OST
Eastern Switzerland
University of Applied Sciences

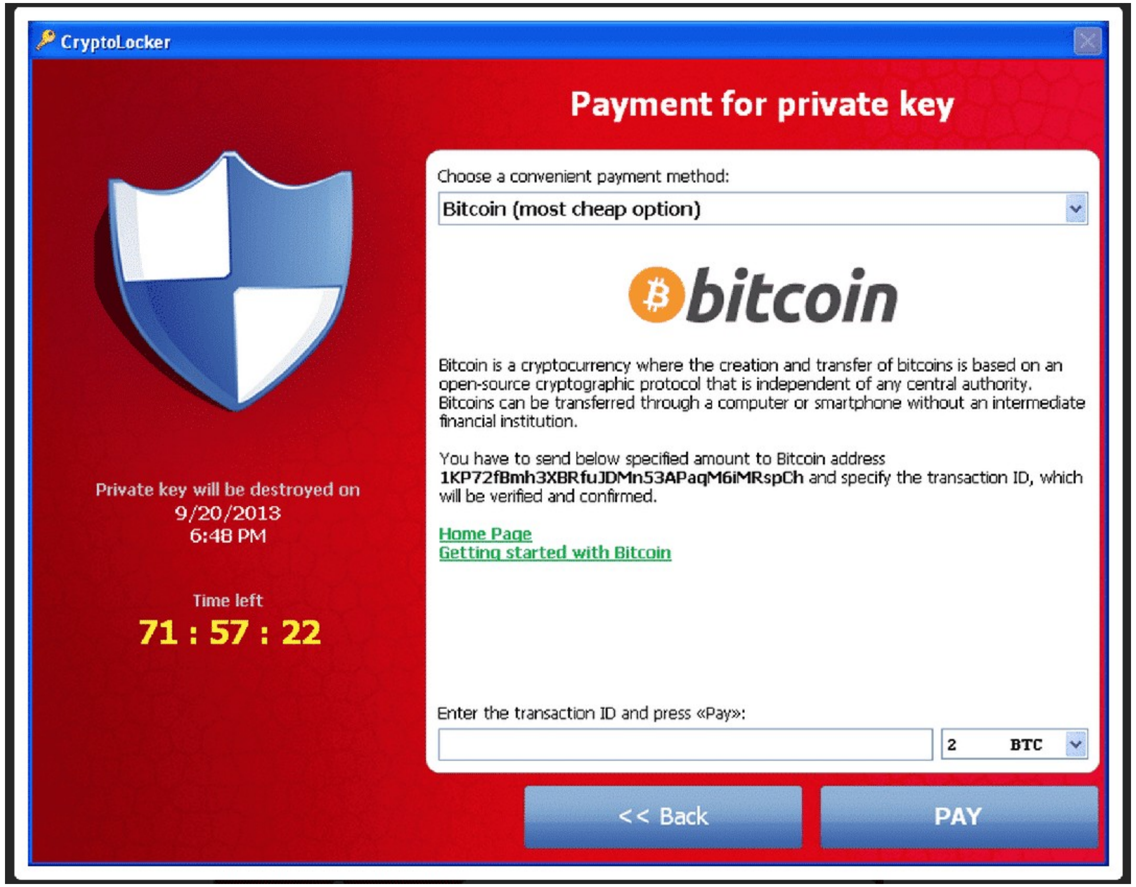
Blockchain (BlCh)

Security Considerations

Thomas Bocek

01.12.2021

Anonymity



Payment for private key

Choose a convenient payment method:
Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address **1KP72fBmh3XBRfuJDMn53APaqM6iMRspCh** and specify the transaction ID, which will be verified and confirmed.

Private key will be destroyed on
9/20/2013
6:48 PM

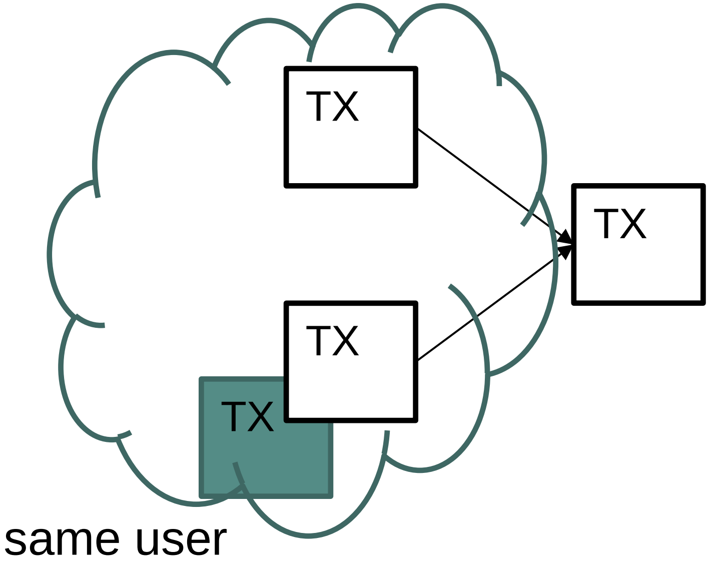
Time left
71 : 57 : 22

Enter the transaction ID and press «Pay»:
2 BTC

- Ransomeware
  - Encrypt files, delete original
  - Only decrypt if payed in BTC
- Pay or not pay?
  - Not pay and not restore data
  - Pay and restore data
  - Pay and not restore data
  - “In research for this article ZDnet traced four bitcoin addresses posted (and re-posted) in forums by multiple CryptoLocker victims, showing movement of 41,928 BTC between October 15 and December 18.” (source)

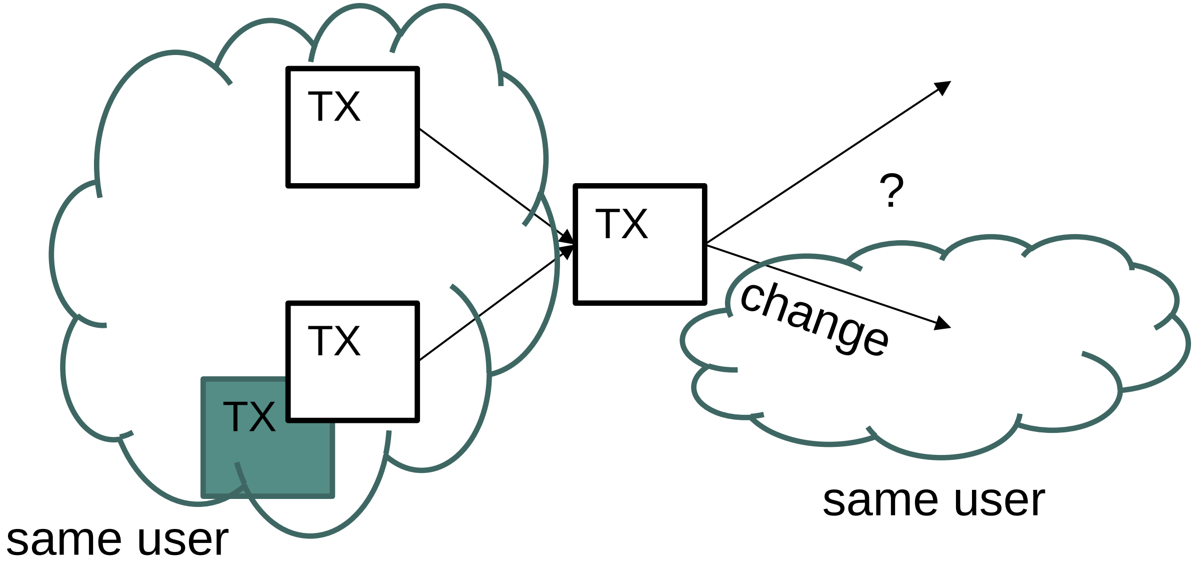
Anonymity

- BitcoinJ: Committed bloom filters for improved wallet performance and SPV security
- HEURISTIC 1
  - If two (or more) addresses are inputs to the same transaction, they are controlled by the same user; i.e., for any transaction t, all pk ∊ inputs(t) are controlled by the same user.



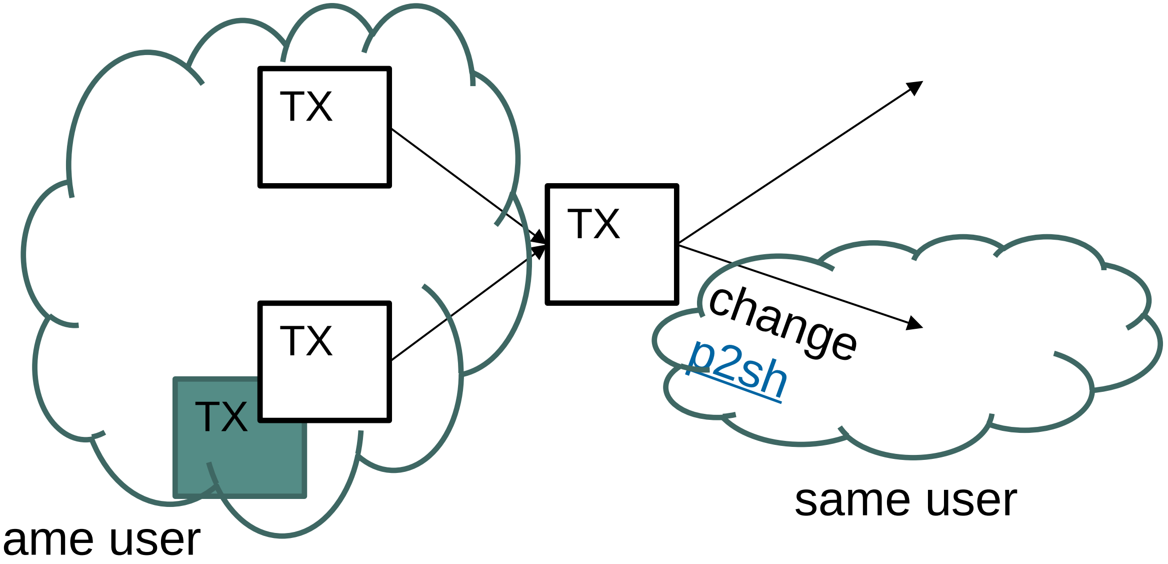
Anonymity

- HEURISTIC 2.
  - The one-time change address is controlled by the same user as the input addresses; i.e., for any transaction t, the controller of inputs(t) also controls the one-time change address pk ∈ outputs(t) (if such an address exists).



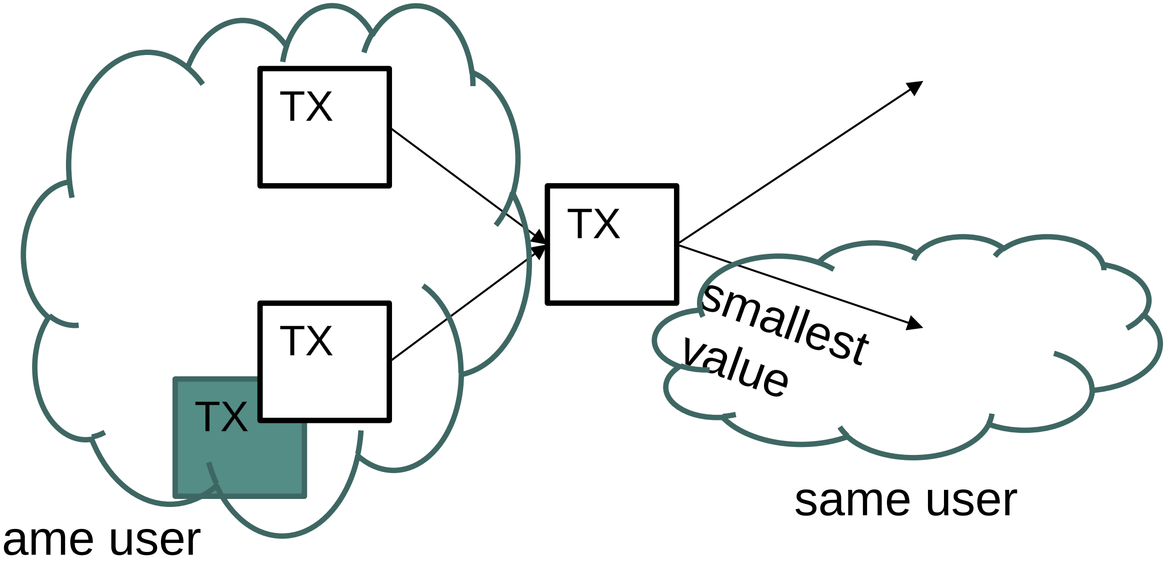
Anonymity

- HEURISTIC 3
  - Multisig wallets usually use p2sh change, but the recipient rarely uses p2sh, which allows to determine the correct change output with high probability.



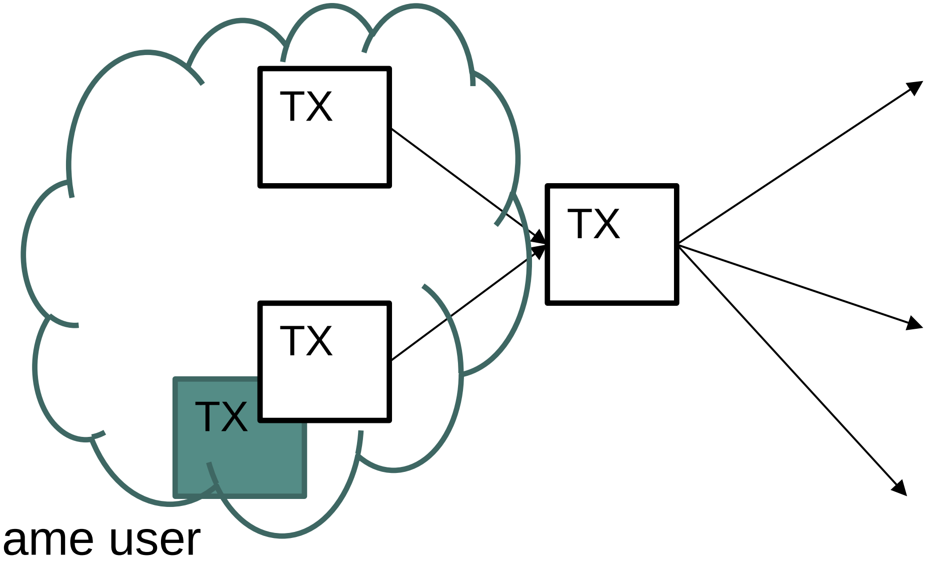
Anonymity

- OPTIMAL CHANGE HEURISTIC
  - The assumption is that wallet software does not spend outputs unnecessarily. Therefore the change value is smaller than any of the spent outputs. Because if the change was larger than one output then this output would be left out and the change would be reduced by the output's value.

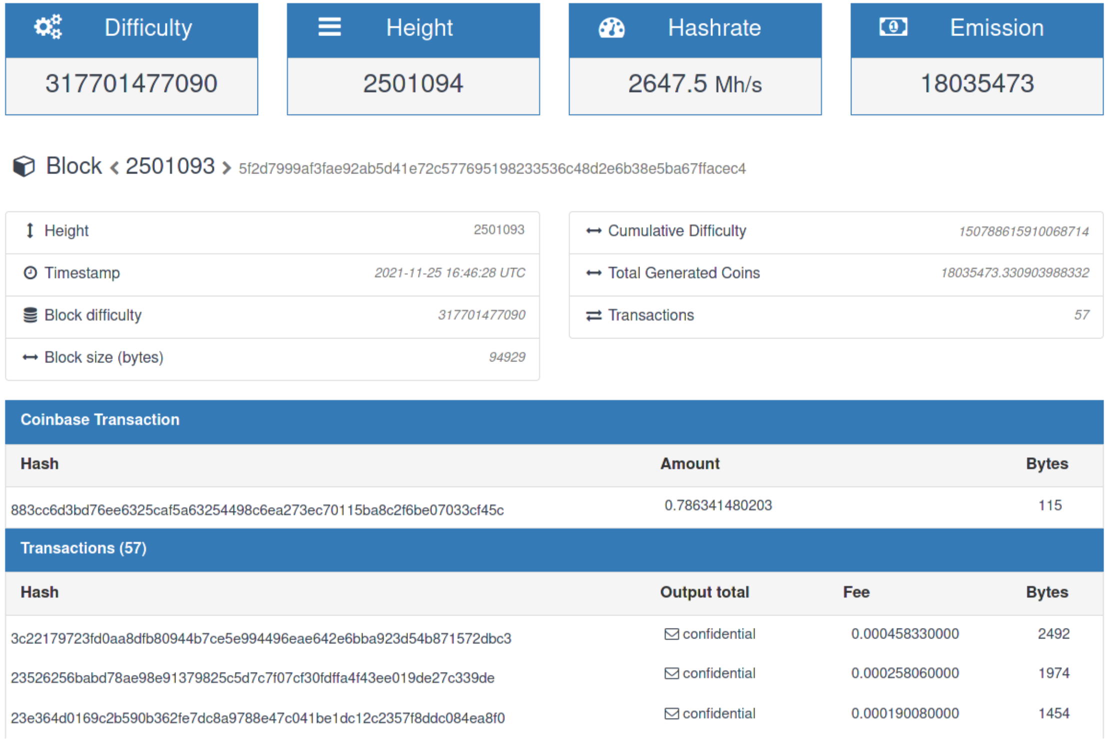


Anonymity

- CONSUMER HEURISTIC
  - Consumer wallets only create transactions with two outputs. Therefore, if an output is spent by a transaction with 3 outputs it is not change.
  - WalletExplorer / Chainalysis



Anonymity



Difficulty	Height	Hashrate	Emission
317701477090	2501094	2647.5 Mh/s	18035473

Block ‹ 2501093 › 5f2d7999af3fae92ab5d41e72c577695198233536c48d2e6b38e5ba67ffacec4

Height	2501093
Timestamp	*2021-11-25 16:46:28 UTC*
Block difficulty	*317701477090*
Block size (bytes)	*94929*

Cumulative Difficulty	*150788615910068714*
Total Generated Coins	*18035473.330903988332*
Transactions	*57*

Coinbase Transaction

Hash	Amount	Bytes
883cc6d3bd76ee6325caf5a63254498c6ea273ec70115ba8c2f6be07033cf45c	0.786341480203	115

Transactions (57)

Hash	Output total	Fee	Bytes
3c22179723fd0aa8dfb80944b7ce5e994496eae642e6bba923d54b871572dbc3	✉ confidential	0.000458330000	2492
23526256babd78ae98e91379825c5d7c7f07cf30fdffa4f43ee019de27c339de	✉ confidential	0.000258060000	1974
23e364d0169c2b590b362fe7dc8a9788e47c041be1dc12c2357f8ddc084ea8f0	✉ confidential	0.000190080000	1454

- Monero
  - Blockexplorer
  - No scripting (no smart contracts)
  - Proof of work algorithm
  - Due to cryptographic algorithms, unknown: addresses trading monero, transaction amounts, address balances, or transaction histories
    - Ring signatures, zero-knowledge proof, stealth addresses: unclear which ring member actually signed
  - 14.11.2020: IRS Will Pay Up To $625,000 If You Can Crack Monero, Other Privacy Coins [link]
  - Malware mining, due to CPU bound PoW
    - Some ransomware groups only accepts Monero

Security Concerns (Theft)

- Bitcoinica – security issue: Linode (cloud provider)
  - gaining root access using the service provider's systems
  - 46K BTC stolen (in 2012 ~$228,000, now ~$308 mio)
- 2 month later: 19K BTC stolen from Bitcoinica
  - “hackers webserver (Rackspace) by resetting a password, most likely through an automated e-mail.”
- Bitfloor, as US-based Bitcoin exchange site
  - 24K BTC stolen (in 2012 ~250'000$)
  - attacker gained accesses to an unencrypted backup of the wallet keys
- Bitcoin-Central
  - Some hundreds Bitcoins stolen
  - Password reset – issue with OVH?
- BitInstant: 333 BTC stolen ~ $12’000
  - Domain registrar Site5: redirected DNS
  - “Armed with knowledge of my place of birth and mother's maiden name alone (both facts easy to locate on the public record) they convinced Site5 staff to add their email address to the account and make it the primary login”
- DeFi Hacks (2020-)
- List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses [link] (old)

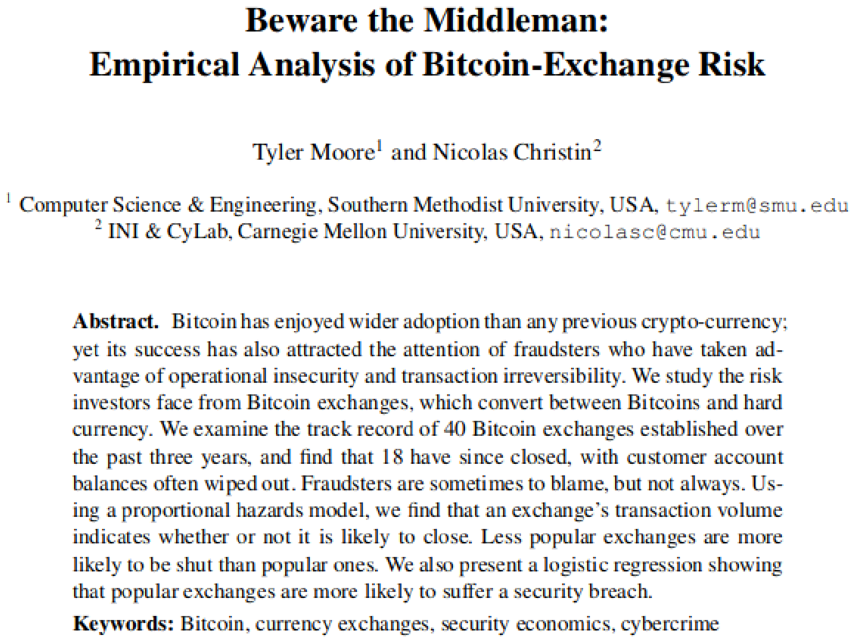
Security Concerns (Theft)

- Outsourcing infrastructure to the cloud

  → outsource the risk!

  - E.g., Bitcoin-Central, Bitcoinica could have had a “secure” system during the theft
- DDoS against Mt. Gox – “Layer 7” April 2013
  - Trading engine lag ~75min.
  - Panic sells – market drop
- Mt.Gox closed, Bitfloor closed, Bitcoin24 closed, many others

- 45 percent of Bitcoin exchanges end up closing [link]
  - 40 Bitcoin exchange sites analyzed over 3 years, 18 closed
  - 5 closed exchange sites - no reimbursement



Beware the Middleman:
Empirical Analysis of Bitcoin-Exchange Risk

Tyler Moore[1] and Nicolas Christin[2]

[1] Computer Science & Engineering, Southern Methodist University, USA, tylerm@smu.edu
[2] INI & CyLab, Carnegie Mellon University, USA, nicolasc@cmu.edu

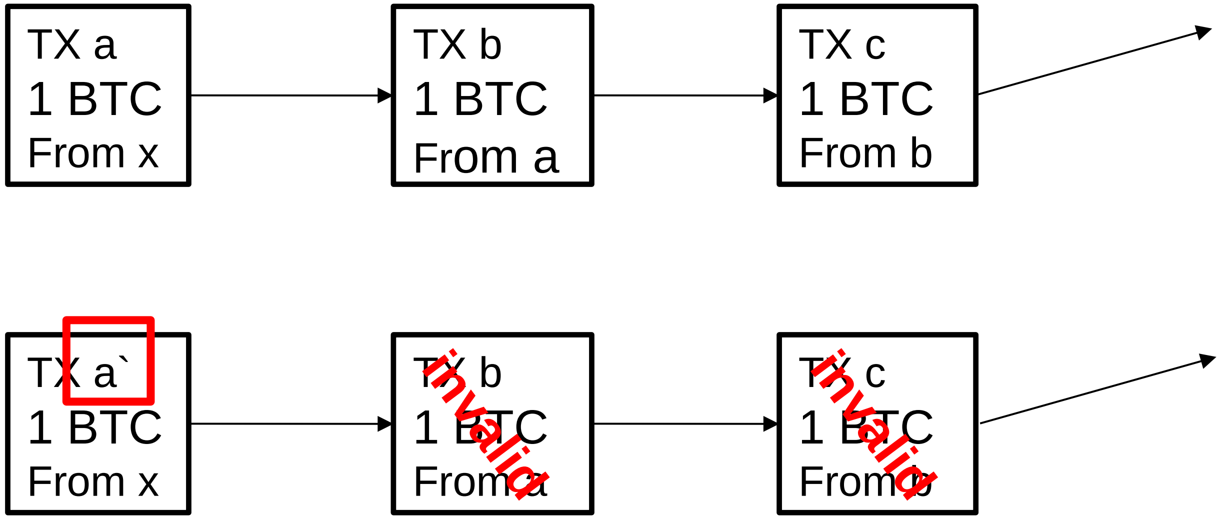
Abstract. Bitcoin has enjoyed wider adoption than any previous crypto-currency; yet its success has also attracted the attention of fraudsters who have taken advantage of operational insecurity and transaction irreversibility. We study the risk investors face from Bitcoin exchanges, which convert between Bitcoins and hard currency. We examine the track record of 40 Bitcoin exchanges established over the past three years, and find that 18 have since closed, with customer account balances often wiped out. Fraudsters are sometimes to blame, but not always. Using a proportional hazards model, we find that an exchange’s transaction volume indicates whether or not it is likely to close. Less popular exchanges are more likely to be shut than popular ones. We also present a logistic regression showing that popular exchanges are more likely to suffer a security breach.

Keywords: Bitcoin, currency exchanges, security economics, cybercrime

Security Concerns (Mt.Gox – Lecture 09)

- Transaction malleability
  - Known since May 2011
  - Transactions are identified by the SHA256
  - Malleability = change data in transaction to change transaction hash, but transaction remains valid (signature still verifiable)
- Signature Malleability
  - Signature is DER-encoded ASN.1, OpenSSL
  - OpenSSL parser not strict (~HTML browser)
- scriptSig Malleability
  - Signature may not sign any data structure containing itself
    - Use OP_0, replace later. Script may be encoded in several different ways

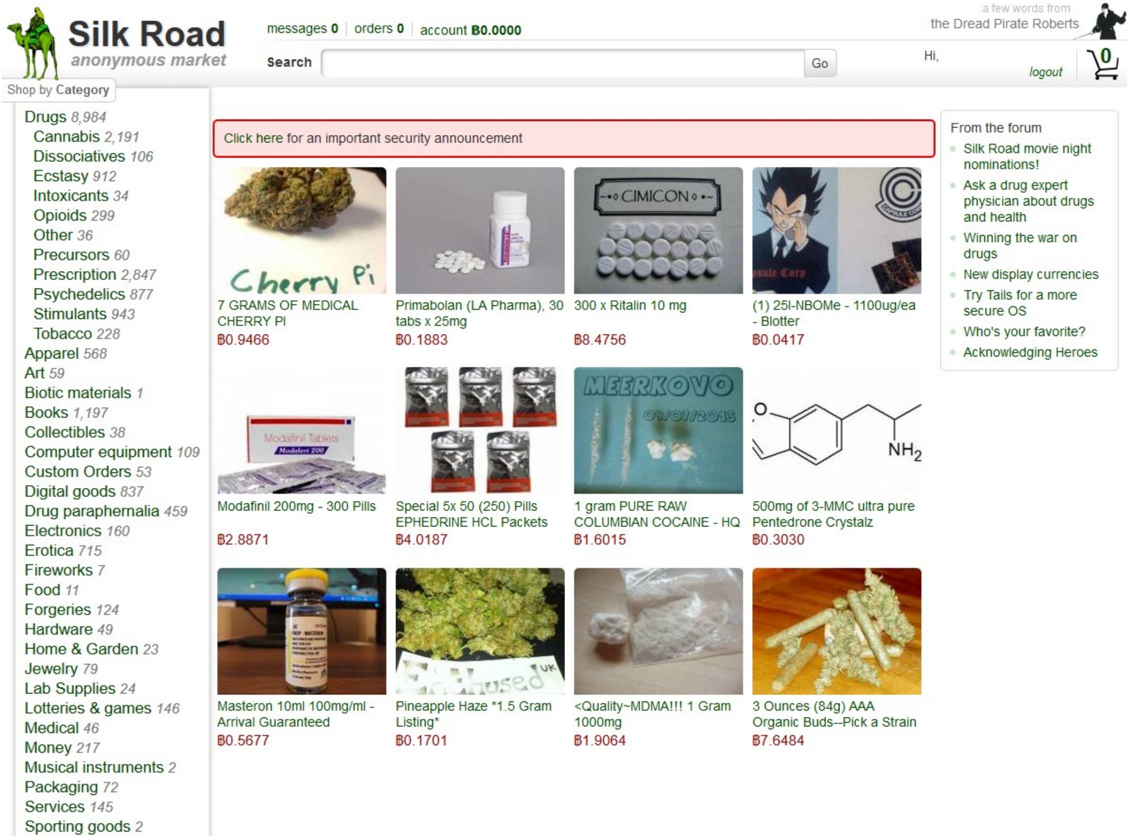
- Chained transactions (not broadcasted yet)
  - References to TX with hash and index



Broadcasted and valid

Security Concerns (Silk Road)

- Founded in February 2011 by “Dread Pirate Roberts“
  - Mainly illegal goods (“eBay for drugs”)
  - Connection through Tor hidden service, payment in Bitcoins
  - 1.2m USD revenue per month,
    92K USD commissions per month
  - Up to 150’000 active customers ~4’000 vendors
    900’000 registered users
  - “... $1.2 billion in transactions were made through the Silk Road.”



Drugs 8,984
- Cannabis 2,191
- Dissociatives 106
- Ecstasy 912
- Intoxicants 34
- Opioids 299
- Other 36
- Precursors 60
- Prescription 2,847
- Psychedelics 877
- Stimulants 943
- Tobacco 228

Apparel 568
Art 59
Biotic materials 1
Books 1,197
Collectibles 38
Computer equipment 109
Custom Orders 53
Digital goods 837
Drug paraphernalia 459
Electronics 160
Erotica 715
Fireworks 7
Food 11
Forgeries 124
Hardware 49
Home & Garden 23
Jewelry 79
Lab Supplies 24
Lotteries & games 146
Medical 46
Money 217
Musical instruments 2
Packaging 72
Services 145
Sporting goods 2

Click here for an important security announcement

7 GRAMS OF MEDICAL CHERRY PI
฿0.9466

Primabolan (LA Pharma), 30 tabs x 25mg
฿0.1883

300 x Ritalin 10 mg
฿8.4756

(1) 25I-NBOMe - 1100ug/ea - Blotter
฿0.0417

Modafinil 200mg - 300 Pills
฿2.8871

Special 5x 50 (250) Pills EPHEDRINE HCL Packets
฿4.0187

1 gram PURE RAW COLUMBIAN COCAINE - HQ
฿1.6015

500mg of 3-MMC ultra pure Pentedrone Crystalz
฿0.3030

Masteron 10ml 100mg/ml - Arrival Guaranteed
฿0.5677

Pineapple Haze *1.5 Gram Listing*
฿0.1701

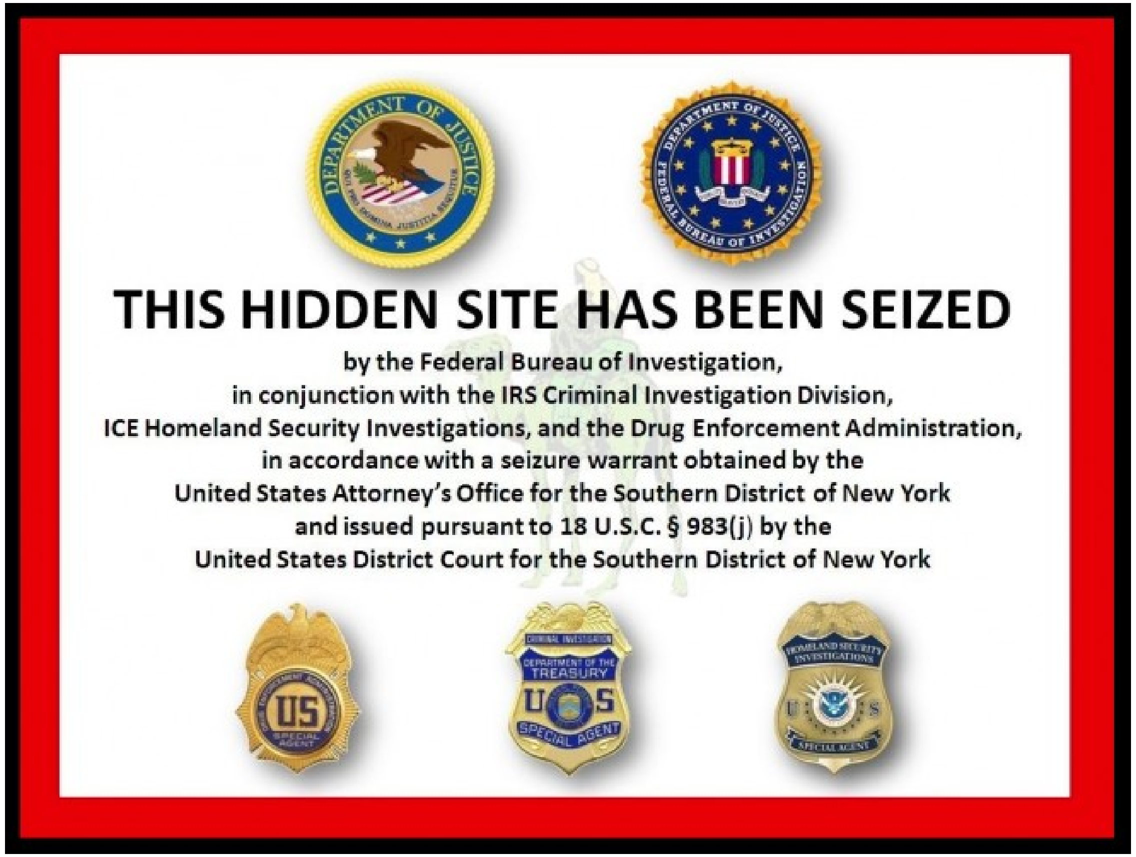
<Quality~MDMA!!! 1 Gram 1000mg
฿1.9064

3 Ounces (84g) AAA Organic Buds--Pick a Strain
฿7.6484

From the forum
- Silk Road movie night nominations!
- Ask a drug expert physician about drugs and health
- Winning the war on drugs
- New display currencies
- Try Tails for a more secure OS
- Who's your favorite?
- Acknowledging Heroes

Security Concerns (Silk Road)

- Take down Oct 2, 2013
  - Could link a forum account of Silk Road to a Gmail account [link]
  - Logged in to his account
- Assets seized:
  - Over 144’000 BTC from Ulbricht, 5 million USD from MtGox frozen
  - “In fact, the 174,000 or so bitcoins that the FBI controls now account for about 1.5% of all bitcoins in circulation.” [link]
- Successors already in place
  - Silk Road 2.0, Silk Road 3.0, OpenBazaar?



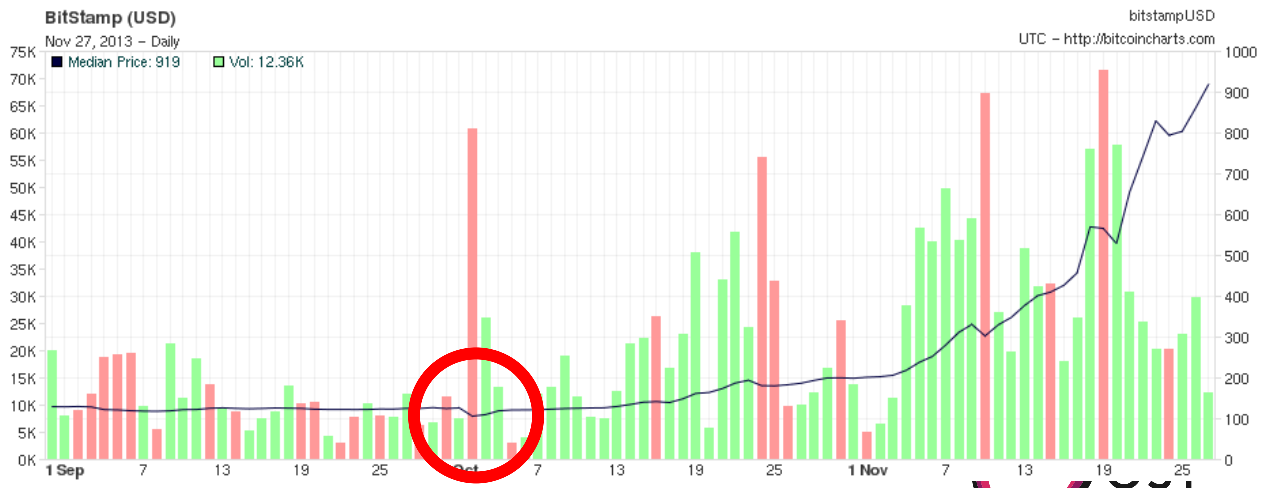
THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation,
in conjunction with the IRS Criminal Investigation Division,
ICE Homeland Security Investigations, and the Drug Enforcement Administration,
in accordance with a seizure warrant obtained by the
United States Attorney’s Office for the Southern District of New York
and issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

Ross Ulbricht

- Double life sentence plus forty years without the possibility of parole (wikipedia)
- Drug market place vs. free market experiment with user anonymity
  - “people should have the right to buy and sell whatever they wanted so long as they were not hurting anyone else”
- 03.10.2018 Lyn Ulbricht, leader of the Free Ross campaign
  - First-time, nonviolent offender
  - One of the 17,000 nonviolent drug offenders serving life in prison in the US

- freeross.org
  - “A former DEA agent pleaded guilty Wednesday to money laundering, obstruction of justice and extortion for his actions during the two years he spent investigating the online drug marketplace Silk Road as an undercover agent.” (source)


BitStamp (USD)
Nov 27, 2013 – Daily
bitstampUSD
UTC – http://bitcoincharts.com
■ Median Price: 919
□ Vol: 12.36K
75K
70K
65K
60K
55K
50K
45K
40K
35K
30K
25K
20K
15K
10K
5K
0K
1 Sep
Oct
1 Nov