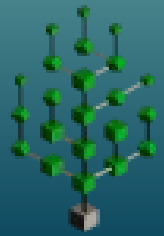
Bitcoin Privacy: On- and Off-Chain



Blockchain Training Conference

AUGUST 28-30 | DENVER

with

Janine Römer

- Independent investigative journalist
- Research focus: Bitcoin / cryptocurrencies, information security, privacy, surveillance, and whistleblowing


- Co-host on **Block Digest** and **zkSNACKS**

No photography for this session. Only audio.

(The slides will all be available online!)

What is Bitcoin Privacy?

Because the Bitcoin blockchain is public, the meaning of **privacy** is more complicated than something “secret,” “hidden,” or “in a state of freedom from intrusion.”

This session will examine privacy as a goal that is currently achieved by increasing **uncertainty** and **computational cost** in blockchain and traffic analysis.

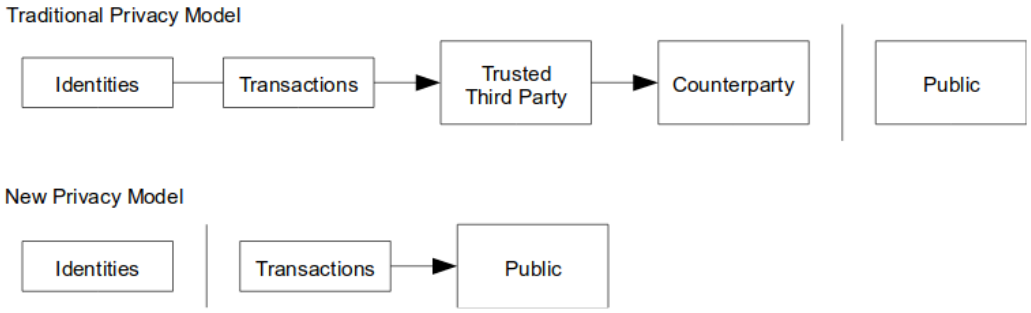
What is Bitcoin Privacy?

"The technology does a lot, but it also requires that you behave in a certain way. That is the important part where a CryptoParty adds value. They help people set up the software properly. But the other thing is, **all the tools also come with certain sets of behaviours**, and those are just as important as the tech itself... A false sense of security can be worse than having no security at all."

– Arjen Kamphuis, *Dutch cybersecurity expert*

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

"Privacy is **the right to consent**. Privacy is the right to withdraw consent, to only provide information to the people you want to provide it to, when you want to provide it.

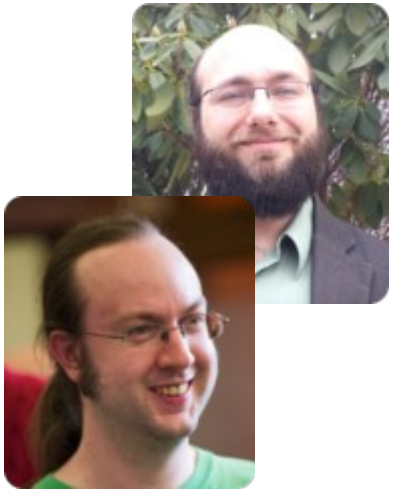
The modern debate around privacy has been focused on its contention with security, and framed to be about terrorism and criminality. Lost in this debate are the very real day to day battles that we all face."

- Sarah Jamie Lewis, Executive Director of Open Privacy & Author of '*Queer Privacy*'

A Modest Privacy Protection Proposal

"My primary takeaway after countless hours of research is that **we give a lot of personal information to many different merchants and service providers that are vulnerable to hacking and social engineering**.

You should assume that over a long enough period of time, any data you give to third parties will be made public—whether or not it happens intentionally is irrelevant. The general solution to many of these data leaks is to use proxies of all kinds: electronic, legal, and human." https://blog.lopp.net/modest-privacy-protection-proposal/



Anonymity Loves Company: Usability and the Network Effect

"Security is **a collaboration between multiple people**: both the sender and the receiver of a secret email must work together to protect its confidentiality.

Thus, in order to protect your own security, you need to make sure that the system you use **is not only usable by yourself, but by the other participants as well**."

- Roger Dingledine and Nick Mathewson, Tor Project founders (January 2006)

https://www.researchgate.net/publication/228348285_Anonymity_loves_company_Usability_and_the_network_effect

Bitcoin Basics

What is a bitcoin?

What is a transaction?

Unspent Transaction Outputs

What is a bitcoin?

A **bitcoin** (BTC) is the displayed unit of value in most Bitcoin applications. The algorithmic maximum supply that will ever be produced is 20,999,999.9769 (rounded, 21 million) bitcoin.

The smallest unit in the code itself, required for on-chain settlement, is the **satoshi** (sat). There are 100,000,000 (one hundred million) satoshis in a bitcoin.

The smallest unit on the Lightning Network is currently the **millisatoshi** (msat). There are 100,000,000,000 (one hundred billion) millisatoshis in a bitcoin.

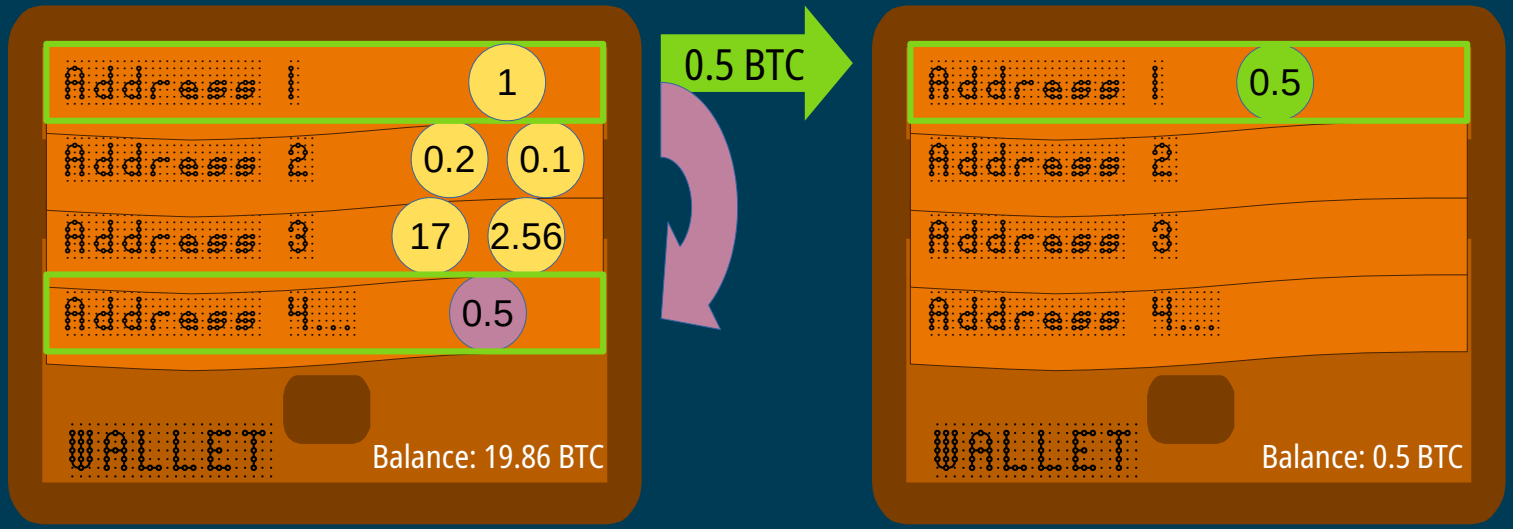
https://en.bitcoin.it/wiki/Units

What is a bitcoin transaction?

A transaction is the transfer, or transformation, of unspent coins from one address to another. The address the coins are transferred to may be in the same wallet, owned by the same person, or it may be a wallet owned by a different person.

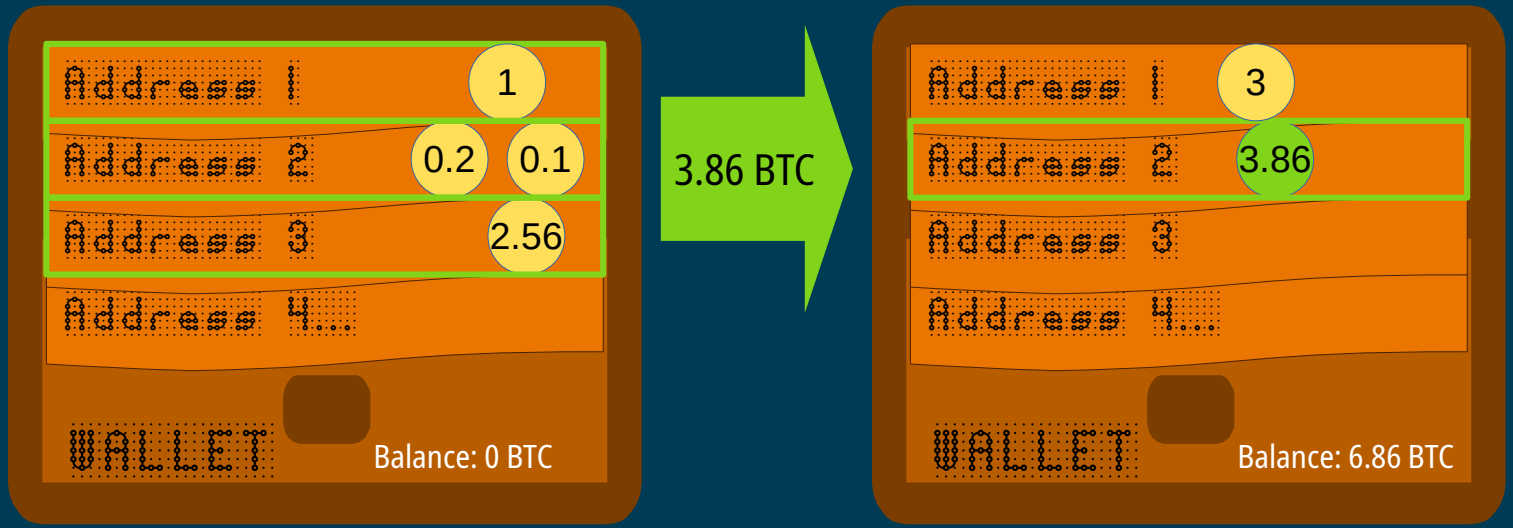
An address is a collection of these unspent transaction outputs (UTXOs), or none if it is a new address. A wallet (alternatively, 'keychain') is a collection of addresses and keys. Addresses are derived from public keys, which are derived from private keys.

Types of Transactions: Common

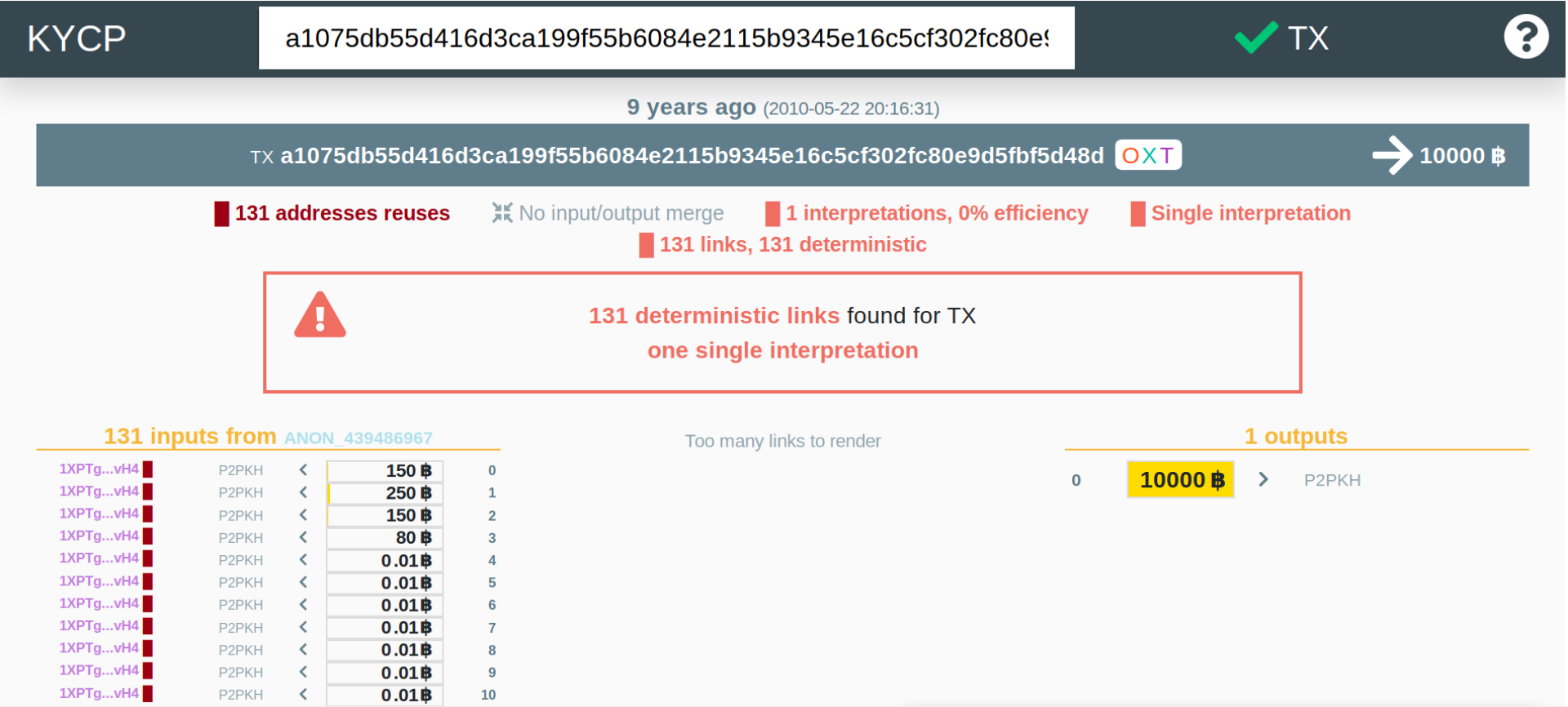


One input, two outputs

Types of Transactions: Aggregating

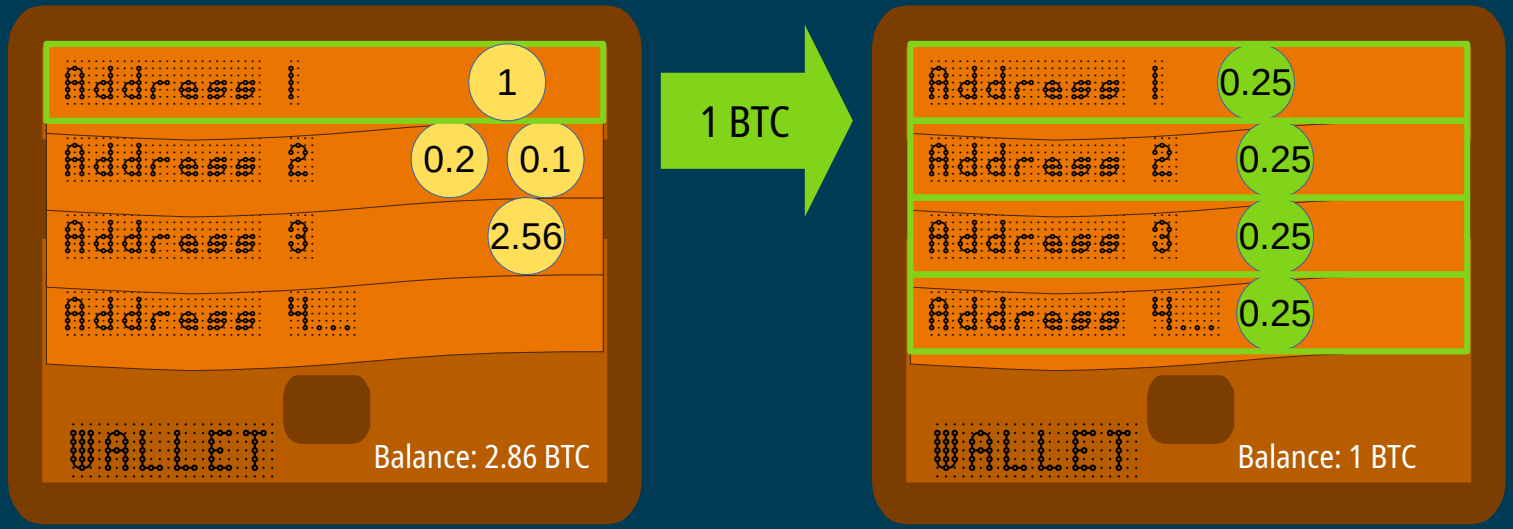


Many inputs, one output



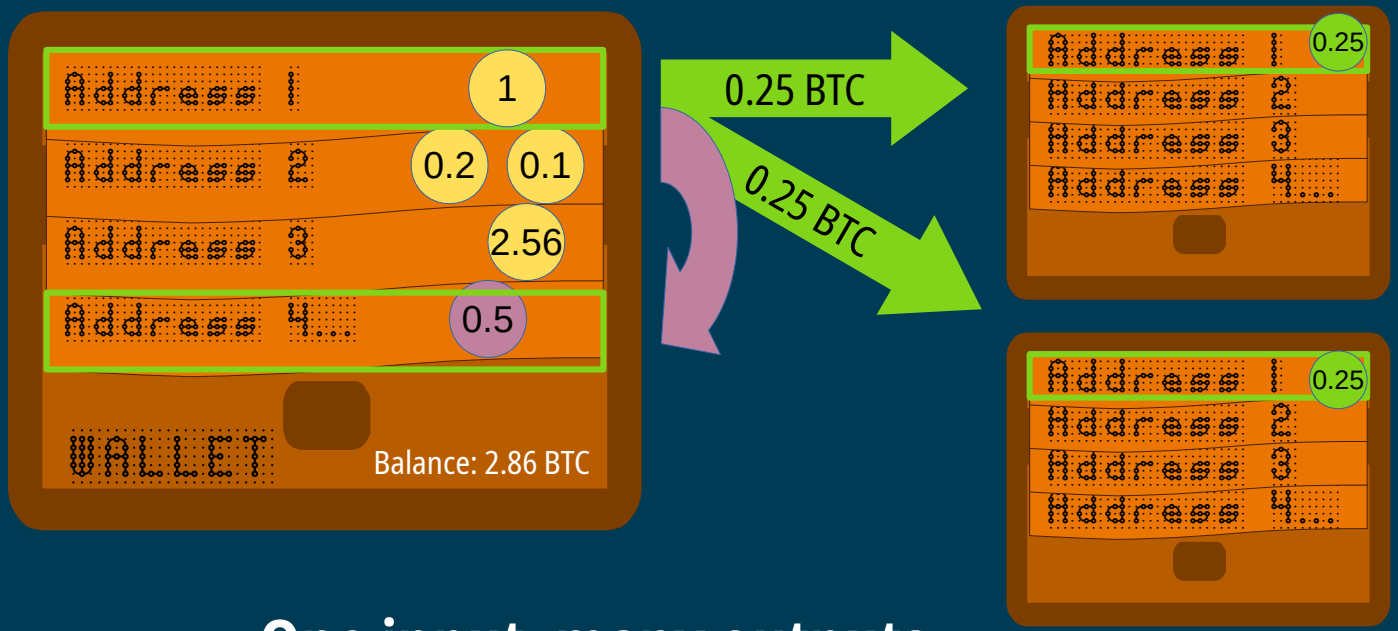
The most famous aggregating transaction in Bitcoin's history...

Types of Transactions: Distributing



One input, many outputs

Types of Transactions: Distributing

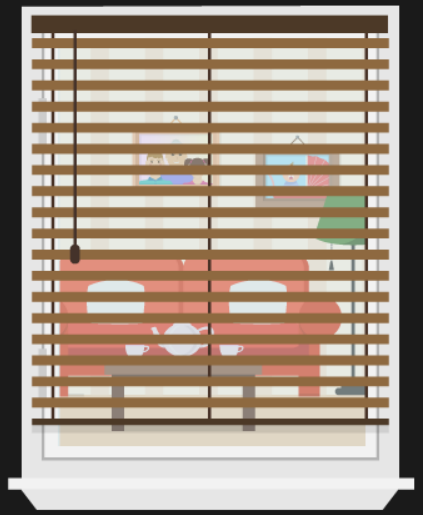


One input, many outputs

Bitcoin Explained

Bitcoin Privacy series

Privacy and UTXO [part 1]: How UTXO works?



Part 1 and **Part 2** by Patrícia Estevão and Marco Agner

Transaction Information

- Transaction data format version number
- The number of transaction inputs and outputs
- A list of the transaction inputs, and their witnesses
- A list of the transaction outputs
- (If enabled) a locktime value in the form of a block number or timestamp, when the funds will become spendable again

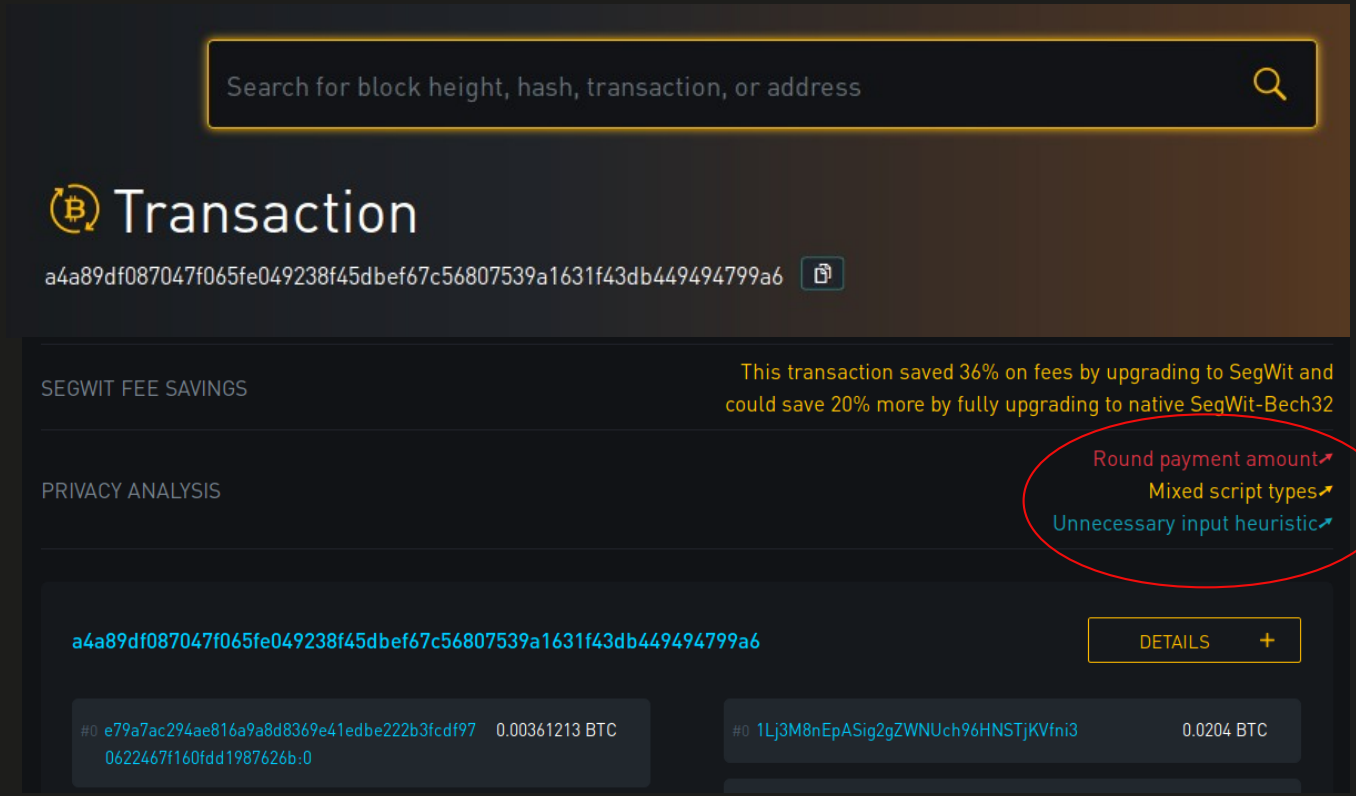
Wallet Fingerprinting

Does your wallet...

- Use particular address formats and scripts, particularly for handling change?
- Always order the change output second?

Most wallets hide details like this from the user, so people are unaware of how their transactions are actually generated.

Blockstream.info



ON-CHAIN ATTACK

Data or activities recorded in the Bitcoin blockchain

Available to **everyone** accessing the network

Cannot be erased

OFF-CHAIN ATTACK

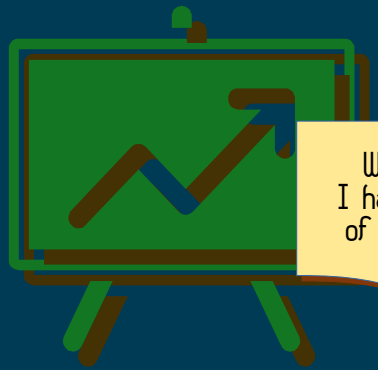
Data or activities **not** recorded in the Bitcoin blockchain

Sometimes available to everyone (ex. public profiles); usually **selectively** collected by various people, services, states

- **Bob**

the Whistleblower

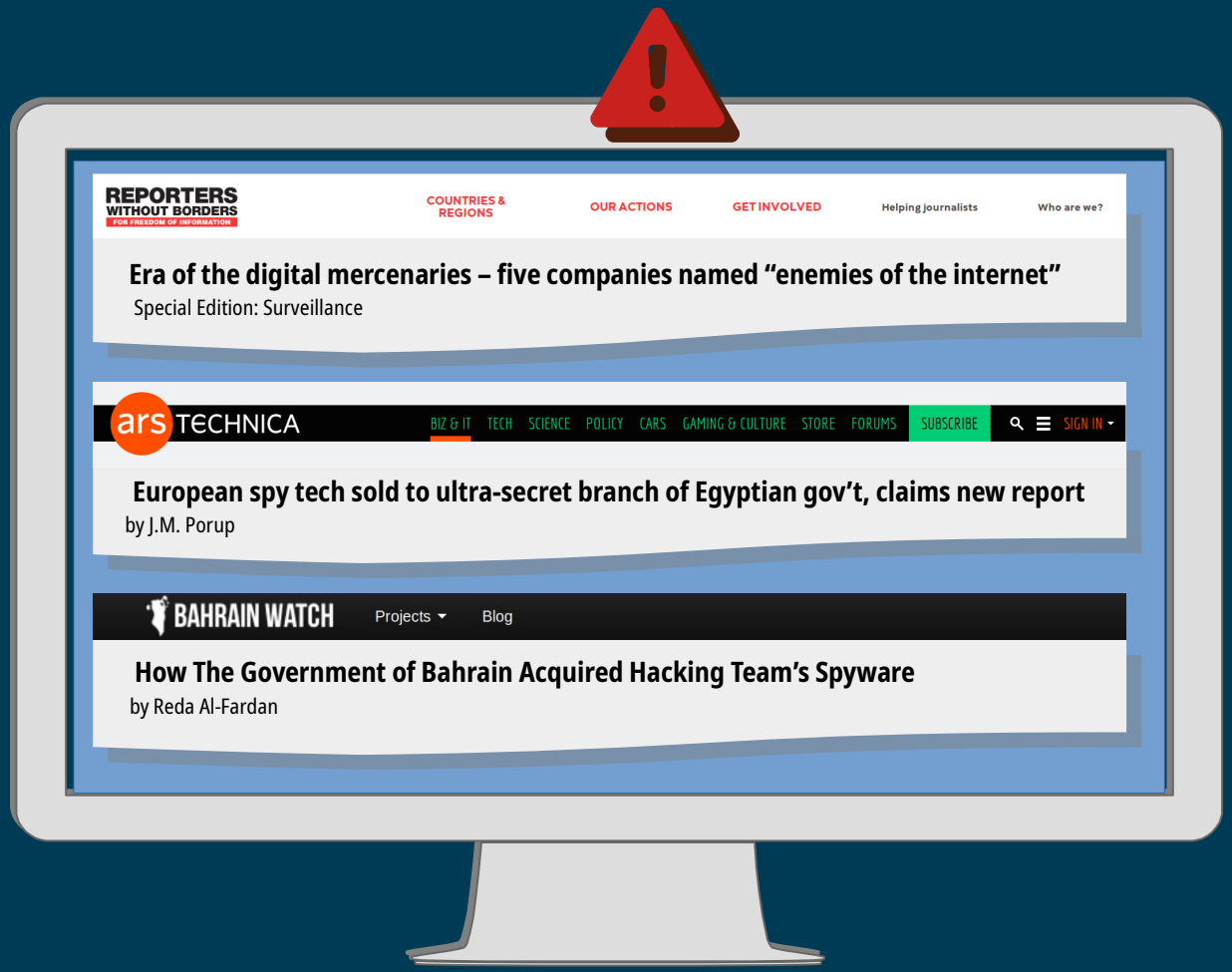
JOB DESCRIPTION:
Mid-level manager at a technology company based in Silicon Valley



Who are they? I have not heard of this company before....

NEW DIRECTIVE:
integrate analytic software of partne firm into product

Keep partnership info private – not for public release!
-Executive Team


REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION
COUNTRIES & REGIONS
OUR ACTIONS
GET INVOLVED
Helping journalists
Who are we?
Era of the digital mercenaries – five companies named "enemies of the internet"
Special Edition: Surveillance
ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
STORE
FORUMS
SUBSCRIBE
SIGN IN
European spy tech sold to ultra-secret branch of Egyptian gov't, claims new report
by J.M. Porup
BAHRAIN WATCH
Projects
Blog
How The Government of Bahrain Acquired Hacking Team's Spyware
by Reda Al-Fardan

>GENERAL WEAKNESSES

privacytools.io

- Hardware
- Operating systems
- Web browsers
- Search engines
- Email and messaging
- Proxies and VPNs
- DNS and VPS providers
- **Google Alternatives (!)**

>JUST ANOTHER ISP

THAT ONE PRIVACY SITE

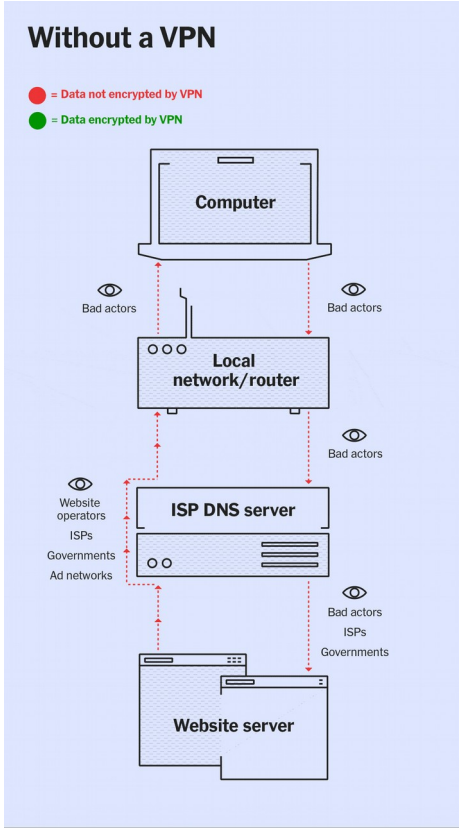
Research and comparison of Virtual Private Networks (VPNs) based on:

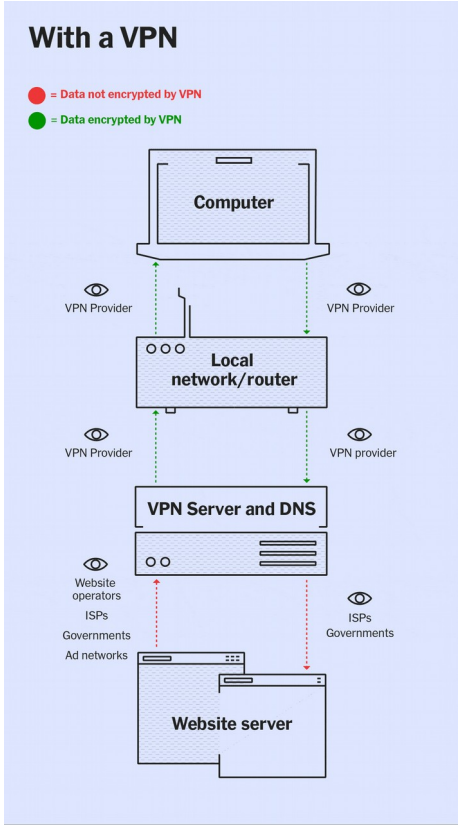
- Jurisdiction
- Logging (traffic, DNS requests)
- Payment methods & pricing
- Security and availability
- Configuration options

https://thatoneprivacysite.net https://www.privacytools.io/providers/vpn/

OFF-CHAIN ATTACK

>JUST ANOTHER ISP





https://thewirecutter.com/reviews/best-vpn-service/

September 4th – Berlin

https://www.meetup.com/ActivationDNL/events/263771516/

>MOBILE PHONES SUCK

Security Advisory: Mobile Phones

1. Phone numbers are horrible identifiers
2. The default security of your telco account is awful
3. Separate your phone number from security functions
   - Instructions for setting up 2FA alternatives
   - Instructions for setting up Google Fi (aka Bad Customer Support as a Feature)

"There is no 100% sure way to prevent the theft of your phone number."

Also see: "Insecurities and Misconceptions on Privacy-Enhancing Tools"

>MOBILE PHONES SUCK

What About Accounts That Require Verification by Phone?

SMS Privacy, **Number Proxy**

Purchase (with bitcoin!) temporary virtual or physical numbers to send / receive calls and texts

>KYC REQUIREMENTS

Most fiat-to-crypto exchanges are custodial and generally require:

- Full name & date of birth
- Email & phone number
- Home address (city, state, country)
- State-issued identification card
- Debit/credit card & bank account
- A selfie

OFF-CHAIN ATTACK

>KYC REQUIREMENTS

We collect the following types of information:

- **Personal Identification Information:** Full name, date of birth, age, nationality, gender, signature, utility bills, photographs, phone number, home address, and/or email.
- **Formal Identification Information:** Tax ID number, passport number, driver's license details, national identity card details, photograph identification cards, and/or visa information.
- **Financial Information:** Bank account information, payment card primary account number (PAN), transaction history, trading data, and/or tax identification.
- **Transaction Information:** Information about the transactions you make on our Services, such as the name of the recipient, your name, the amount, and/or timestamp.
- **Employment Information:** Office location, job title, and/or description of role.
- **Online Identifiers:** Geo location/tracking details, browser fingerprint, OS, browser name and version, and/or personal IP addresses.
- **Usage Data:** Survey responses, information provided to our support team, public social networking posts, authentication data, security questions, user ID, click-stream data and other data collected via cookies and similar technologies. Please read our Cookie Policy for more information.

OFF-CHAIN ATTACK

>PII COLLECTION

Menu Search **Bloomberg** Sign In **Subscribe**

Cryptocurrencies

Criminal Past Haunts Surviving Founder of Troubled Crypto Exchange

By Doug Alexander and Matt Robinson

Dhanani's name change certificate *Photographer: British Columbia's Vital Statistics Agency*

In the U.S., Dhanani had been charged with numerous crimes. He pleaded guilty to conspiracy to commit credit-and-bank card fraud at the age of 22 in 2005, according to a statement from the U.S. Justice Department. Dhanani helped operate shadowcrew.com, a now defunct marketplace for trafficking stolen credit and bank card numbers. Dhanani also admitted guilt in 2007 to separate criminal cases for burglary, grand larceny and computer fraud, according to California state court records.

>PEER-TO-PEER EXCHANGE

https://hodlhodl.com

EXCHANGES

- Minimal PII collection; identity verification is optional unless resolving a dispute
- Non-custodial; multi-signature escrow
- “We operate in every country”... unless you are a U.S. resident or citizen (legally)

https://bisq.network

- No PII collection; can be shared peer-to-peer with trading partners if necessary
- Decentralized; multi-sig escrow & cash trades
- Works in every country, no matter your residence or citizenship

OFF-CHAIN ATTACK

>PII COLLECTION

U.S., DENVER AREA:

coinstar
digital mint
COINFLIP
BITCOIN DEPOT

EUROPE:

VÄRDEX SUISSE
BITY
bitc
SatoshiPoint
shitcoins.club

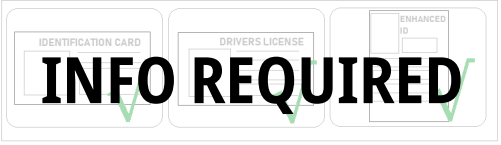
FUNCTION

1) "ATMs" (Vending Machines, Teller)

One-way, only buy with cash, sometimes card

2) ATMs

Two-way, buy & sell with cash, sometimes card



1) Full KYC (state-issued photo ID, address, etc.)

2) KYC-Lite (name, phone number or email)

3) No KYC (only a bitcoin address)

Requirements will vary based on amount and jurisdiction.

SOLUTIONS

Find a meetup group –
someone can help you peer-to-peer!

>NOT YOUR KEYS...

When choosing a wallet, consider:

- Who will hold the **private keys** to your coins?
- Who will give the balance for **addresses**?
- Who will broadcast your **transactions**?

Ideally, for *maximum* privacy, the answer to all of these questions should be:

You and your full node.

OFF-CHAIN ATTACK

>NOT YOUR KEYS...

Reasons to use our own node:

Trustlessness

Security

Privacy

"All other lightweight wallets leak information about which addresses are yours because they must query third-party servers."

- Chris Belcher (@chris_belcher_)

https://en.bitcoin.it/wiki/Clearing_Up_Misconceptions_About_Full_Nodes

>FULL NODE

Non-custodial mobile and desktop wallets that allow connecting to your own node:

- Green Address
- Electrum & Electrum Personal Server
  - Compatible with hardware wallets like Trezor, Coldcard, Ledger, KeepKey, etc.
- Wasabi (also HW compatible)
- JoinMarket (node required) **ADVANCED!**
- NEW: Samourai Wallet with the Dojo

pairing guide, installation guide for Rasp Pi 4, or relying on existing node

Blockchain Analysis vs. Surveillance

The difference is: intent, consent, and transparency.

Blockchain analysis is “the process of inspecting, identifying, clustering, modeling and visually representing data” on the blockchain. Ex. Block explorers, academic research

Blockchain surveillance performs analysis with the intent to deanonymize for intelligence or law enforcement purposes (without warrants), aggregating PII data that was often not provided through consent from users; the tools are not transparent and the results are rarely publicly available.

>OWNERSHIP HEURISTIC

Goals of Blockchain Surveillance:

1. Create clusters of UTXOs, addresses, and wallets that *probably* belong to the same entity based on linked transaction history and spending patterns
2. Tie those clusters to real-world identities or organizations and track the movement of bitcoin across the ecosystem
3. Identify the nature of those movements (i.e. why is it moving?)

>OWNERSHIP HEURISTIC

Transaction Patterns

- Common input / co-spending: “All inputs to a transaction belong to the same person.”
- Consumer heuristic: “Consumer wallets usually produce transactions with two or few outputs.”
- Rounded numbers: “Payment amounts are usually nice round numbers, while leftovers (change) are non-rounded amounts.”

>COIN MANAGEMENT

What is the solution?

- **Better:** Wallets with coin selection features, i.e. the ability to manage not just accounts or addresses, but your UTXO pool

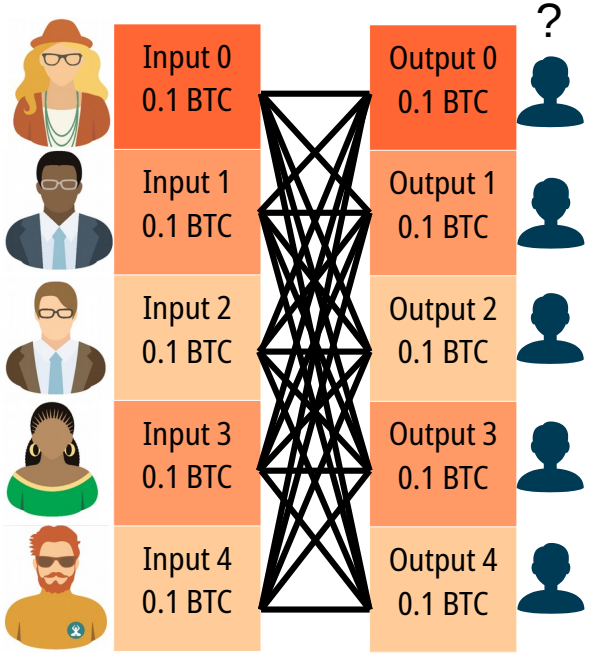
- **Best:** Wallets with coin selection algorithms, e.g. one that will perform analysis on your UTXO pool and proactively warn you about spending choices that could damage your privacy

Pop Quiz!

What kind of transaction is this?

9a53907e6e4800ae4fb3469ddbf9f935
03f876677d81573b350cf77641d5abf3

>COINJOIN



Breaking the Heuristic

- Outlined by Greg Maxwell in August 2013
- Multiple people cooperate to create and sign a single transaction which spends all of their inputs together
- "If these transactions become widespread they improve the privacy even of people who do not use them, because ***no longer will input co-joining be strong evidence of common control***."

>COINJOIN WALLETS

- Round-based mixing model; centralized coordinator with blind signatures
- CoinJoins are set at 0.1 BTC (plus fee)
- Higher anon set, but takes time (+100 now)
- 'bc1' addresses (BIP-84 bech32 native SegWit)

JoinMarket

see: Adam Gibson's presentation for 'Understanding Bitcoin' event

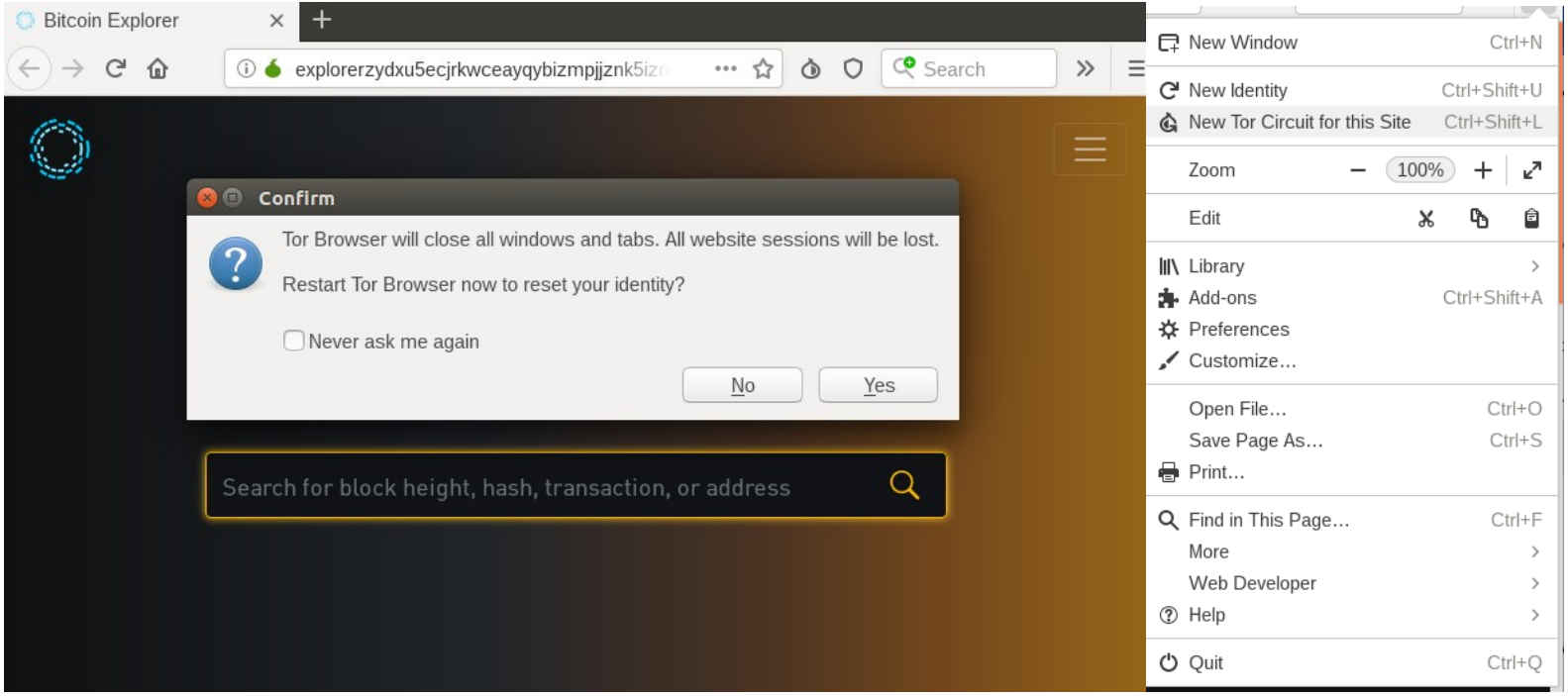
ADVANCED!

requires running Bitcoin Core as backend

- Maker / Taker mixing model; as a maker, you can earn passive income from fees
- CoinJoins can be a variety of amounts (usually between 0.01 to 30 BTC)
- Lower practical limit for anon set, but fast
- '3' addresses (BIP-49 backwards-compatible SegWit)

OFF-CHAIN ATTACK

>THIRD PARTY SITES



1. If not your own node, use block explorers that allow you to connect over Tor.
2. Change your 'Tor Circuit' often (per address or tx query, even)
3. Change your 'Identity' after using a block explorer to refresh session

CONCLUSION

>MISSION COMPLETE

- Bob buys new devices with cash.
- Bob sets up the minimal operating system features and software needed (Tor browser, VPN, non-custodial wallet software, etc.)
- Bob goes to a meetup and buys bitcoin from an attendee willing to help him acquire his first coins.
- Bob moves the coins a few times and then mixes them using a wallet with CoinJoin support, so that even the meetup attendee who helped him can't follow where they go.

CONCLUSION

>MISSION COMPLETE

- Bob uses the bitcoin to buy an encrypted email account (ex. ProtonMail, StartMail) and a VPS service (ex. Njalla). He uses the rest to donate to other privacy-preserving services / software that he may need to use (ex. The Tor Project), and guides that helped him along the way (ex. PrivacyTools).

Warning: This theoretical scenario does not suffice as technical or legal advice for whistleblowers, particularly those who face nation-state level adversaries. *Please seek out journalists, information security and legal professionals who specialize in whistleblower protection for individualized guidance!*

Inspired by a True Story:

Edward Snowden, NSA Whistleblower

Blockstack Berlin 2018

- “When I was working on the greatest project of my life back in 2013, trying to figure out things like 'how could I get this archive of material to journalists?’ ...There's the question of 'do I need server infrastructure of my own?' Maybe the answer is: yes. ‘Okay, how do I pay for that anonymously?’ Maybe someone like me used bitcoin for something like that!”

Bitcoin 2019 – San Francisco

- “While I won’t say whether I have bitcoin or anything else... The servers that I used to transfer this information to journalists – because I didn’t want these records connected to my name, when I understood how this system of mass surveillance worked – they were paid for using bitcoin.”

- **Alice**

the Kid

Hello, my name is Alice!
I am 12 years old.
My dad's name is Bob.
I have been programming since
I was 6 years old.

This summer, I want to earn money from bug bounties, and buy things online.

Dad says I can't open a bank account until I am 16. :(

Project Ideas
- Lightning powered candy machine
- Anti-Mallory device

I wonder if I could pay your allowance in bitcoin...
-Dad

ON-CHAIN ATTACK

>AMOUNT CORRELATION

Hmm, what if someone tries to find my reward?

Thanks!

kraken

Thanks for participating in our **Bug Bounty** program! Here is 100 USD in bitcoin.

Woo! Just got $100 in bitcoin for my first bug report!

Tweeted: 8:23 PM · Aug 22, 2019

> Exchange rate bitcoin
> Block explorer
Loading...

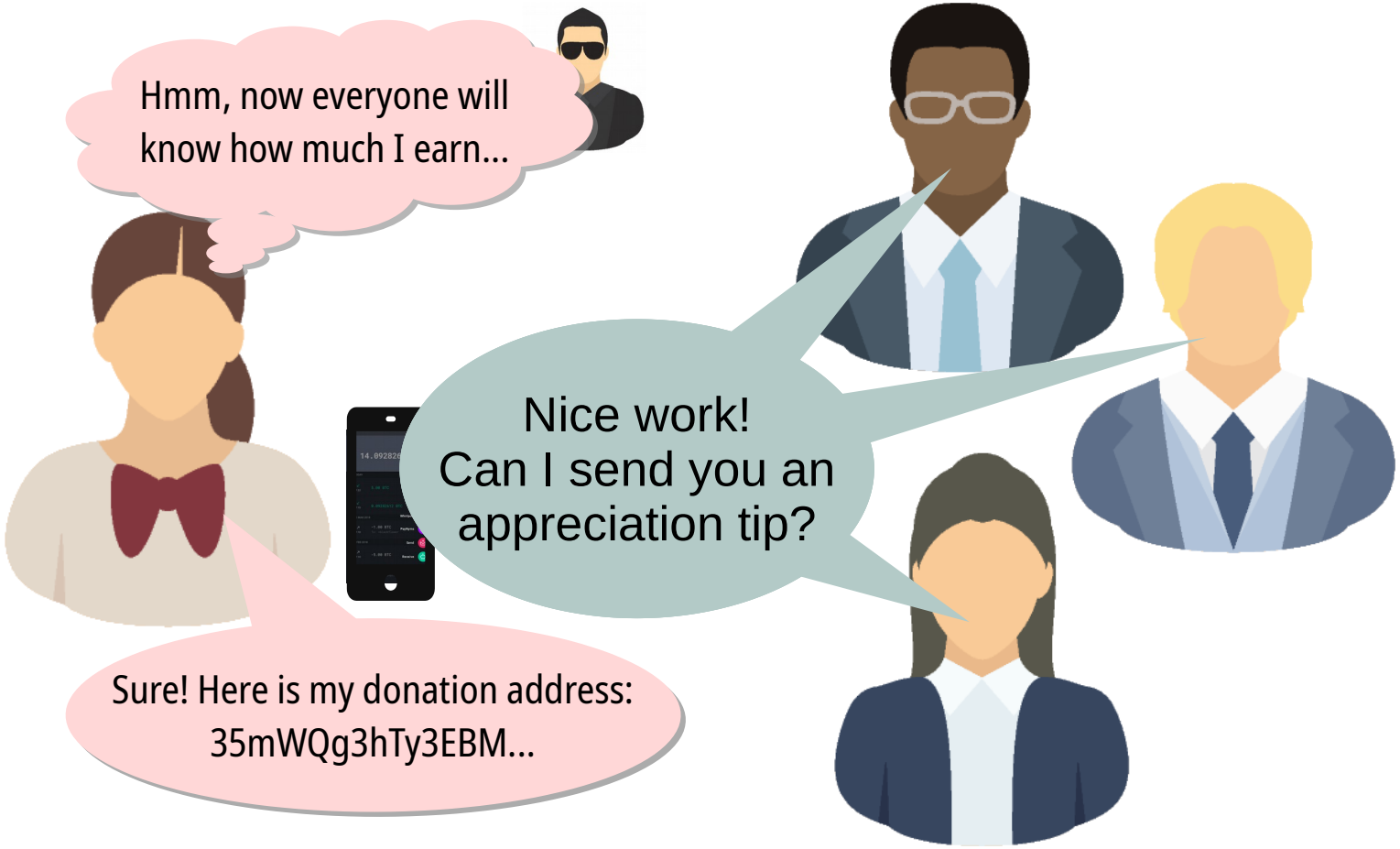
SOLUTIONS

>COINS UNCHAINED

- Small, disposable, USB hardware wallets that can be used ‘like cash’
- Stores private key; must be unsealed to then spend on the blockchain

ON-CHAIN ATTACK

>ADDRESS REUSE



>PAYNYMS

+pinkcloud238

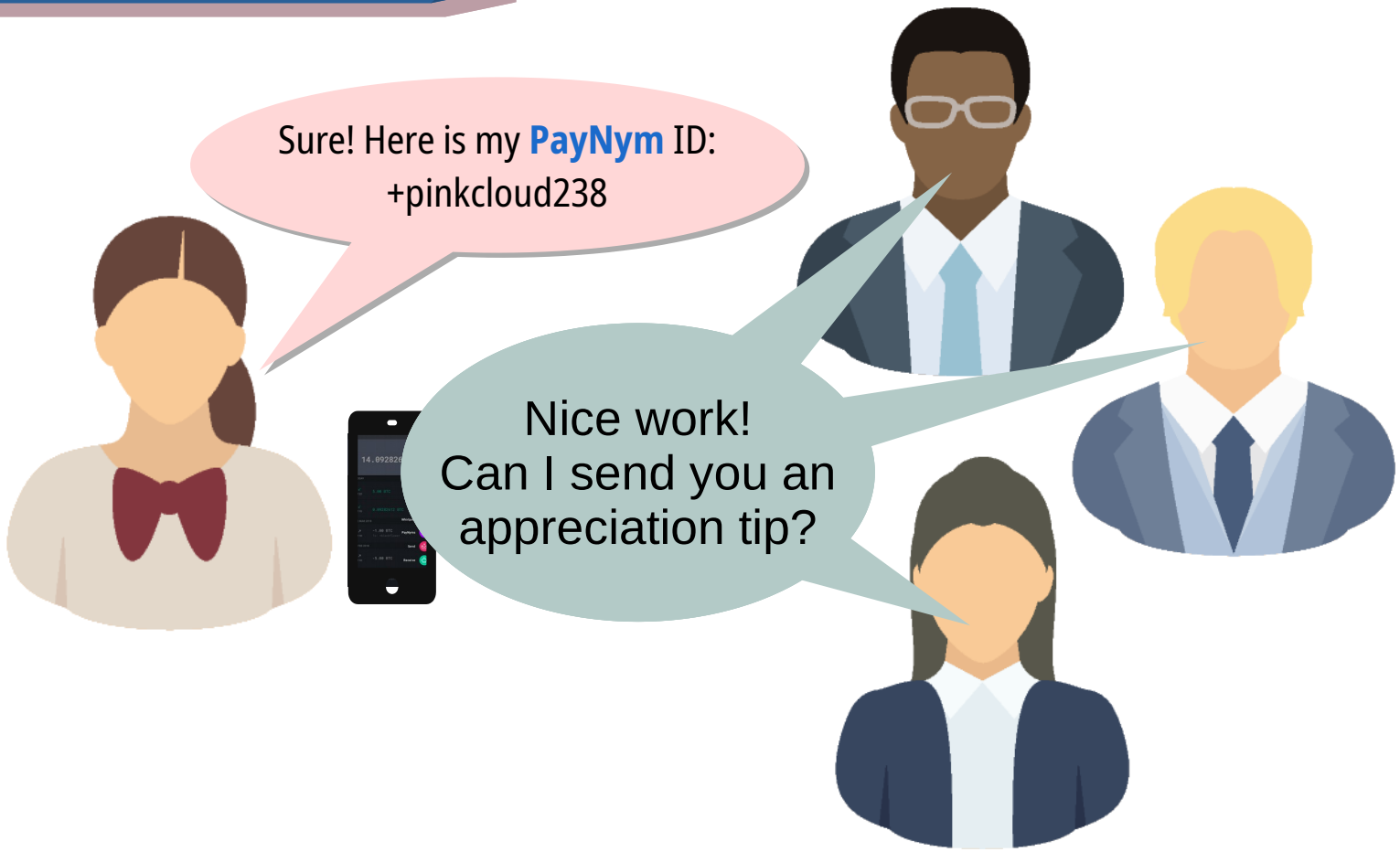
BIP-47 Reusable Payment Codes

- Allow for **publicly advertised identities** that easily generate and share new bitcoin addresses with each sender; *only sender and receiver can link their payments together*
- Utilizes the HD wallet feature of generating child keys from the extended public key
- After shared secret is exchanged, someone could send “up to 2^{32}“ stealth transactions
- Currently only implemented by Samourai

Note: Requires backing up some metadata for full wallet recovery.

SOLUTIONS

>PAYNYMS



>LIGHTNING NETWORK

TOMORROW – August 29th
Join the Lightning Network
Beatrive Leung (Introductory)

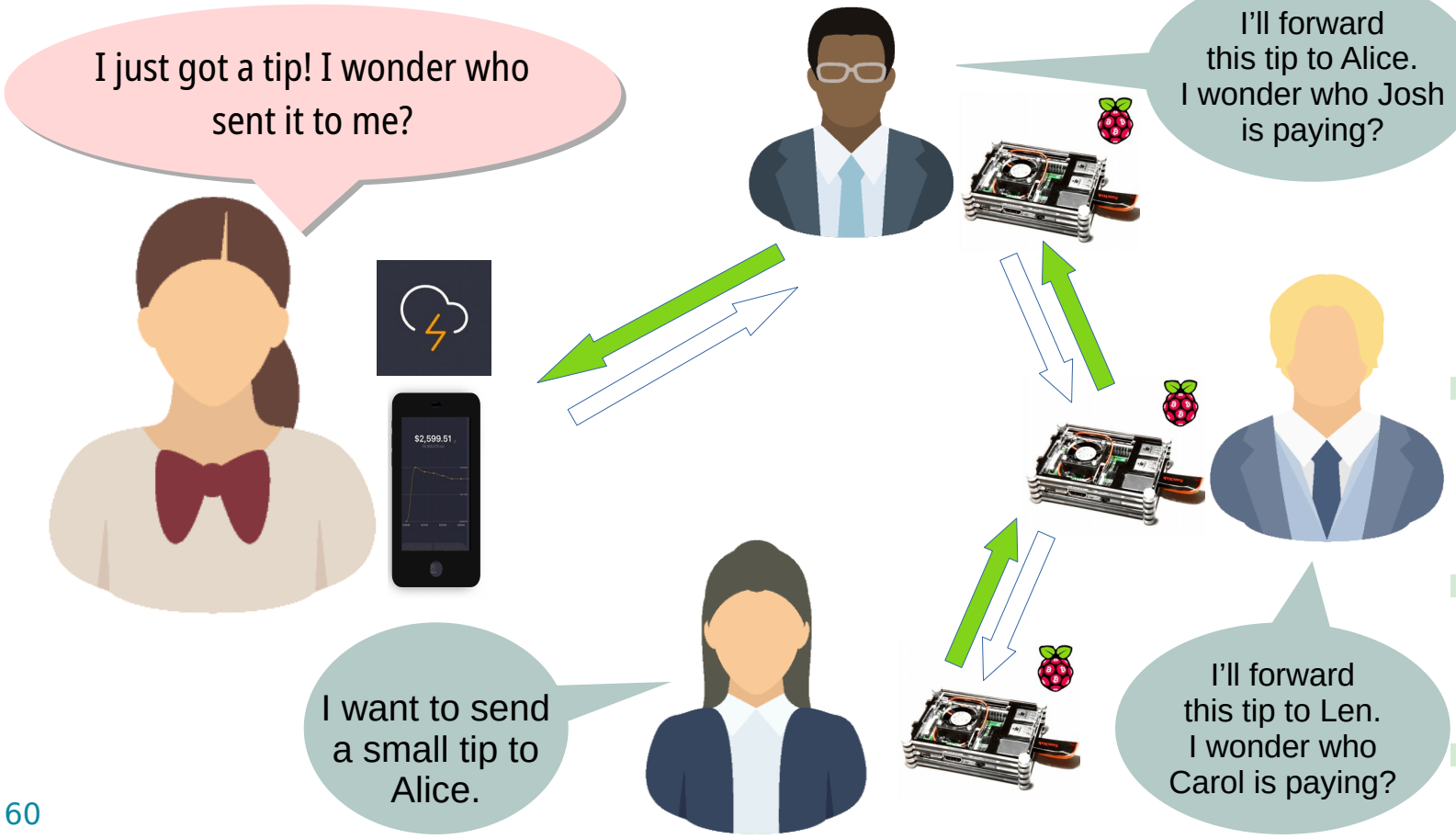
TOMORROW – August 29th
Onion Routing Bitcoin Payments
René Pickhardt (Technical)

FRIDAY – August 30th
Pathfinding, Autopilots and Topology Creation of the Lightning Network
René Pickhardt (Technical)

TOMORROW – August 29th
Bitcoin and Lightning for Commerce
Hannah Rosenberg (Professionals)

ON-CHAIN ATTACK

>ONION ROUTING

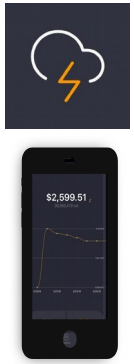


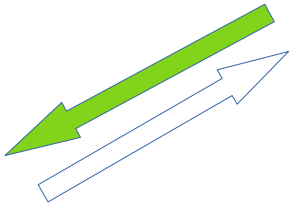
ON-CHAIN ATTACK

>ONION ROUTING

I just got a tip! I wonder who sent it to me?

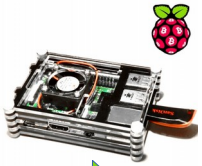
Node D





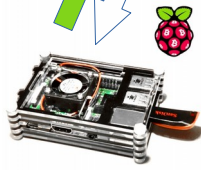
Node C

I'll forward this tip to Node D. I wonder who Node B is paying?



Node B

I'll forward this tip to Node C. I wonder who Node A is paying?

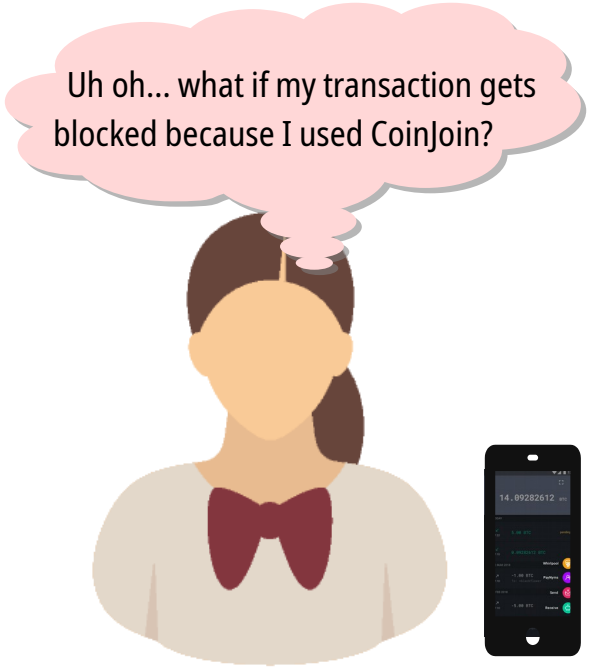


Node A

I want to send a small tip to Node D.

ON-CHAIN ATTACK

>BLACKLISTING



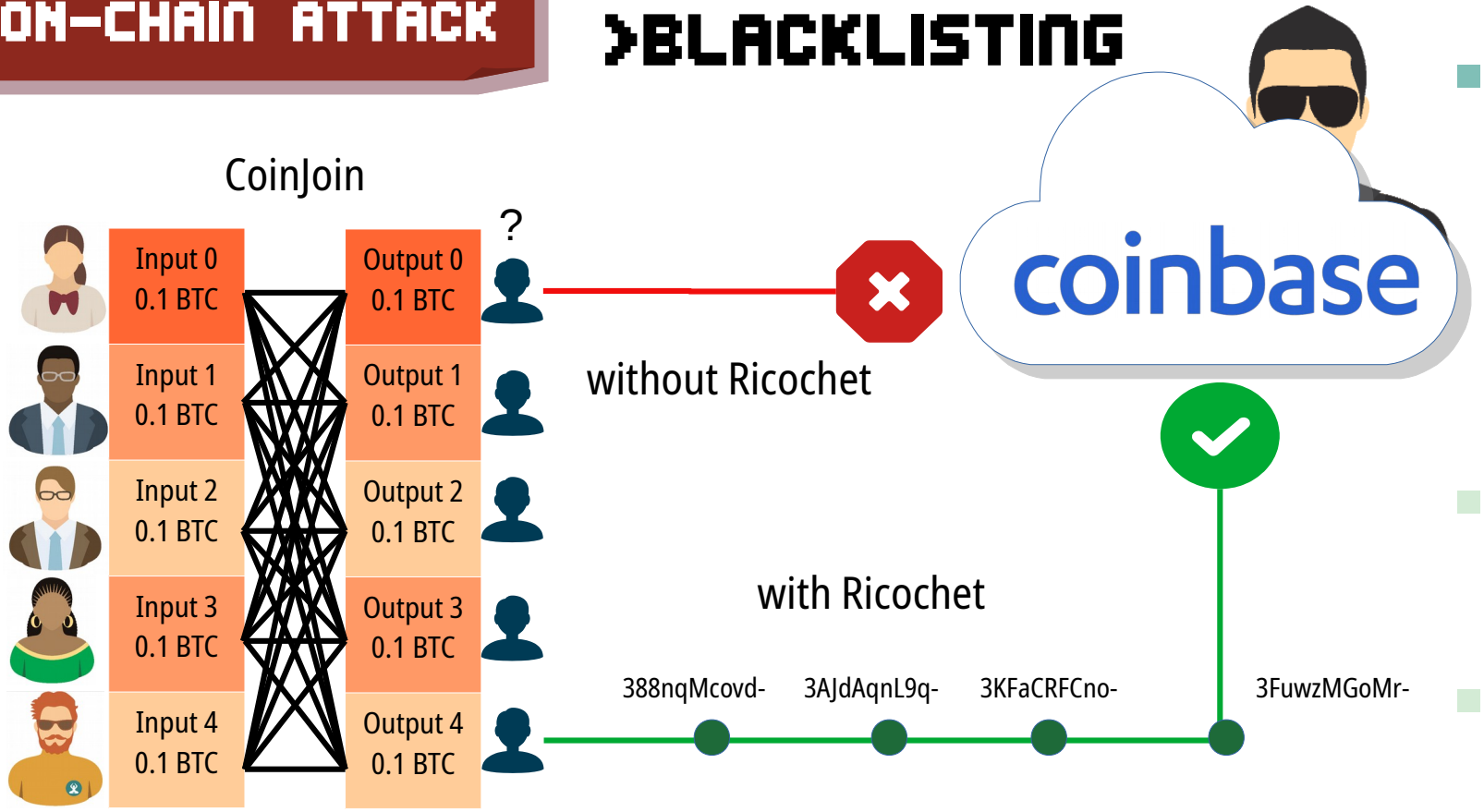
COINTELEGRAPH

Coinbase CEO Praises Privacy While Allegedly Blacklisting Anonymous Transactions

by Adrian Zmudzinski

ON-CHAIN ATTACK

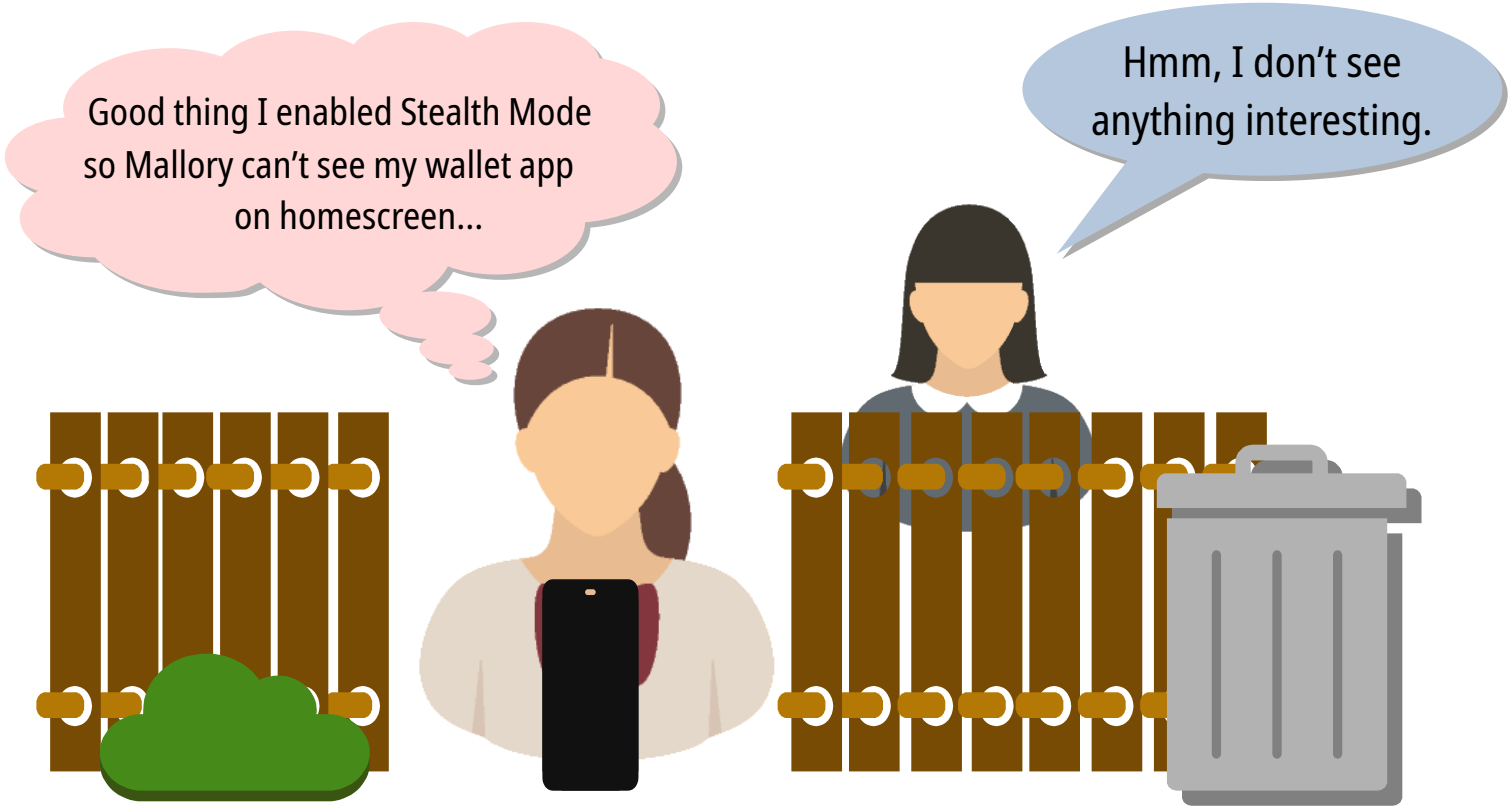
>BLACKLISTING



https://support.samourai.io/article/14-making-your-first-ricochet-send

OFF-CHAIN ATTACK

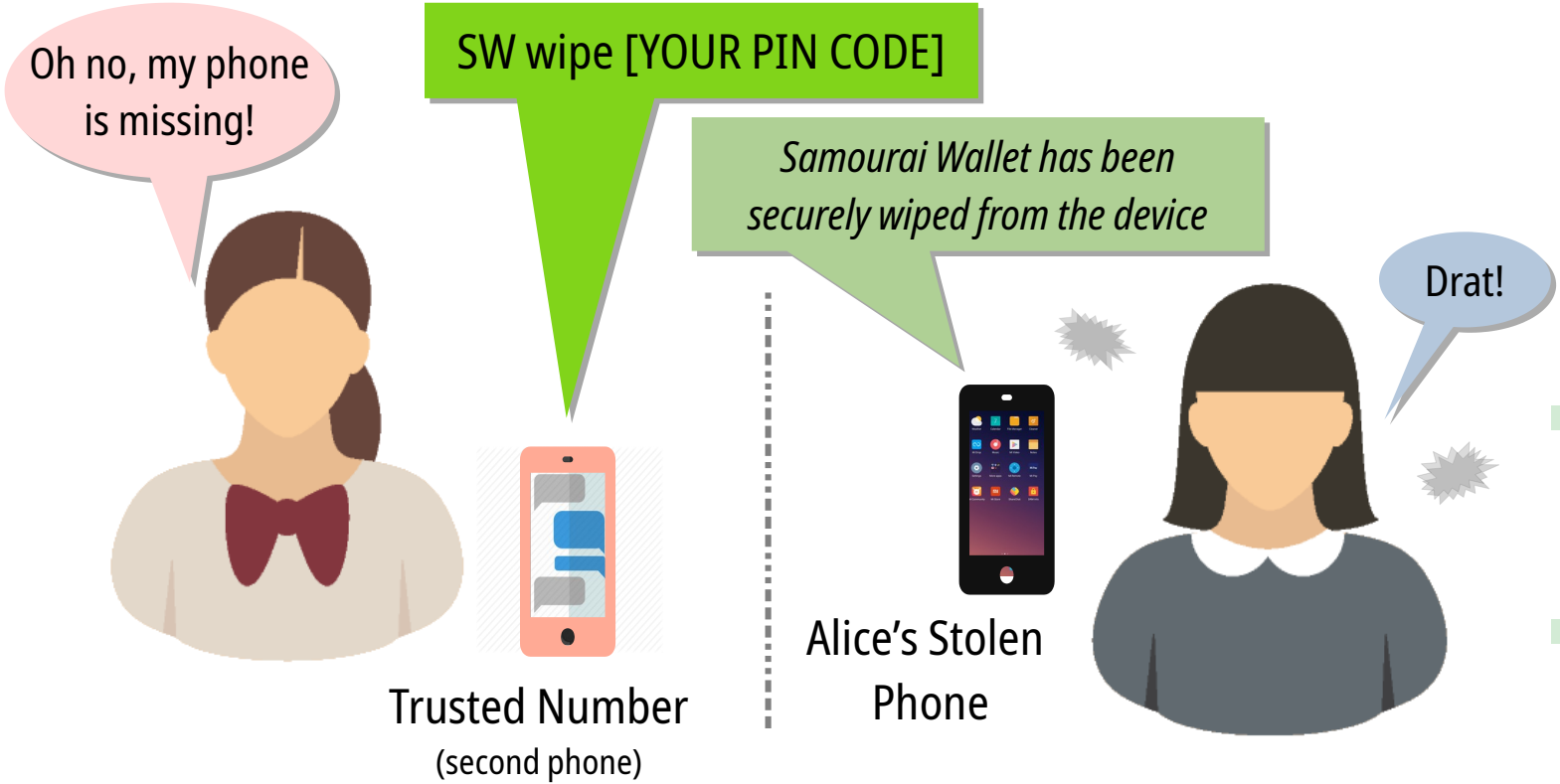
>SHOULDER SNOOPING



https://samourai.kayako.com/article/31-enable-stealth-mode-in-your-wallet

OFF-CHAIN ATTACK

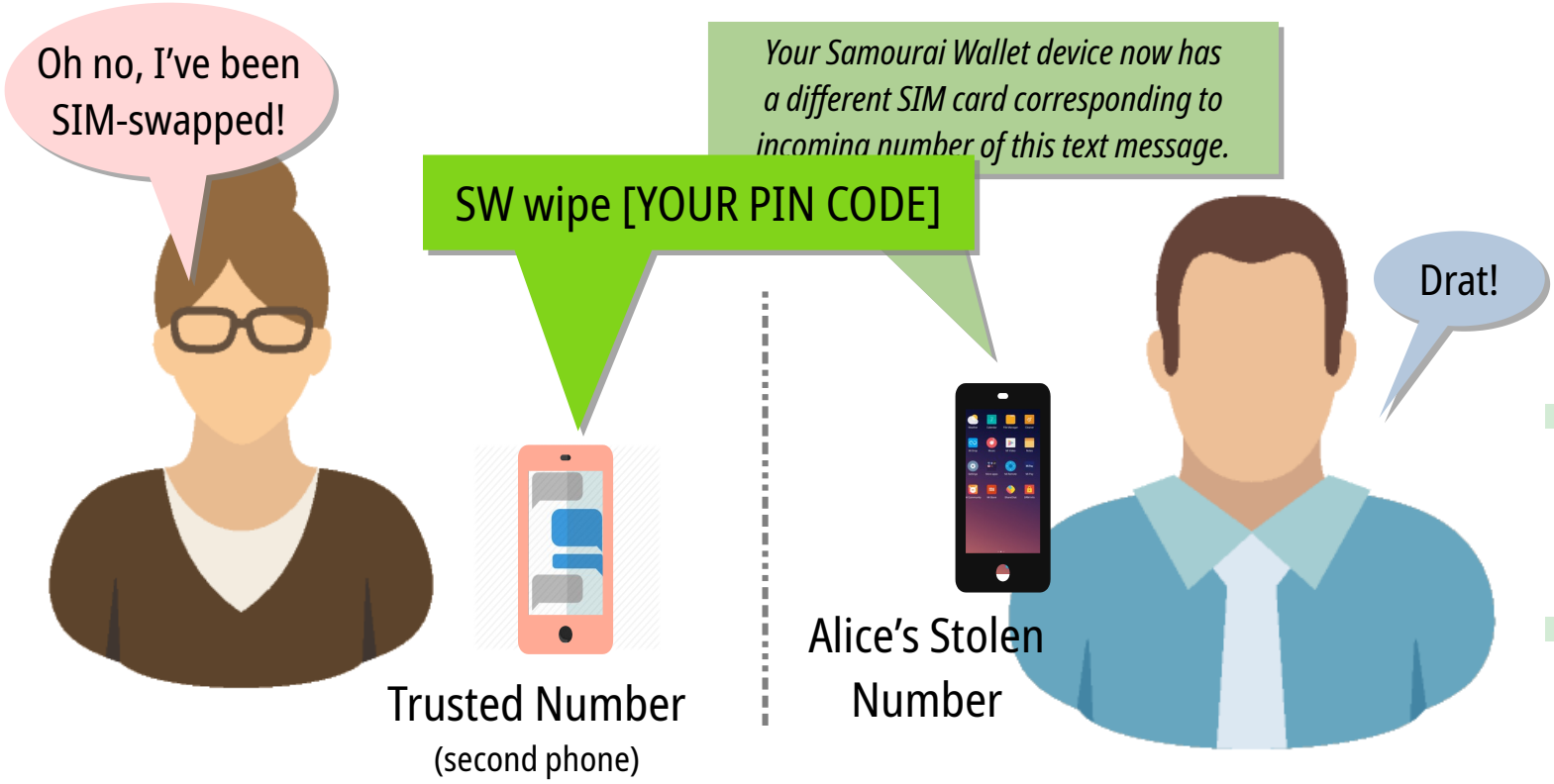
>STOLEN OR LOST



https://support.samourai.io/section/34-remote-sms-commands

OFF-CHAIN ATTACK

>SIM SWAP/SPOOF



https://support.samourai.io/article/34-enable-sim-switch-defense

OFF-CHAIN ATTACK

>SIM SWAP/SPOOF

Samourai Wallet

Jan 07
2019

Temporarily disabling Stealth Mode, Remote SMS, and SIM Switch Defense features due to restrictive Google Play Store policies.

It is with great sadness that we are disabling the following features within Samourai Wallet as of version 0.99.04 - which will be released tomorrow - due to new extremely restrictive policies Google has decided to introduce in their effort to become more of a “walled garden” experience:

- Stealth Mode
- SIM Switch Defense
- Remote SMS Commands

OFF-CHAIN ATTACK

>PHONES REALLY SUCK

Motherboard

T-Mobile 'Put My Life in Danger' Says Woman Stalked With Black Market Location Data

Telecom giants are giving up customers' real-time location data to stalkers and bounty hunters. Now, Motherboard speaks to a victim.

How to lose $8k worth of bitcoin in 15 minutes with Verizon and Coinbase.com

Cody Brown Follow
May 31, 2017 · 9 min read ★

Cryptocurrency Thief Gets 10 Years in Prison

For release on April 22, 2019

OPINION

Spyware and GPS tracking: the next frontier for family violence

Jenna Price
Columnist and academic at the University of Technology Sydney


Pinned Tweet
belcher
@chris_belcher_
For the last few weeks I've been working on a literature review for bitcoin privacy: en.bitcoin.it/wiki/Privacy It aims to cover about all privacy issues in bitcoin, including Lightning network, and has a bunch of examples to help demonstrate how the concepts work in practice.
9:17 PM · Feb 23, 2019 · Twitter Web Client

Future Upgrades

Dandelion routing (BIP156)

Schnorr signatures (Draft BIP)

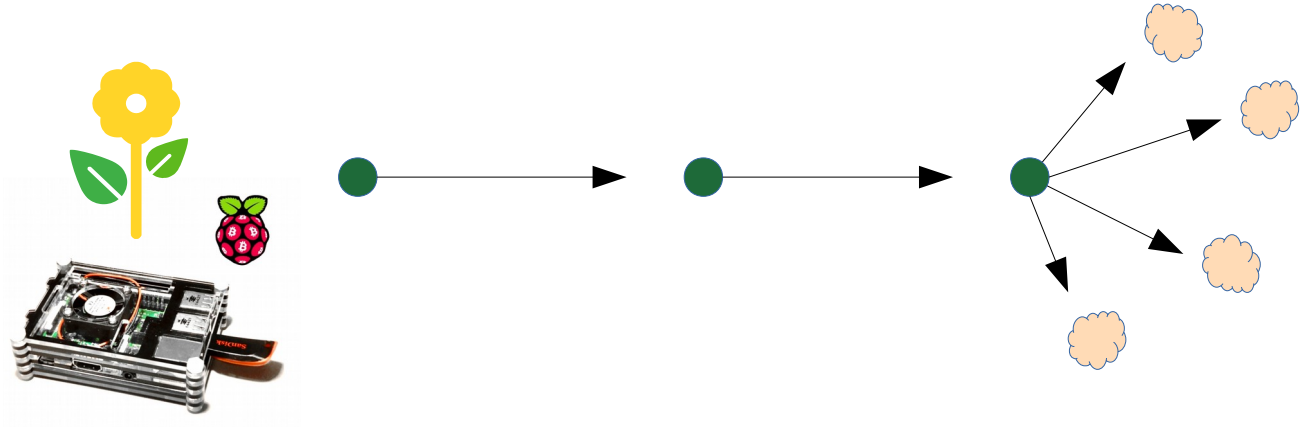
Taproot (Draft BIP)

Confidential transactions

>DANDELION ROUTING

Bitcoin Improvement Proposal (BIP)

"Dandelion enhances user privacy by **sending transactions through an anonymity phase** before diffusing them throughout the network."



>TAPROOT

Draft Bitcoin Improvement Proposal (BIP)

Adds smart contract-like capabilities to Bitcoin where complex spending conditions are selectively revealed, hiding the fact that alternative spending paths exist, and are virtually indistiguishable from standard on-chain transactions.

See: “On-Chain Defense in Depth” by Bob McElrath

>SCHNORR SIGNATURES

Draft Bitcoin Improvement Proposal (BIP)

"Schnorr signatures admit a very simple **blind signature construction** which is a signature that a signer produces at the behest of another party without learning what he has signed. These can for example be used in Partially Blind Atomic Swaps, a construction to enable transferring of coins, mediated by an untrusted escrow agent, without connecting the transactors in the public blockchain transaction graph."

Aaron Van Wirdum

Aaron van Wirdum is interested in technology and how it affects social and political structures. He has been covering Bitcoin since 2013, focusing on privacy, scalability and more. Hodls BTC.

September 6, 2018

PRIVACY & SECURITY

Battle of the Privacycoins: Why Dash Is Not Really That Private

Bitcoin News › Articles › Battle of the Privacycoins: Why Dash Is Not Really That Private

Aaron Van Wirdum

Aaron van Wirdum is interested in technology and how it affects social and political structures. He has been covering Bitcoin since 2013, focusing on privacy, scalability and more. Hodls BTC.

September 18, 2018

PRIVACY & SECURITY

Battle of the Privacycoins: Verge Offers Little Privacy and Nothing Unique

Bitcoin News › Articles › Battle of the Privacycoins: Verge Offers Little Privacy and Nothing Unique

Aaron Van Wirdum

Aaron van Wirdum is interested in technology and how it affects social and political structures. He has been covering Bitcoin since 2013, focusing on privacy, scalability and more. Hodls BTC.

September 25, 2018

PRIVACY & SECURITY

Battle of the Privacycoins: Zcash Is Groundbreaking (If You Trust It)

Bitcoin News › Articles › Battle of the Privacycoins: Zcash Is Groundbreaking (If You Trust It)

شتر دیدی؟ ندیدی
@arbedout

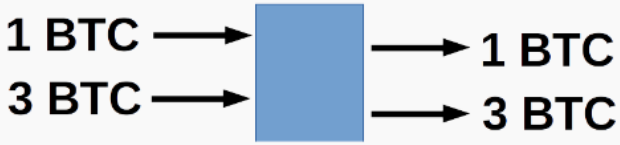
From the SEC's complaint against Veritaseum.

🎶🎶 I always I feel like 🎶🎶 somebody's waaaatching meeeee 🎶🎶 and I have no privacy 🎶🎶

10. On July 30, 2019, the day Commission staff informed Defendants' counsel that the staff was likely to recommend that the Commission approve the filing of an enforcement action against Defendants, and on July 31, 2019, Defendants moved more than $2 million in remaining Offering proceeds from a blockchain address they controlled into other addresses, and used a portion of those funds to purchase more precious metals.

5:25 PM · Aug 13, 2019 · Twitter Web App

Who owns it?



A Alice pays Bob 1 coin with 4 coins, Alice gets 3 change

B "CoinJoin" - Alice pays Alice 1, Bob pays Bob 3

C Alice pays Bob 2 (!) - Alice pays 3, gets 1, Bob pays 1, gets 3

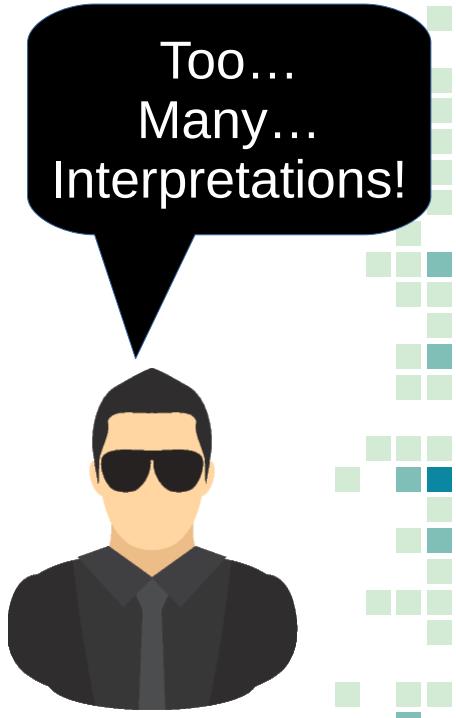
D Alice pays Bob 4 coins (in 2 outputs for some reason)

E Fake payment/Coinjoin - Alice owns everything

F Alice pays Bob 3 coins and Carol 1 coin

G Alice pays 3, Bob pays 1, Carol receives 3, David receives 1

H Alice and Bob pay Carol 4 coins

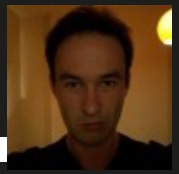


Adam Gibson, "CoinJoinXT" for *Building on Bitcoin 2018*

Boltzmann Analysis

Boltzmann is a python script computing a set of metrics for a Bitcoin transaction :

* entropy of the transaction : a metrics measuring how many possible mappings of inputs to outputs are possible given the values,
* link probability between an input and an output : the probability that an input has sent some funds to an output,
* linkability matrix of the transaction : a matrix storing the link probabilities between inputs and outputs of the transaction



LAURENT
@LaurentMT
Developer of OXT

KRISTOV
@kristovatlas
Engineer, OPP

TDEVD
@SamouraiDev
Samourai wallet dev

KYCP

Bitcoin TXID or TX-OUT...

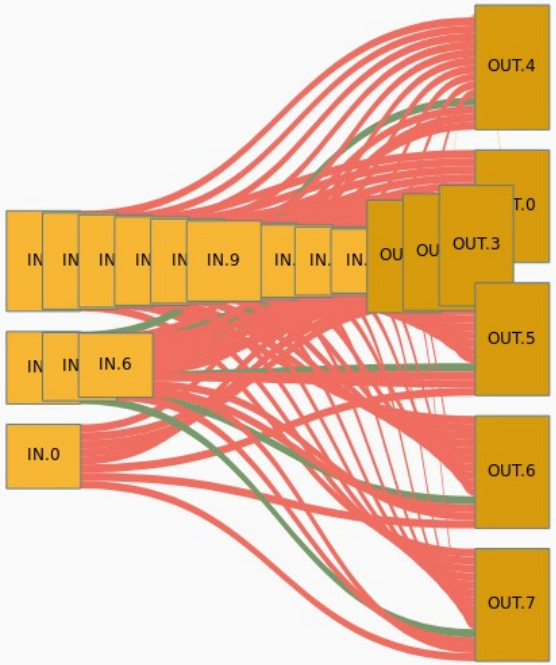
Ready

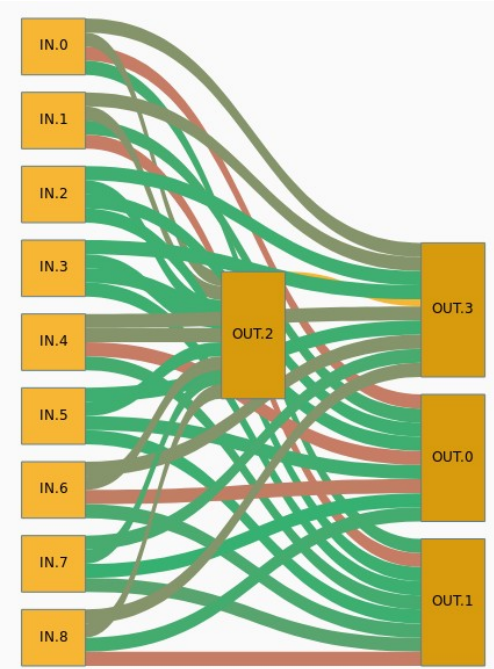
Browsing personal transactions? use **Tor/VPN** and **switch identity** frequently for your privacy.

Know Your Coin Privacy

14 inputs from ANON_483767160

	P2PKH	<	6.54829324 ฿	0
bd486...d18	P2PKH	<	0.0012839 ฿	1
bd486...d18	P2PKH	<	0.00114098 ฿	2
bf824...604	P2PKH	<	0.00113122 ฿	3
bd486...d18	P2PKH	<	0.00112836 ฿	4
bf824...604	P2PKH	<	0.00111714 ฿	5
bf824...604	P2PKH	<	0.00111647 ฿	6
bd486...d18	P2PKH	<	0.00111489 ฿	7
bd486...d18	P2PKH	<	0.00108984 ฿	8
bd486...d18	P2PKH	<	0.00108616 ฿	9
bd486...d18	P2PKH	<	0.00107342 ฿	10
bd486...d18	P2PKH	<	0.00106755 ฿	11
bd486...d18	P2PKH	<	0.00106512 ฿	12
bd486...d18	P2PKH	<	0.00106471 ฿	13





ADAM FISCOR

@nopara73

Co-Founder, CTO

zkSNACKs
Unfairly private

REPORTS FROM CHAINALYSIS WEBINARS

- **Ep. #179:** Ransomware Attacks
- **Ep. #184:** Darknet Market Report
- **Ep. #187:** Cryptocurrency Topologies – Who's Who on the Blockchain?

On analyzing mixing services: "We can identify funds going into mixing services... For the most part, it is not generally traceable [going out]."

On the illicit nature of mixed coins: "A lot of people are just using mixers for personal privacy."

CHAINALYSIS EMPLOYEE HOLDS AMA

ADAM FISCOR

@nopara73

Co-Founder, CTO

zkSNACKs
Unfairly private

- **Thoughts on Wasabi and Samourai**
  "[They] destroy the need for our / their software. It can make the software completely irrelevant."
  "Wasabi is enemy number one [for Chainalysis]."
- **Who are their main clients?**
  "American exchanges and governments."
  "Bigger the exchange, bigger the check."
  "CIA (through In-Q-Tel)"
- **General attitude of fellow colleagues?**
  "Self righteous." "[The company hasn't] displayed any sort of concern over the ethics of our software except for one person... He left."

Blockchain Surveillance Companies

Name	CEO	Funding	Clients
Chainalysis https://www.chainalysis.com/	Michael Gronager	Benchmark, Accel, Mitsubishi UFJ Financial Group (MUFG), Sozo Ventures, Point Nine, Digital Currency Group, TechStars, CVP Management, FundersClub	U.S. intelligence agencies, BitPay, Bitstamp, Binance, Korbit ("180+ customers across 40 countries")
Elliptic https://elliptic.co/	Dr. James Smith	SignalFire, NCSC Cyber Accelerator, Octopus Ventures, Digital Currency Group, Santander InnoVentures, Paladin Capital Group, Upscale, John Power, Seedcamp	U.S. intelligence agencies
Ciphertrace https://ciphertrace.com/	Dave Jevans	Aspect Ventures, WestWave Capital, NeoTribe Ventures, Galaxy Digital LP	U.S. intelligence agencies

rebekah
@rbkhmrcr

oh i was only looking at California's ICE contracts, turns out last year @chainalysis had another ~$1 million contract with ICE. guess we have even more motivation for stronger privacy in cryptocurrencies

3821	70CMSD18P00	$999,942	9/5/2018	2018	CHAINALYSIS, INC.	79827246	NEW YORK	NY
3822	70CMSD18P00	$7,997	5/30/2018	2018	CHAINALYSIS, INC.	79827246	NEW YORK	NY
3823	HSCEMD17P0(	$409,050	9/19/2017	2017	CHAINALYSIS, INC.	79827246	PALO ALTO	CA
3824	HSCEMD17P0(	$29,940	9/6/2017	2017	CHAINALYSIS, INC.	79827246	PALO ALTO	CA
3825	HSCETE17P00	$29,940	6/16/2017	2017	CHAINALYSIS, INC.	79827246	PALO ALTO	CA
3826	HSCETE17P00	$0	5/1/2017	2017	CHAINALYSIS, INC.	79827246	PALO ALTO	CA
3827	HSCETE17P00	$12,089	1/18/2017	2017	CHAINALYSIS, INC.	79827246	PALO ALTO	CA
3828	HSCETE17P00	$29,940	12/8/2016	2016	CHAINALYSIS, INC.	79827246	PALO ALTO	CA
3829	HSCETC16P00	$3,297	9/12/2016	2016	CHAINALYSIS, INC.	79827246	PALO ALTO	CA

7:15 PM · Aug 26, 2019 · Twitter Web App

Blockchain Surveillance Companies

Name	CEO	Funding	Clients
Crystal Blockchain https://crystalblockchain.com/	**Marina Khaustova**	**Subsidiary of BitFury**	**U.S. government**
Neutrino https://www.neutrino.nu/	**Giancarlo Russo** ***Former Hacking Team COO*** **(?)**	**Acquired by Coinbase**	
BlockSeer https://www.blockseer.com/	**Dan Reitzik (DMG Blockchain Solutions)** **Danny Yang**	**Acquired by DMG Blockchain Solutions** **Plug and Play, Amasia, ZhenFund, Charlie Lee, Bobby Lee, Ceyuan Ventures, Bill Tai (BitFury)**	**U.S. government**

Coming soon:


THE ARCHIVE NETWORK
Archive
ARCHIVE NAME
Blockchain Surveillance Watch
PUBLIC ARCHIVE SUBDOMAIN
https://bswatch.thearchive.network
DESCRIPTION
Blockchain Surveillance Watch (BSWATCH) is a collection of documents relating to the operation, activities, and relationships of cryptocurrency and blockchain analytics companies around the world.

THANKS!

Any questions?

Credit: Presentation template by SlidesCarnival