# Privacy in and around the Blockchain

SCOTT ANECITO

#### Who am I?

#### Privacy and security enthusiast

Cookies of '00

#### Portland State University

- B.S Computer Science
- Associates in International Studies, Japanese
- Member of ACM, CTF/War Games club

Monero Contributor

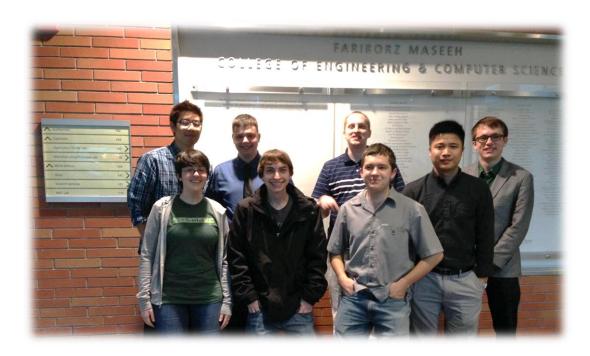
Automation Engineer at Intel

/u/xmrscott





https://github.com/sanecito/monero-presentations



#### Presentation Outline

Why does privacy matter?

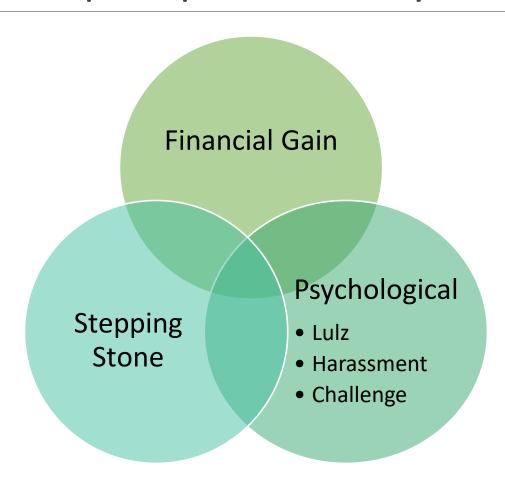
What is visible in a transaction?

What are some case studies of no privacy?

What can I do to protect my data?

How do I identify 'privacy focused' cryptocurrency scams?

#### Why would people want your data?



#### World's Biggest Data Breaches

interesting story

Selected losses greater than 30,000 records



Sony Pictures

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

AKA Smashing SMS-2FA for Fun and Profit

### Why does financial privacy matter?

People know your income, wealth accumulation

Targeting and/or advertisements based on transactions

Interaction with unknown person of interest







People know your vendors and partners

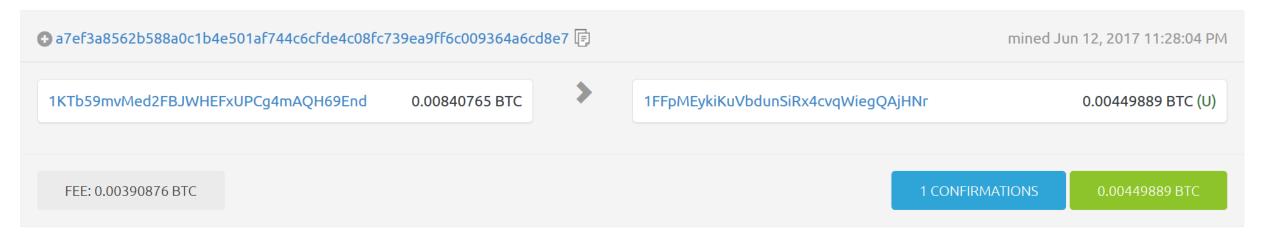
## Would you be willing to post this online?

Date	Description	Amount	Current Balance
27-Oct	Direct Deposit	\$2,000	[]
29-Oct	WinCo	\$105	[]
29-Oct	Chevron	\$30	[]
1-Nov	Apartment Complex	\$500	[]
1-Nov	SRP	\$120	[]
1-Nov	Water	\$20	[]
5-Nov	WinCo	\$100	[]
5-Nov	Chevron	\$27	[]
12-Nov	WinCo	\$95	[]
15-Nov	Verizon	\$200	[]
[]	[]	[]	[]
24-Nov	Direct Deposit	\$2,000	[]
26-Nov	WinCo	\$102	[]
26-Nov	Chevron	\$31	[]
1-Dec	Apartment Complex	\$500	[]
1-Dec	SRP	\$115	[]
1-Dec	Water	\$22	[]

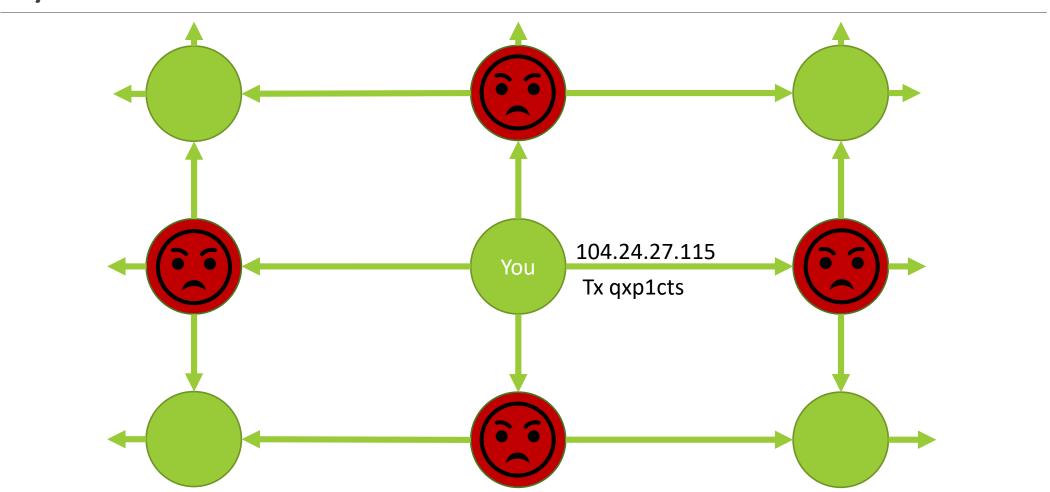
## Would you be willing to post this online?

Date	Description	Amount	Current Balance
27-Oct	oK5FEwnDro	+\$2,000	[]
29-Oct	2IwrtuyvFM	\$105	[]
29-Oct	MI4qD1qEox	\$30	[]
1-Nov	KHpHlyv7sJ	\$500	[]
1-Nov	EsyJKzC0FI	\$120	[]
1-Nov	sq8pxwDpu8	\$20	[]
5-Nov	2IwrtuyvFM	\$100	[]
5-Nov	MI4qD1qEox	\$27	[]
12-Nov	2IwrtuyvFM	\$95	[]
15-Nov	IGFHuznxv1	\$200	[]
[]	[]	[]	[]
24-Nov	oK5FEwnDro	+\$2,000	[]
26-Nov	2IwrtuyvFM	\$102	[]
26-Nov	MI4qD1qEox	\$31	[]
1-Dec	KHpHlyv7sJ	\$500	[]
1-Dec	EsyJKzC0FI	\$115	[]
1-Dec	sq8pxwDpu8	\$22	[]

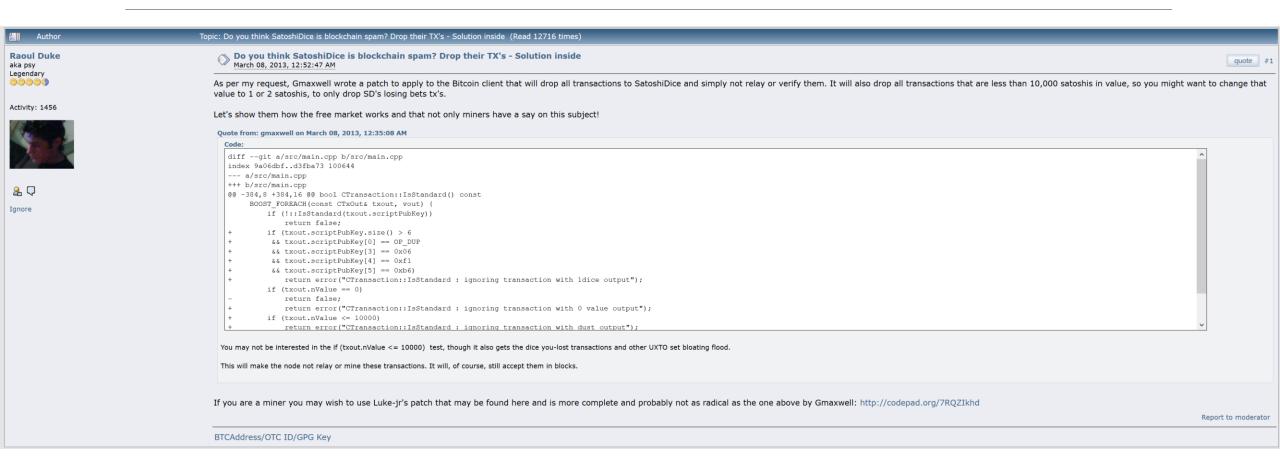
### What makes up a Bitcoin transaction?



## Sybil Attack



#### Tx Censorship by Node - 2013 Ex



#### Bitcoin De-anonymization by Exchange

- 1. Vinny Troia, Night Lion Security CEO, Certified White Hat Hacker
- 2. Sent a compliance letter from CoinBase
- 3. "We do breach investigations a lot of times. If a fraudster is saying they're selling my client's stolen documents, the only way to make sure they have what they say they have is to buy those documents." Mr. Troia
- 4. Account shut down. All attempts w/ family info shut down

## Bitcoin Tracing by Law Enforcement and Ledger Analysis Companies

#### WannaCry

- Three addresses receive ~\$140,000
- Convert ~\$37,000 in Bitcoin into Monero via ShapeShift
- ShapeShift soon blacklists addr associated with WannaCry

#### AlphaBay, BTC-e

- AlphaBay DoJ / Feds determine amount of illegally gained capital
- BTC-e L.E. & L.A.C (WizSec & Chainalysis)

Chainalysis has recently gotten a contract with IRS

#### What can I do to protect my ledger privacy?

Only use Cryptocurrencies that have well documented/vetted obfuscation techniques for:

- 1. Sender Wallet Address
- 2. Receiver Wallet Address
- 3. Tx Amount

(Origin node IP can be masked via Tor/I2P, Trusted VPN)

## How do I identify 'privacy focused' cryptocurrency scams?

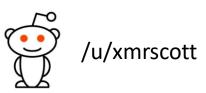
Does it obfuscate:

1. Sender Wallet Address

2. Receiver Wallet Address

3. Tx Amount

## Thanks for listening! Questions?







https://github.com/sanecito/monero-presentations