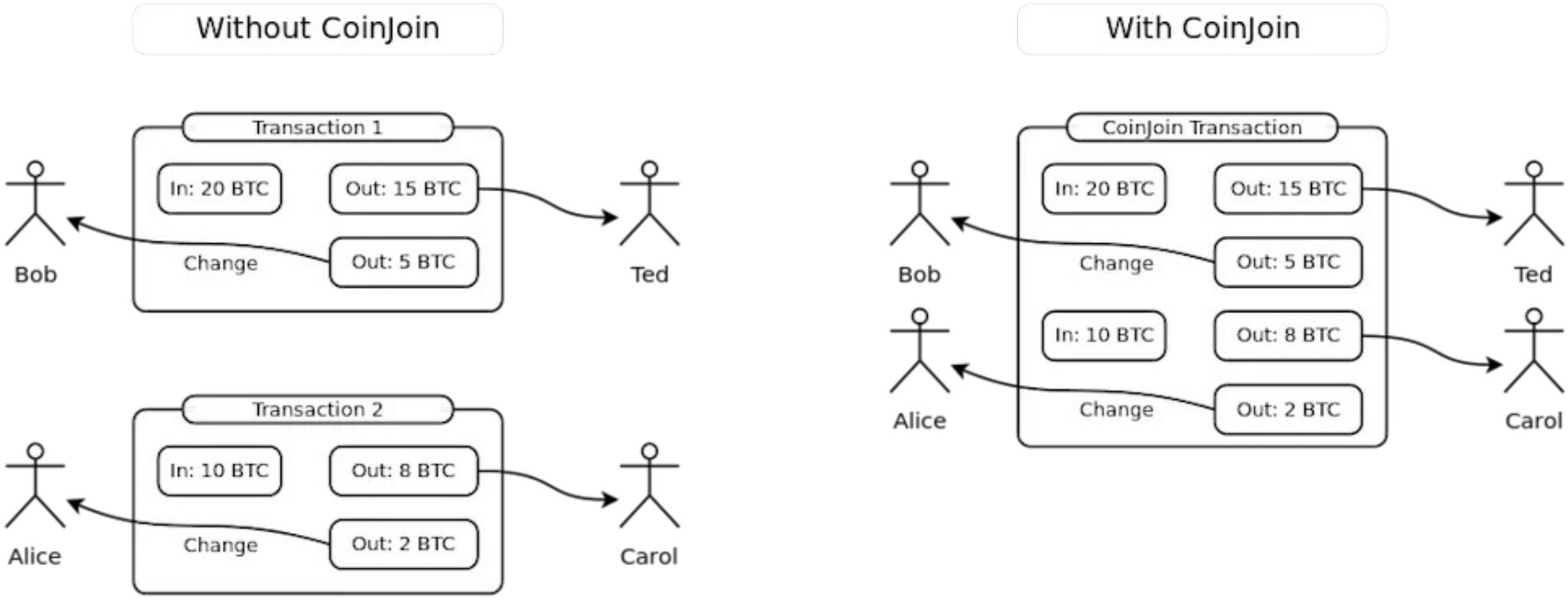
- Claimed that Sterlingov didn't actually operate Fog, just used it
- Competing expert report (Chainalysis vs Ciphertrace – sunk when MC bought Ciphertrace)

Convicted on March 12, 2024 on all counts (<2 mos ago)

Other big central mixers: Blender.io (sanctioned), ChipMixer (seized, arrested), Helix also (seized, arrested)

Coinjoin

Key idea: instead of sending to central party, combine inputs and outputs in a single transaction



e4abb15310348edc606e597effc81697bfce4b6de7598347f17c2befd4febf3b

1CAbbXyRpdtpA6TKXss2Ydd1gWfPGyCJdK (0.49351286 BTC - Output)
17z7pTV1n7gVy6J7Y9uKUqi1VPqyAdwS73 (0.334 BTC - Output)
1ArxXhpbbJcjB7ng2mj6uCWr8NR47wDCGu (0.33360272 BTC - Output)
1624YkFkRw8yGtg484yznDpifBSAj28qLv (0.329 BTC - Output)
1E1Vtqb6jHYfT6JEuKTNF24Z1rAsc34QMw (0.32271551 BTC - Output)
17rmhXWZQrwVBG33p11LPBvZiiqRBwYuo5 (0.49214683 BTC - Output)
1DcXDP8cTrtW7LNXh7Rr9wpQ1UW6ynKPPq (0.29779446 BTC - Output)
1FwZa5NEGPMAuk9dwv6HADkGTBMrybFMe9 (0.308 BTC - Output)
15a8ciZjezFVBEUgA5JmsbrDuEsAUb2q3q (0.32024259 BTC - Output)
1KMwYxPyhrFQfTUnt5sRqajQNSUwCZot3J (0.34964265 BTC - Output)
18P4s3AtsSXq5v417ucEaPizACqmnKzP7F (0.29530619 BTC - Output)
1NM7nn2E3RDKkn91NSxzF91rhnVbqsotZD (0.5160944 BTC - Output)
1FniswCdYUhbUmyp8yLU6yXmbuupiXbrPL (0.3326536 BTC - Output)
1Py9pYrZdAGJRpngQvJod7Xp4KXTnxVG24 (0.33238122 BTC - Output)
1DeivCdXGjDQa68Ddbd3p4vGbgcqD7a5LA (0.31798686 BTC - Output)
1GVeNJUw2982pqD7tyNgYGWV53wDaqnmvV (0.31777828 BTC - Output)
12yiM7SGE7LT7EqPVZxgMkUN2C2go72SgD (0.32411878 BTC - Output)
19MkjA25FyVYMoHjiJdh8xsQ9gXfM5McDc (0.33803037 BTC - Output)
1LgcFveG3Aw1tkL25W5EMr2Cw3z5mBeQse (0.318 BTC - Output)
13Lxtz8eGATA1jig6hnbGb4N9C8wq54vLq (182.30544491 BTC - Output)
1EfCXe188LoQnHfvPQr1xvAwBzKYJ3ziDS (0.336 BTC - Output)
144WPEuNgGiEPFBgqgKJvXiNwT3KdR2uBu (0.331 BTC - Output)
1LHVP7znzpTv4wzMkWVvkcWMmaPrUcQzuB (0.49217385 BTC - Output)
1BYzrWzFSTU47Xdkid87gHpHs7eXbwUZwi (0.52646585 BTC - Output)
148LP8cPVBzzXVrVQdLUnswNH4dfPSho3a (0.31353747 BTC - Output)
1L52zb7Yj3m4rYNSszhA4PKMEpi8XqezFz (0.3702 BTC - Output)
1FcYMAtG57ZSvDbTCz7fBDQxA9XfvoXqR9 (0.49522705 BTC - Output)
1PN4WV39WshZNnMkkAHaB6b61YkX1qbRDP (0.3471018 BTC - Output)
19nDjzrd61B8e7ZoYrnqGiCL9QufooU7xF (0.51101907 BTC - Output)
1MSZE1TYTdqhzkoKLWzSSduHtF4omouM21 (0.350404 BTC - Output)
14gVdGPDYPzrnrdZtQ1Nubu3G9GVoDLd9q (0.34499411 BTC - Output)
1BMSVaDpGV7T8TxYo1BkJts33bhkB7rE7x (0.33990561 BTC - Output)
1PLmWVRe6TtdvCkwcVyGDRdPm67BiXXGQM (0.32806178 BTC - Output)
1EVi1zMTeEiFhvuR5TZCuX6NYhh8xMsrNw (0.34360208 BTC - Output)
1BdabhFXRbUN2bXH5nNqtnM6A9JRoesn1A (0.349462 BTC - Output)
1KGQzrkzPiQ82hV7QKQagGf67emidnptgi (0.49903187 BTC - Output)
1Z4NnmAC1Z4E7MnGvrvc22hb8CmZWZVEj (0.32618186 BTC - Output)

1MQ9wTnSMABoPLo6uze7rkW969GAuifvKM - (Spent) 1.11009124 BTC
1JMx2YQq8hDT68KwdpcotADE5qanRJHhag - (Spent) 1.03263711 BTC
1JTr8iWdjwTKnsaHC6yMPAxbSePDLpqzeW - (Spent) 0.96532807 BTC
1EP3sDKzeNHmPFsE7nXyeEpSoSbyVuva4R - (Spent) 0.99034642 BTC
1NdLcTXm1KossL3m3bg3n3izQt3wjezXmQ - (Spent) 0.95985165 BTC
157DkvZ5fdoyui9SBnbmSs9nRz31e2mh56 - (Spent) 1.0460556 BTC
13Cst9ErfTxDFyNe39BuZA2Pqiyf3FLzUT - (Spent) 1.04012544 BTC
15TyYkyZWk8Xm7jaSE5ug5a9fBMNqxMUTV - (Spent) 1.09853614 BTC
1LbmSrETzEfWPZojsA2Vq7NmMZ8AnNHPBH - (Spent) 0.99762768 BTC
1APaJRKUtBSJHNSqqcBHmuCeRp4KNU6zBz - (Spent)
1PtLzhHkCywHf8St3TNb8xudiSDdVU6XTw - (Spent) 1.04519906 BTC
13EfNEbVpmGpc8aCzKYuymysHrHodTEiP5 - (Spent) 1.03320177 BTC
1hBgKb7YGSSGb64d67svTvifiFCZdSFdm - (Spent) 0.99505215 BTC
1P2dJRewoeEsKdCXVvSVZwN29EgTxpyqYn - (Spent) 1.10898935 BTC
1KUfW1bHptXRj5N6PzWBCxLr8Xp5mquoDz - (Spent) 1.03873536 BTC
1CjHhyKESaXdyoCdG3q2QSS2P2TcUFd43V - (Spent) 1.07513614 BTC
13ef6gEBpRBnSZnbu6efY4iY35bRnWhEsW - (Spent) 0.9360219 BTC
1AxRUvU9LCqtszERgmqb5KU5bT5peTxAuU - (Spent) 0.94561868 BTC
1bfwZ9KaB4miraL1QTitPB7Ke2VjN8bra - (Spent) 1.06755426 BTC
13ykZwWajKpH2r6qr5XqXCJmQ8CqPPxCMV - (Spent) 1.12150712 BTC
194G5fwgUApHCGFKM1vJPuBotVgWXMtW71 - (Spent) 0.98511548 BTC
1N9mFfPwUpoEUGurnQngCPp5opg4hD8aua - (Spent) 1.02630932 BTC
1Jc3HLyKqXbEHM6D73WjGBDuvftYjVjTqP - (Spent) 0.9491876 BTC
1363BvZVEx6dn2DwciuKnRktEWFJDNdTbv - (Spent) 0.94748384 BTC
1KYjfqkyx1gADXK3dfz3hKgaMW6sf6nuZd - (Spent) 0.96147492 BTC
1QDpuuktmMDo9EQMzD4GgJeNSKNAch23AN - 0.90706647 BTC
(Spent) 1.04059457 BTC
14qWyTg79UYBvLF9D1hoayr3g1QU8AApC6 - (Spent) 1.12381189 BTC
1GLUmZSS7sWs2gQKLKbFBQ1HyH5v8BG8Qy - (Spent)
12dPDGaUtsvxEeovKZkrhupmyevkySKmzN - (Spent) 0.94860091 BTC
1GXPeZVb2YV5YdnpatVG1mZuJLU6wv7sXt - (Spent) 1.07438381 BTC
1795pWUsNYE6DL3qcAJDDjFyPTNk33eHxf - (Spent) 0.94347978 BTC
16TaRnwkEXKJpvSe3UpEpJgZ8cthkY9bDL - (Spent) 1.12598 BTC
1W1KZVo4LmfhtD83avCB4v2SvKZxXSejU - (Spent) 153.48631148 BTC
1DxVSWmuCcVHND2AYkFLhoonwaN9CZ6bRW - 1.10072263 BTC
(Spent) 1.00659829 BTC
1L5d7WsjU7hkG3D5nTnncNMX1VSJ6LRM9U - (Spent) 0.9948825 BTC
1ADCq8gmV1mjMFujAvNEWuz1fvRuAZJVzg - (Spent) 1.05596004 BTC
1vDC2eMKwC2YMGqA57L6qWki7HphQd12Q - (Spent) 1.12557235 BTC
1jhqJLhcnmC9bX9Db6VqV3EH9DbxeYq4v - (Spent) 1.04838227 BTC
1QFLhpRtCxYWhu1XbZHZ9tAhHepnYLZZww - (Spent) 0.95676223 BTC
1FrrK3tbNcABVpjbir1KyyTrPvgPzhAUob - (Spent) 1.0807014 BTC

Coinjoin

Ok, but doesn't this mean the sending parties need to share private keys?

- No. Signatures in Bitcoin are provided per input, so can sign inputs separately
  - This is one of the big pluses of CoinJoin – compatible with existing Bitcoin protocol
- Note: this totally breaks co-spending heuristic from last class

How to construct transaction then?

- Some kind of coordinating party (chat group, server, protocol, etc) where participants propose their inputs and outputs (have to make sure they add up)
  - One party issues the multi-input/output transaction
- Some trickiness in the coordination protocol
  - Online chat: all the parties learn inputs and outputs
  - Central server: server learns inputs outputs
  - Privacy-preserving versions of the central server protocol that obviate this risk (e.g. chaum blind signatures, Schnorr blind signatures)

Tradeoffs

- Size of anonymity set vs (time to completion or risk of blocked transaction)
  - Note risk of denial-of-service – any party can block a coinjoin
- Multi-level coinjoin mixes vs latency

Quick aside: L3 anonymity

All Mixnets

- If mix server can log input IPs then it can "name" inputs
- Solution: access server via ToR to hide origin IP; use multiple ToR connections so each interaction has different IP

Bitcoin P2P network itself (not related to Mixes)

- If you can monitor all/many Bitcoin nodes you can infer that the first IP address that proposes a transaction may have originated that transaction
- Solutions:
  - Hide IPs: Some nodes connect via ToR (tend to be outbound only),
  - Deny SuperNodes: Ad hoc rules to make it hard to "join" lots of nodes to monitor them
  - New relay protocols: Dandelion, Clover (I don't think these are used in practice yet)
- Aside: a bunch of "big" nodes clearly don't follow standard P2P protocol

Coinjoin in practice

Primarily offered by wallet services

- Wasabi Wallet
  - Large transactions, Schnorr blinded signatures (ZK) to hide input/output mapping
  - Transactions can have significant latency to gather anonymity set (depends on load)
- Samourai Wallet
  - Smaller transactions, some kind of Chaum blinded signature, multi-level mix
  - Somewhat lower latency, unclear impact on linkability

Typically work based on fixed denominations
(to support indistinguishability)

- E.g., Wasabi supports a bunch of different denomination pools

Charge fees (typically on first transaction, remixing free)

Legality

Coinjoin proponents argue that they are very different from central mixers, because they never touch the money

They just help coordinate the transaction, they don't **do** it – so this is ok

FinCEN GUIDANCE

FIN-2019-G001

Issued: May 9, 2019

Subject: Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies

4.5.1. Providers of anonymizing services for CVCs

Providers of anonymizing services, commonly referred to as "mixers" or "tumblers," are either persons that accept CVCs and retransmit them in a manner designed to prevent others from tracing the transmission back to its source (anonymizing services provider), or suppliers of software a transmitt***or*** would use for the same purpose (anonymizing software provider).

exclusively of providing secured money transmission. Therefore, a person (acting by itself, through employees or agents, or by using mechanical or software agencies) who provides anonymizing services by accepting value from a customer and transmitting the same or another type of value to the recipient, in a way designed to mask the identity of the transmitt***or***, is a money transmitter under FinCEN regulations.

Six days ago…

PRESS RELEASE

Founders And CEO Of Cryptocurrency Mixing Service Arrested And Charged With Money Laundering And Unlicensed Money Transmitting Offenses

Wednesday, April 24, 2024

Share

For Immediate Release

U.S. Attorney's Office, Southern Dist

Keonne Rodriguez and William Lonergan Hill Are Charged with Operating Samourai Unlicensed Money Transmitting Business That Executed Over $2 Billion in Unlawfu Laundered Over $100 Million in Criminal Proceeds

Three days ago…

ZKSNACKS IS NOW BLOCKING U.S. RESIDENTS AND CITIZENS

Saturday, April 27th 2024—Effective immediately and until further notice, zkSNACKs is now blocking U.S. citizens and residents from visiting its websites, downloading and using Wasabi Wallet and any related products and services, including APIs and RPC interfaces.

In light of recent announcements by U.S. authorities, zkSNACKs is now strictly prohibiting U.S. users from using its services. An IP address blocking for U.S. residents is effective on *wasabiwallet.io*, *api.wasabiwallet.io* and *zksnacks.com*.

"U.S." refers to "United States" and includes the several states of the United States and related territories. If you are a United States Citizen or United States Resident, you are not allowed to visit any sites aforementioned, download Wasabi Wallet or use the Wasabi Wallet coinjoin feature. This includes if you are a U.S. permanent resident or if you are an individual that holds a U.S. passport.

Tornado Cash

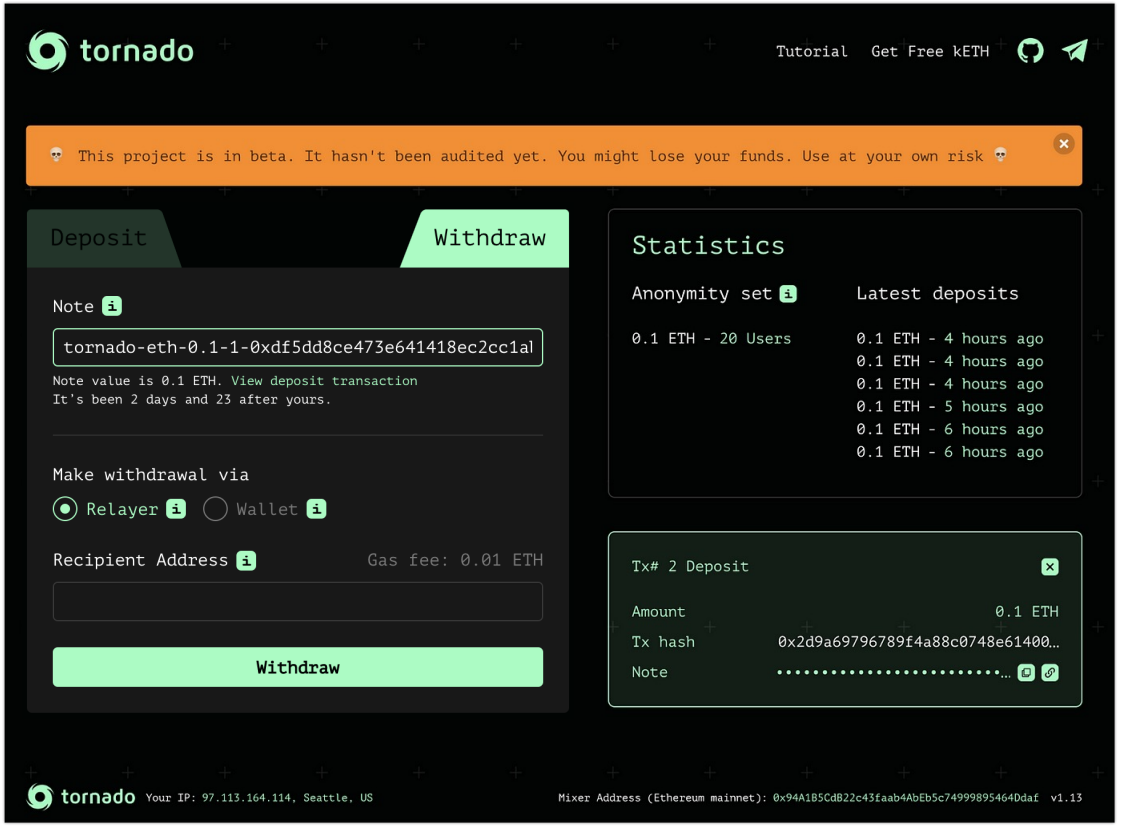
Introducing Private Transactions On Ethereum NOW!

Like other mixes, but done via smart contracts

- Step 1: Deposit say 0.1 ETH into pool from address A
- Step 2: wait
- Step 3: withdrawal 0.1 ETH later to address B

Goal: can't link A and B

- What makes this hard?



Tornado Cash

Deposit:

- You deposit 0.1 ETH from A and a cryptographic commitment C=H(r||k)
- Contract adds the commitment to the Merkle tree
- Addition to the tree ~ "coin"

```
/**
  @dev Deposit funds into the contract. The caller must send (for ETH) or approve (for ERC20) value equal to or `denomination` of this instance.
  @param _commitment the note commitment, which is PedersenHash(nullifier + secret)
*/
function deposit(bytes32 _commitment) external payable nonReentrant {
  require(!commitments[_commitment], "The commitment has been submitted");

  uint32 insertedIndex = _insert(_commitment);
  commitments[_commitment] = true;
  _processDeposit();

  emit Deposit(_commitment, insertedIndex, block.timestamp);
}
```

```
function _processDeposit() internal override {
  require(msg.value == 0, "ETH value is supposed to be 0 for ERC20 instance");
  token.safeTransferFrom(msg.sender, address(this), denomination);
}
```

```
/**
  @dev Withdraw a deposit from the contract. `proof` is a zkSNARK proof data, and input is an array of circuit public inputs
  `input` array consists of:
    - merkle root of all deposits in the contract
    - hash of unique deposit nullifier to prevent double spends
    - the recipient of funds
    - optional fee that goes to the transaction sender (usually a relay)
*/
function withdraw(
  bytes calldata _proof,
  bytes32 _root,
  bytes32 _nullifierHash,
  address payable _recipient,
  address payable _relayer,
  uint256 _fee,
  uint256 _refund
) external payable nonReentrant {
  require(_fee <= denomination, "Fee exceeds transfer value");
  require(!nullifierHashes[_nullifierHash], "The note has been alread
  require(isKnownRoot(_root), "Cannot find your merkle root"); // Mak
  require(
    verifier.verifyProof(
      _proof,
      [uint256(_root), uint256(_nullifierHash), uint256(_recipient),
    ),
    "Invalid withdraw proof"
  );

  nullifierHashes[_nullifierHash] = true;
  _processWithdraw(_recipient, _relayer, _fee, _refund);
  emit Withdrawal(_recipient, _nullifierHash, _relayer, _fee);
}
```

```
function _processWithdraw(
  address payable _recipient,
  address payable _relayer,
  uint256 _fee,
  uint256 _refund
) internal override {
  require(msg.value == _refund, "Incorrect refund amount received by the contract");

  token.safeTransfer(_recipient, denomination - _fee);
  if (_fee > 0) {
    token.safeTransfer(_relayer, _fee);
  }

  if (_refund > 0) {
    (bool success, ) = _recipient.call{ value: _refund }("");
    if (!success) {
      // let's return _refund back to the relayer
      _relayer.transfer(_refund);
    }
  }
}
```

Tornado Cash

Withdrawal:

- Provide proof that you own the coin (given the pre-image and Merkle tree)
- Contract verifies proof and ensure you haven't spent it
- ERC20 transfer

What's the point of the relayer?

- If C pays for gas to withdraw 0.1 ETH to address B: we can link C to B…. and C probably got the gas money from an exchange!
- Paying relayer a fee removes the link from B to C.. this is how they makey money

Tornado Cash

Aug 22: Tornado Cash is now on the OFAC denylist

- Github removes Tornado Cash repo and suspends dev accounts
- Circle freezes 75K belonging to Tornado Cash
- Alexey Pertsev arrested for money laundering (Netherlands)
  - Verdict in 14 days
- EFF and Matt Green bring back code on GitHub (free speech)

May 202:

- Hacker mints $TORN DAO voting tokens
- Uses Tornado cash to launder ~$900USD worth of ETH they got from exchanging $TORN for ETH

Tornado Cash Founders Charged With Money Laundering And Sanctions Violations

Wednesday, August 23, 2023

Share

For Immediate Release

U.S. Attorney's Office, Southern District of New York

Roman Storm and Roman Semenov Charged with Operating the Tornado Cash Service, Laundering More Than $1 Billion in Criminal Proceeds

Damian Williams, the United States Attorney for the Southern District of New York, Merrick B. Garland, the Attorney General of the United States, Christopher A. Wray, the Director of the Federal Bureau of Investigation ("FBI"), Nicole M. Argentieri, the Acting Assistant Attorney General of the Justice Department's Criminal Division, Matthew G. Olsen, the Assistant Attorney General of the Justice Department's National Security Division, James Smith, the Assistant Director in Charge of the New York Field Office of the FBI, and Bryant Jackson, the Special Agent in Charge of the Cincinnati Field Office of the Internal Revenue Service, Criminal Investigation ("IRS-CI"), announced today the unsealing of an Indictment charging ROMAN STORM and ROMAN SEMENOV with conspiracy to commit money laundering, conspiracy to commit sanctions violations, and conspiracy to operate an unlicensed money transmitting business. The charges in the Indictment arise from the defendants' alleged creation, operation, and promotion of Tornado Cash, a cryptocurrency mixer that facilitated more than $1 billion in money laundering transactions and

US Law and Mixers (my opinion)

Maybe mixing services are not illegal… but if you run one you ***must***

- Register as a money transmitter with FinCEN
- Maintain fully complaint AML program (including KYC obligations for clients)
- Meet all record keeping and reporting obligations (e.g., BSA++)

Basically no one does this

Aside: Sanctioning

Financial sanctions are meant to deny an organization access to financial services. Thing of this is a financial firewall implemented by banks, where the govt updates the rules with the names of people/orgs

In the US, this is implemented by the Office of Foreign Asset Control (OFAC) (similar organizations in the UK, EU, etc)

What about crypto? How to sanction?

- Sets of addresses are sanctioned (associated with entity)
- Illegal to act on transactions to/from those addresses if under jurisdiction
- Some obligation to do some basic tracing to identify "taint"
  (this is one of the lines of business for companies like Chainalysis)

Blender.io and Tornado Cash sanctioned

- Illegal to accept transactions with coins derived from their addresses

Privacy coins



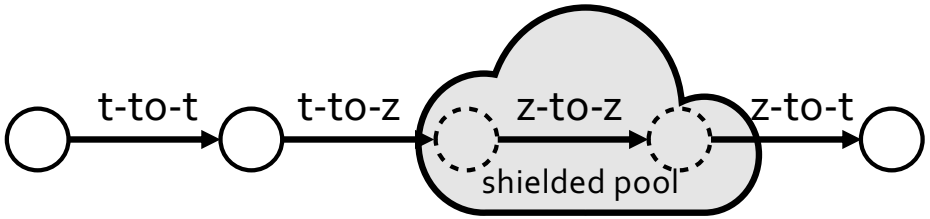
Another option:

- Blockchains designed to complicate tracing
- E.g., Zerocash, Monero, Dash (aka Darkcoin)

How do these work?

- Most make some use of zkSnarks:
  Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
- Basic idea: cryptographic mechanism to make an assertion that one possesses a piece of information, which can be validated without revealing the information to the verifier

Zcash



Basic substrate: standard PoW Bitcoin-like system

- Original version actually interoperated w/Bitcoin

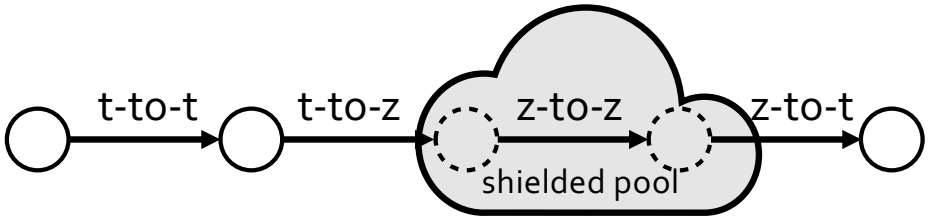
Two different kinds of addresses: t and z

- T addresses are just like normal bitcoin addresses – no additional anonymity
- Z addresses and transactions between them encrypted
  (don't know counterparty addresses, don't know value);
  validated by miners using zkSnarks

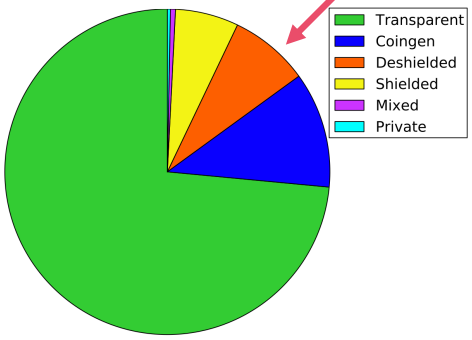
  Note: all mining rewards are born in the shielded pool (i.e., with z addresses)

Zcash in practice

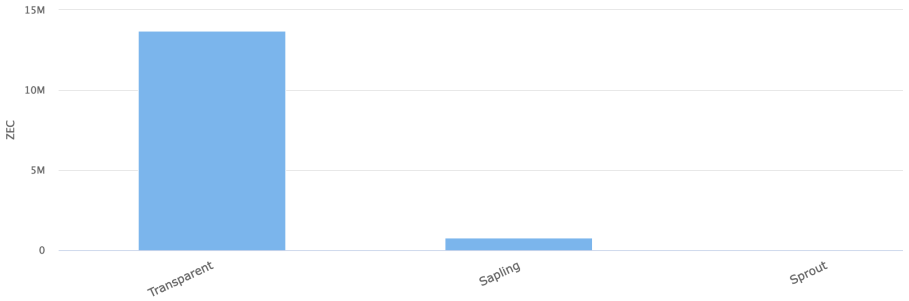
An Empirical Analysis of Anonymity in Zcash, Kappos et al, 2018



only 15% of txs use the pool at all!



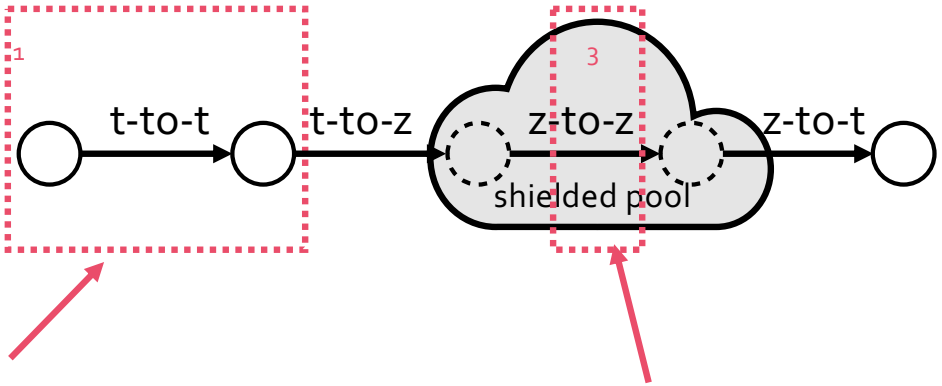
(Jan 2018)



(Jun 2022)

Zcash in practice

An Empirical Analysis of Anonymity in Zcash, Kappos et al, 2018

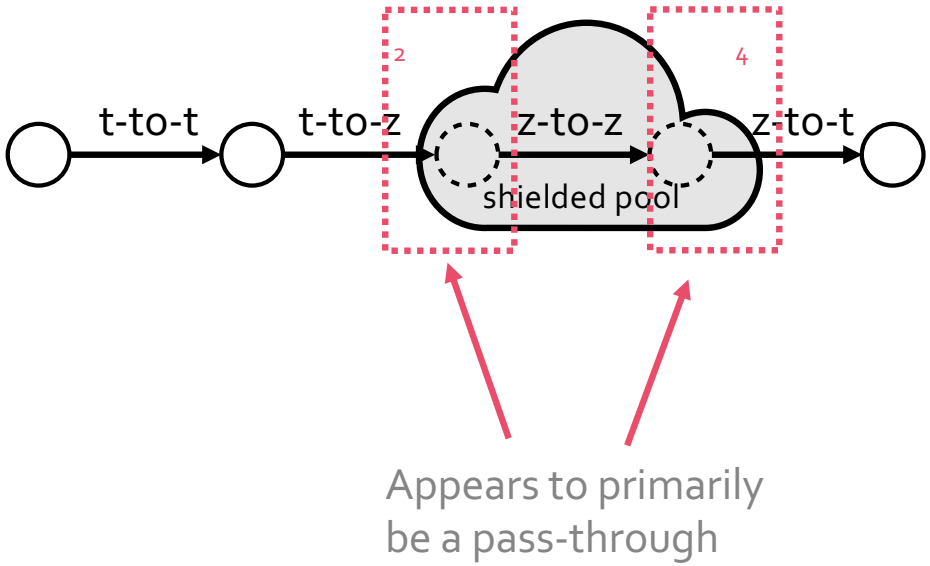


Just like Bitcoin,
dominated by exchanges
Traditional clustering works

Hard to deanonymize
but rarely used

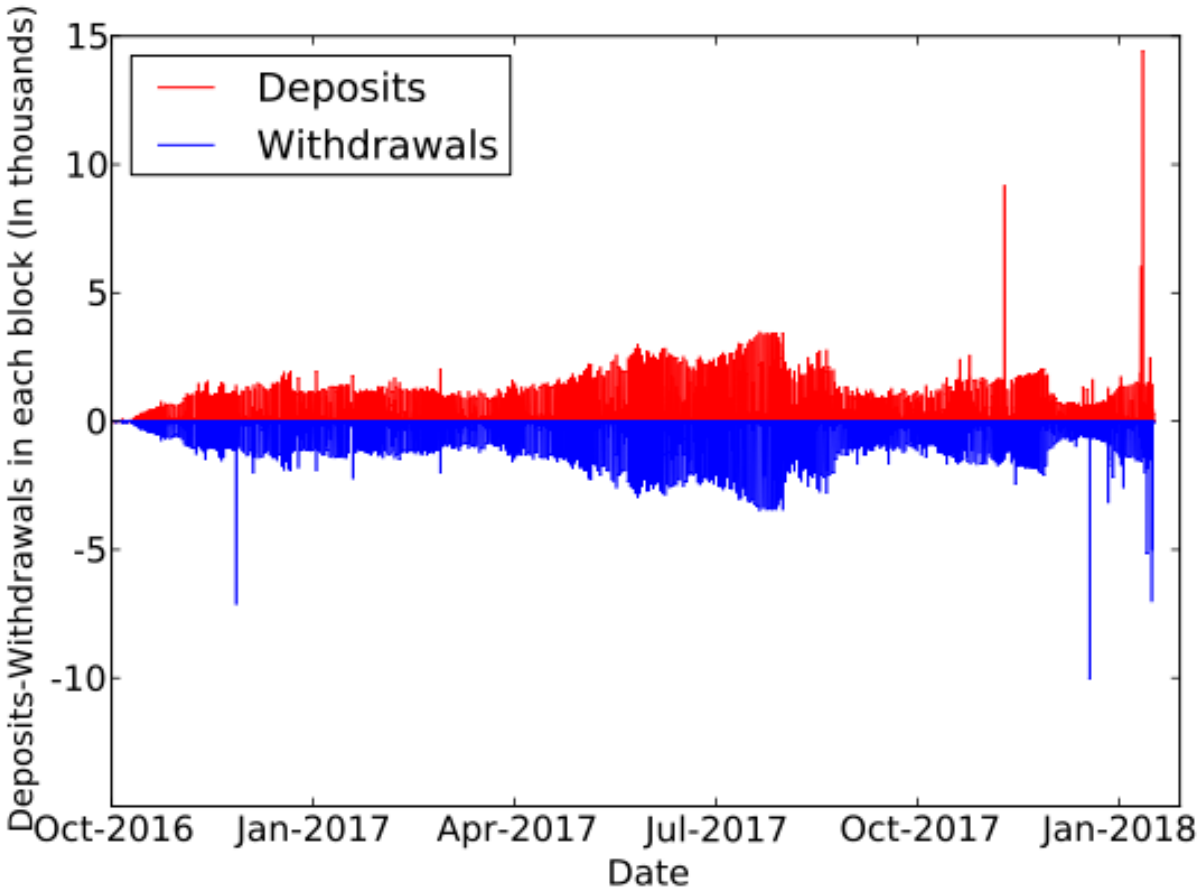
Zcash in practice

An Empirical Analysis of Anonymity in Zcash, Kappos et al, 2018



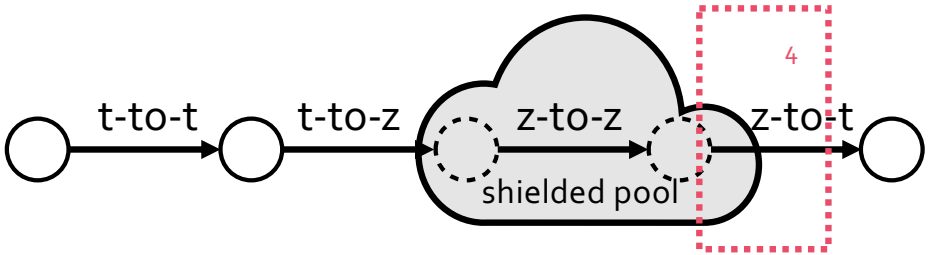
Zcash in practice

An Empirical Analysis of Anonymity in Zcash, Kappos et al, 2018



Zcash in practice

An Empirical Analysis of Anonymity in Zcash, Kappos et al, 2018



Zcash mining

- Miners get 12.5 ZEC block reward
- Founders get 2.5 ZEC

Simple heuristics reduce anonymity set of z-to-t by > 67%

- If z-to-t transaction has > 100 t-addresses and one is associated with a mining pool then they're all miners
- If transaction is for 250.01 ZEC then it's a founder (common pattern)

Some similar issues w/Monero

(although both have improved since these papers were written)

Malte Möser*, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin

An Empirical Analysis of Traceability in the Monero Blockchain

coins they spend. In this paper, we empirically evaluate two weaknesses in Monero's mixin sampling strategy. First, about 62% of transaction inputs with one or more mixins are vulnerable to "chain-reaction" analysis — that is, the real input can be deduced by elimination. Second, Monero mixins are sampled in such a way that they can be easily distinguished from the real coins by their age distribution; in short, the real input is usually the "newest" input. We estimate that this heuristic can be used to guess the real input with 80 % accuracy over all transactions with 1 or more mixins.

Note – multiple crypto tracing companies imply they can trace Monero

Legality and privacy coins

So far… legal in the US

Banned in Japan

Exchanges not allowed to offer (Australia, South Korea)

A number of exchanges operating under EU jurisdiction have chosen to delist privacy coins in response to 5AMLD regulation

- Requires KYC and monitoring

Regulatory future does not seem bright…

> (c) a person that develops a *decentralized* CVC payment system will become a money transmitter if that person also engages as a business in the acceptance and transmission of value denominated in the CVC it developed (even if the CVC value was mined at an earlier date). The person would not be a money transmitter if that person uses the CVC it mined to pay for goods and services on his or her own behalf.[64]

To summarize

A bunch of ways to try to defeat crypto tracing

- Break input/output link and hide within chaff of other transactions
  - Mixes & Coinjoins
- New blockchains that use ZK (some new ones use FHE) to hide contents and addresses of transactions

Both are tricky to get right against careful analysis

- Big part of the problem is user demand
  - Want to get money out of system into something liquid
  - Don't like to wait
  - Fine for small amounts… tough for large amounts

Increasingly illegal to do such things in a way that undermines ability of govt to pursue anti-money laundering agenda