Bitcoin and Cryptocurrencies

Lecture 4: Bitcoin In Real Life: Wallets, Mining, and More

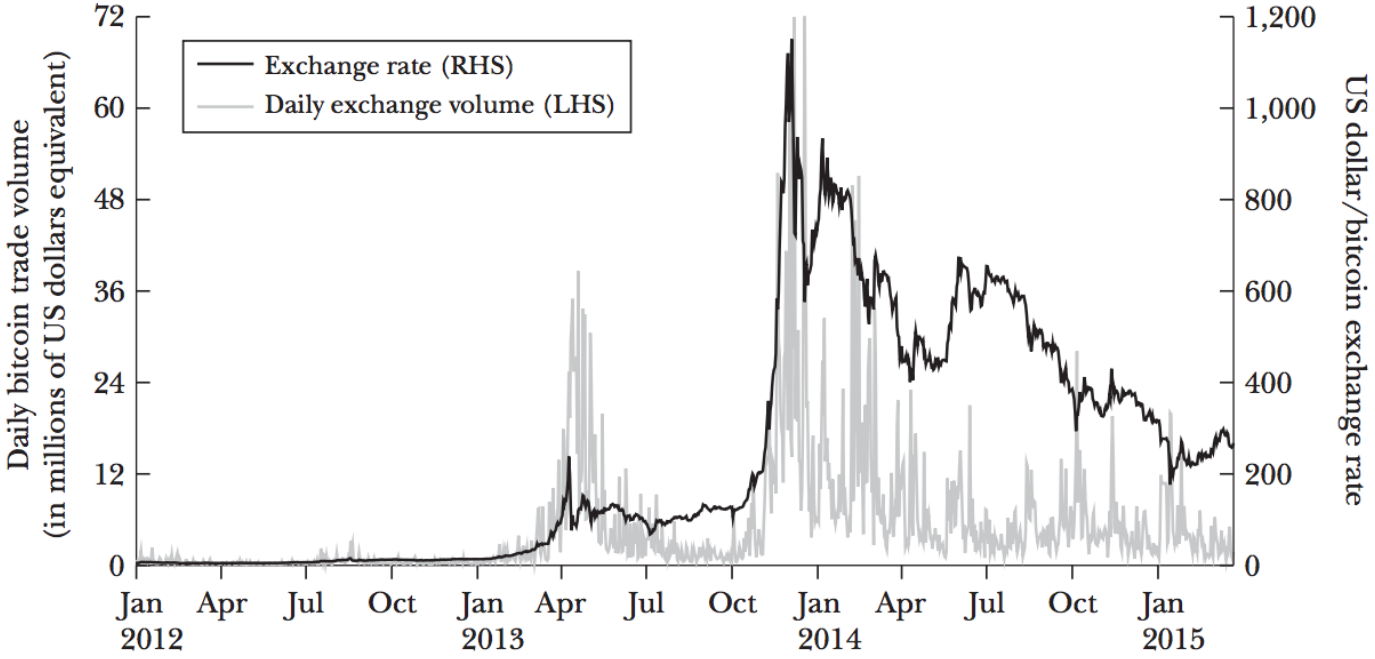
Professor Radjabov Mukhammad

Risks in Bitcoin

1. Market Risk
2. Shallow Markets Problem
3. Counterparty Risk
4. Transaction Risk
5. Operational Risk
6. Privacy-Related Risk
7. Legal and Regulatory Risk

1. Market Risk

US Dollar–Bitcoin Exchange Rate, January 2012–March 2015, along with Daily Bitcoin Trade Volume (in US Dollar Equivalent) at Four Top Currency Exchanges

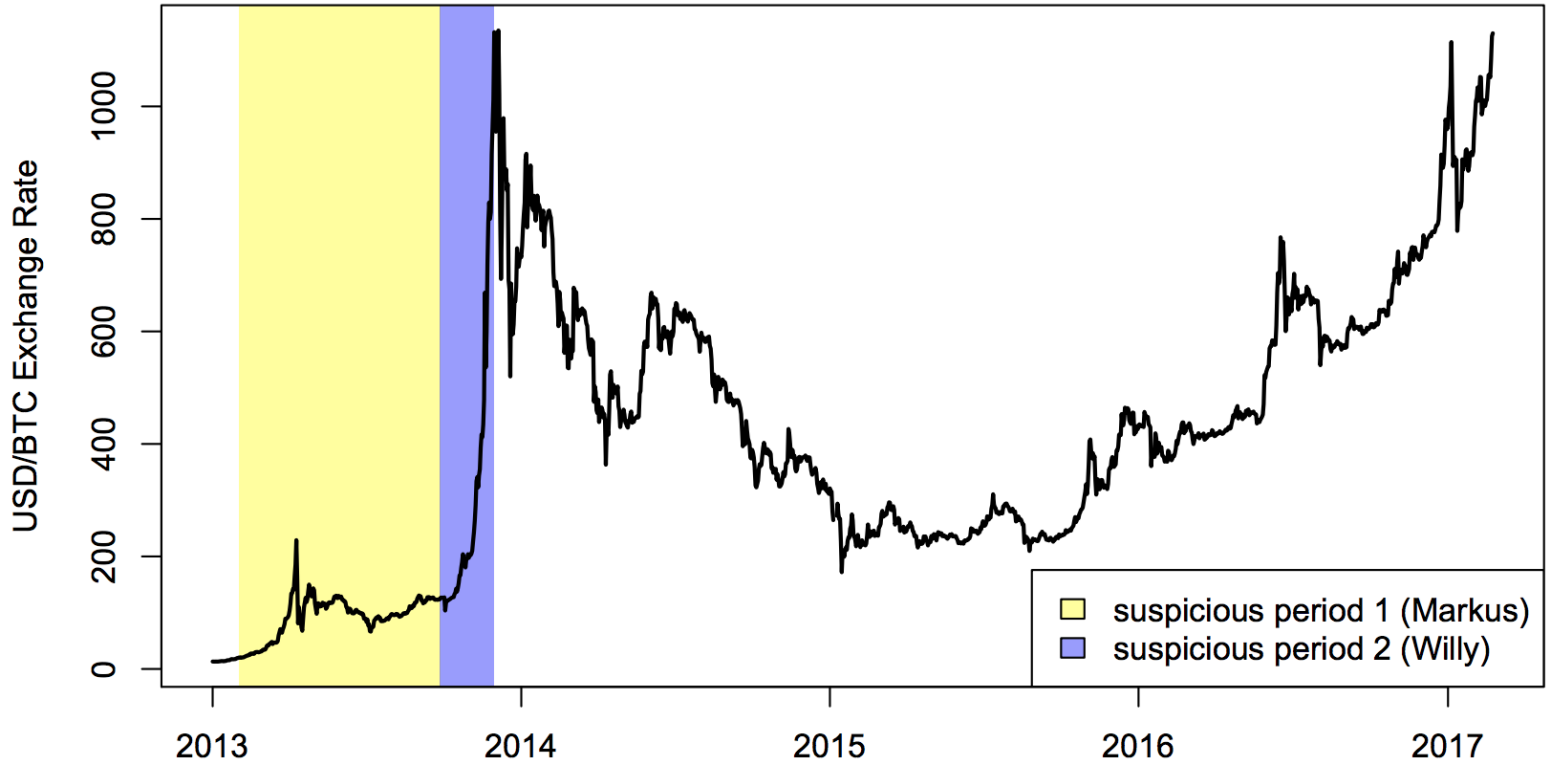


Market Price (USD)

Average USD market price across major bitcoin exchanges.

Source: blockchain.info

Market Risk or Price Manipulation?



Market Risk or Price Manipulation

Table: Average daily rate changes in USD-BTC exchange rate by period in $, %

	2012-12-01 2013-02-28	2013-03-01 2013-05-31	2013-06-01 2013-08-31		2013-09-01 2013-11-30	
			Markus active	Markus not active	Willy active	Willy not active
Rate change $	0.21	1.00	3.15	-0.51	**21.85**	**-0.88**
% change	1.0	1.8	**2.9**	**-0.5**	**5.0**	**-0.2**
# days	90	92	17	75	50	41

Gandal et. al, Journal of Monetary Economics: https://tylermoore.utulsa.edu/jme17.pdf

2. Shallow Markets Problem

Buying or selling large amounts of bitcoin will affect the market price

Many “Bitcoin Millionaires” cannot readily convert their fortunes into hard currency

3. Counterparty Risk

Exchanges serve as de facto banks

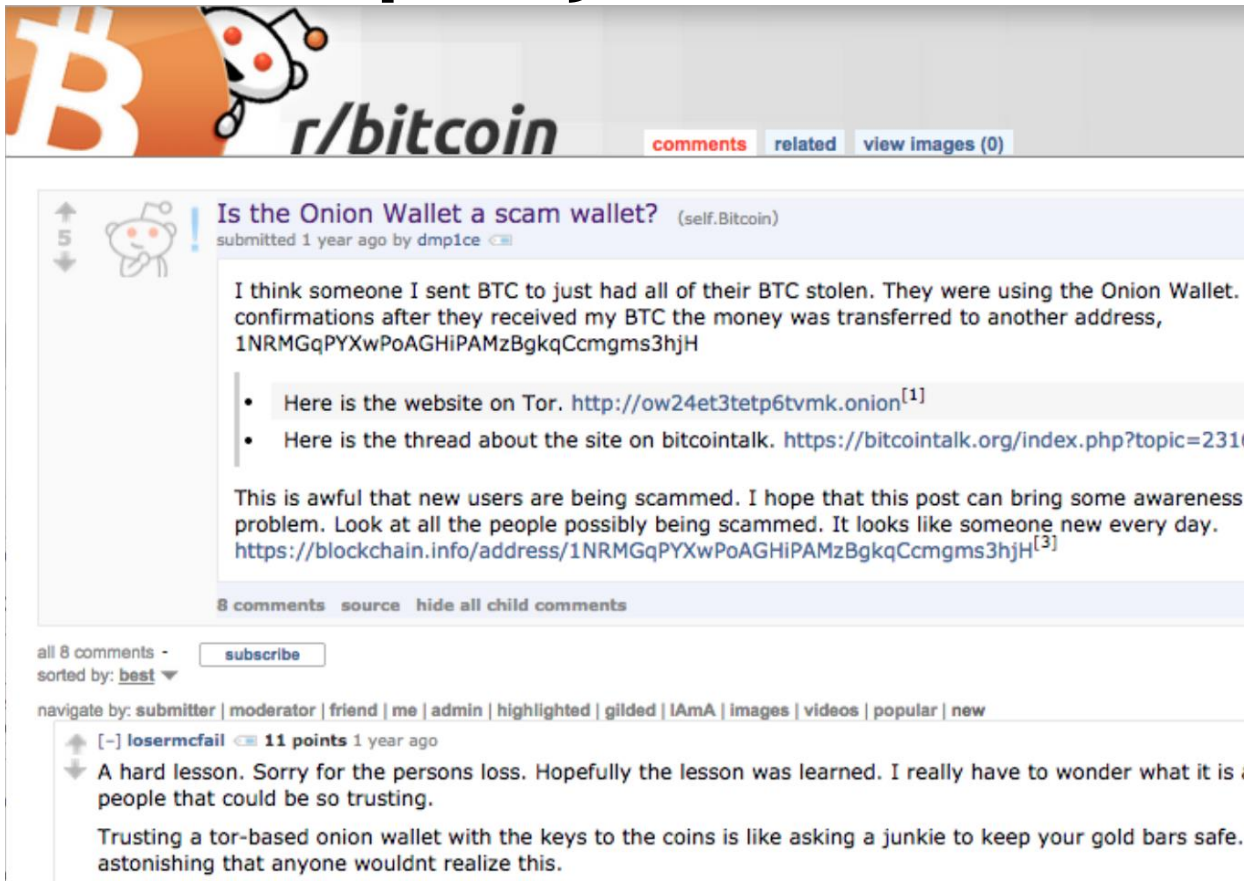
> Around half close, sometimes suddenly and without reimbursing customers (Moore and Christin, FC 2013)

Digital wallet services and exchanges are frequent targets for theft of coins

Some services are simply scams

3. Counterparty Risk

3. Counterparty Risk



r/bitcoin

comments related view images (0)

5

Is the Onion Wallet a scam wallet? (self.Bitcoin)

submitted 1 year ago by dmp1ce

I think someone I sent BTC to just had all of their BTC stolen. They were using the Onion Wallet. confirmations after they received my BTC the money was transferred to another address, 1NRMGqPYXwPoAGHiPAMzBgkqCcmgms3hjH

- Here is the website on Tor. http://ow24et3tetp6tvmk.onion[1]
- Here is the thread about the site on bitcointalk. https://bitcointalk.org/index.php?topic=231

This is awful that new users are being scammed. I hope that this post can bring some awareness problem. Look at all the people possibly being scammed. It looks like someone new every day. https://blockchain.info/address/1NRMGqPYXwPoAGHiPAMzBgkqCcmgms3hjH[3]

8 comments source hide all child comments

all 8 comments - subscribe

sorted by: best

navigate by: submitter | moderator | friend | me | admin | highlighted | gilded | IAmA | images | videos | popular | new

[–] losermcfail 11 points 1 year ago

A hard lesson. Sorry for the persons loss. Hopefully the lesson was learned. I really have to wonder what it is people that could be so trusting.

Trusting a tor-based onion wallet with the keys to the coins is like asking a junkie to keep your gold bars safe. astonishing that anyone wouldnt realize this.

3. Counterparty Risk

Scam	Lifetime		Payout to scammer	
	Days	Alive?	BTC	USD
Scam wallets	535	yes	4 105	$359 902
Scam exchanges				
BTC Promo	98	yes	44	$22 112
btcQuick		no	929	$73 218
CoinOpend	29	no	575	$264 466
Ubitex	91	no	30	$96[16]
Mining scams	Data Source			
Labcoin	Blockchain		241	$48 562
AMC	BitFunder		18 041	$1 327 590
Ice Drill	BitFunder		14 426	$1 558 008
Asic Mining	Blockchain		12.6	$5 532
Dragon Miner	Blockchain		1.63	$1 019

Vasek & Moore, Financial Crypto 2015: https://tylermoore.utulsa.edu/fc15.pdf

4. Transaction Risk

Irreversibility of bitcoin payments creates elevated transaction risk

- No clear resolution mechanism when fraud or error arises

Risks due to delay in clearing transactions

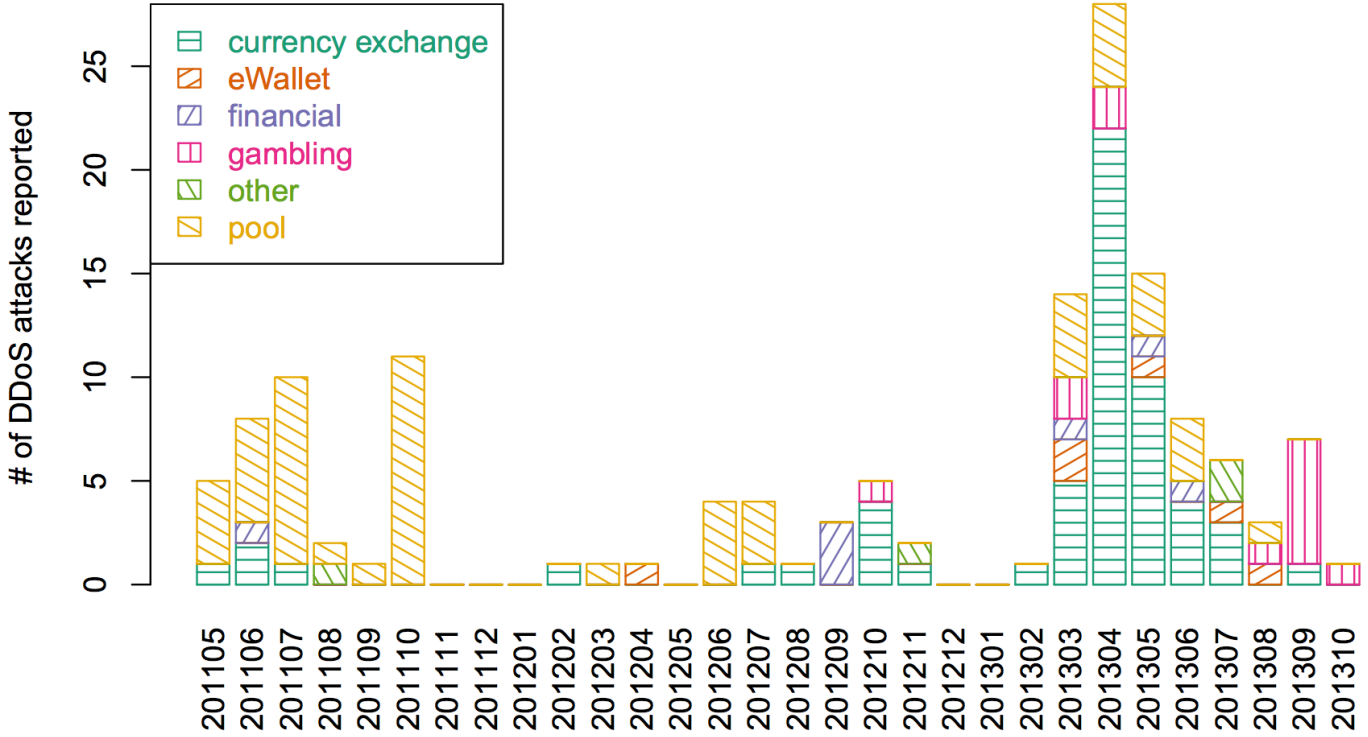
- Uncertainty over what becomes authoritative block
- Double-spending risk

5. Operational Risk

Any action that undermines Bitcoin's technical infrastructure and security assumptions

- Malware in wallets
- Operator error
- Vulnerabilities in bitcoin core software
- Distributed denial-of-service attacks

5. Operational Risk



Vasek, Thornton & Moore, BITCOIN 2014: https://tylermoore.utulsa.edu/bitcoin14ddos.pdf

6. Privacy Risk

Risk that transactions can be linked back to the people that made them

See Section 6.2 in the Princeton book

We now take a brief digression into how to de-anonymize Bitcoin

Overview

Risks in Bitcoin

Digression on deanonymizing transactions

Regulating Bitcoin

Some say Bitcoin provides anonymity

“ Bitcoin is a secure and anonymous digital currency ”

— WikiLeaks donations page

Others say it doesn’t

“ Bitcoin won't hide you from the NSA's prying eyes”

— Wired UK

What do we mean by anonymity?

Literally: anonymous = without a name

Bitcoin addresses are public key hashes rather than real identities

Computer scientists call this pseudonymity

Anonymity in computer science

Anonymity = pseudonymity + unlinkability

Different interactions of the same user with the system should not be linkable to each other

Pseudonymity vs anonymity in forums

Reddit: pick a long-term pseudonym

vs.

4Chan: make posts with no attribution at all

Defining unlinkability in Bitcoin

Hard to link different addresses of the same user

Hard to link different transactions of the same user

Hard to link sender of a payment to its recipient

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

`13DFamCvSxG8EG16VyXzdpfqxyooifswYx`

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

To generate a new, private address for your donation, click the refresh button above.

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

`16nLrMAQma6GJ4AavfxXLaZoeCHBBqqzX3`

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (http://bitcoin.org) or read more on Wikipedia.

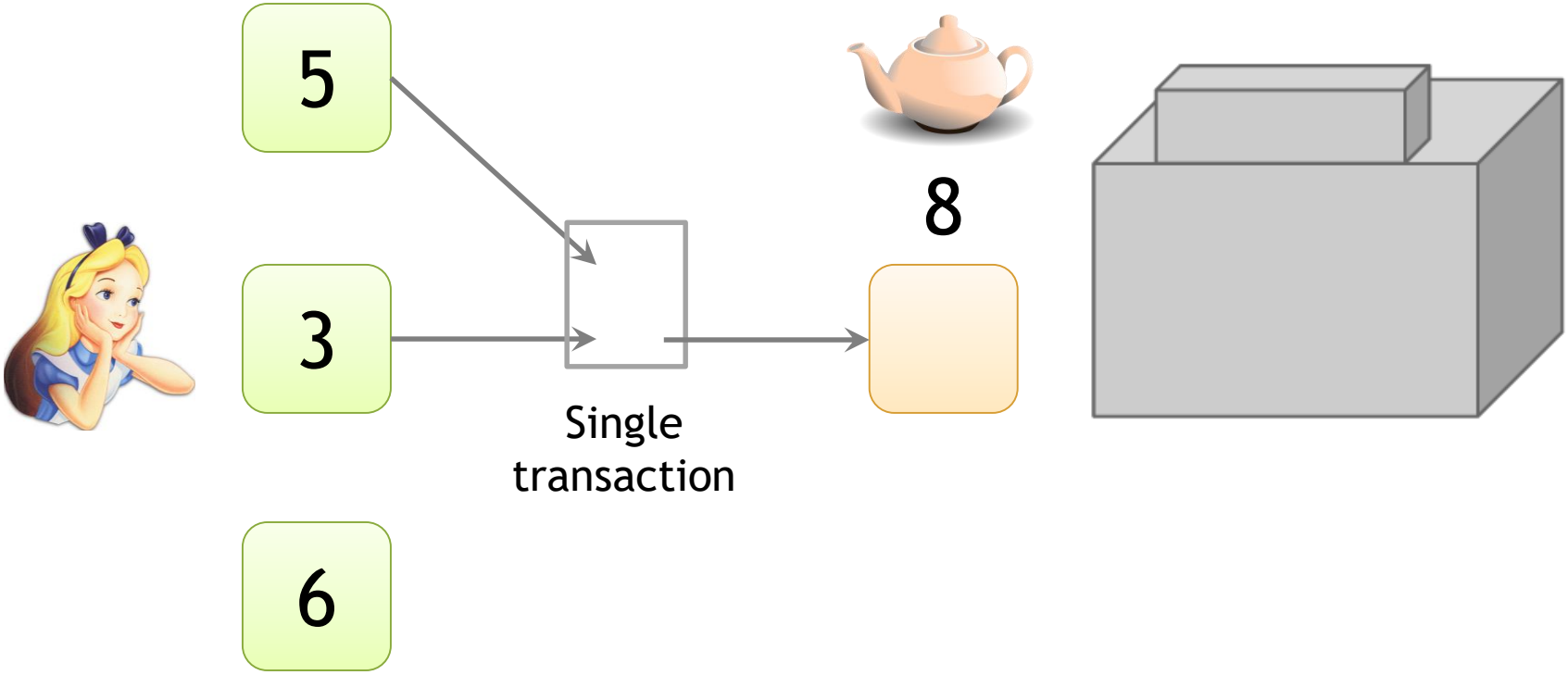
To generate a new, private address for your donation, click the refresh button above.

Trivial to create new address

Best practice: always receive at fresh address

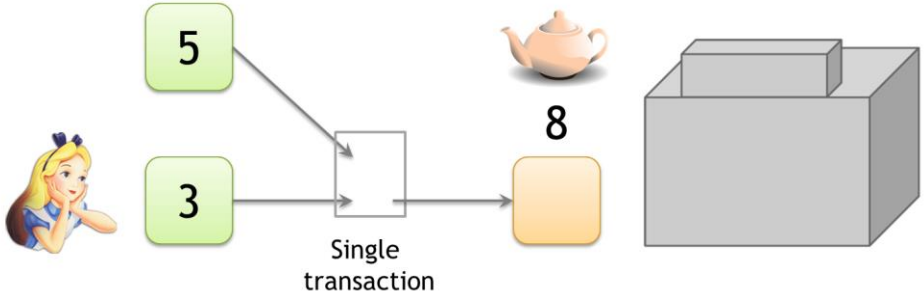
So, unlinkable?

Alice buys a teapot at Big box store



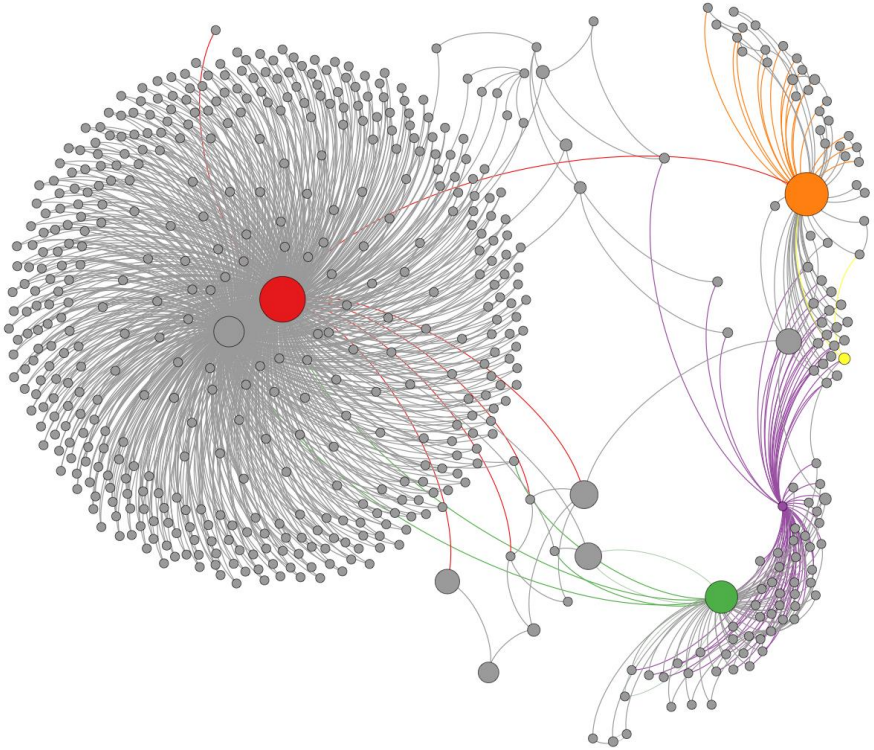
Linking addresses

Shared spending is evidence of joint control



Addresses can be linked transitively

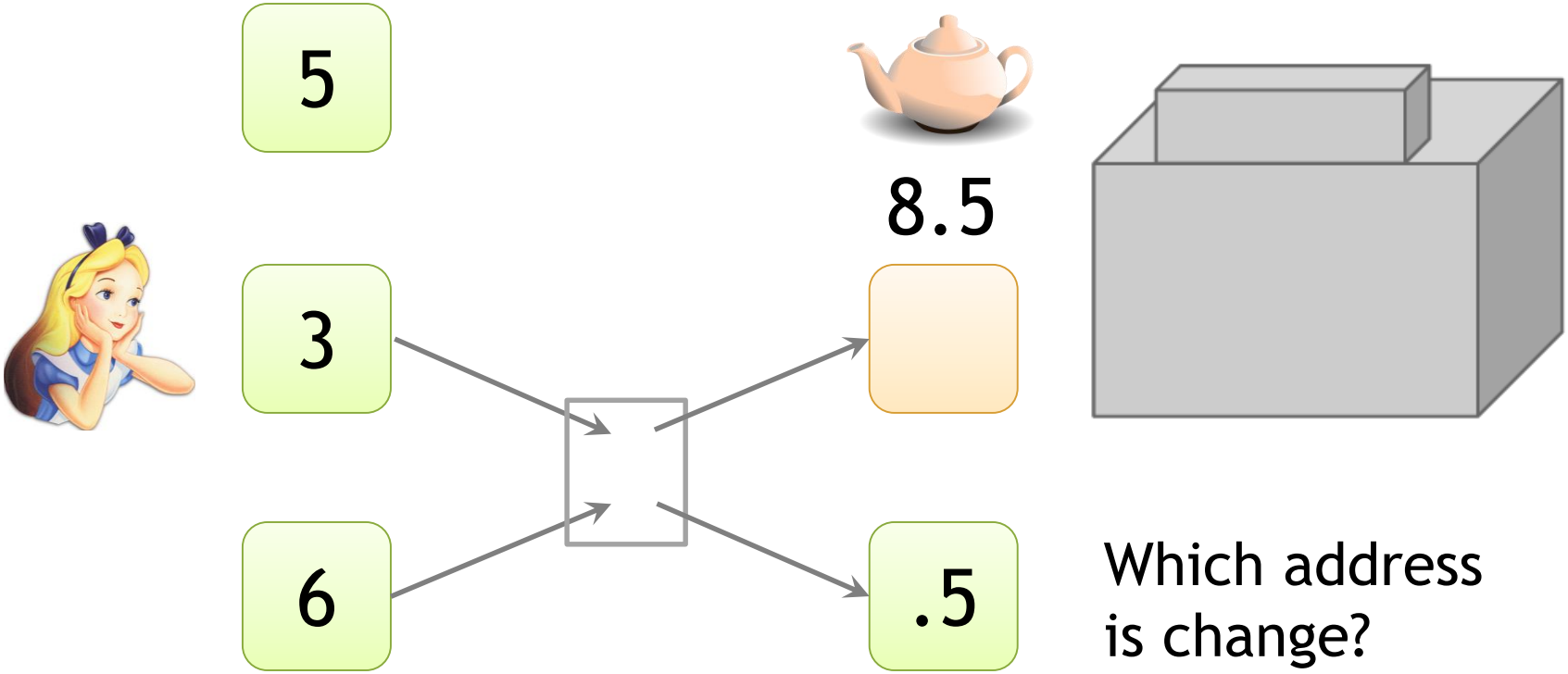
Clustering of addresses



An Analysis of Anonymity in the Bitcoin System

F. Reid and M. Harrigan
PASSAT 2011

Change addresses

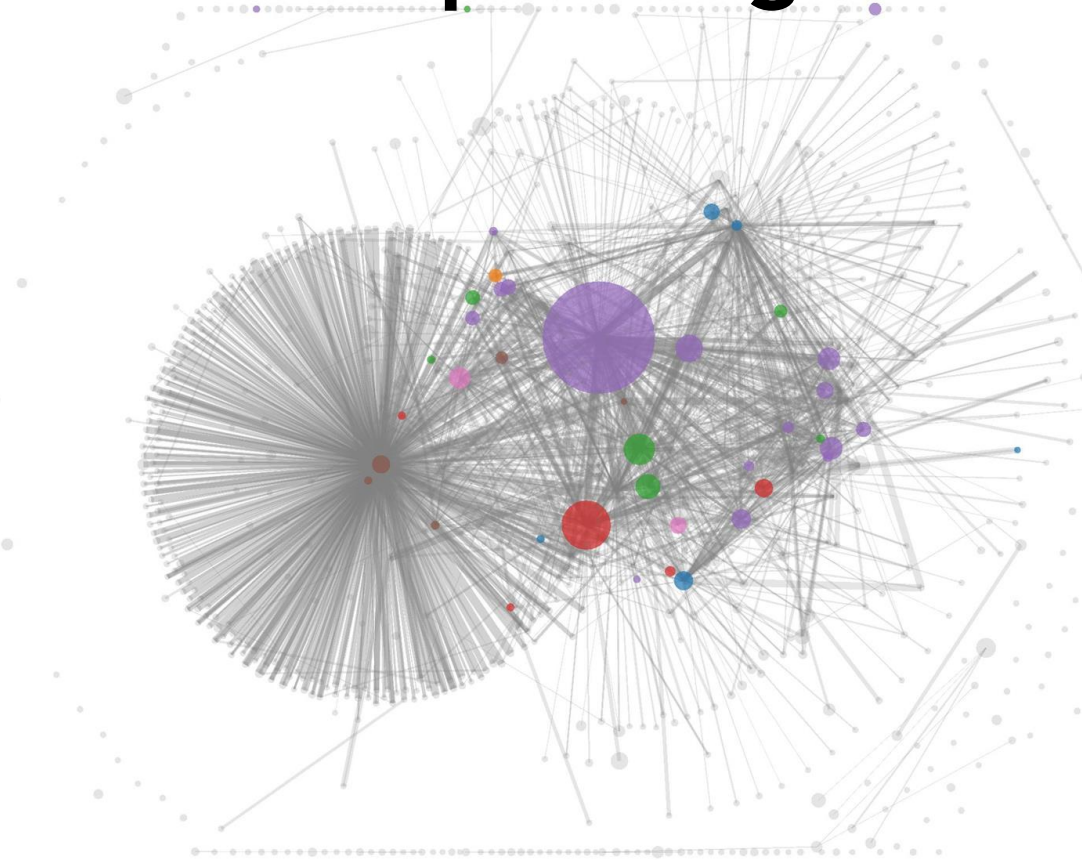


“Idioms of use”

Idiosyncratic features of wallet software

e.g., each address used only once as change

Shared spending + idioms of use



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.
IMC 2013

To tag service providers: transact!

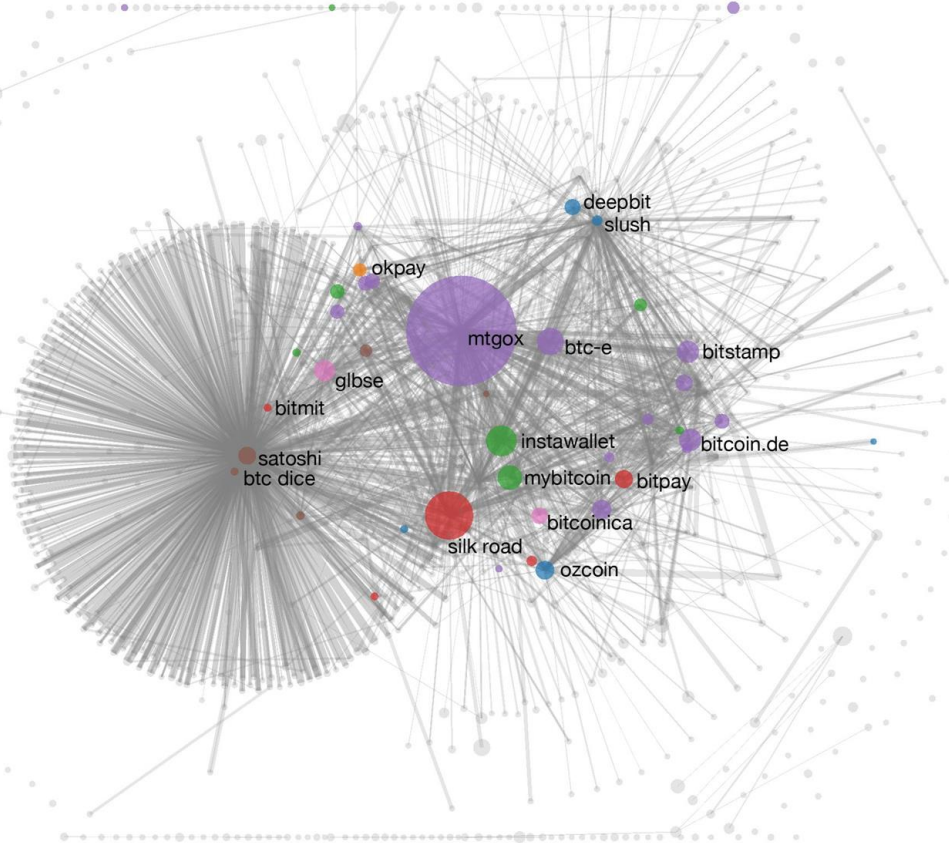
A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.

344 transactions

- Mining pools
- Wallet services
- Exchanges
- Vendors
- Gambling sites

Shared spending + idioms of use



A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

S. Meiklejohn et al.

From services to users

1. High centralization in service providers

   Most flows pass through one of these — in a traceable way

2. Address — identity links in forums

Conclusion

Virtual currencies create many opportunities, but also introduce many risks

As Bitcoin (or its successor) becomes more popular, regulation will inevitably take hold

Reference

The Bitcoin Standard: The Decentralized Alternative to Central Banking – Illustrated, April 24, 2018 by Saifedean Ammous

The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them (Cryptography, Crypto Trading, Derivatives, Digital Assets) – Illustrated, September 15, 2018 by Antony Lewis (Author)

Blockchain Bubble or Revolution: The Future of Bitcoin, Blockchains, and Cryptocurrencies – June 12, 2019 by Neel Mehta (Author), Aditya Agashe (Author), Parth Detroja (Author)

Cryptocurrency Investing For Dummies – March 6, 2019 by Kiana Danial

Cryptocurrency Mining For Dummies– Illustrated, December 5, 2019 by Peter Kent

Cryptocurrency Mining: A Complete Beginners Guide to Mining Cryptocurrencies, Including Bitcoin, Litecoin, Ethereum, Altcoin, Monero, and Others – February 21, 2018 by Crypto Tech Academy (Author)