Plausible Deniability and Cryptocurrency Privacy

three things to cover
1. attack surface
2. case studies
3. tools

Workshop at HOPE 2022 https://scheduler.hope.net/new-hope/talk/CKQDT7/

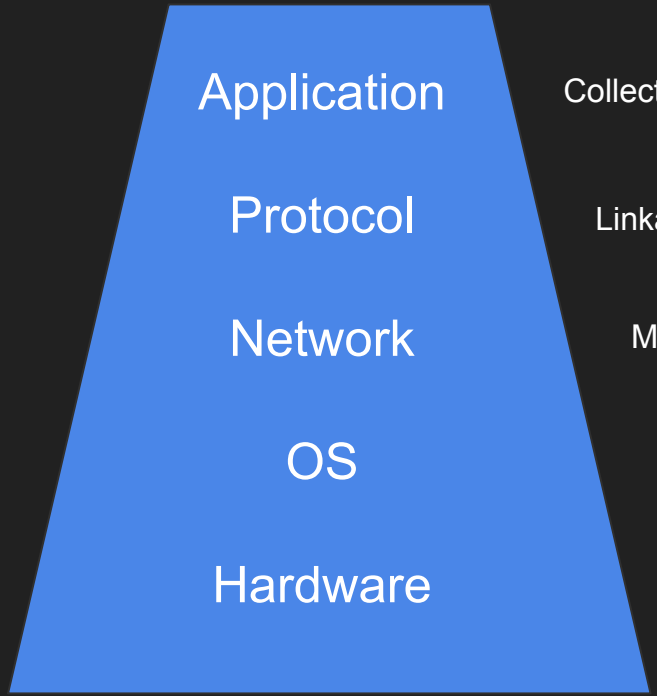
Lane Rettig @lrettig | Michelle Lai @michlai007
Ahmed Ghappour @ghappour | Arctic Byte

22 July 2022

quick overview of “the stack”: let’s start with the basics + where do we leak data

[Arctic Byte]

Privacy across the stack



Collecting IP addresses & other user data

Linkable interactions, RPC endpoints

Metadata, who you're talking to, where you are

OS vulnerabilities

Supply chain attacks, device fingerprinting

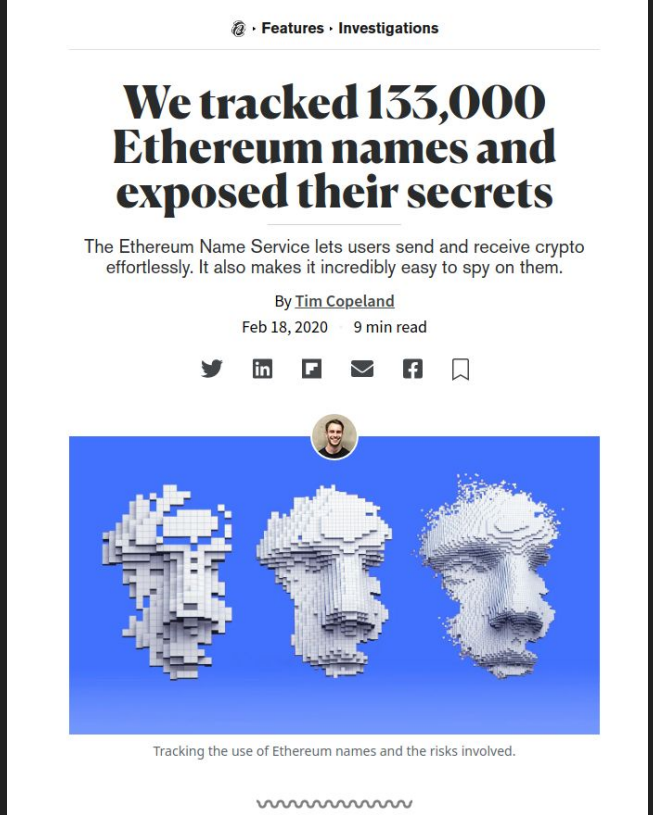
Case studies

(1) ENS tracing

ENS tracing

Situation

- 2020
- High-profile people identified
- Business deals were visible
- Data sources: ENS, Twitter, Proof of Humanity



· Features · Investigations

We tracked 133,000 Ethereum names and exposed their secrets

The Ethereum Name Service lets users send and receive crypto effortlessly. It also makes it incredibly easy to spy on them.

By Tim Copeland

Feb 18, 2020 · 9 min read

Tracking the use of Ethereum names and the risks involved.

In brief

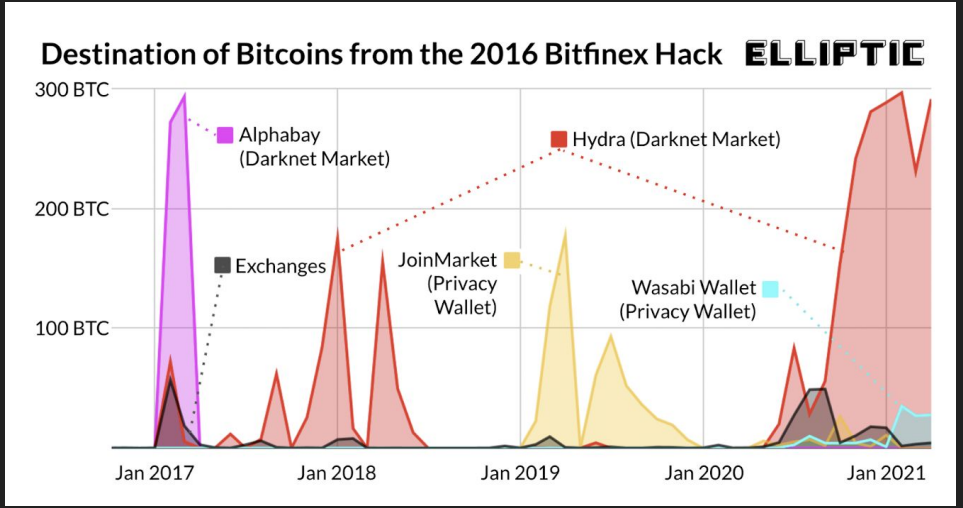
- We analyzed 133,000 Ethereum names and their respective balances.
- We found it was possible to identify several high-profile people, even if they weren't using their real names.
- We were able to see business deals and watch people's movements, just using the blockchain.

(2) Arrested: Bitfinex hackers

Bitfinex hackers

Situation

- 2016
- 120,000 $BTC stolen ($72mn then, $7bn last year)
    - Spread to thousands of addresses; uploaded to Reddit
- Impact: haircut customers 36% (paid back over 1 year)
- 5 years later (mid-2021), only 4% laundered (exchanges), 21% moved
- Feb 2022: caught!



Source: https://www.elliptic.co/blog/elliptic-analysis-bitcoin-bitfinex-theft

Bitfinex hackers

How they got caught

- **Blacklisted addresses** - could be followed as they move. Not accepted by regulated exchanges
- **KYC'd under his real ID** at an exchange that was one hop among many hops (he had fake IDs)
- **ISP records** (access to darknet sites?)
- **Bad luck: AlphaBay founder** knew his ID, and was arrested
- FBI **cracked encryption** on a file with the private keys of >2,000 blacklisted addresses

Source: https://www.bloomberg.com/news/features/2022-06-30/how-the-world-s-biggest-bitcoin-btc-hack-at-bitfinex-got-botche

(3) Suspected: The DAO hacker

The DAO Hack

Situation

- 2016
- First ever DAO on Ethereum, a decentralized VC
- $136mn ETH raised
- Weeks later, 31% stolen (5% of all ETH in existence)
  - Resulted in the only hard fork of ETH
  - “ETH” > “ETC”
- Unsolved as of today, but strong clues point to the high profile crypto founder of a startup that ceased operations in 2020

Movement of ETC

1. Shapeshift exchange
   - **ETC > BTC exchange**
   - No KYC: illicit funds could trade
   - Shapeshift kept blocking their trades. Left $3.2mn
2. Wasabi Wallet (privacy wallet)
   a. **Blacklisted BTC > anon. BTC**
   b. Coinjoin BTC to obscure illicit source
3. More exchanges
   a. **Anon. BTC > other tokens e.g. Grin, fiat**

Source: https://www.forbes.com/sites/laurashin/2022/02/22/exclusive-austrian-programmer-and-ex-crypto-ceo-likely-stole-11-billion-of-ether/

The DAO Hack

Forensics

1. Alex van de Sande in Brazil
    a. **Coinfirm forensics report on early cashouts**
    b. Swiss and Russian suspects
    c. But cash outs 9am-12mn Tokyo
2. Chainalysis
    a. **De-mixed Wasabi wallet transactions**
    b. Tracked to 4 exchanges (no subpoena yet?)
    c. One employee disclosed BTC > Grin, and Grin withdrawn to node called grin.toby.ai
    d. Email address: [exchange]@tobi.ai

Corroborating evidence

1. IP address
    a. Also hosted lightning nodes called ...toby.ai, and TenX
    b. Hosted on Amazon Singapore
2. Public stance
    a. Publicly and privately expressed concerns about The DAO's vulnerabilities before the hack
    b. Supportive of ETC after the fork

The DAO Hack: De-mixing Wasabi CoinJoins?

> *If you are using wasabi, you need to read this thread: https://t.co/FL7f30nWeC*
>
> *"With Wasabi if you are mixing 10 BTC, I can trivially track that 10 BTC as it is peeled down into smaller utxos. The left over change is part of the mix tx, and thus creates a determinstic link" pic.twitter.com/yTqJCp0YLp*
>
> *— ODELL (@ODELL) July 18, 2019*

Source: https://news.bitcoin.com/de-mixing-wasabi-coinjoin-transactions-a-deep-dive-into-chainalysis-deanonymizing-claims/ | https://twitter.com/ODELL/status/1151882688053334016

The DAO Hack: De-mixing Wasabi CoinJoins?

Amir Taaki Calls Coinjoin Schemes 'Absolute Garbage,' Gavin Andresen Wouldn't Be Surprised if '85% of Tornado Cash Usage Was Not Private'

In addition to Wasabi, the Coinjoin mixing scheme itself has been criticized for leaking specifics about the mixing participants. Essentially, Coinjoin is an anonymization scheme first proposed by the developer Gregory Maxwell and it allows participants to combine multiple payments into a single transaction in order to obfuscate the transaction process. It's true that Coinjoin offers a deeper anonymity set, but if a user mixes a bunch of coins and eventually consolidates them into one address, it can still leave behind some traces to the original owner.

> ***Not because the cryptography is broken, but because it is really hard for mere mortals to use something like Tornado (or Coinjoin or other similar technologies) in a way that doesn't leak information about their wallet.***

101: law enforcement access to data

[Ahmed Ghappour]

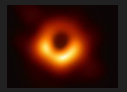
Considerations

- Types of information (example: email)
  - Account Information (name, physical address)
  - Session Metadata (network addr, time, duration)
  - Message Metadata (to, from, time, length)
  - Message Content (subject, body)
- Info collection
  - Retrospective
  - Prospective
- Standards
  - Relevance
  - Reasonable articulable suspicion (RAS)
  - Probable cause (PC)
- Types of orders
  - Prospective surveillance
    - Subpoena
    - Pen/Trap Order
    - Wiretap Order
  - Historical surveillance
    - Subpoena
    - D-Order
    - Warrant

Demos:
tools at different levels of the stack

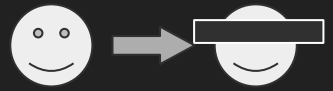
Definitions of transaction privacy

Identity: do you know know who I am?

mypaypal@gmail.com vs *0x19748Drw…* vs 

Pseudonymous (no real identifiers) |vs| Anonymous (no address)

Sender |vs| Receiver (who knows whom)



Relationship: do you know who sent whom funds?

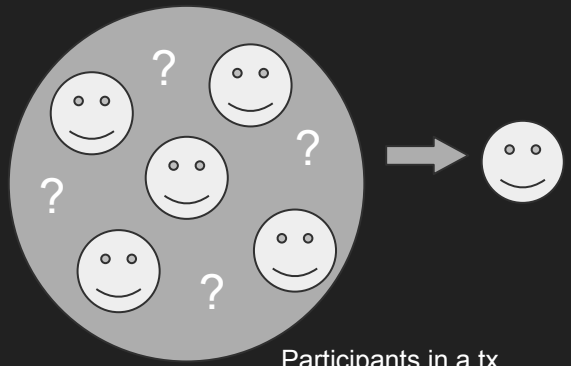
Probabilistic Guess/Plausible Deniability (set anonymity) |vs| Impractical to Guess (full anonymity)

Lost in the Crowd: larger the crowd, greater the anonymity

Amount

How much was moved in a tx

Can you see someone's balances



Participants in a tx

Satoshi: “anonymous”?

Bitcoin P2P e-cash paper

Satoshi Nakamoto satoshi at vistomail.com
Fri Oct 31 14:10:00 EDT 2008

- Previous message: Fw: SHA-3 lounge
- **Messages sorted by:** [date] [thread] [subject] [author]

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

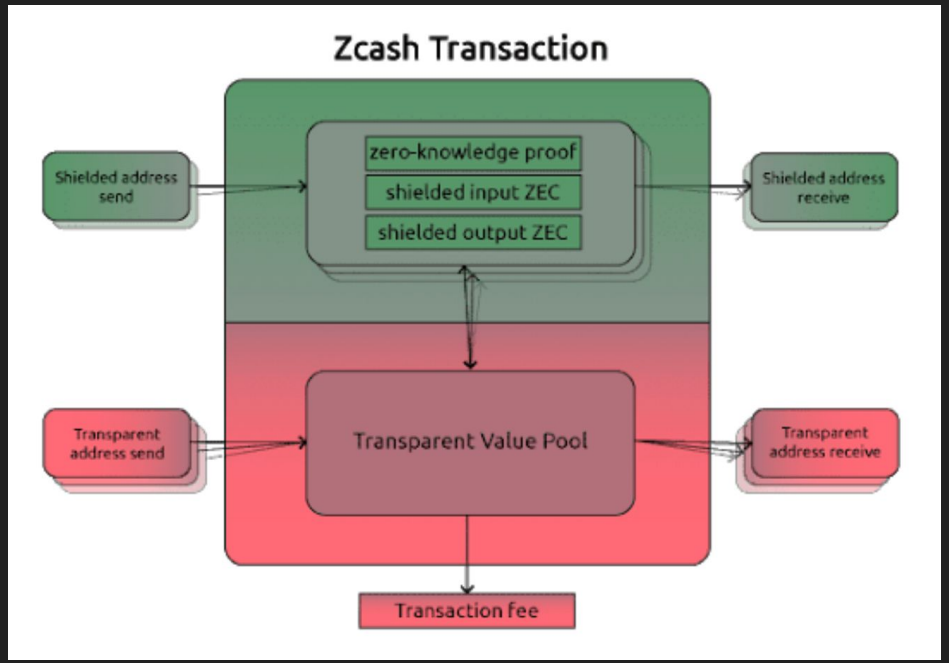
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main

Levels of Anonymity

#	crypto-currency	Anonymity Tier: pseudo-anonymity	set anonymity	full anonymity	+CT
1	Bitcoin	✓			
2	Ethereum	✓			
3	Ethereum Classic	✓			
4	Bitcoin Cash	✓			
5	Bitcoin Diamond	✓			
6	Litecoin	✓			
7	Cardano	✓			
8	IOTA	✓			
9	Dogecoin	✓			
10	NEM	✓			
11	Nano	✓			
12	Lisk	✓			
13	Waves	✓			
14	Tether	✓			
15	USD Coin	✓			
16	Dash		✓		
17	Bytecoin		✓		
18	Monero		✓		✓
19	Zerocoin			✓(2)	
20	Zcash			✓(3)	✓

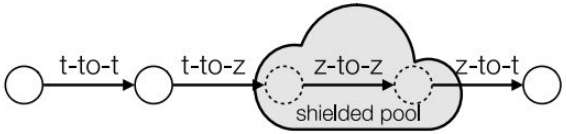
Source: https://eprints.lancs.ac.uk/id/eprint/139412/1/main.pdf

Sender vs Receiver Privacy



Source: https://eprint.iacr.org/2020/593.pdf

What is wanted?



A simple diagrams illustrating the different types of Zcash transactions

- Users
  - Perform fast, quickly verified, cheap and private transactions
- Miners
  - Maximise short term profit and long term health of the network (*tragedy of the commons* [4])
  - Regular flow of transactions to benefit from fees
- Governance
  - Long term network health
  - Enforce changes to design, protocol and additional features

	Sender	Receiver	Amount
Public	✓	✓	✓
Shielded	✓	×	✓
Private	×	×	×
De-shielded	×	✓	✓

Data revealed per transaction type

Source: https://arxiv.org/pdf/1901.02695.pdf

(1) Network level:
Layer Zero privacy protection [AG]

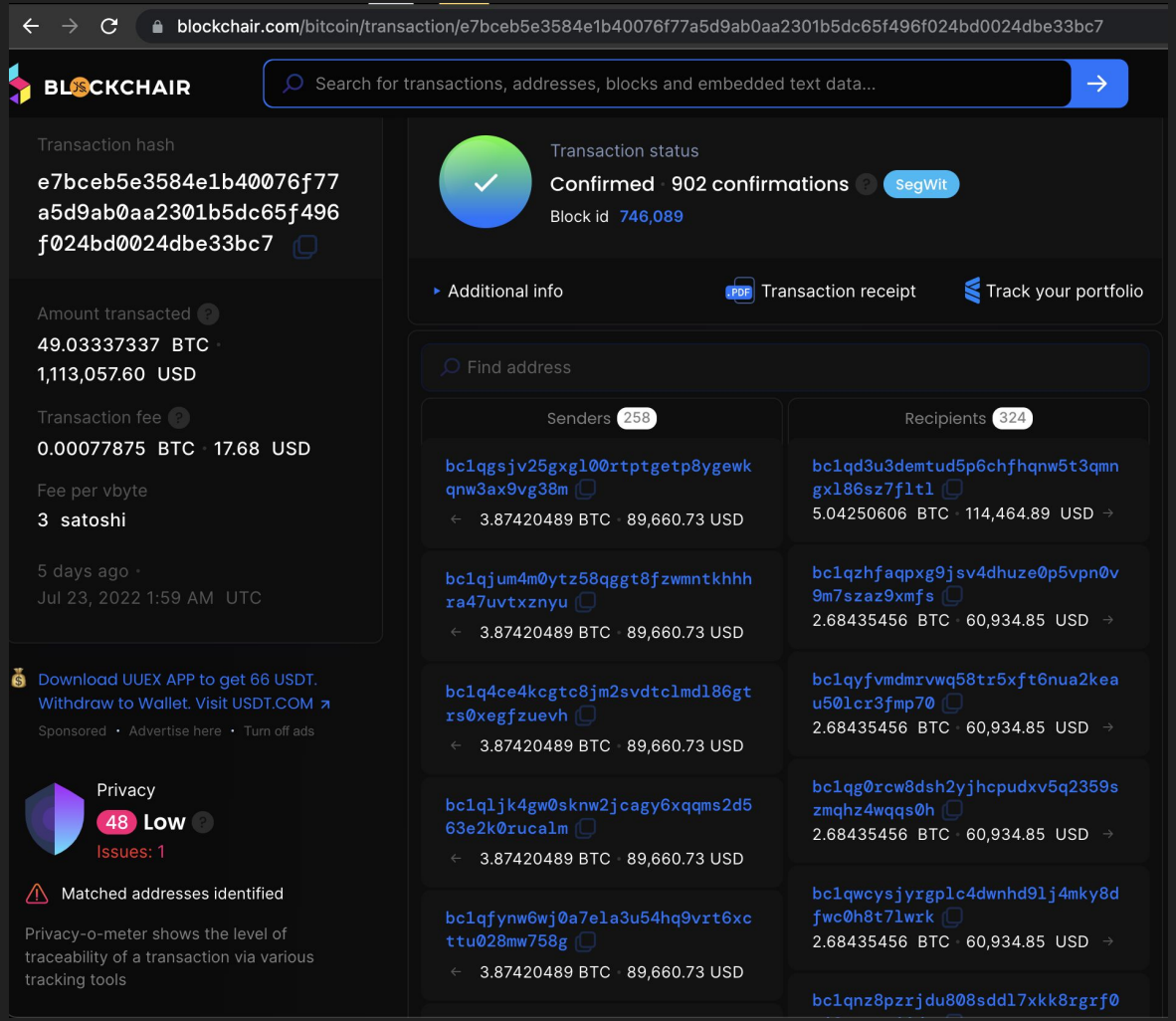
(2) Wallet level

(Lane Rettig)

Wallet-level privacy

1. Wallet basics, address management
2. Lightning network
3. De-anon realtime demo
4. Mixers
5. Bitcoin privacy demo: Wasabi wallet
6. And why they aren’t foolproof, either

Wasabi Wallet



Source: https://blockchair.com/bitcoin/transaction/e7bceb5e3584e1b40076f77a5d9ab0aa2301b5dc65f496f024bd0024dbe33bc7

(3) Protocol level

Michelle Lai

@michlai007

Protocol level privacy demos

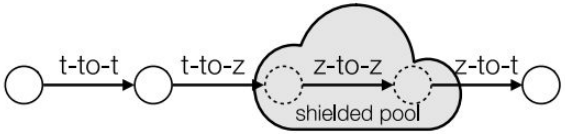
1. Privacy coin: Zcash
2. Mixer: Tornado Cash
3. Private smart contract platforms
    a. Rollup on Ethereum: Zk.money / Aztec Protocol
    b. L1: Manta Network (Polkadot parachain)
    c. L1: Secret Network (Cosmos network) (TEE, not zero-knowledge)

Privacy coin: Zcash

Demo:

1. t-to-t transaction (“public” transaction)
2. **t-to-z transaction (“shielding”)**
3. **z-to-z (“private” transaction)**
    a. **Viewing key**
4. z-to-t (“unshielding”)

What is wanted?



A simple diagrams illustrating the different types of Zcash transactions

- Users
  - Perform fast, quickly verified, cheap and private transactions
- Miners
  - Maximise short term profit and long term health of the network (*tragedy of the commons* [4])
  - Regular flow of transactions to benefit from fees
- Governance
  - Long term network health
  - Enforce changes to design, protocol and additional features

	Sender	Receiver	Amount
Public	✓	✓	✓
Shielded	✓	×	✓
Private	×	×	×
De-shielded	×	✓	✓

Data revealed per transaction type

Mixer: Tornado Cash

Walkthrough:
https://docs.tornado.cash/tornado-cash-classic/deposit-withdraw

Chains & Tokens:

Ethereum Blockchain : ETH (Ethereum), DAI (Dai), cDAI (Compound Dai), USDC (USD Coin), USDT (Tether) & WBTC (Wrapped Bitcoin),

Binance Smart Chain: BNB (Binance Coin),

Polygon Network: MATIC (Polygon),

Gnosis Chain (former xDAI Chain): xDAI (xDai),

Avalanche Mainnet: AVAX (Avalanche),

Optimism, as a Layer-2 for ETH (Ethereum),

Arbitrum One, as a Layer-2 ETH (Ethereum).

Source: https://github.com/tornadocash/docs/blob/en/README.md

Zk.money / Aztec Protocol *(Rollup on Ethereum)*

Demo:

1. **Register your Ethereum address**
   a. Create and connect it to an ID on the L2
2. **Shield some ETH**
   a. ETH / zkETH
   b. Proof takes about a minute
3. Send ETH within the rollup, privately
4. Unshield

Manta Network *(Polkadot parachain)*

Demo:

1. **Private transfers**
    a. **Desktop ZKP generator means fast proofs (few seconds)**

Secret Network *(Cosmos network)*

Demo:

1. **Buy an NFT publicly**
2. **Buy an NFT privately**
    a. Generate viewing key
    b. View hidden details

Note: TEE, not zero-knowledge proofs

Lane Rettig: @lrettig
Michelle Lai: @michlai007
Ahmed Ghappour: @ghappour
Arctic Byte: anon.