

HS18

DISTRIBUTED SYSTEMS ADVANCED & BLOCKCHAIN

Security Considerations

T. Bocek

thomas.bocek@hsr.ch

■ 07.10.2018 [Tell HN: Executing a 51% attack on a real live Cryptocurrency, livestream](#)

- Not sure if this happened
- Nevertheless, 51% is an [issue](#)
- Small blockchains: PoS is important

■ Ethereum Block Size

- Getting big...

Client / Mode	Block Number	Disk Space
=====	=====	=====
parity light	5_600_000	89M
parity warp fast	5_600_000	82G
parity full fast	5_600_000	78G
parity full archive	5_600_000	1.1T

■ 04.10.2018 [Venezuela's Petro White Paper 'Blatantly' Copied Dash, Ethereum Developer Says](#)

- Petro has to be used to pay for [passport](#)
- “Bloomberg notes that around 5,000 citizens flee Venezuela each day.”

■ 02.10.2018 [I Analyzed 258 Decentralized Exchanges and This Is What I Found](#)

- Liquidity, UX, trustless, low fees, ...

■ 01.10.2018 [Why P2P deserves another chance](#)

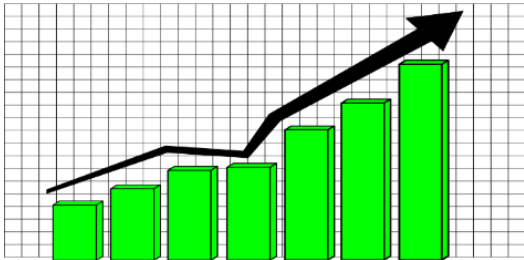
- “Think of what happens when your app is purely P2P: now you're not spinning up a server, paying for monitoring, or listening to a pager.”

URL: b.socrative.com/student/

Room: HSR

■ Advantages

- «Low» (fixed) tx fees
 - [4 satoshi](#) per byte ([chart](#))
- Scalable
 - Hardware/storage gets faster



- Anonymity
 - No privacy concerns/ datamining difficult

■ Disadvantages

- [Power consumption](#)
 - ~ 8400 Megawatt (KKW Beznau ~730MW)
- Not scalable
 - [Bitcoin with 3-7 tps](#) vs. VISA 57,000 tps (23.12) [tps: transactions per sec]

- Anonymity
 - Can be used for illegal activities





■ Ransomware

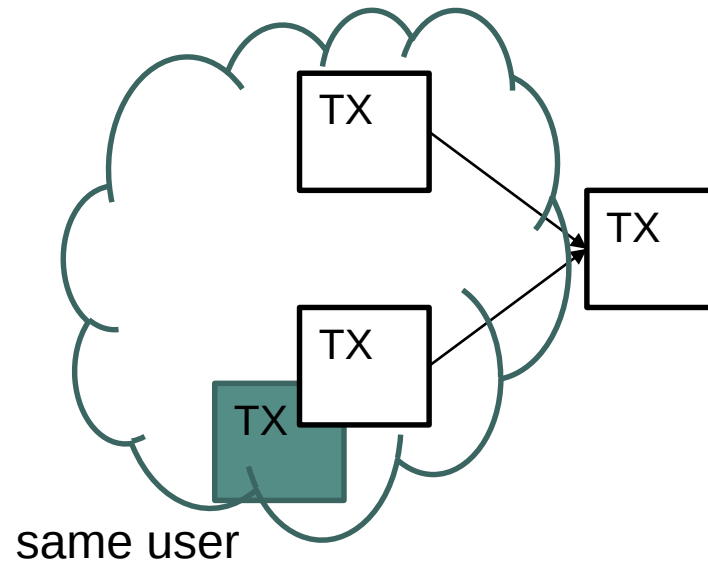
- Encrypt files, delete original
- Only decrypt if payed in BTC

■ 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](#))

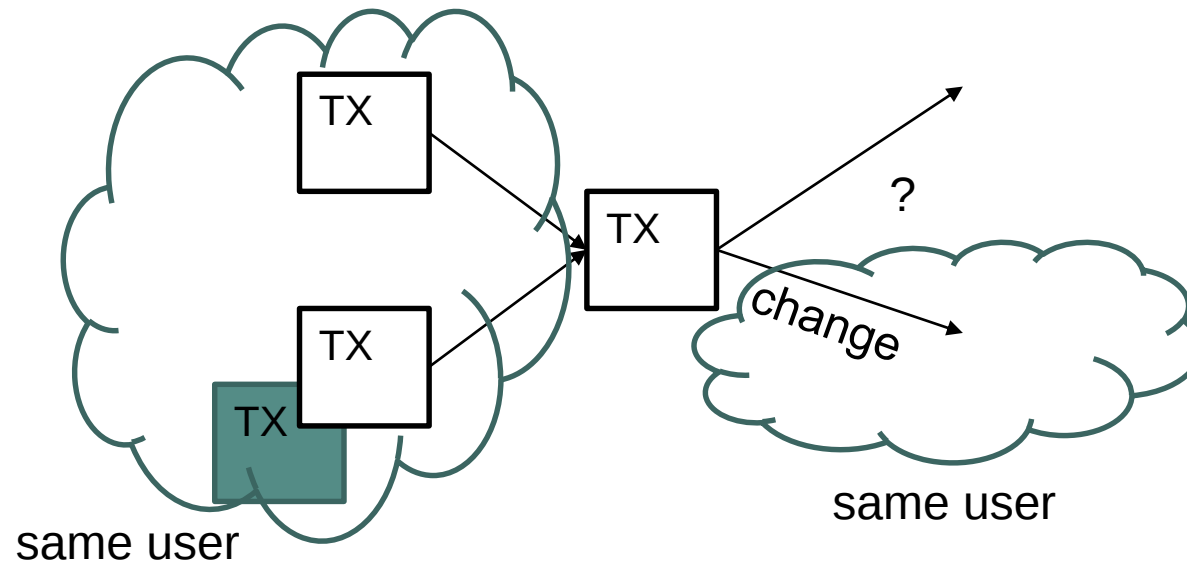
Anonymity

- 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 $pk \in \text{inputs}(t)$ are controlled by the same user.



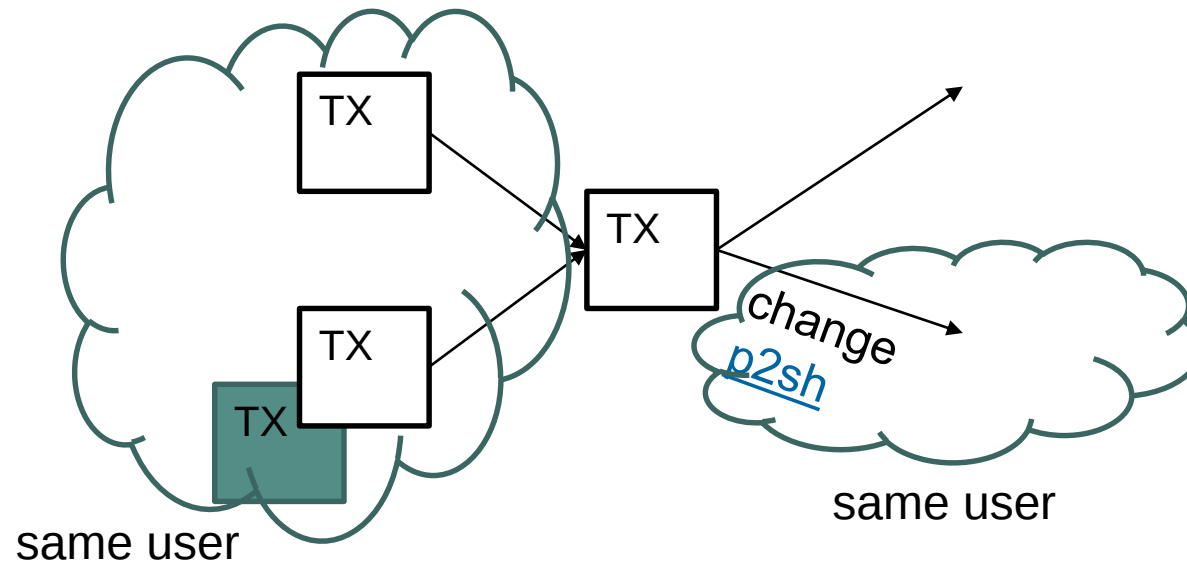
■ HEURISTIC 2.

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



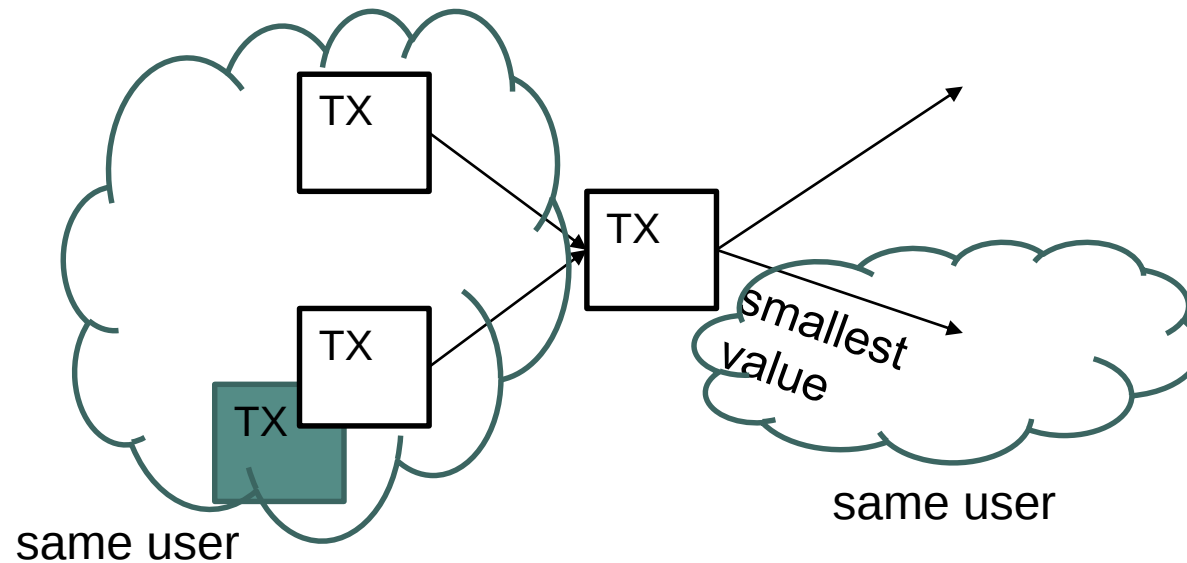
■ HEURISTIC 3

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



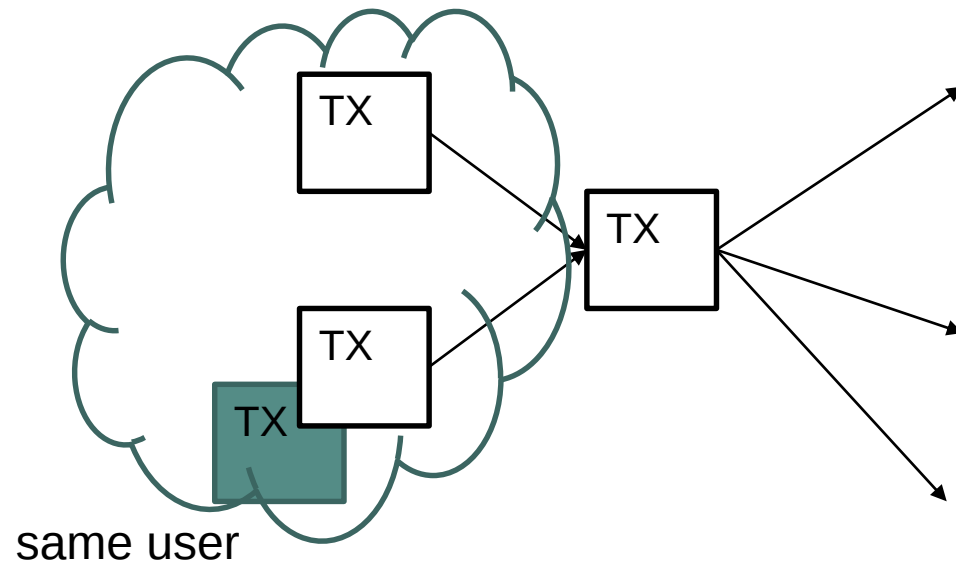
■ OPTIMAL CHANGE HEURISTIC

- 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.



■ 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

- **Every transaction on Ethereum / Bitcoin is public**
 - Someone selling MOD tokens, immediately public discussions in the Telegram channel

Yes Andrew, that "must" be the reason



Steven

Andrew
Why?

Zero communication... no profit forecasts....

*forecast

Pi Ko joined the group



Crypto Crave

Will Modum always be an ERC-20 token?



Steven

Haha great

everything is green..



Dranmi

Andrew
Why?

Because someone sent 350.000 Mod to binance recently 🤔

URL: b.socrative.com/student/

Room: HSR

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\$, now ~\$160 mio)
- 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 (now ~\$2.2mio)

- 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”

■ List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses

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
- [Christan Decker Theft](#) (2012) ~ 9222BTC (now ~62mio)
- 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](#)
 - 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 Moore¹ and Nicolas Christin²

¹ Computer Science & Engineering, Southern Methodist University, USA, tylerm@smu.edu

² INI & CyLab, Carnegie Mellon University, USA, nicolasc@cmu.edu

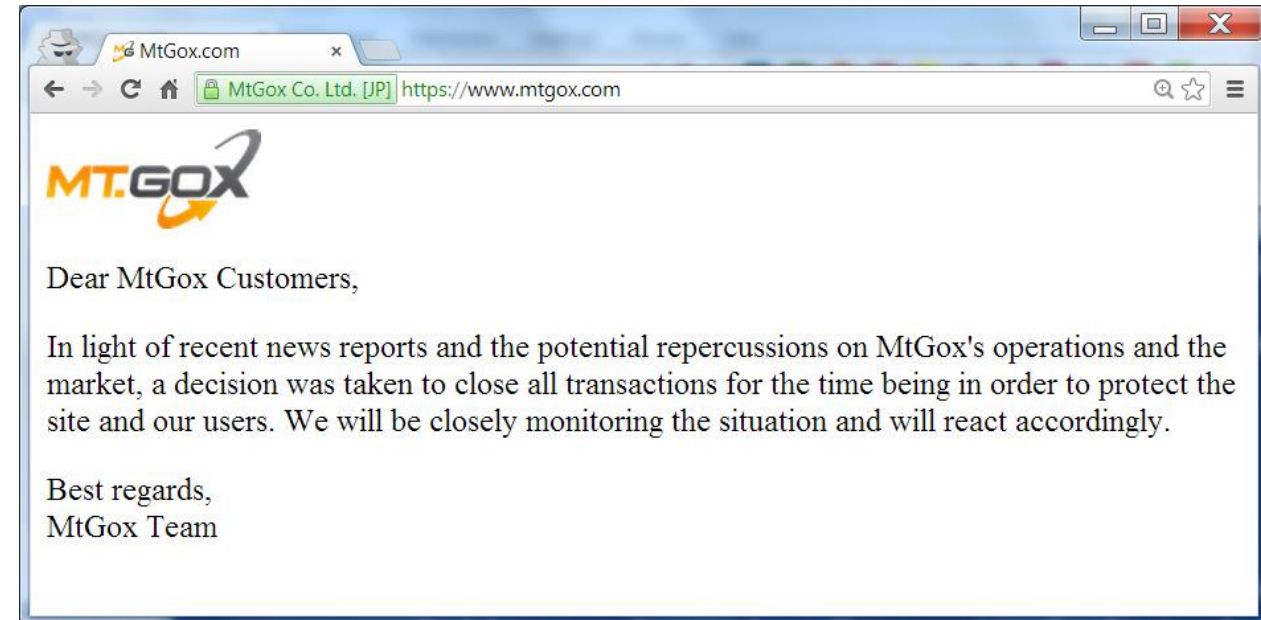
Abstract. Bitcoin has enjoyed wider adoption than any previous crypto-currency; yet its success has also attracted the attention of fraudsters who have taken advantage of operational insecurity and transaction irreversibility. We study the risk investors face from Bitcoin exchanges, which convert between 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)

- Mt. Gox (short for Magic: The Gathering Online Exchange)
 - July 2010 reused domain name, started Bitcoin trading platform
- **April 2013, handled 70% of Bitcoin trades**
- **November 2013, users reported payout delays**
 - Exchange rates different from other trading platforms
- **7. February 2014, suspended all BTC withdrawals**
 - “Bug in the Bitcoin system”: transaction malleability
- **20. February, suspended all withdrawals**

- **24. February, all trading suspended, blank page**
- **9. March 2014, filed for bankruptcy**



Security Concerns (Mt.Gox)

■ 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

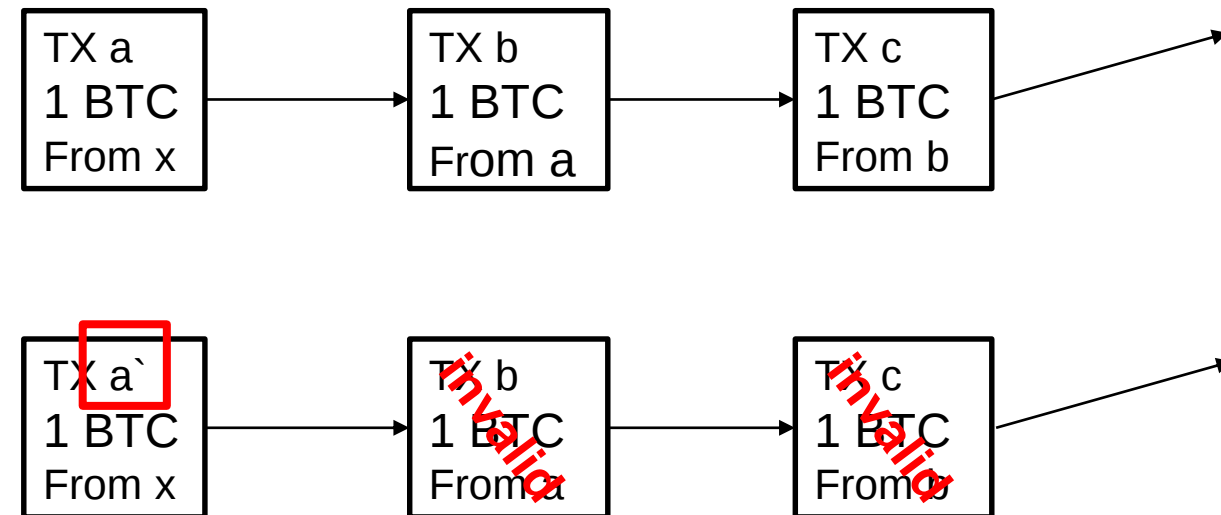
- Signature is DER-encoded ASN.1, OpenSSL
- OpenSSL parser not strict (~HTML browser)

■ 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

Transaction Malleability / Mt. Gox now

■ Bitcoin Transaction Malleability and MtGox

- Christian Decker, Roger Wattenhofer ETH

■ **Measurements**

- Created specialized nodes that would trace all transactions from 2013
- 302,700 bitcoins that were involved in malleability attacks
- Successful attacks: 64,564 bitcoins
- Attacks before stopping withdrawal (7.Feb): **1,811 bitcoins,**
- **~successful 386 bitcoins**

■ **Mt.Gox: 850`000 bitcoins lost**

- Majority of Attacks happened after the malleability press release

■ **20 March 2014: found 199999.99 bitcoins**

■ **April 2015**

- "most or all of the missing bitcoins were stolen straight out of the Mt. Gox hot wallet over time, beginning in late 2011."

■ **March 2018: enough BTC has been sold to cover the claims of creditors**

- Lost 473 m\$ in 2014, found 200k BTC, now worth 1.2 b\$
- price was \$483, now around \$6700
- "between December 2017 and February 2018 and has been repeatedly blamed for causing the price of BTC to crash" ([source](#))
- Rest will be distributed

URL: b.socrative.com/student/

Room: HSR

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.”

The screenshot shows the Silk Road anonymous market website. At the top, there's a navigation bar with a camel logo, the text "Silk Road anonymous market", and user statistics: "messages 0 | orders 0 | account B0.0000". A search bar is present with a "Go" button. Below the navigation bar, there's a "Shop by Category" sidebar listing various categories like Drugs, Cannabis, Ecstasy, etc., with item counts. The main content area displays a grid of product listings, each with an image, a title, and a price in Bitcoin (B0). Examples include "Cherry Pi", "Primobolan (LA Pharma)", "300 x Ritalin 10 mg", and "1 gram PURE RAW COLUMBIAN COCAINE". A red banner at the top of the main area says "Click here for an important security announcement". On the right side, there's a "From the forum" section with links to various forum topics.

Shop by Category

- 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

messages 0 | orders 0 | account B0.0000

Search Go Hi, logout

Click here for an important security announcement

Cherry Pi
7 GRAMS OF MEDICAL CHERRY PI
B0.9466

Primobolan (LA Pharma), 30 tabs x 25mg
B0.1883

300 x Ritalin 10 mg
B8.4756

(1) 25I-NBOMe - 1100ug/ea - Blotter
B0.0417

Modafinil 200mg - 300 Pills
B2.8871

Special 5x 50 (250) Pills EPHEDRINE HCL Packets
B4.0187

1 gram PURE RAW COLUMBIAN COCAINE - HQ
B1.6015

500mg of 3-MMC ultra pure Pentadone Crystall
B0.3030

Masteron 10ml 100mg/ml - Arrival Guaranteed
B0.5677

Pineapple Haze *1.5 Gram Listing*
B0.1701

<Quality~MDMA!!! 1 Gram 1000mg
B1.9064

3 Ounces (84g) AAA Organic Buds--Pick a Strain
B7.6484

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](#)
- 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."*](#)

■ Successors already in place

- Silk Road 2.0, Silk Road 3.0, OpenBazaar?



- **“Ross William Ulbricht (born March 27, 1984) is a convicted American drug trafficker and darknet market operator” ([wikipedia](#))**

- Double life sentence plus forty years without the possibility of parole.

- **Silk Road: 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

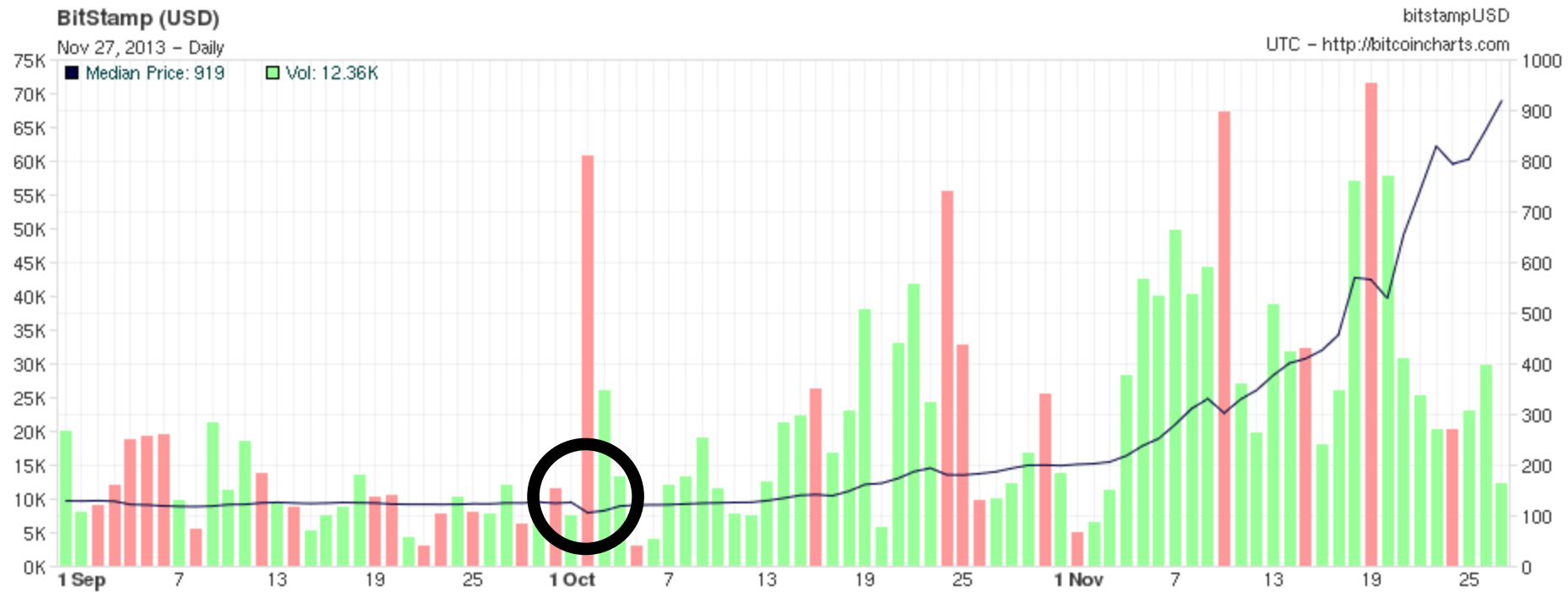
- **[freeross.org](#)**

- “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](#))
- Silk Road 2.0 Blake Benthall
- <https://www.blockchain.com/btc/address/1Ross5Np5doy4ajF9iGXzgKaC2Q3Pwwwxv>

Security Concerns (Silk Road)

■ Exchange rate development

- Not much happened



Questions?

Prof. Dr. Thomas Bocek thomas.bocek@hsr.ch
Roman Blum roman.blum@hsr.ch