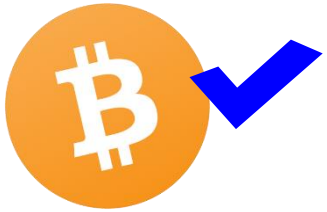
Bitcoin and Cryptocurrencies

- Lecture 1: Real-world aspects of Bitcoin
- Professor Radjabov Mukhammad

Bitcoin

- Intent of Bitcoin: replacing banks!



- Technical guarantees:
  - Distributed consensus
  - Pseudo-anonymous

Microsoft

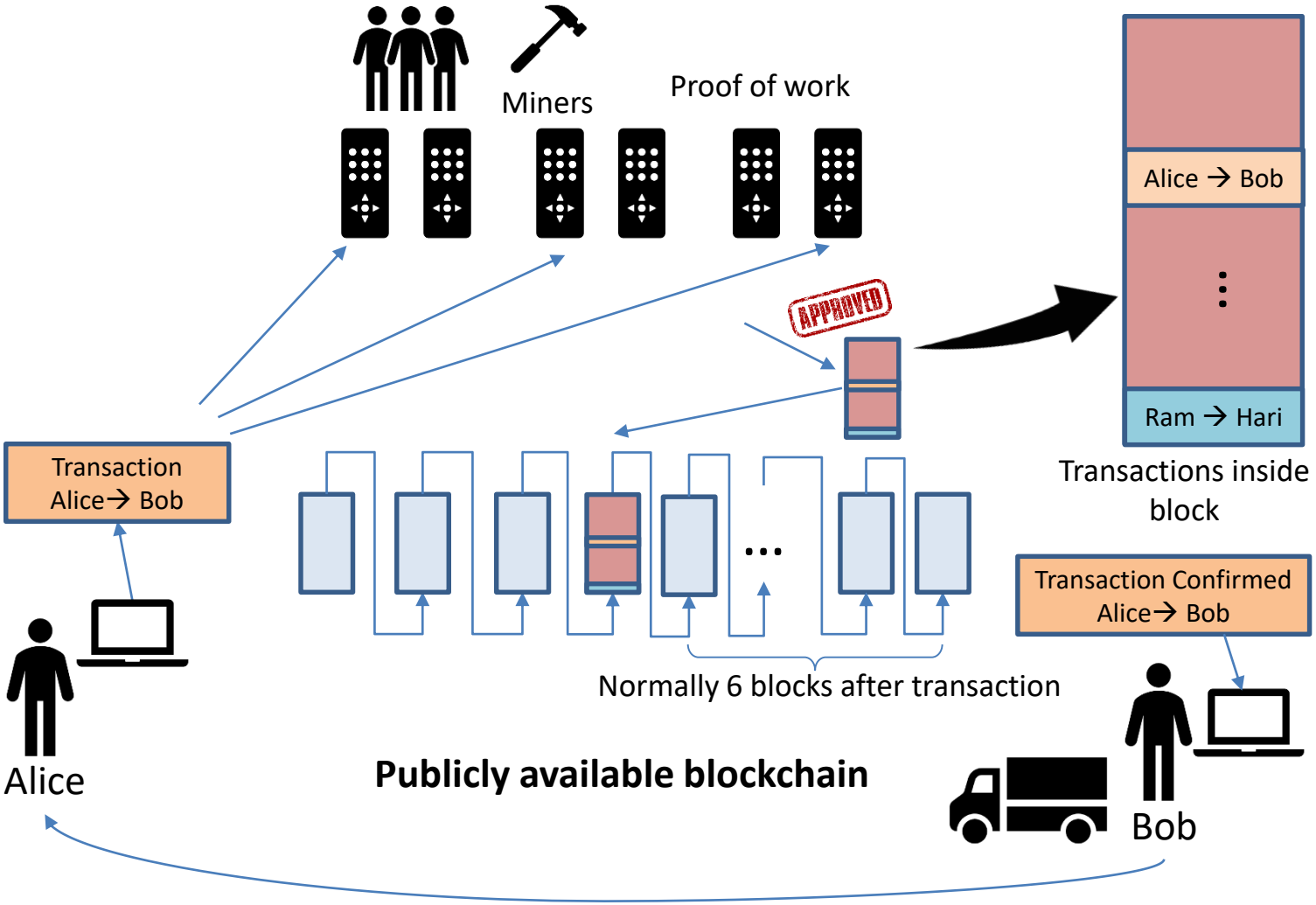
WIKIPEDIA
The Free Encyclopedia

Expedia

overstock.com

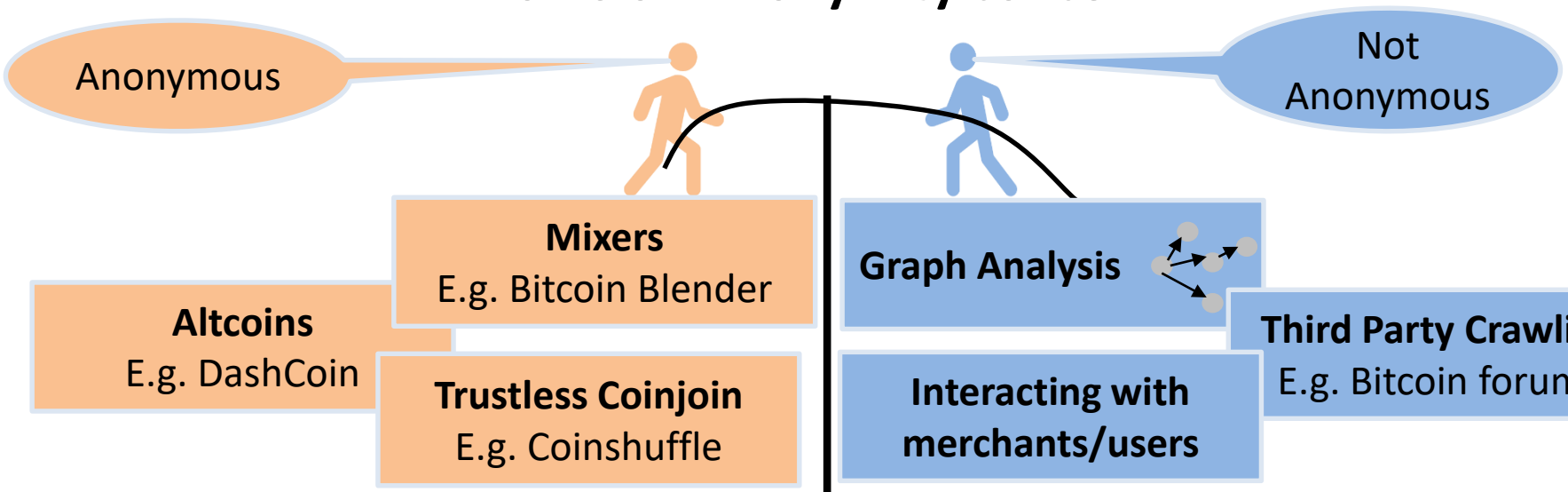
dish NETWORK

How Does Bitcoin Work?



Background and Related Work

Works on Anonymity concern:-



References:

1. Tim Ruffing, et al. Coinshuffle: Practical decentralized coin mixing for bitcoin. In European Symposium on Research in Computer Security, pages 345–364. Springer, 2014.
2. Gregory Maxwell. Coinjoin: Bitcoin privacy for the real world,2013. Available at https://bitcointalk.org/?topic=279249.
3. DashCoin, Anonymous peer-to-peer Internet currency. Available at http://dashcoin.info/

References:

1. Malte Moser, et al. An inquiry into money laundering tools in the bitcoin ecosystem. In eCrime Researchers Summit (eCRS), 2013, pages 1–14. IEEE, 2013
2. Michael Fleder, et al. Bitcoin transaction graph analysis. arXiv reprint arXiv:1502.01657, 2015
3. Sarah Meiklejohn, et al. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference, pages 127–140. ACM, 2013

But, do users really care about anonymity? Or to what extent they care about it?

Contributions

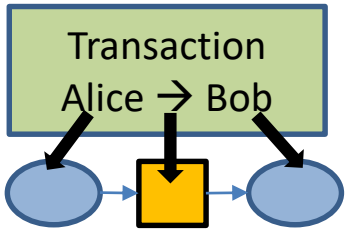
- Anonymity Metrics
  - Direct metric: hide their real-world identity?
  - Indirect metric: hide their intention?

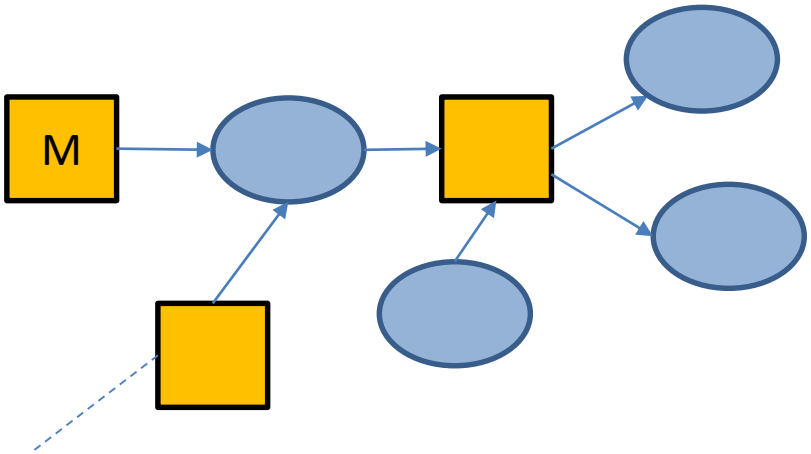
- Macro view analysis of anonymity concern of users
  - The collective anonymity concerns from all users

- Micro view analysis of critical addresses
  - **Addresses from big organizations**: Hot and cold wallet addresses.
  - **Bitcoin "believers":** Stock buyer addresses
  - **Addresses from backbone participants:** Miners addresses

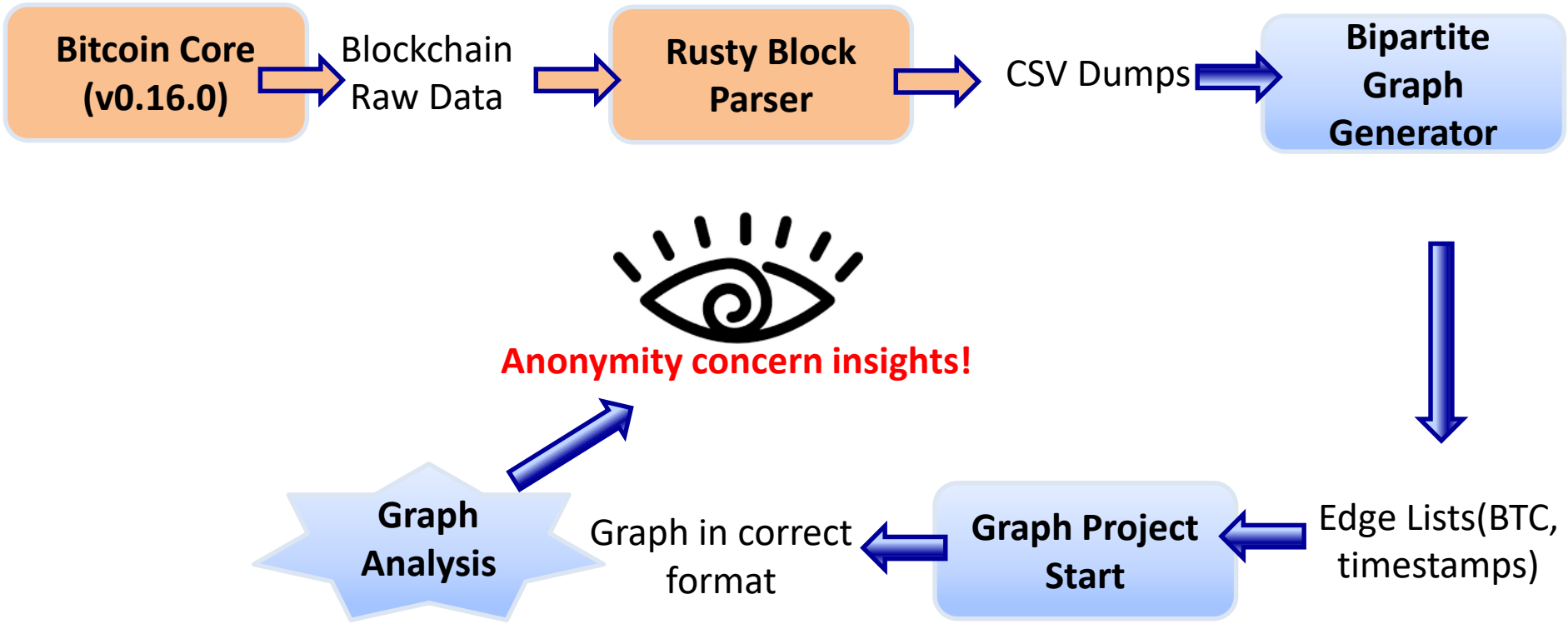
- **BIGDATA**: ~10 years of transaction data (~230 GB)!

Bitcoin Transaction Graph Looks Like





Constructing Bitcoin Transaction Graph



References:

- Bitcoin Core Software. Available at https://bitcoin.org/en/bitcoin-core/
- Rusty blockparser github repository. Available at https://github.com/gcarq/rusty-blockparser

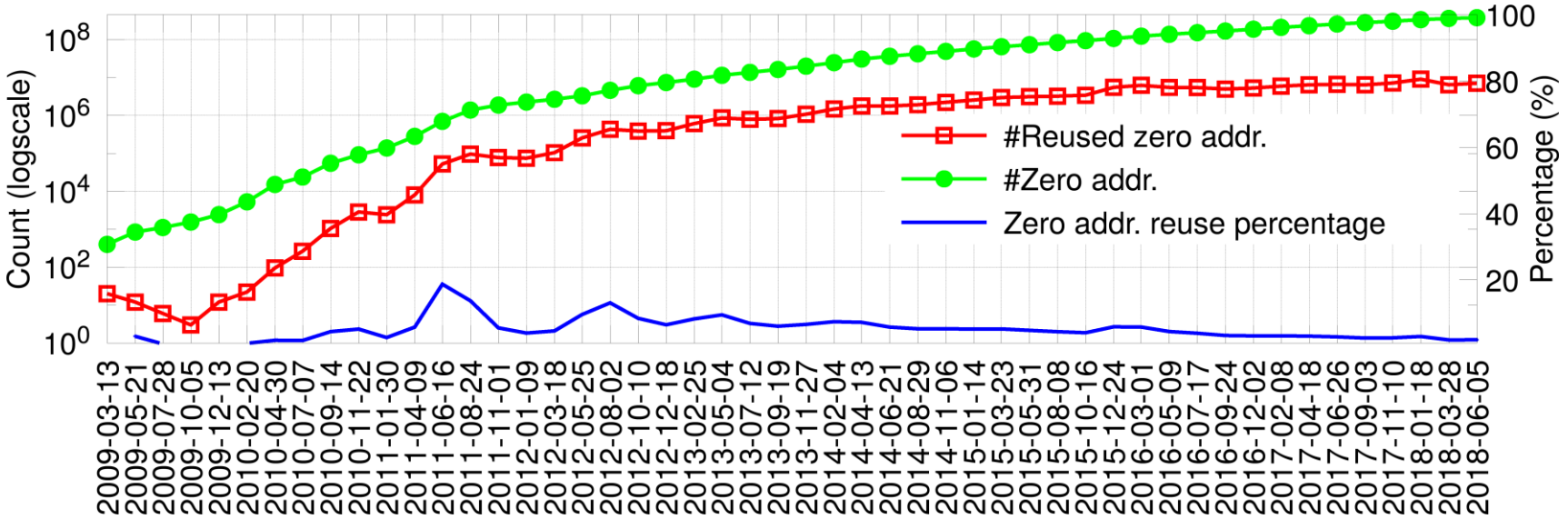
Outline

- Introduction and Background
- Anonymity Metrics
- Macro Analysis
- Micro Analysis
- Conclusions

Anonymity Metrics: How to Detect Anonymity Concern?

Metric 1 (Address Reusing Frequency)**.** *Reusing an address = low concern on anonymity.*

- AddressReuse. Available at https://en.bitcoin.it/wiki/Address reuse
- Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008

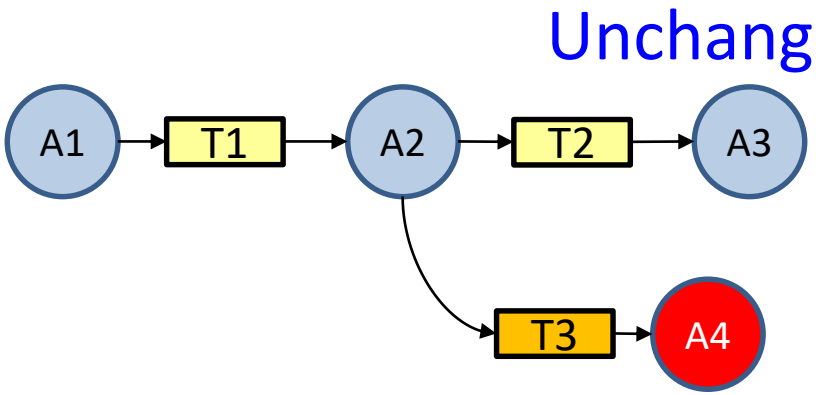


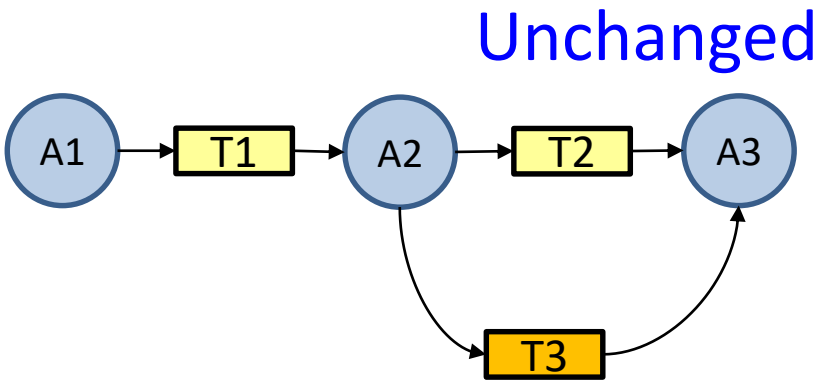
Metric 2 (Zero Balance)**.** *Addresses turned into zero balance = concern about anonymity.*

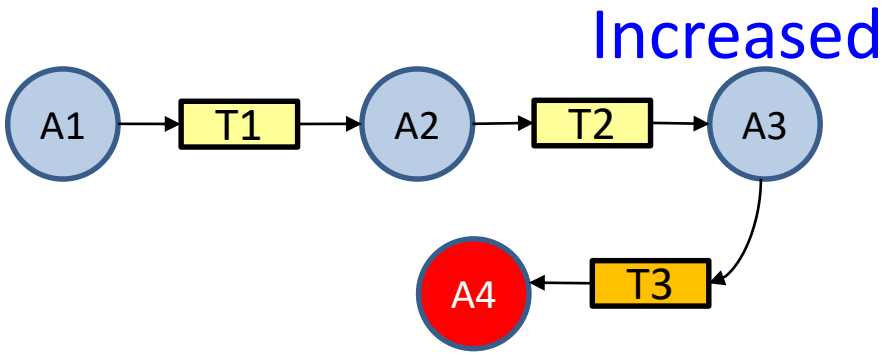
Metric 3 (Address Intention)**.** *Hiding intention = cares about anonymity.*

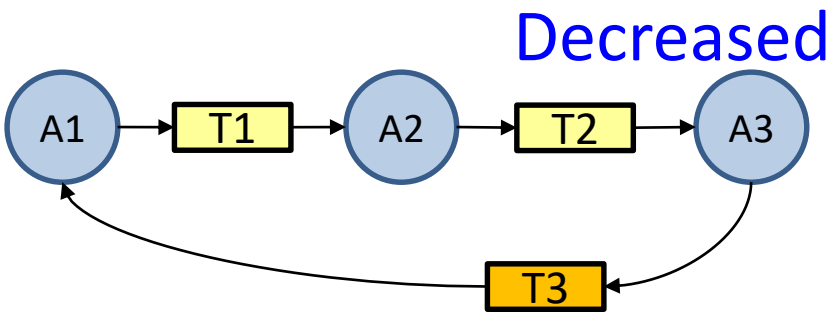
- Important because identifying the intentions of the addresses helps grouping them together into some category to speed up the deanonymization process

Causes of Diameter Dynamics





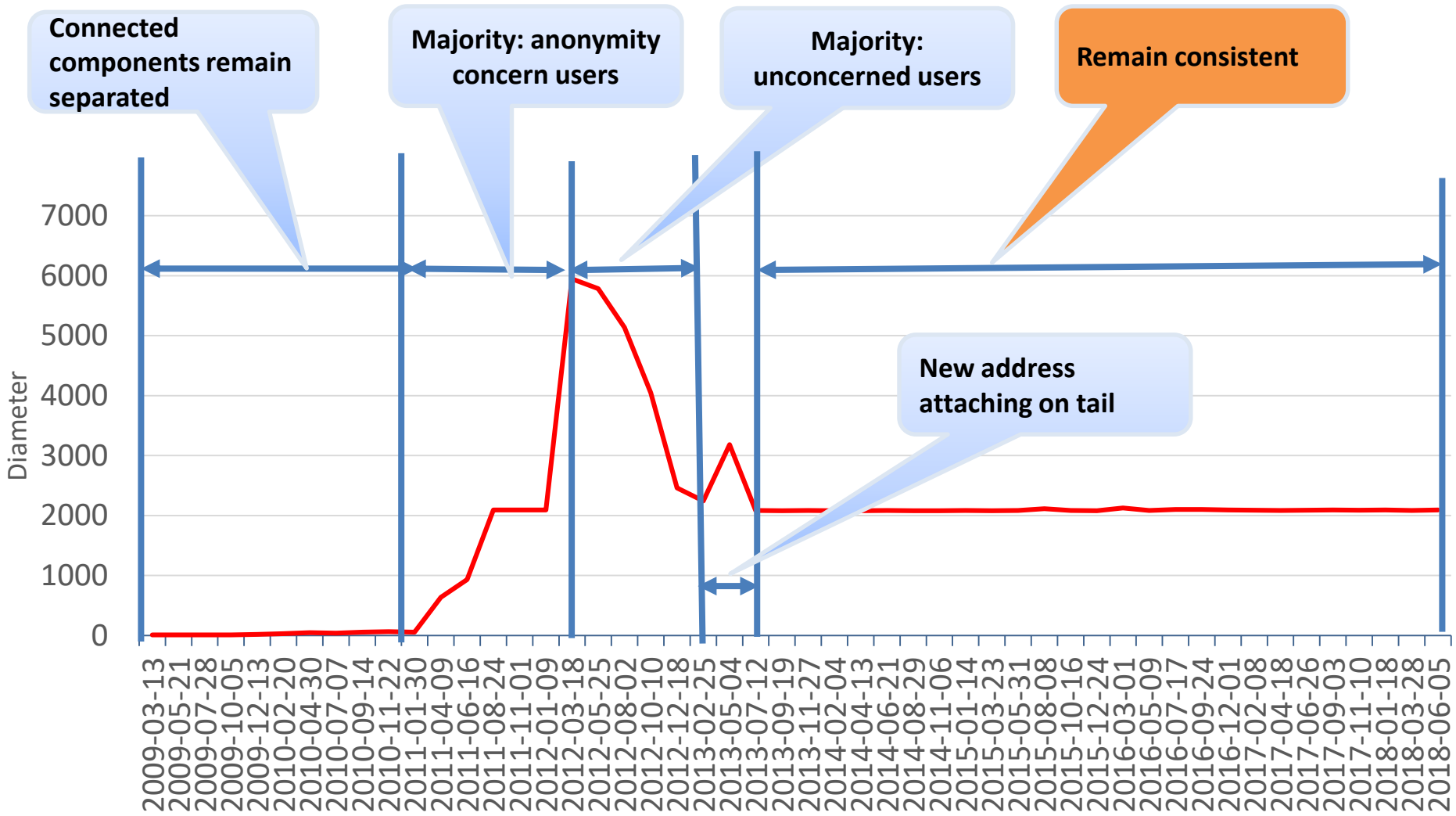




- **New addresses:** Diameter remains unchanged or increases
- **No new addresses:** Diameter remains unchanged or decreases

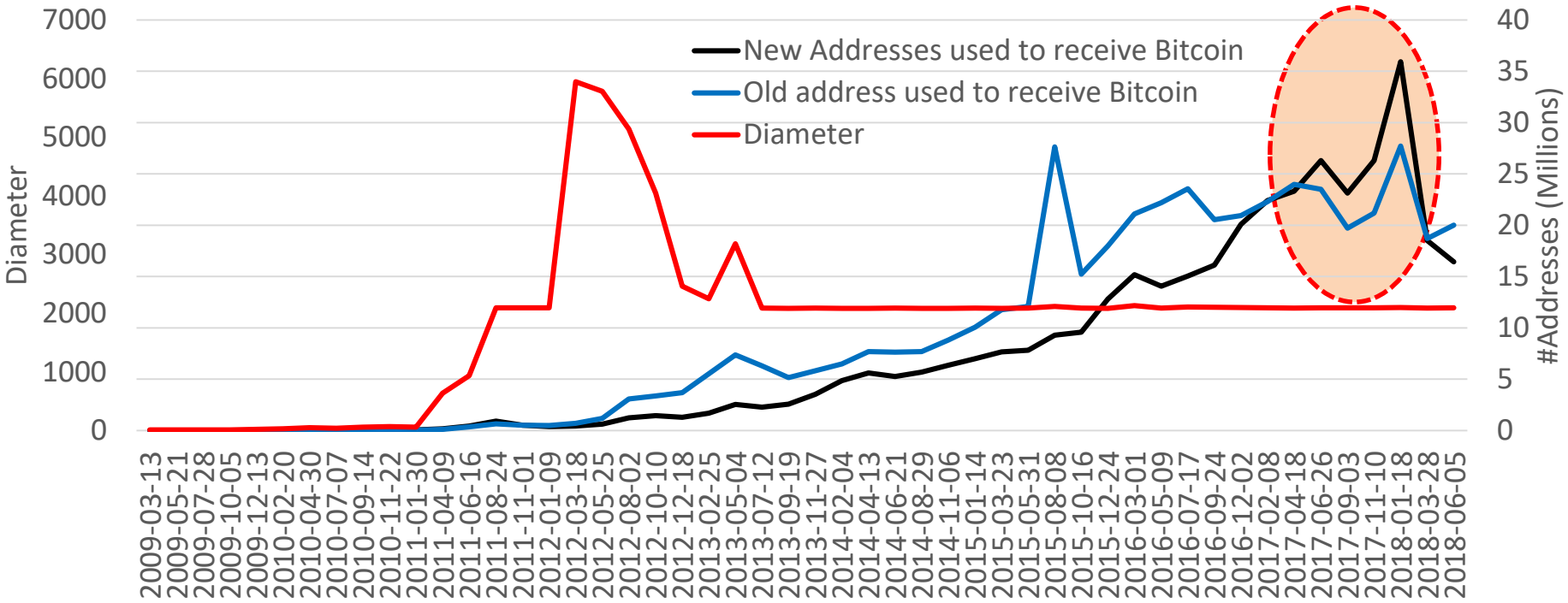
Diameter: The maximum shortest path between any 2 vertices in graph.

Macro View Analysis of Anonymity Concerns



Diameter : Main connected component with majority of vertices

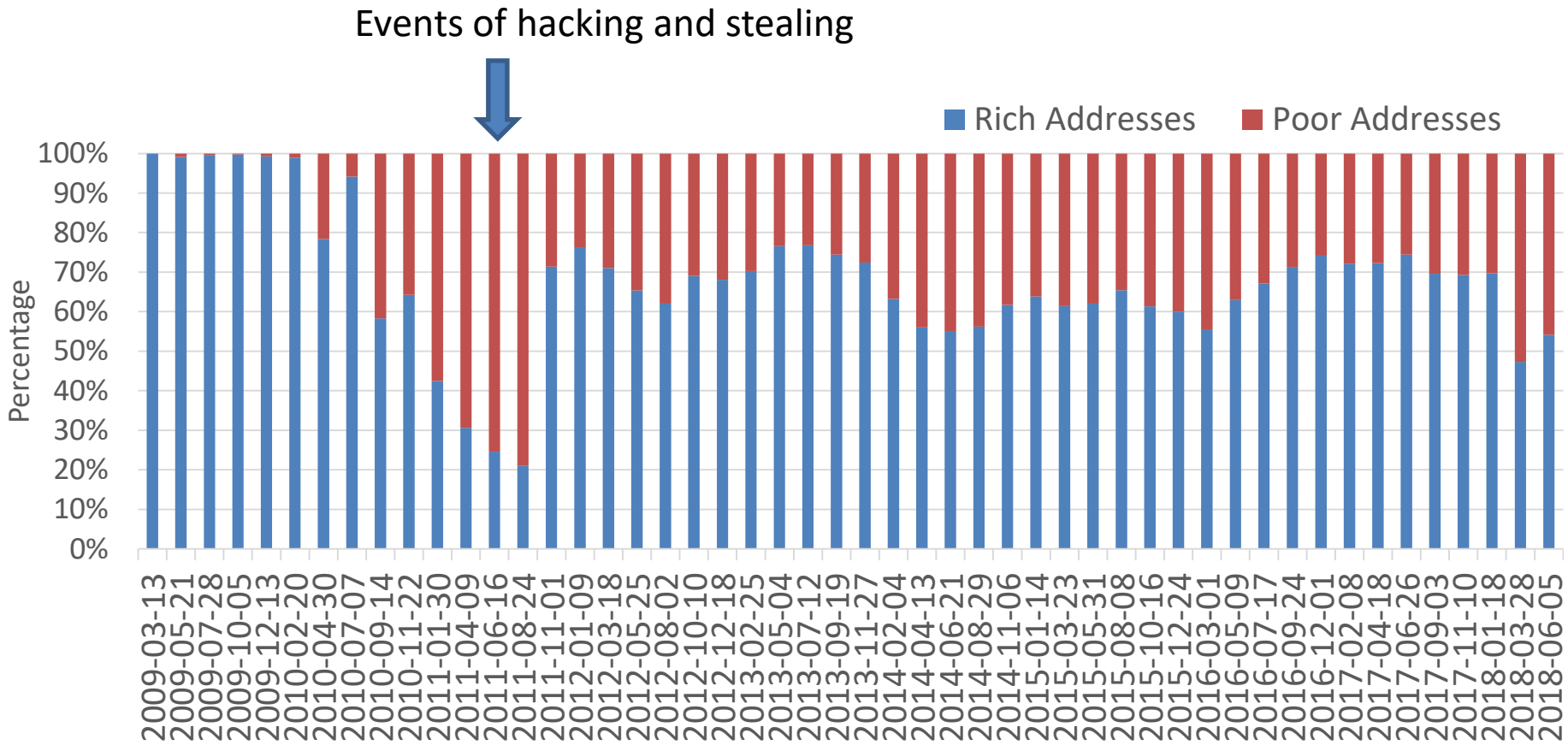
New Address vs Old Address to Receive Bitcoin



- On average, old addresses: 55.25% vs new addresses: 44.75% to receive Bitcoin

- **Exception:** establishment of Bitcoin exchange centers + price hike *probably* caused
  - New users joining Bitcoin → the increase of new address usage.

Rich Vs Poor Addresses



Rich Addresses: Top 25% rich Bitcoin addresses.

Poor Addresses: Remaining non-zero Bitcoin addresses.

Rich addresses are more concerned about anonymity.

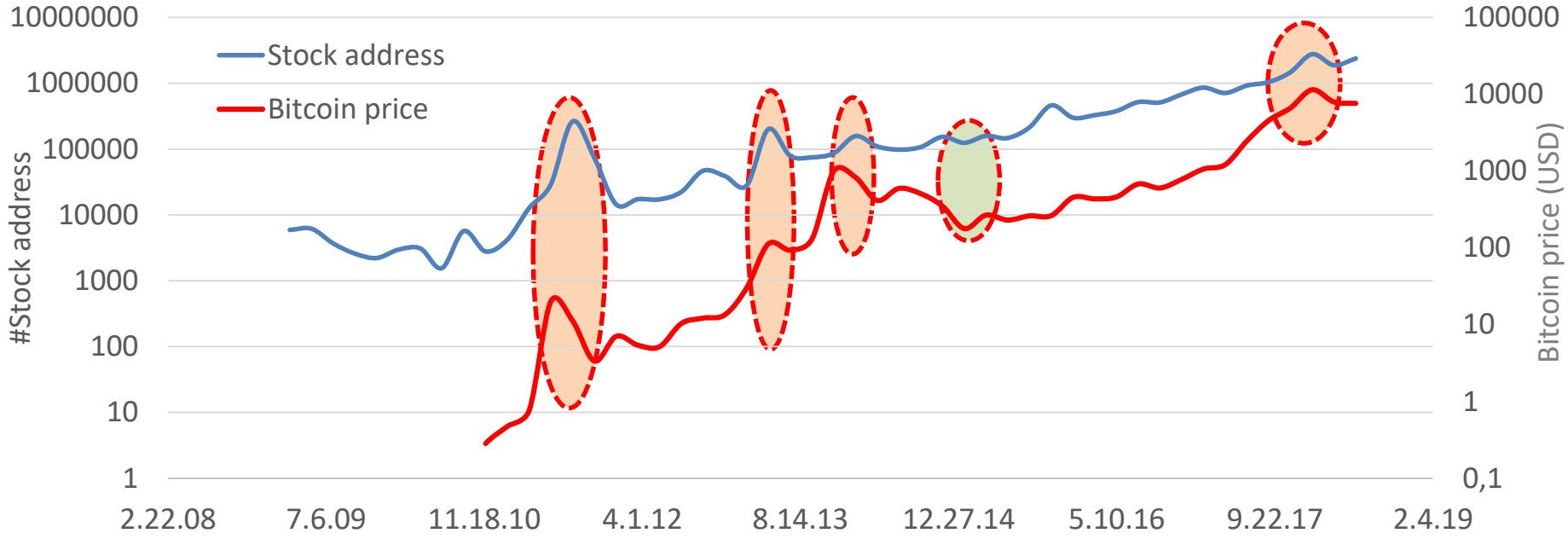
References:

- Timithy B. Lee. A brief history of Bitcoin hacks and frauds. Available at https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/

Outline

- Introduction and Background
- Anonymity Metrics
- Macro Analysis
- Micro Analysis
- Conclusions

Stock Buyer Addresses



- **Stock buyer address features:** only receive the Bitcoin but never spent
  - Out-degree = 0.
  - This is how we reveal their intentions.

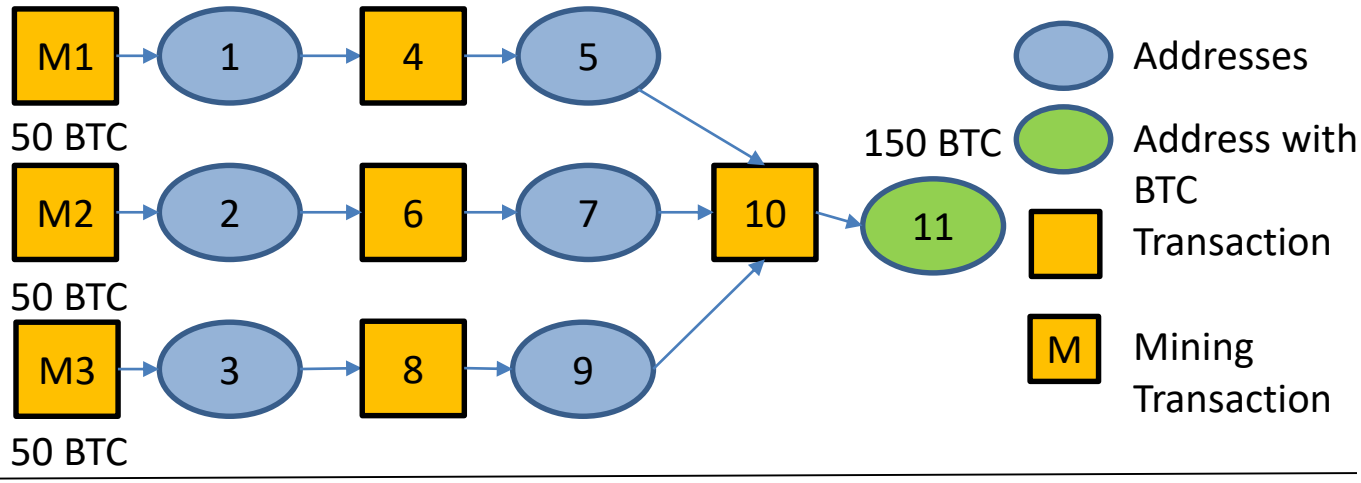
- **More insights:** stock addresses are immediately influenced by the exchange rate of Bitcoin.

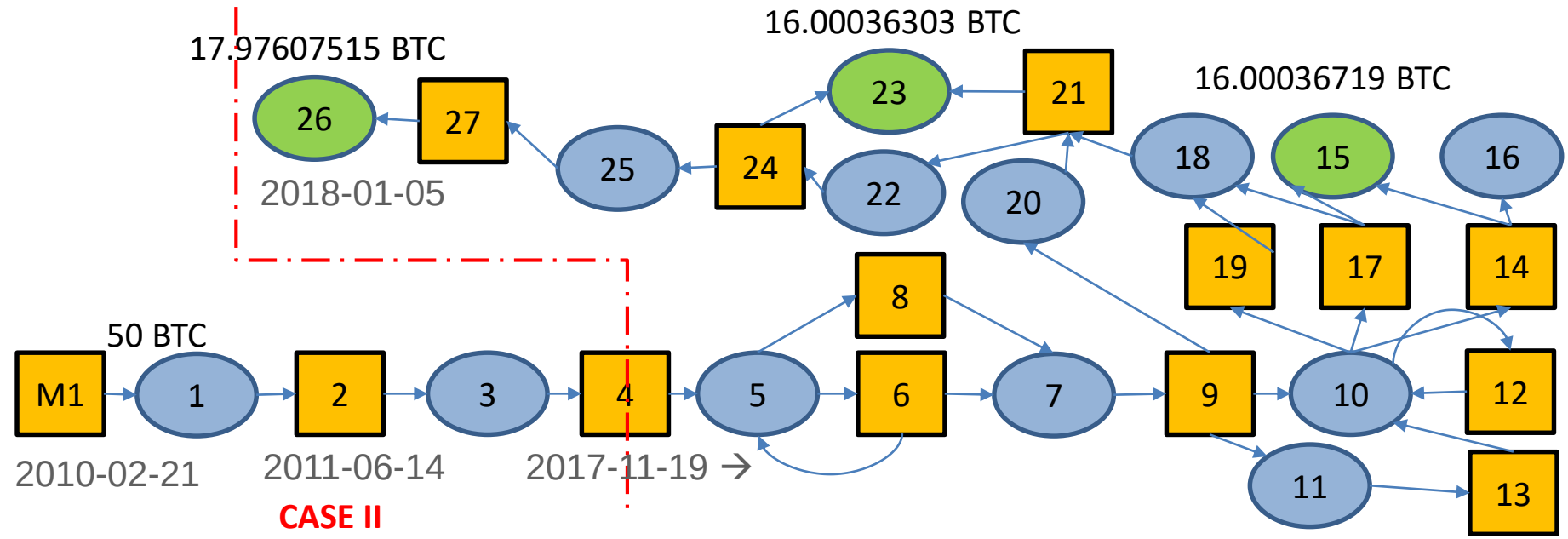
Miners: Before and After Bitcoin Price Hike (2 real cases)

CASE I

- **Miner accumulates the mined Bitcoins**
- **Low Anonymity concern**

2010-06-04 to 2010-06-15





CASE II

Miner splits the mined Bitcoins, when Bitcoin price rises.

Change in anonymity concern

Hot and Cold Wallets of Big Organizations

Hot Wallet	Cold Wallet
Connected to the internet	Offline (hard disk or paper)
Convenient to use but vulnerable to hacking	More secured but not convenient to use

Hot Wallet Addresses of Big Organizations

Tag	Address ID	Total inflow from other addresses	Bitcoin balance	Degree
Deepbit	1VayNert3x1KzbpzMGt2qdqrAThiRovi8	25467352.64	0.2	1565611
SatoshiDICE Hot Wallet	18uvwkMJsg9cxFEd1QDFgQpoeXWmmSnqSs	399678.8714	0.00053	414842
SatoshiDICE Hot Wallet	1MSzmVTBaaSpKDARK3VGvP8v7aCtwZ9zbw	386456.4036	0.00033	414270
SatoshiDICE Hot Wallet	1PeohaRGaTF8cSzDqP1yYfzDah66xiriEQ	384443.0361	0.00079806	413407
SatoshiDICE Hot Wallet	1Bd5wrFxHYRkk4UCFttcPNMYzqJnQKfXUE	383879.8434	0.05339999	415362
SatoshiDICE Hot Wallet	15fXdTyFL1p53qQ8NkrjBqPUbPWvWmZ3G9	383444.5918	0.00028	415042
FoxBit Hot Wallet	1FoxBitjXcBeZUS4eDzPZ7b124q3N7QJK7	156329.1069	0.04314468	560202
Unknown	13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	17600542.04	0.00306531	1011905
Unknown	19iVyH1qUxgywY8LJSbpV4VavjZmyuFyxV	9326468.877	0.00000651	430643

- Hot wallet addresses of big organizations:
  - **Private key** is online for convenience
  - Has relatively high degree, with low accumulations of Bitcoin but higher flow through them.
  - Feature: **Degree >= 50,000, flow >= 150,000 BTC , Accumulated BTC <=10 BTC**

We can help uncover hidden (similar) hot wallets!

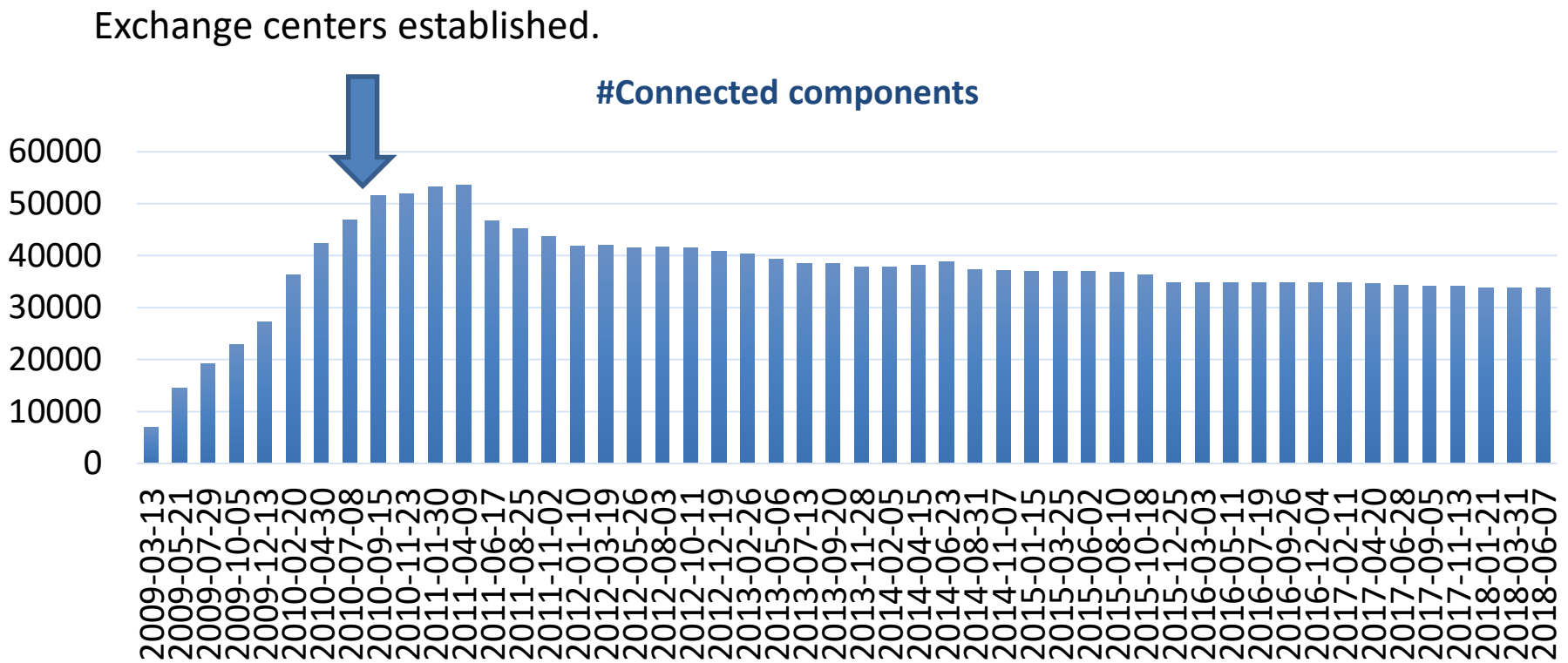
Conclusions

- Majority of the users **don't care** about the anonymity
- Most of the addresses that are concerned about anonymity are rich addresses
- Users start concerning about anonymity when the price of Bitcoin goes high
  - Seen with a real examples of miners
  - Rich addresses concerning more when price hiked, and hacking events started

Conclusions

- Stock addresses don’t hide their intent of making profits on Bitcoin price hike.
- With design of some filters, one can find the hot wallet addresses and cold wallet addresses of big organizations (like exchange centers, gambling sites, miners etc.)

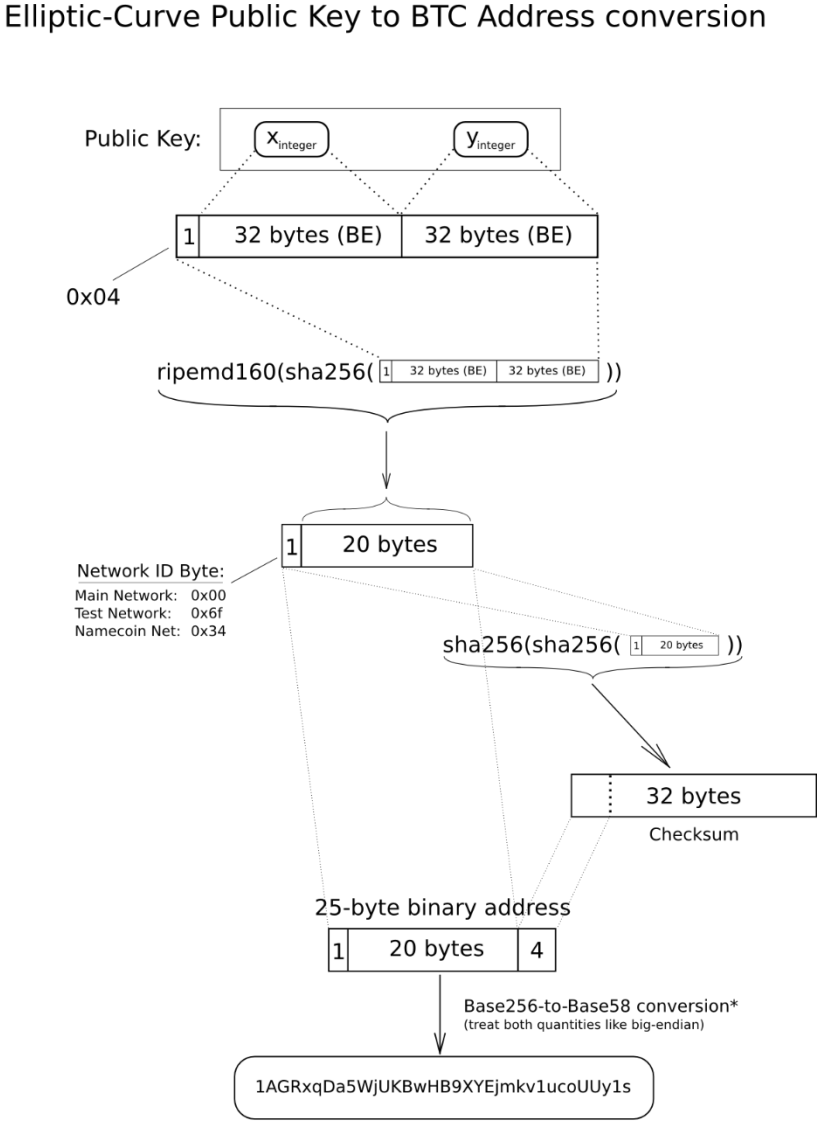
Miners Addresses



Method of anonymity analysis: **Claim 3 (Intention)**

- The mining addresses along with their transactions remain as separate connected component if none of them transact with main connected component.
  - Detected intentions of saving Bitcoin!
- At the date of download, some of the small connected components were detected from around 2010

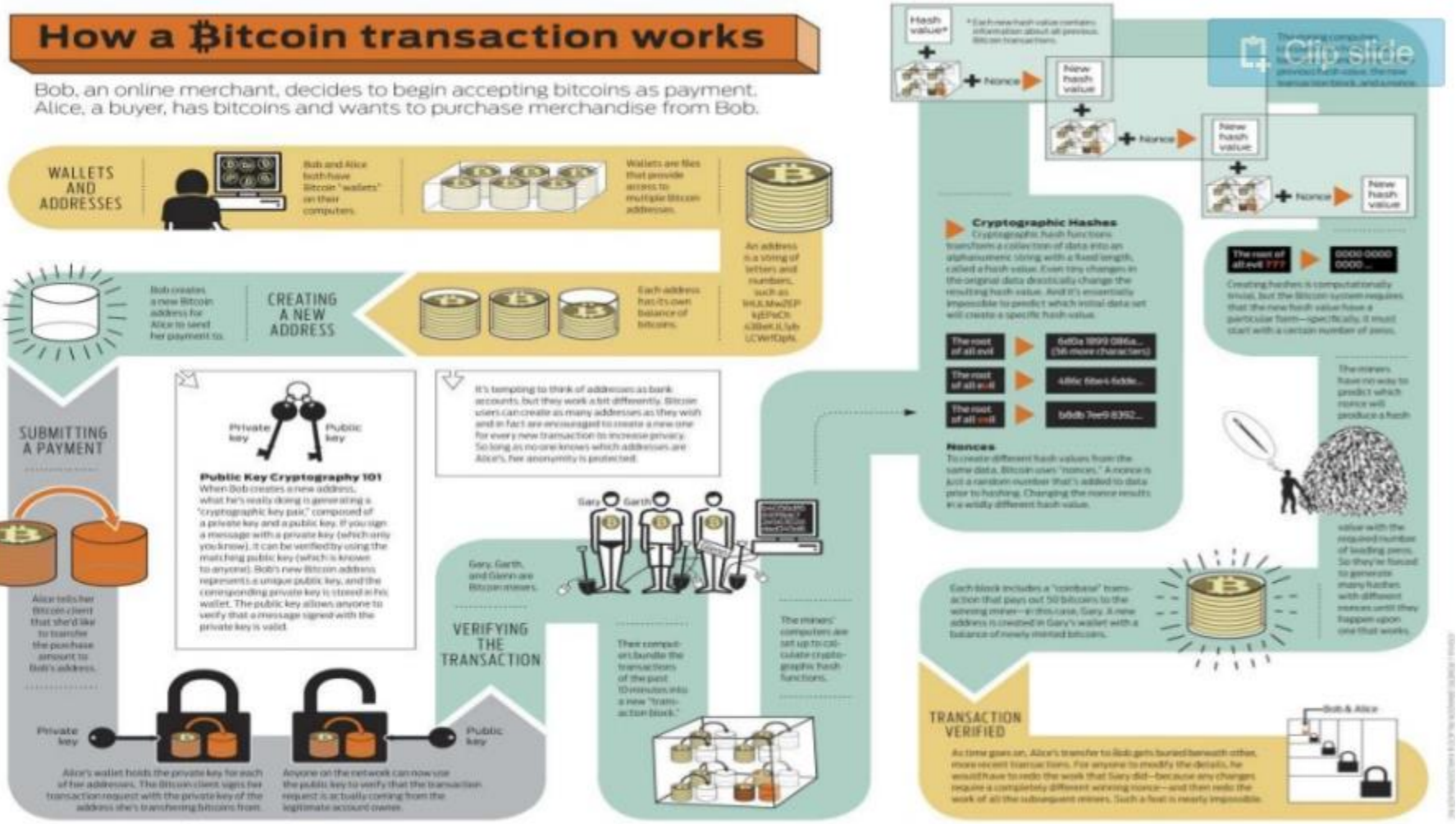
Bitcoin Address



*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

- A Bitcoin address is a 160-bit hash of the public portion of a public/private ECDSA keypair. Using public-key cryptography, you can "sign" data with your private key and anyone who knows your public key can verify that the signature is valid.

How addresses are created?



How a transaction is verified cryptographically?

- Suppose Alice receives m, digital signature { m, $sig=sign(m,K_R)$ }
- Alice verifies m signed by Bob by applying Bob's public key K_u to *sig* then checks $verify(m, sig, K_u)$ = true or false?
- If true, whoever signed m must have used Bob's private key.

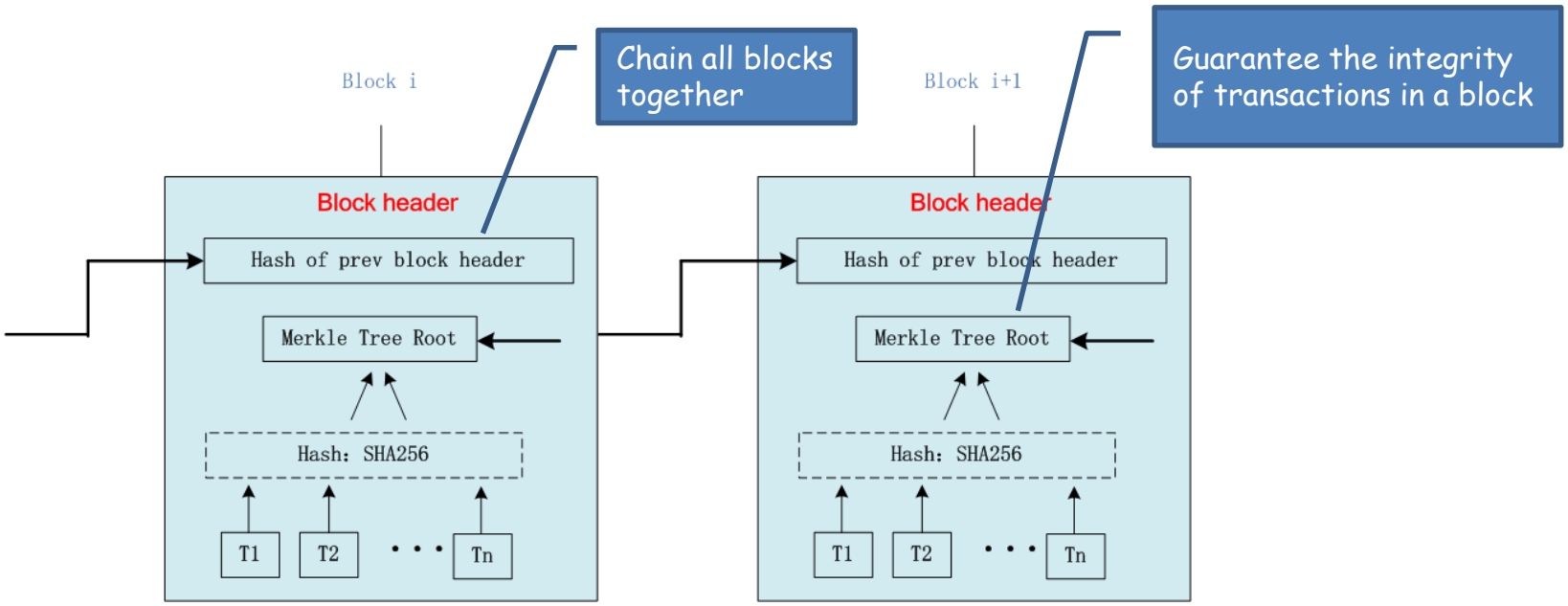
Alice thus verifies that:

- ✓ Bob signed m.
- ✓ No one else signed m.
- ✓ Bob signed m and not m'.

Non-repudiation:

- ✓ Alice can take (m, *sig*) to court and prove that Bob signed m.

2.2 Block format in Bitcoin



- A block contains “block head” and “block body”,
- “block head” stores the previous hash of the last block header.

Core : Proof of Work --- solving a puzzle

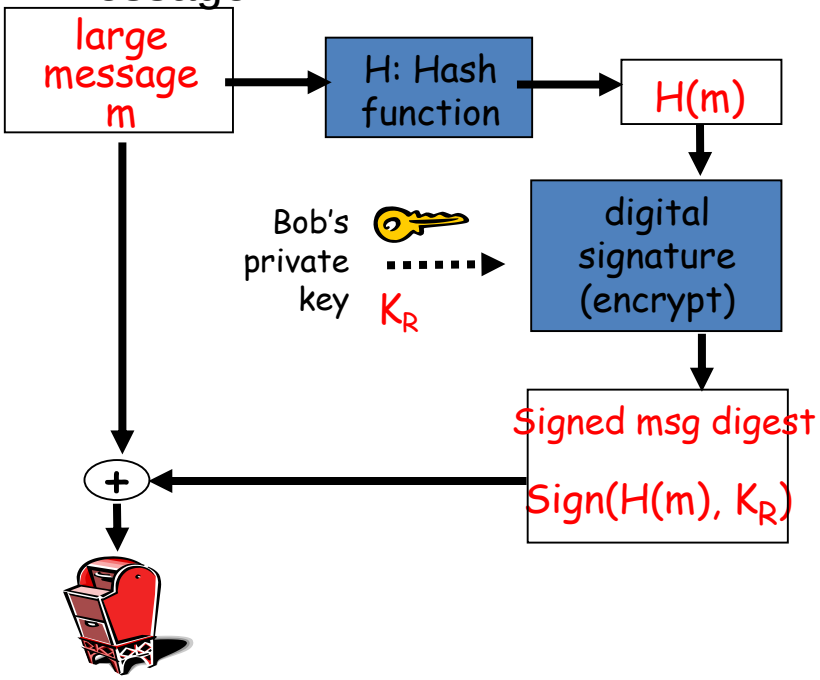
- Definition 4 --- Bitcoin Proof-of-Work function $\boldsymbol{F_d(c,x) \rightarrow \{true, false\}}$:

$$\boldsymbol{SHA256\big(SHA256(c|x)\big) < \frac{2^{224}}{d}}$$

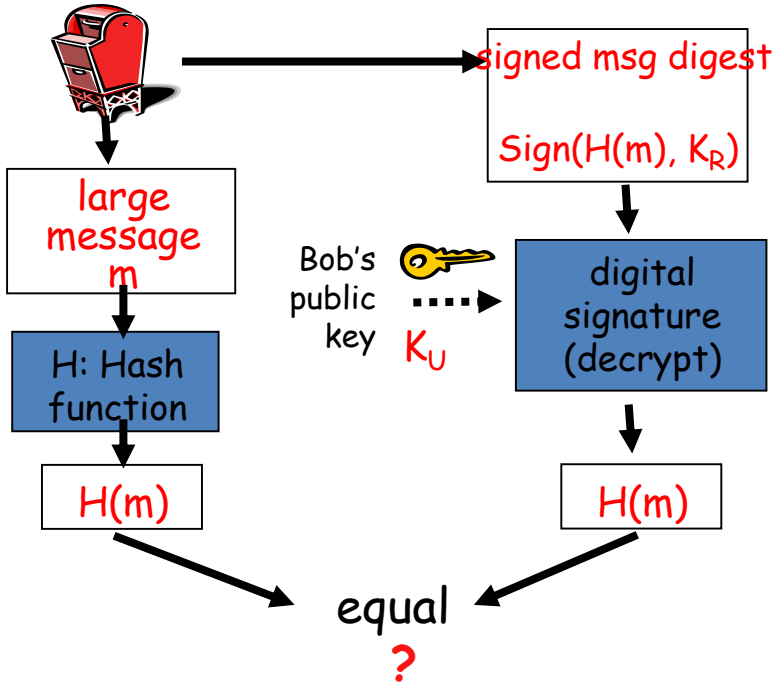
- Given difficulty *d*, challenger *c,* nonce *x,* it is easy to compute $F_d(c,x)$
- Given *d* and *c*, find *x* so that $F_d(c,x) = true$ is possible, but difficult
- $SHA256(x) \in \{0,1,\dots,2^{256}-1\}$. Increase *d*, the target range decrease, and the difficulty of finding *x* increases.

Digital signature = signed message digest

Bob sends digitally signed message:



Alice verifies signature and integrity of digitally signed message:



Hot wallet and cold wallet addresses

Tag	Address ID	Total inflow from other addresses	Bitcoin balance	Degree
Deepbit	1VayNert3x1KzbpzMGt2qdqrAThiRovi8	25467352.64	0.2	1565611
SatoshiDICE Hot Wallet	18uvwkMJsg9cxFEd1QDFgQpoeXWmmSnqSs	399678.8714	0.00053	414842
SatoshiDICE Hot Wallet	1MSzmVTBaaSpKDARK3VGvP8v7aCtwZ9zbw	386456.4036	0.00033	414270
SatoshiDICE Hot Wallet	1PeohaRGaTF8cSzDqP1yYfzDah66xiriEQ	384443.0361	0.00079806	413407
SatoshiDICE Hot Wallet	1Bd5wrFxHYRkk4UCFttcPNMYzqJnQKfXUE	383879.8434	0.05339999	415362
SatoshiDICE Hot Wallet	15fXdTyFL1p53qQ8NkrjBqPUbPWvWmZ3G9	383444.5918	0.00028	415042
FoxBit Hot Wallet	1FoxBitjXcBeZUS4eDzPZ7b124q3N7QJK7	156329.1069	0.04314468	560202
Unknown	13vHWR3iLsHeYwT42RnuKYNBoVPrKKZgRv	17600542.04	0.00306531	1011905
Unknown	19iVyH1qUxgywY8LJSbpV4VavjZmyuEyxV	9326468.877	0.00000651	430643

- Hot wallet addresses of large organizations:
  - Private key is online for convenience
  - Has relatively high degree
  - Filter: Degree >= 50,000, flow >= 150,000 BTC , Accumulated BTC <=10 BTC

Hot wallet and cold wallet addresses

Tags	Address Id	Bitcoin balance	Degree
wallet: Bitfinex-coldwallet	3D2oetdNuZUqQHPJmcMDDHYoqkyNVsFk9r	172236.0323	9065
wallet: Bittrex-coldwallet	16rCmCmbuWDhPjWTrpQGaU3EPdZF7MTdUk	117203.0673	213
wallet:Bitstamp-coldwallet	3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v	97848.28321	238
wallet: Coincheck-coldwallet	336xGpGweq1wtY4kRTuA4w6d7yDkBU9czU	34276.54041	11007
Unknown	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	79957.17569	196
Unknown	16FSBGvQfy4K8dYvPPWWpmzgKM6CvrCoVy	35970.01951	865
Unknown	1AhTjUMztCihiTyA4K6E3QEpobjWLwKhkR	66378.8101	204

- Cold wallet addresses of large organizations:
  - Private key is offline for security
  - Has relatively degree.
  - Filter: BFS with depth 2, from detected hot wallet addresses and Bitcoin accumulation > 10,000 BTC.

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)