Privacy Protocols
What are they and why should we care?

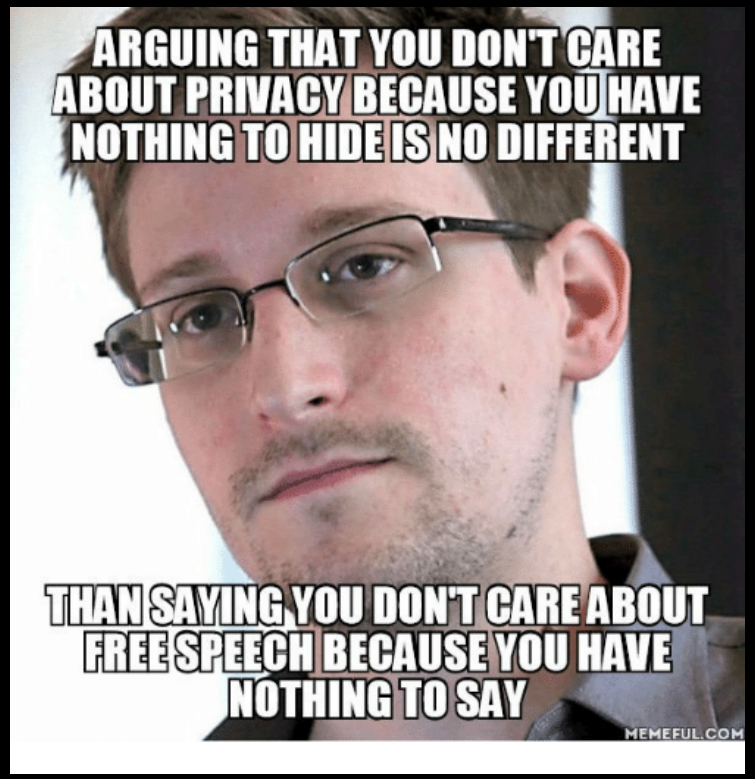
17 November 2018
BlockBali

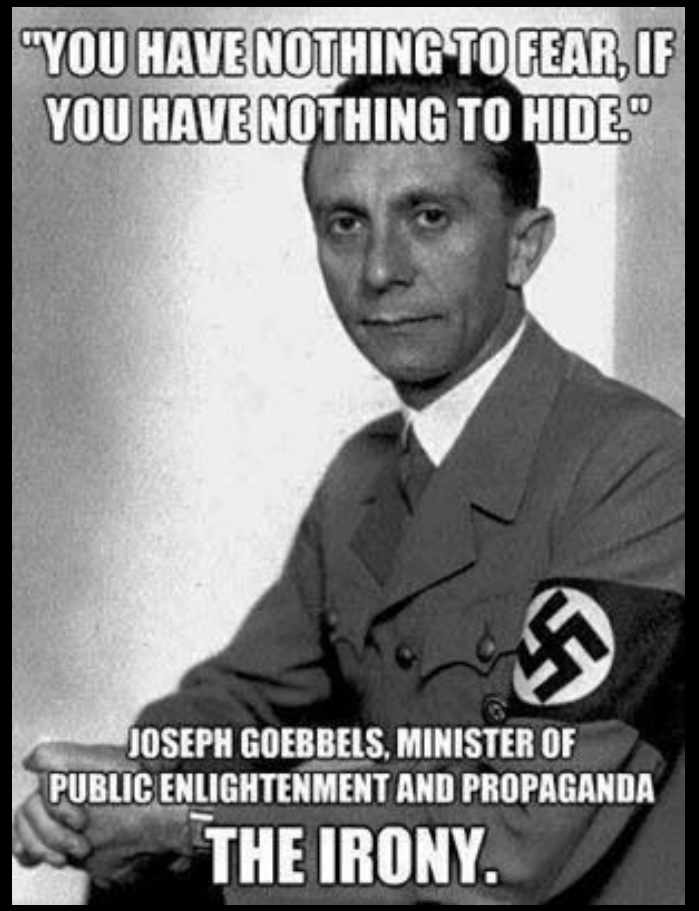
Reuben Yap
COO of Zcoin

Why do we need financial privacy?

- If I have nothing to hide, why should I care? If I have nothing to hide, I have nothing to fear
- Financial privacy is to hide illicit activity?

Privacy: Nothing to hide





"When you say, 'I have nothing to hide,' you're saying, 'I don't care about this right.' You're saying, 'I don't have this right, because I've got to the point where I have to justify it.' The way rights work is, **the government has to justify its intrusion into your rights.**"

Why do we need financial privacy?

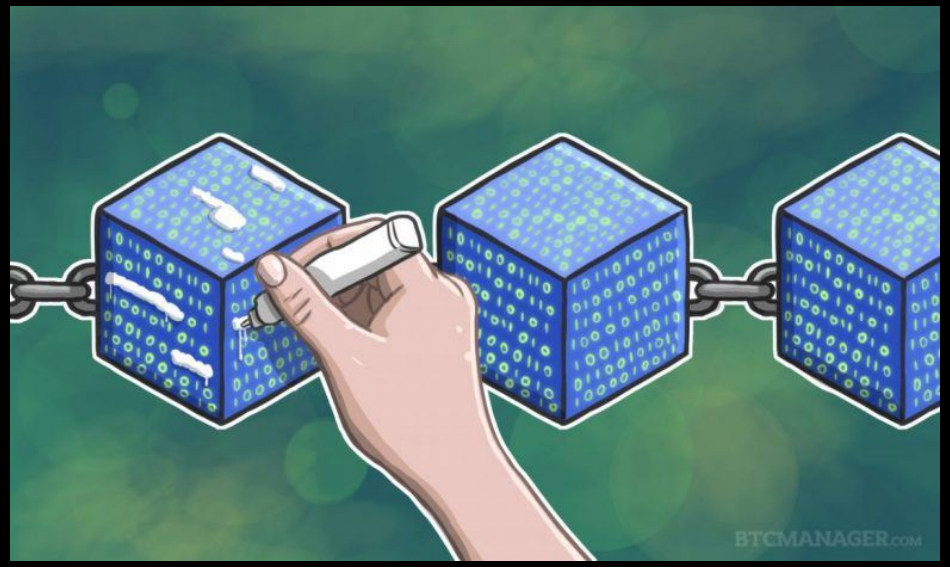
- Are you comfortable with anyone being able to look up your financial history and balances?
  - What you spent on
  - How much you have
  - Who you receive money from

- Banking has always provided some form of privacy or confidentiality. In the US with the Gramm-Leach-Biley Act and in Malaysia with BAFIA 1989 and now the Financial Services Act 2013 which prohibit banks from producing, divulging, revealing, publishing or disclosing any information pertaining to the affairs and conduct of customer accounts to another party.
- Business activity, contracts

Why do we need privacy on the blockchain?

What about privacy on the blockchain

- Unlike banking transactions and balances, all transactions on the blockchain are permanently stored and available for public view.
- The movement of every single coin can be traced to its origin and point of creation.
- But isn’t Bitcoin anonymous?



Privacy in Bitcoin

(and ETH, LTC, NEO…etc and yes XVG)

and why it isn’t enough

Privacy on Bitcoin and why it isn’t enough

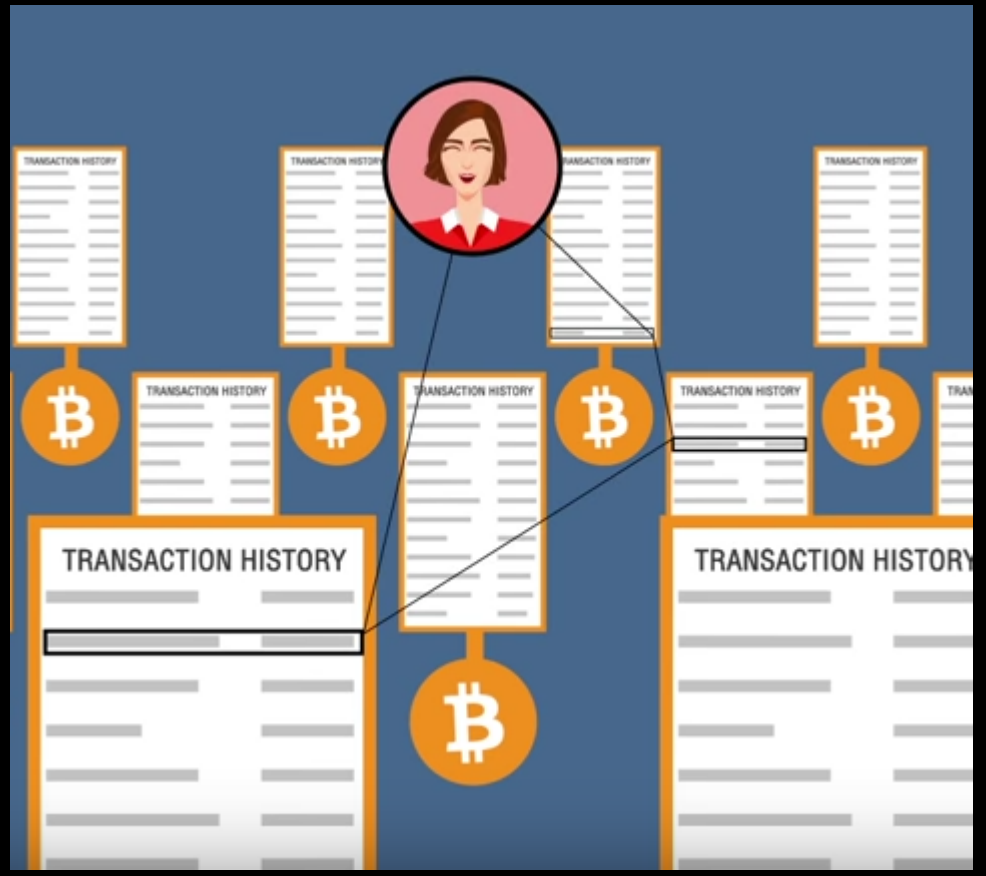
Pseudonymity

- You can see **what the person is doing** but you don’t know who it is.
- For example Superman is a pseudonym for Clark Kent. I know everything that Superman does, I just don’t know his real identity.
- Bitcoin addresses are the same.
- People can create a new Bitcoin address for every single transaction so it’s harder to discern behaviour from a single address.

Privacy on Bitcoin and why it isn't enough

Blockchain Analysis

- We are humans and we have predictable behaviours: for e.g. we make periodic repeat purchases or transact at certain times
- We transact with entities that know our identities: exchanges, vendors
- Outside information such as your internet IP address/social media can further narrow down.
- **All the time in the world** to analyse since the blockchain is a permanent record.

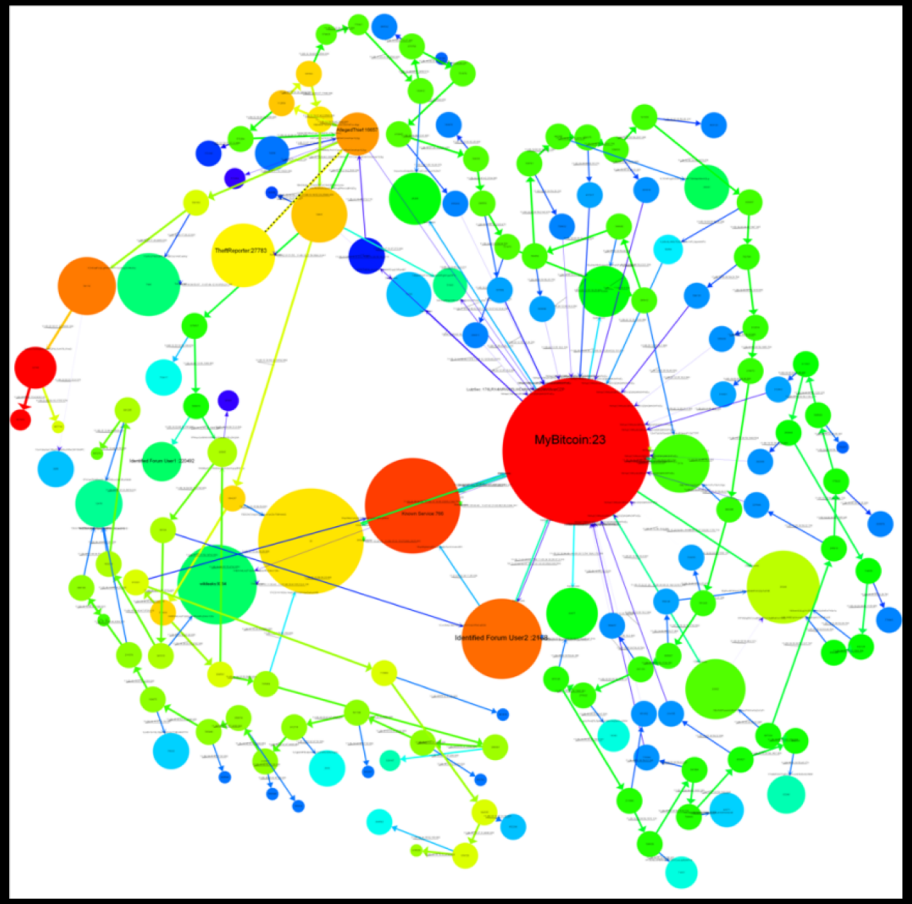


Privacy on Bitcoin and why it isn’t enough

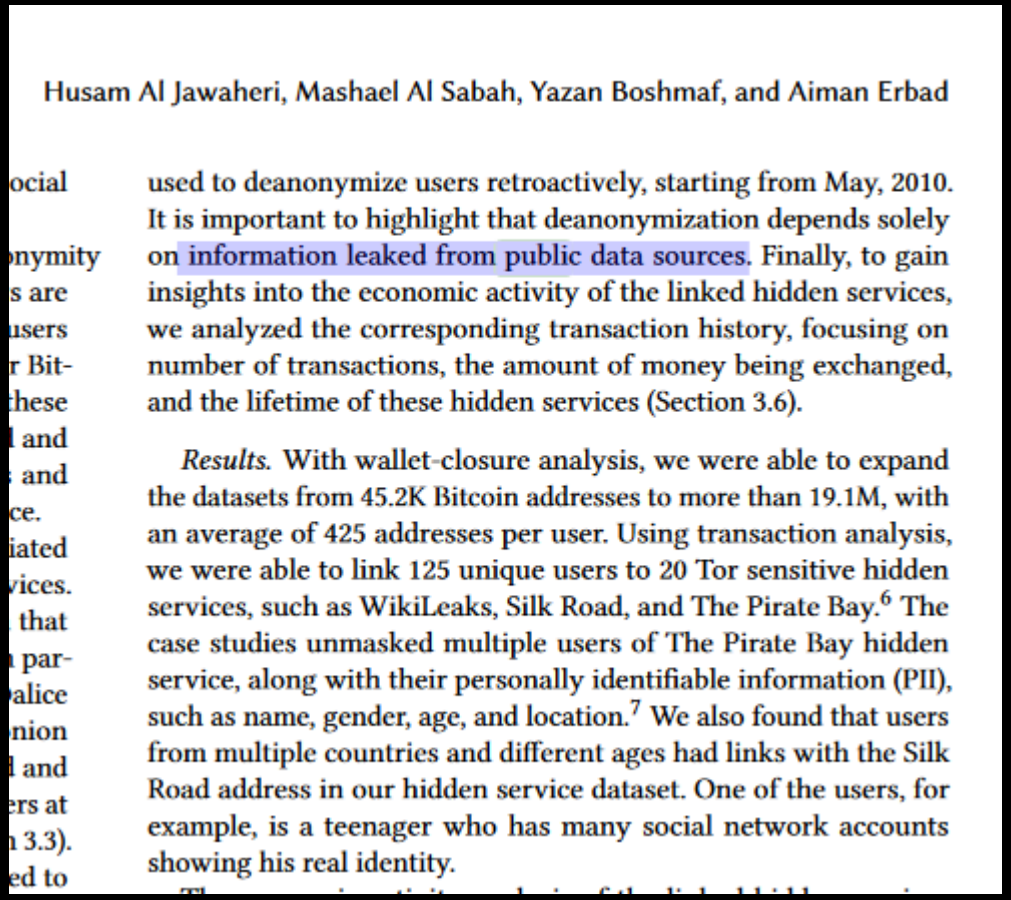
Blockchain Analysis Firms

- Coinfirm
- Chainalysis
- Ellliptic
- Numisight
- Skry

Combines various data sources, big data, law enforcement agencies, to identify owners of Bitcoin addresses.



Publicly Available Tools for Blockchain Analysis



Husam Al Jawaheri, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad

used to deanonymize users retroactively, starting from May, 2010. It is important to highlight that deanonymization depends solely on information leaked from public data sources. Finally, to gain insights into the economic activity of the linked hidden services, we analyzed the corresponding transaction history, focusing on number of transactions, the amount of money being exchanged, and the lifetime of these hidden services (Section 3.6).

Results. With wallet-closure analysis, we were able to expand the datasets from 45.2K Bitcoin addresses to more than 19.1M, with an average of 425 addresses per user. Using transaction analysis, we were able to link 125 unique users to 20 Tor sensitive hidden services, such as WikiLeaks, Silk Road, and The Pirate Bay.[6] The case studies unmasked multiple users of The Pirate Bay hidden service, along with their personally identifiable information (PII), such as name, gender, age, and location.[7] We also found that users from multiple countries and different ages had links with the Silk Road address in our hidden service dataset. One of the users, for example, is a teenager who has many social network accounts showing his real identity.

When A Small Leak Sinks A Great Ship: Deanonymizing Tor Hidden Service Users Through Bitcoin Transactions Analysis

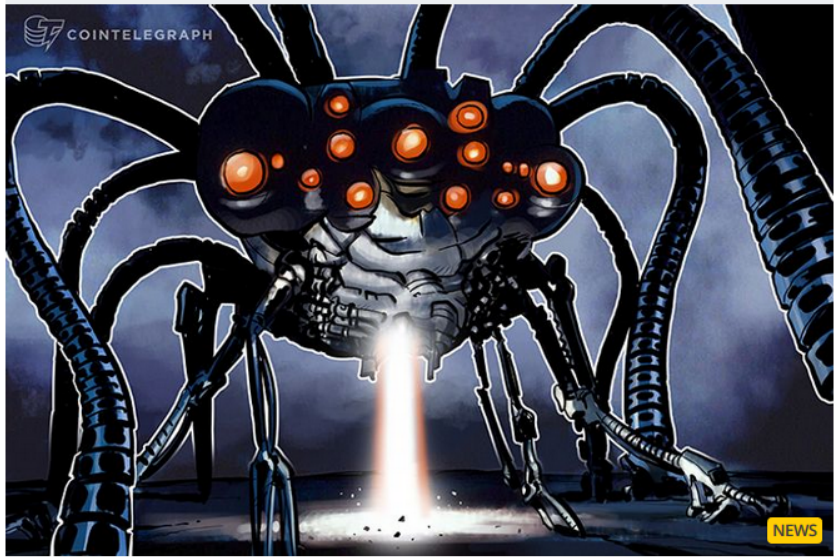
Combined with Non Public Information

By JEFF JOHN ROBERTS August 22, 2017

One benefit of using bitcoin is the digital currency can be anonymous—its owners can move money around the world without revealing who they are. Well, in theory at least. In reality, bitcoin is less secret than people think.

The latest reminder of this comes via a report that the Internal Revenue Service is using software to unmask bitcoin users who have failed to report profits. According to a contract unearthed by the Daily Beast, the IRS is paying a company called Chainalysis to help identify the owners of digital "wallets" that users employ to store their bitcoins.

US National Security Agency Develops System To Identify Bitcoin Users, Say Leaked Docs



The US National Security Agency (NSA) is reportedly able to locate senders and receivers of Bitcoin around the world, as classified documents provided by Edward Snowden reveal, The Intercept reports March 20.

The sources used for this article were disclosed to The Intercept, a publication dedicated to 'adversarial journalism' founded by Glenn Greenwald, Laura Poitras, and Jeremy Scahill following Edward Snowden's revelations of mass reconnaissance in 2013.

The NSA managed this by creating a system for harvesting, analyzing, and processing raw global internet traffic using a program disguised as a popular anonymizing software, according to other documents dating March 2013.

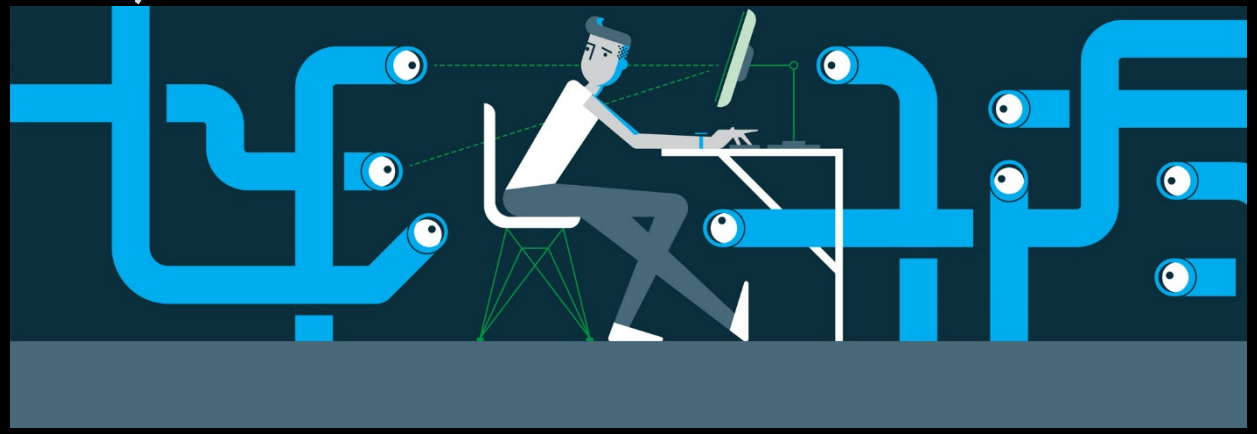
Privacy Protocols on the Blockchain

The Conflict

- Blockchain is about transparency and where every single transaction is permanently visible so that everyone can verify balances and transactions.
- How do you retain privacy in a transparent system that records every transaction?

Privacy Protocols

- Coin mixers / tumblers (Dash)
- Ring Signatures (Monero XMR)
- Zerocoin (Zcoin XZC)
- Zerocash (Zcash ZEC)
- Mimblewimble (Grin)

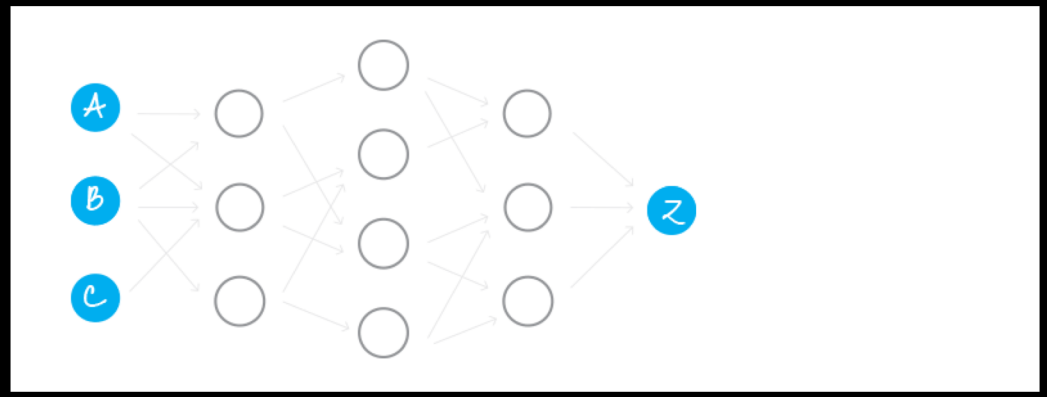


Coin Mixers / Tumblers

Bitcoin tumblers

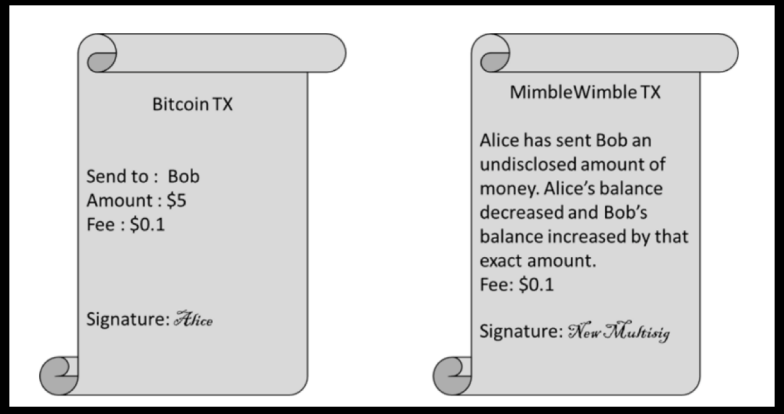
- People place their money into these tumblers and they mix it around with other people's funds. The trail gets obscured.
- You get back coins that still have history but have been obscured and may not be the original coins you deposited.
- Problems if you have to trust these tumblers to do the job and not to run away with your money (new protocols don't do this)

Cryptonote: How it works on a high level



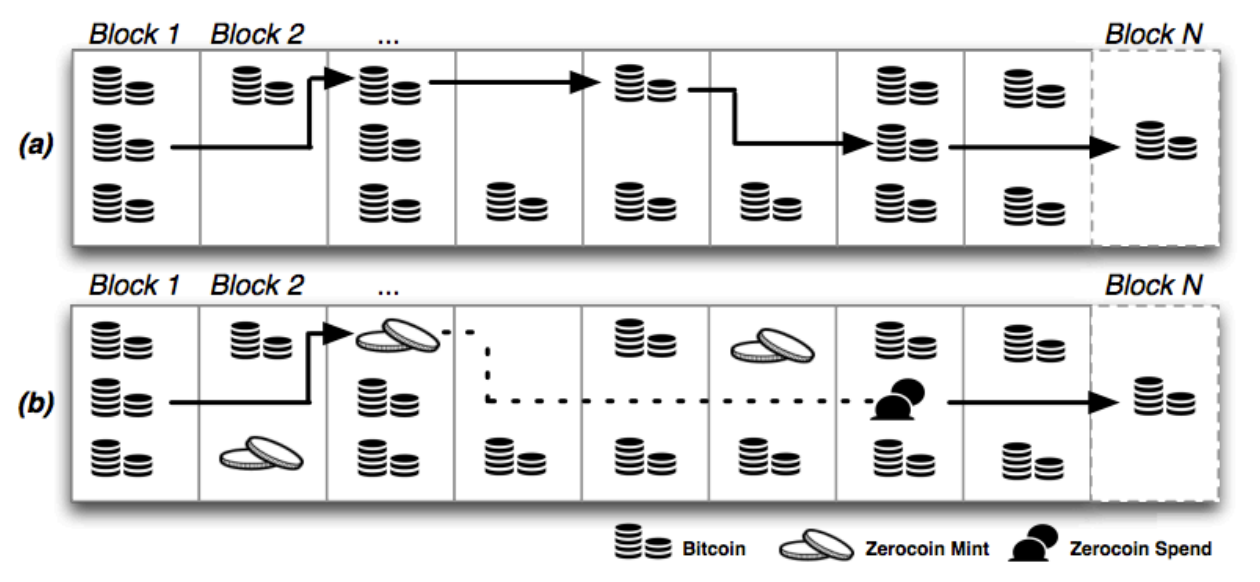
- When a user wants to send a transaction, it auto scans the blockchain for other outputs to use as dummy inputs
- In other words, when funds are sent, the sender randomly chooses other user funds as possible sources for the funds being sent.
- No one can tell which of the funds was the true source of the transaction. Other users can also use your funds as possible dummy sources.
- It is in effect, automated mixing that does not require the other users to be online.

Mimblewimble



- Mimblewimble works by aggregating all transaction in one single huge transaction. It works because hidden amounts.
- Blockchain size can decrease in certain cases!
- No addresses, but receiver and sender need to interact.
- When MW transaction are first broadcasted, their tx inputs and outputs are still visible. You can record as transactions come into the mempool. Work needs to be done.
- Multi party transactions are complicated
- Grin and Beam to implement.

Zerocoin: Zero knowledge proofs in action

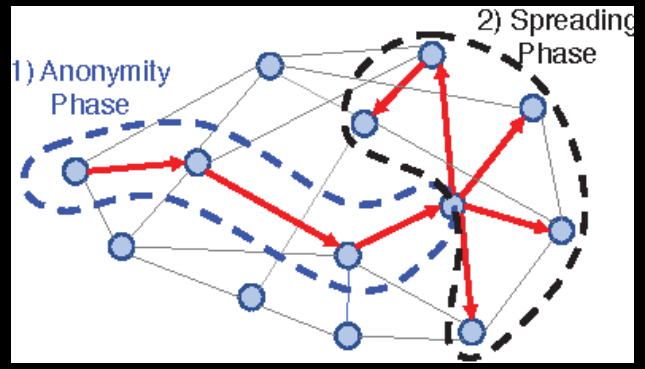


- Zerocoin as implemented first by Zcoin. Other coins such as PIVX, Zoin, Hexx have then also implemented it either using Zcoin's code or drawing inspiration from it.
- User destroys a coin using a Zerocoin mint transaction.
- At some time in the future, he redeems a brand new coin that has no transaction history through a Zerocoin spend transaction by showing proof that he did destroy the coin in the past.
- The proof is the **zero knowledge proof** that he burnt the coin, without showing which coin he burnt.
- Particularly useful in voting on the blockchain where votes are not duplicated and can be verified, without having to show which way a person voted.

Network/IP Privacy and how it differs from blockchain privacy

- **IP address privacy**
  - Hiding one identifier (can use VPNs or TOR)
  - Still requires work to pinpoint originating transaction.
  - Blockchain doesn't record IP addresses
  - Doesn't help with fungibility
- **Dandelion**
  - Techniques to hide originating transaction
  - Stem and fluff phases
  - Zcoin first to implement it

- **Blockchain Privacy**
  - Hiding your behaviour
  - Either through obfuscation or wiping transaction history
  - Behaviour and links are the primary way to deanonymize and are recorded permanently on the blockchain



Regulatory Responses to Privacy Coins

Forbes

18,241 views | Apr 30, 2018, 3:57 am

Japan's Financial Regulator Is Pushing Crypto Exchanges To Drop 'Altcoins' Favored By Criminals

Jake Adelstein Contributor

(NHAC NGUYEN/AFP/Getty Images)

In order to prevent money laundering and other criminal activity, Japan's Financial Services Agency, is quietly pressuring cryptocurrency exchanges to give up handling Monero (XMR), Zcash (ZEC), and Dash (DASH) and other cryptocurrencies favored by criminals and hackers. Sources close to the FSA confirmed that they were taking all available steps to discourage the use of certain alternative virtual currencies that have become attractive to the underworld because they are difficult to track. In September of last year, the European Union's law enforcement agency, Europol, released a report that warned "other cryptocurrencies such as Monero, Ethereum and Zcash are gaining popularity within the digital underground."

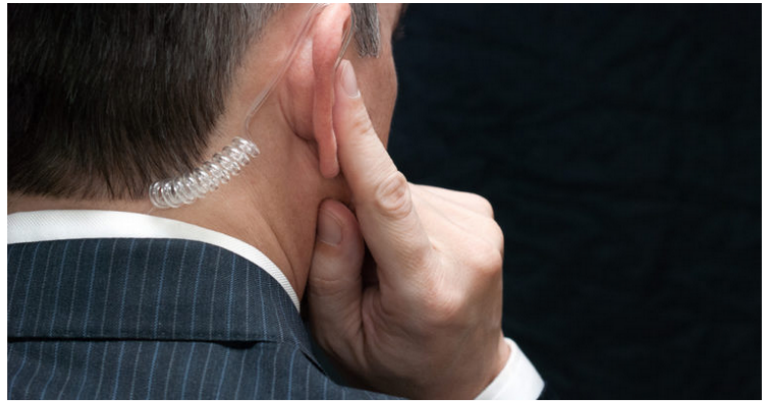
Forbes

In this picture taken on early January 27, 2018, Coincheck president Koichiro Wada (L) bows in apology at the end a press conference in Tokyo. Japan's government said on January 29 it would impose administrative measures on virtual currency exchange Coincheck after hackers stole hundreds of millions of dollars in digital assets from the Tokyo-based firm. (AFP/Getty Images)

Coincheck, the troubled Japanese cryptocurrency exchange, handled all three currencies mentioned above before they were hacked on January 26. After suspending operations and fully returning to business, the firm stopped handling all three currencies. Coincheck had applied to be a registered entity with the FSA in September of 2017 in line with the newly revised payment services laws but had not been approved at the time of the hack.

On March 16, Jiji Press reported that Coincheck was dropping transactions in Monero and two other hard-to-track cryptocurrencies; the report suggested that this was part of the company's attempt to show better compliance standards. After the January 26 hack of Coincheck, the FSA has ramped up their inspections of all operating registered cryptocurrency exchanges. The FSA has also informed other exchanges applying to be registered, that dealing with these three highly anonymous cryptocurrencies would be detrimental to gaining approval.

Congress Should Take Action Against Privacy Coins: Secret Service Official



A top official in the US Secret Service has asked Congress to take action against privacy-centric cryptocurrencies like zcash and monero, which include features designed to help users make anonymous transactions.

In prepared testimony given on Wednesday before the House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance, Robert Novy — deputy assistant director of the Secret Service's office of investigations — called on legislators to adopt measures which would curb the usage of so-called "privacy coins."

"We should also consider additional legislative or regulatory actions to address

Two Options for Regulators: Ban or Regulate?

- **BAN**
  - If privacy coins are banned, liquidity goes to other regulatory safe havens.
  - Even locally, it will move to p2p exchanges for e.g. Localbitcoins, Remitano
  - There will always be places to swap privacy coins to Bitcoin and vice versa. The rise of decentralized exchanges
  - What about private smart contracts? Where to draw the line?
- **REGULATE**
  - All points of conversion from cryptocurrencies to fiat are regulated (local exchanges) with AML/KYC procedures.
  - Trading liquidity will be primarily on regulated exchanges making money laundering harder (many existing ways to do this through fiat anyway)
  - Exchanges accepting privacy cryptocurrencies who know the identity is no different than allowing cash deposits.

Q&A

Questions and answers session

Thank you

zcoin.io

Twitter: @zcoinofficial

Telegram: @zcoinproject
Traded on Indodax, Binance, Bittrex, Huobi