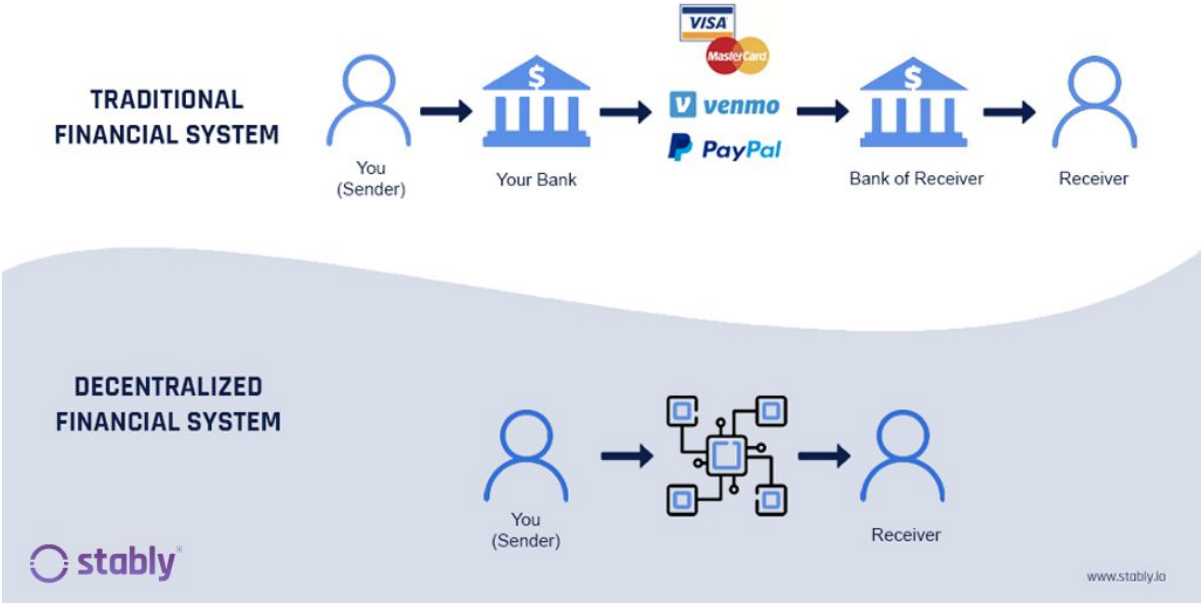
Privacy when Everyone is watching

Privacy on the Blockchain in the presence of KYC laws

IEOR 4575 Project | December 2021

Sofia Calatrava, Mikha Diaz, Roy Rinberg, Aldin Traljic

Blockchain



- Decentralized
- Public Ledger
- Pseudonymity, not anonymity

Problem 1: Blockchains are public by default

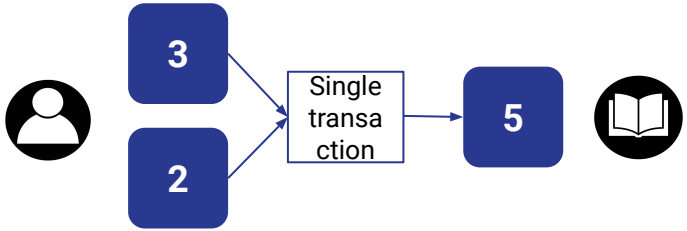
It is a common misconception that blockchain networks like bitcoin are anonymous.

- They are inherently NOT private.
- To be private, we have to make them so.

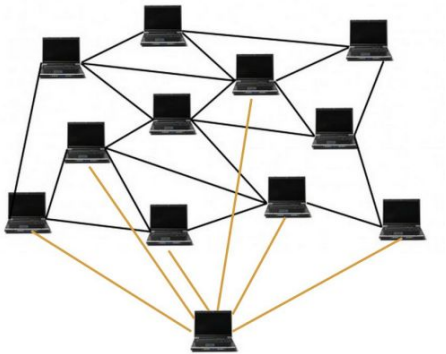
https://coinmarketcap.com/charts/

Deanonymization tools

Shared Spending



P2P network-layer deanonymization



Bitcoin P2P Network (Narayanan et al., 2016)

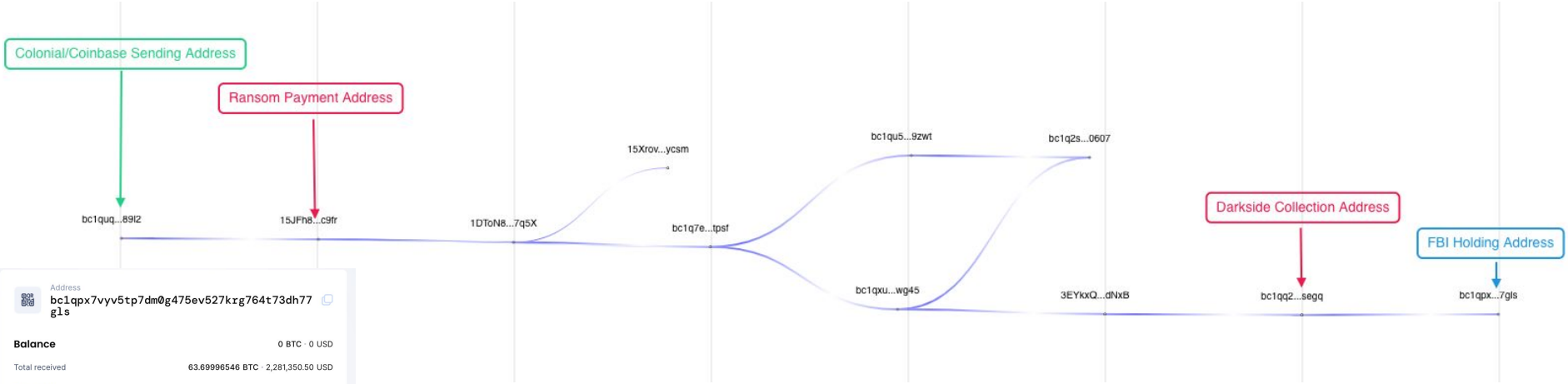
Case Study: Colonial Pipeline Co

- On May 7, 2021, suffered a ransomware cyberattack on billing system
  - On May 12, 2021, service resumed
- Led to fuel shortages across the East Coast
- Paid 75 BTC (about $4.4 million) as ransom payment
  - Identified the hackers as affiliates of Russia-linked criminal cybercrime group DarkSide
- On June 7, the DOJ reported successful recovery of 63.7 BTC from the ransom

Reconstruction: FBI’s recovery of BTC ransom payment

1. Query Bitcoin network for partial matches to address
2. Use Bitcoin Explorer (e.g. BlockChair) to find transactions belonging to the address
3. Obtain Private Keys from host

Reconstruction: FBI’s recovery of BTC ransom payment



Address
bc1qpx7vyv5tp7dm0g475ev527krg764t73dh77gls

Balance	0 BTC · 0 USD
Total received	63.69996546 BTC · 2,281,350.50 USD
Total spent	63.69996546 BTC · 2,836,814.25 USD

Transaction history — Show inputs and outputs

Sent — Confirmed
63.69996546 BTC — Aug 18, 2021, 4:44 PM UTC
Transaction hash: 6f8fcc22e2167b39f4dd5f47971a0f4e688c64064c2feaec2dae69f079c20c74
Senders: 1 Recipients: 2

Received — Confirmed
63.69996546 BTC — Jun 7, 2021, 5:45 PM UTC
Transaction hash: 943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a
Senders: 1 Recipients: 2

Solution to Problem 1: Privacy Coins

- Privacy coins trade transparency in favor of privacy
  a. Examples: ZCash and Monero
- Two major focuses:
  a. **Anonymity**: hiding the identities of individuals behind transactions
  b. **Untraceability**: making it difficult or impossible to *follow the money*
- Examples of Privacy Tools:
  a. Stealth addresses
  b. Ring-addresses
  c. Coin Mixers
  d. ZK-SNARKs

A quick description of ZK-SNARKs

- **Z**ero-**K**nowledge **S**uccinct **N**on-interactive **AR**gument of **K**nowledge

In another order:

- **AR**gument of **K**nowledge : A proof that you know something
- **Z**ero-**K**nowledge : That doesn't reveal any information about the thing
- **N**on-interactive: That doesn't require a back-and-forth with a verifier
- **S**uccinct : That is short to write

"A ZK-SNARK is a collection of words that mathematicians put together, in order to get the word 'SNARK'" - unattributed

Know Your Customer (KYC) laws?

- Require customers to reveal PII to an intermediary (i.e. social security number, physical address, government issue ID).

- Objective:
  - prevent illicit activities such as money laundering, financing terrorism, and tax evasion (FATF, FinCEN, US Infrastructure Bill)
  - Identify and track assets for taxes and accounting (e.g. SEC, IRS)

Problem 2: Regulators think that KYC laws are good

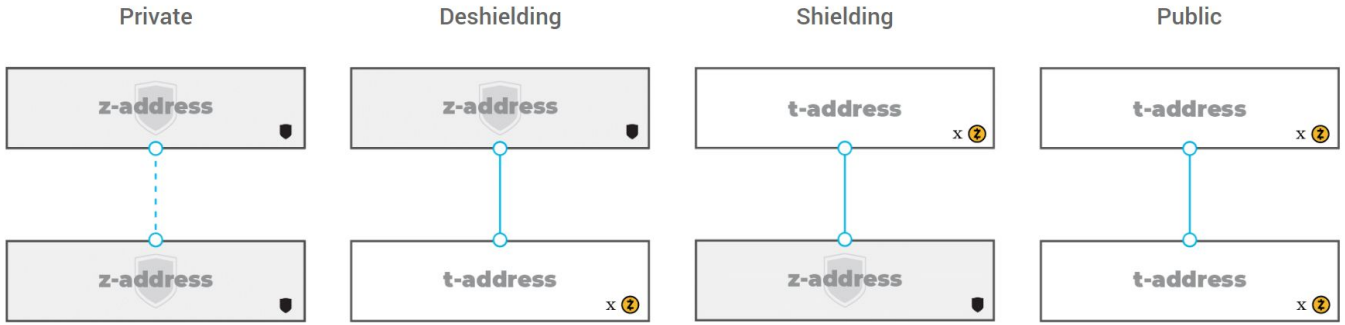
Issues with KYC:

- Increases risk of data-breaches with customer data
- Centralizes power and information
- Naive-KYC reduces privacy

“All [KYC laws] have elements that are generally incompatible with unhosted wallets and decentralized finance” - Eran Tromer (Co-founder of ZCash)

Concrete Arguments that strict KYC laws are bad

- Zcash, which many consider the most private coin, is forced to do transactions with t-addresses to comply



- This means that anyone who wants to buy a coffee basically “tweets” their purchase

Argument against KYC laws: for Taxes

- Difficult-to-track currencies already exist, we already use them daily.

  Cash.

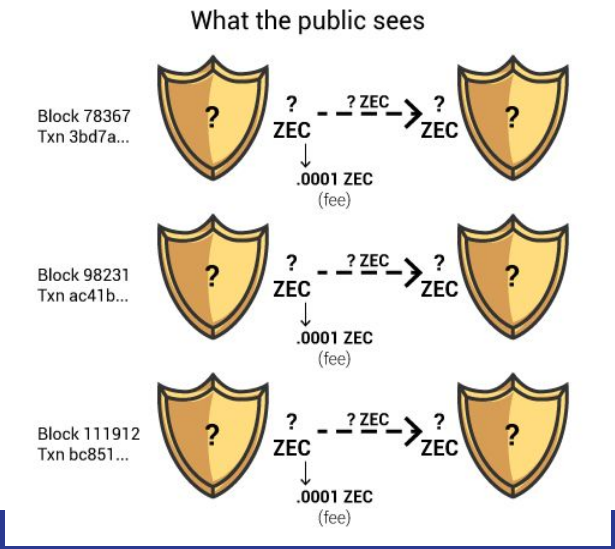
- In theory, people can avoid taxes by being paid entirely in cash and not reporting on it. But this *basically* doesn't happen.
  - Tracking everyone's every transaction in order to track taxes, is not maintaining the status quo, it is a dramatic increase in centralized power.

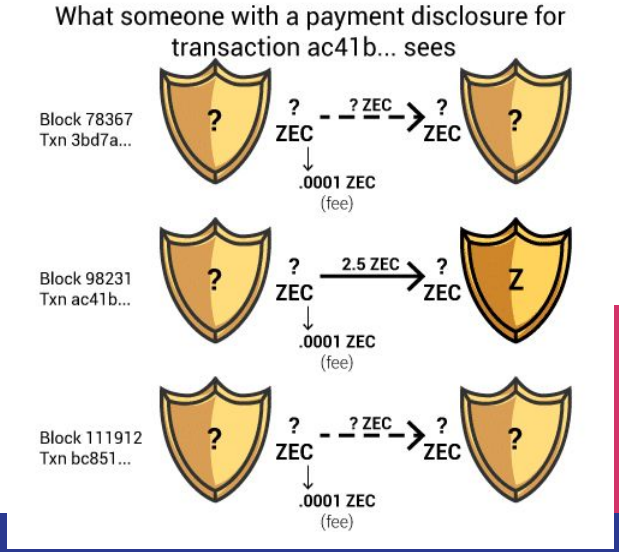
Argument against KYC laws: for Money Laundering

- Crimes occur in any country.
  - Law-enforcement keeps track of identities when people enter or leave the country
  - Law-enforcement works by tying a crime to a human person, and then connecting that human person to an identity that they know.
- Strict Money-Laundering laws would be the equivalent of tracking everyone at all times in order to identify crimes.
  - This is not how we do law-enforcement today, and would be a dramatic increase in governmental and centralized power.

Solution to Problem 2 : Selective Disclosure

Selective disclosure is a situation when a publicly traded company discloses material information to a single person, or a limited group of people or investors, as opposed to disclosing the information to all investors at the same time.”





Summary of Proposal

Main Objective: Increase privacy on the blockchain

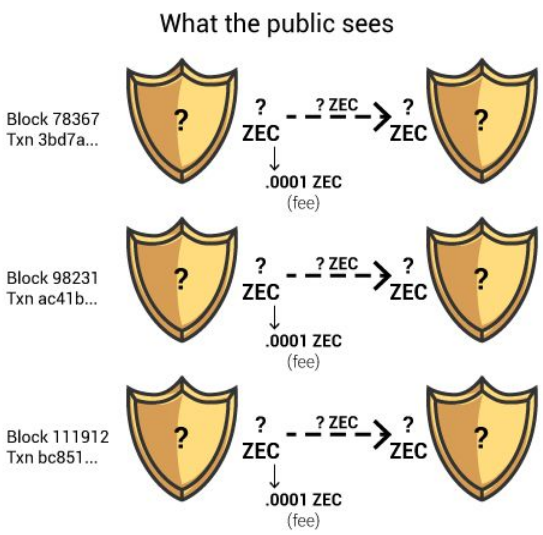
Proposal:

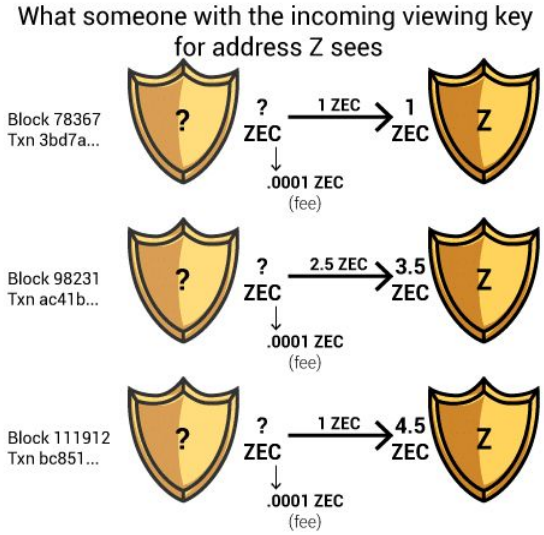
- Advocate for less strict KYC laws!
- Improve technology to support Shielded transactions and Selective disclosures
  - Hardware wallet support
  - Selective Disclosure support
  - Reduced transaction fees
- Improve technology for other privacy tools for non-privacy-aware coins, like mixers for Ethereum (Tornado Cash)

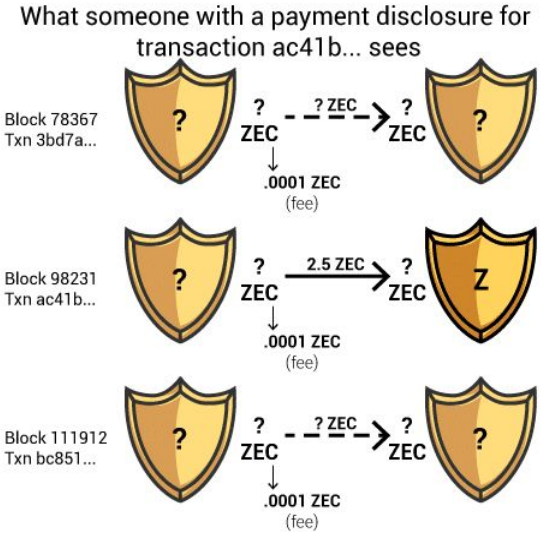
Fin

Solution to Problem 2 : Selective Disclosure

Selective disclosure is a situation when a publicly traded company discloses material information to a single person, or a limited group of people or investors, as opposed to disclosing the information to all investors at the same time.”







Measurement of Success

Main Objective: Increase privacy on the blockchain

- Zcash and other privacy coins experience increase in shielded transactions
- More privacy tools, like mixers for Ethereum, become readily available for non-privacy coins
- Overly strict KYC laws in the infrastructure bill do not pass
- Raise Awareness

What is the Spectrum of KYC?

Strict KYC Laws:

- Any entity wishing to interact with an exchange must account for each dollar they use, and provide a fully transaction history of where it came from

Lenient KYC laws:

- Any entity wishing to interact with an exchange must account for each dollar they use, and only the account they got it from

More Abstract Arguments against KYC laws

- Security and economic risks to individuals.
  - “Even minor data leaks can cause disproportionate privacy harm to customers”
- Imposing Excessive Information Security Costs on Small Entities.
- Harmful to innovation in the cryptocurrency space.
- Harms US competitiveness.
- Ineffective and trivial to circumvent.
  - “nefarious parties ... would easily circumvent such requirements by relaying their transactions with third parties through their own unhosted wallet.”

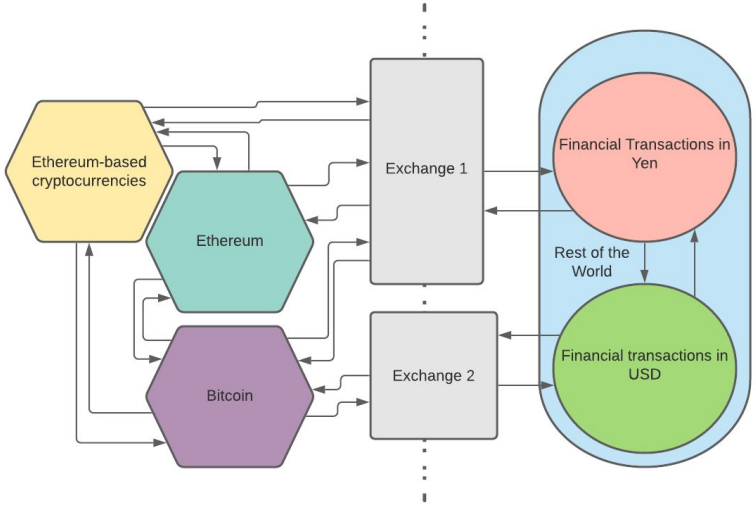
Comments on FINCEN-2020-0020

What about other Privacy Solutions

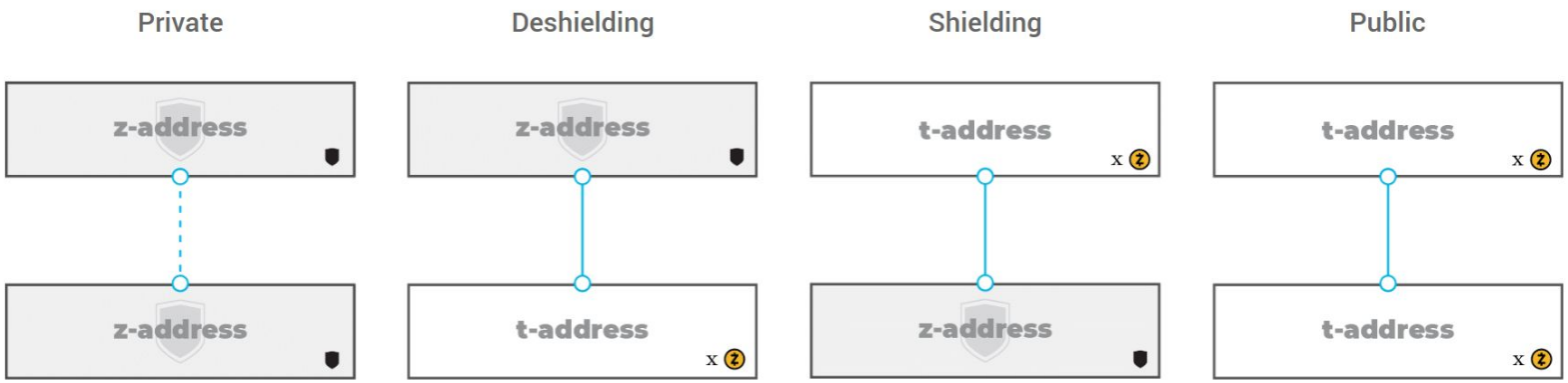
Bonus Slide: Future speculation

Why do KYC Laws Exist? (Roy's Version, if we want to change)

- **Know Your Customer (KYC)** :
  - **What is KYC:**
    -
- Objective:
  - Identify and track assets for **taxes and accounting** (SEC, IRS)
  - Prevent crimes such as **money laundering**, financing terrorism, and tax evasion (FATF, FinCEN, US Infrastructure Bill)



Heading


Private
z-address
z-address
Deshielding
z-address
t-address
x
Shielding
t-address
x
z-address
Public
t-address
x
t-address
x

III. Cryptocurrency Regulations

KYC Considerations

Summary

Mikha or Sofia