Privacy in and around the Blockchain

SCOTT ANECITO

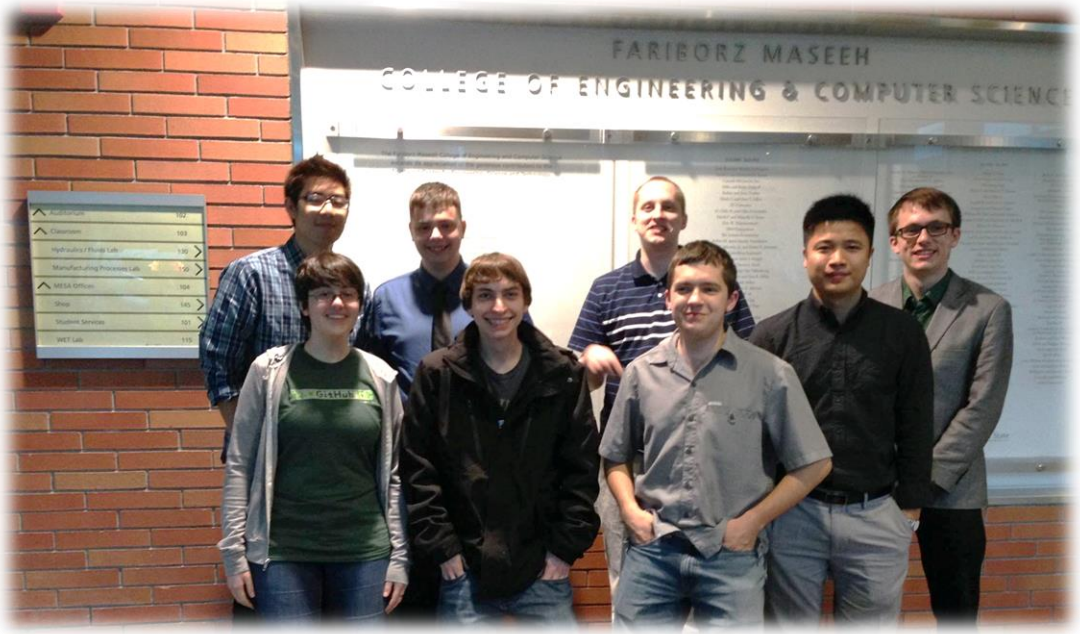
Who am I?

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

irc: xmrscott@freenode

https://github.com/sanecito/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?

SEE ALSO: HTTPS://WWW.TED.COM/TALKS/GLENN_GREENWALD_WHY_PRIVACY_MATTERS

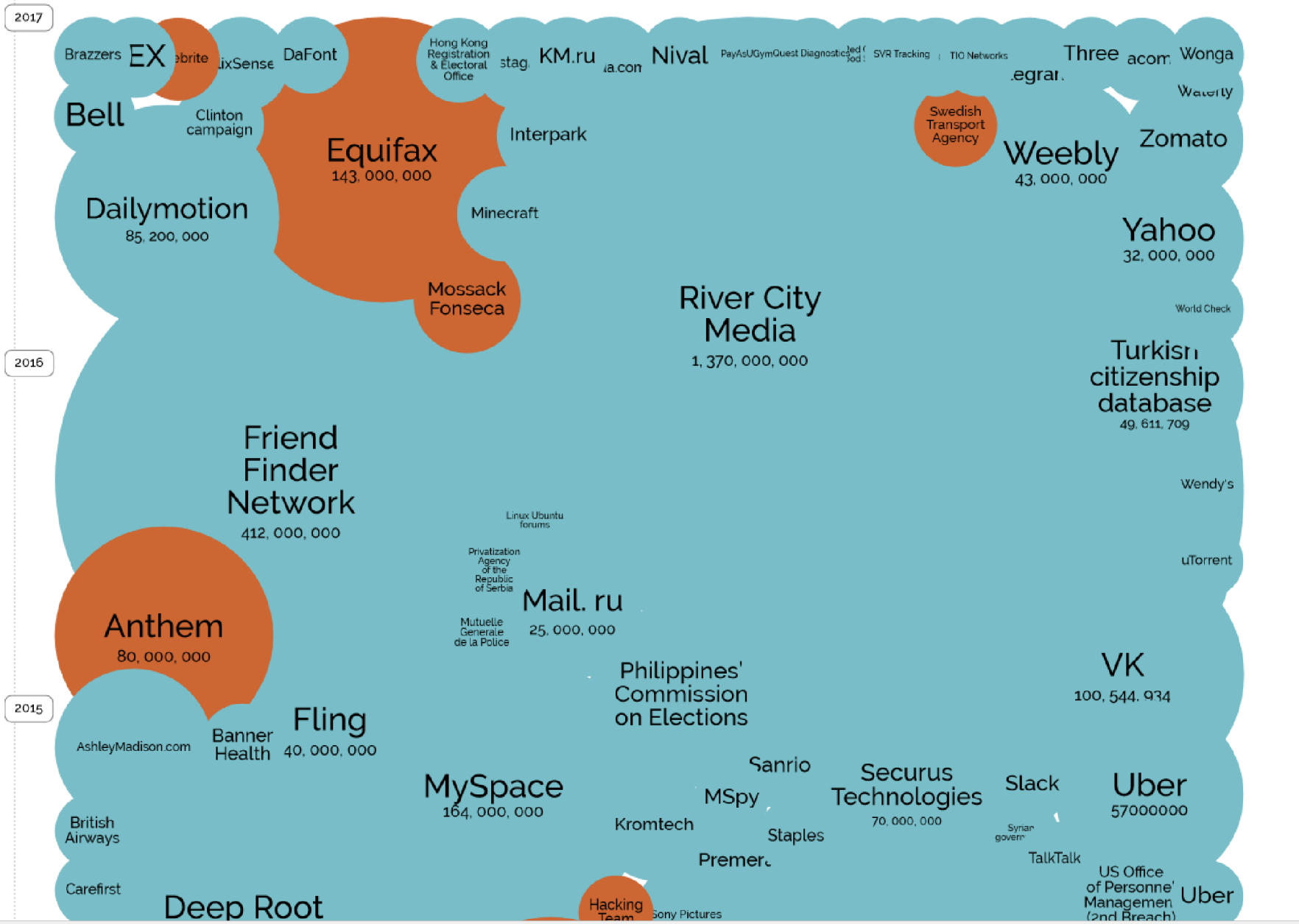
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 10th Sep 2017)

interesting story

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



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

AKA Smashing SMS-2FA for Fun and Profit

SOURCE: HTTPS://MEDIUM.COM/@CODYBROWN/HOW-TO-LOSE-8K-WORTH-OF-BITCOIN-IN-15-MINUTES-WITH-VERIZON-AND-COINBASE-COM-BA75FB8D0BAC
SEE ALSO: HTTPS://WWW.FORBES.COM/SITES/LAURASHIN/2016/12/20/HACKERS-HAVE-STOLEN-MILLIONS-OF-DOLLARS-IN-BITCOIN-USING-ONLY-PHONE-NUMBERS/AMP/

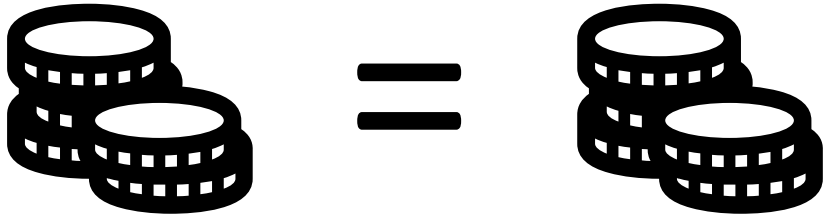
Why does *financial privacy* matter?

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	[…]

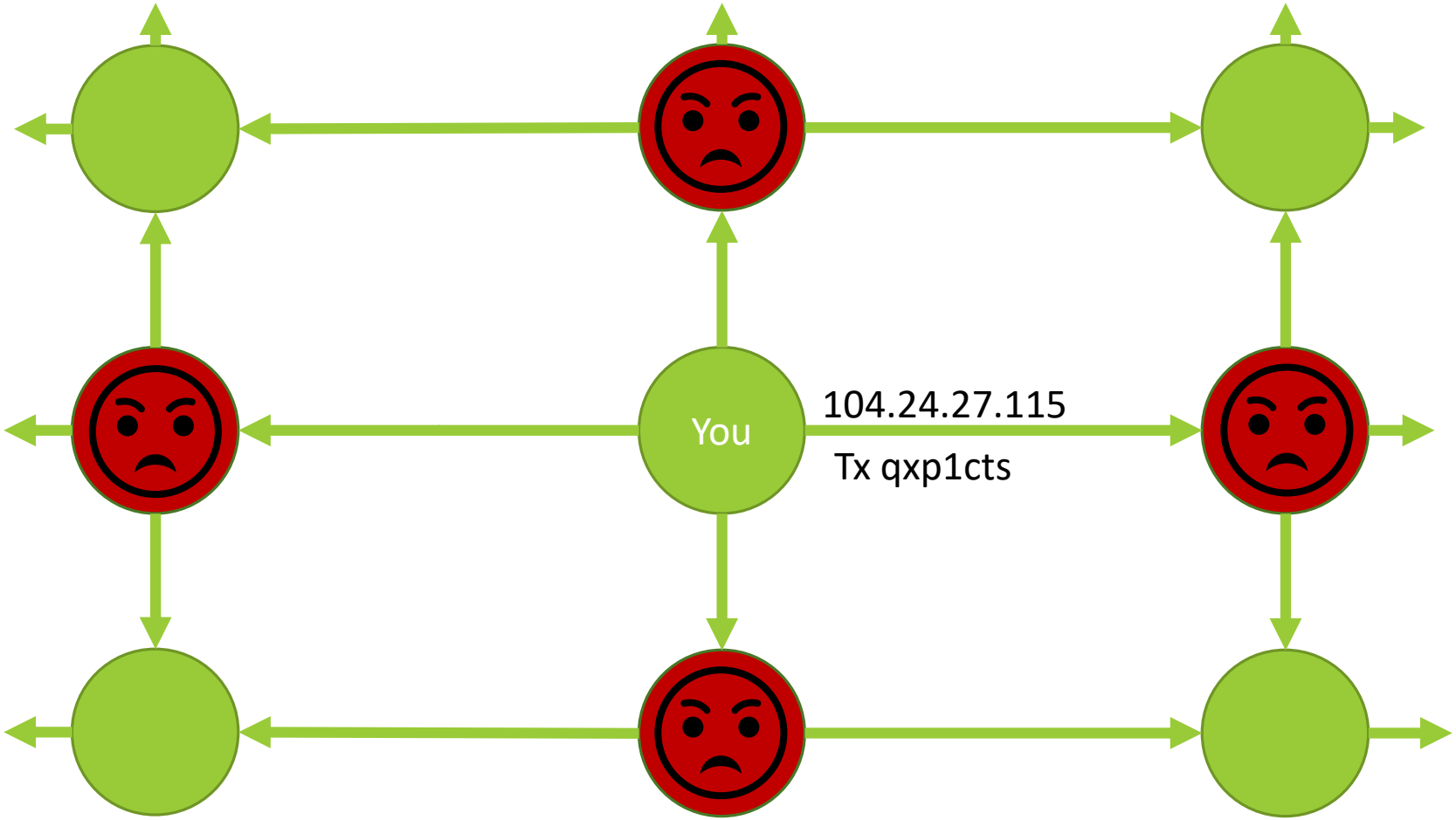
Would you be willing to post this online?

Date	Description	Amount	Current Balance
27-Oct	oK5FEwnDro	+$2,000	[…]
29-Oct	2IwrtuyvFM	$105	[…]
29-Oct	MI4qD1qEox	$30	[…]
1-Nov	KHpHIyv7sJ	$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	KHpHIyv7sJ	$500	[…]
1-Dec	EsyJKzC0FI	$115	[…]
1-Dec	sq8pxwDpu8	$22	[…]

What makes up a Bitcoin transaction?

SOURCE: BLOCKEXPLORER.COM

Sybil Attack



Tx Censorship by Node - 2013 Ex

Author | Topic: Do you think SatoshiDice is blockchain spam? Drop their TX's - Solution inside (Read 12716 times)

Raoul Duke
aka psy
Legendary

Activity: 1456

Ignore

Do you think SatoshiDice is blockchain spam? Drop their TX's - Solution inside
March 08, 2013, 12:52:47 AM

quote #1

As per my request, Gmaxwell wrote a patch to apply to the Bitcoin client that will drop all transactions to SatoshiDice and simply not relay or verify them. It will also drop all transactions that are less than 10,000 satoshis in value, so you might want to change that value to 1 or 2 satoshis, to only drop SD's losing bets tx's.

Let's show them how the free market works and that not only miners have a say on this subject!

Quote from: gmaxwell on March 08, 2013, 12:35:08 AM

Code:

```
diff --git a/src/main.cpp b/src/main.cpp
index 9a06dbf..d3fba73 100644
--- a/src/main.cpp
+++ b/src/main.cpp
@@ -384,8 +384,16 @@ bool CTransaction::IsStandard() const
     BOOST_FOREACH(const CTxOut& txout, vout) {
         if (!::IsStandard(txout.scriptPubKey))
             return false;
+        if (txout.scriptPubKey.size() > 6
+         && txout.scriptPubKey[0] == OP_DUP
+         && txout.scriptPubKey[3] == 0x06
+         && txout.scriptPubKey[4] == 0xf1
+         && txout.scriptPubKey[5] == 0xb6)
+            return error("CTransaction::IsStandard : ignoring transaction with 1dice output");
         if (txout.nValue == 0)
-            return false;
+            return error("CTransaction::IsStandard : ignoring transaction with 0 value output");
+        if (txout.nValue <= 10000)
+            return error("CTransaction::IsStandard : ignoring transaction with dust output");
```

You may not be interested in the if (txout.nValue <= 10000) test, though it also gets the dice you-lost transactions and other UXTO set bloating flood.

This will make the node not relay or mine these transactions. It will, of course, still accept them in blocks.

If you are a miner you may wish to use Luke-jr's patch that may be found here and is more complete and probably not as radical as the one above by Gmaxwell: http://codepad.org/7RQZIkhd

Report to moderator

BTCAddress/OTC ID/GPG Key

SOURCE: HTTPS://BITCOINTALK.ORG/INDEX.PHP?TOPIC=150405.0

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

SOURCES: HTTP://WWW.COINDESK.COM/COINBASE-WHITE-HAT-HACKER-DONT-WANT-BITCOIN/

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

SOURCES: HTTPS://WWW.COINDESK.COM/WANNACRY-MOVE-BITCOIN-THEFT-EVOLVES-MULTI-BLOCKCHAIN-WORLD/
HTTPS://WWW.FORBES.COM/SITES/THOMASBREWSTER/2017/08/03/WANNACRY-HACKERS-USE-SHAPESHIFT-TO-LAUNDER-BITCOIN/
HTTPS://WWW.COINDESK.COM/COINDESK-EXPLAINER-BTC-E-ARREST-MT-GOX-CONNECTION-BIG-NEWS/
HTTPS://WWW.JUSTICE.GOV/OPA/PR/ALPHABAY-LARGEST-ONLINE-DARK-MARKET-SHUT-DOWN
HTTPS://WWW.COINDESK.COM/IRS-USING-BITCOIN-TRACKING-SOFTWARE-SINCE-2015/

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?

/u/xmrscott

irc: xmrscott@freenode

https://github.com/sanecito/presentations