Bitcoin Anonymity

Nicolas T. Courtois

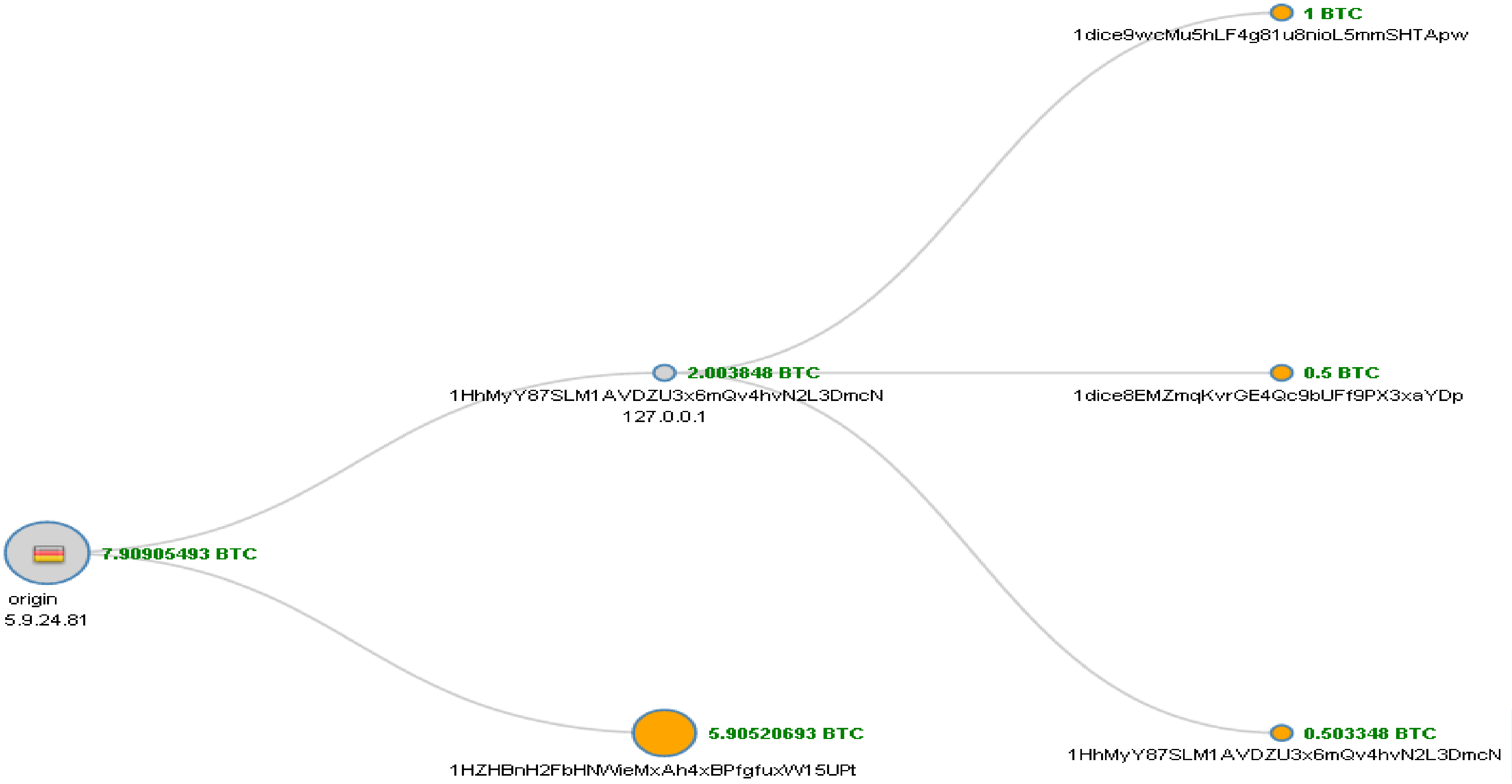
- **U**niversity **C**ollege **L**ondon, UK

Anonymity

Anonymity???

Transactions: ≥0 inputs, ≥1 inputs

Due to practical reasons, most of the time (???)
ALL inputs belong to the same person or to people who know each other.


1 BTC
1dice9wcMu5hLF4g81u8nioL5mmSHTApw
2.003848 BTC
1HhMyY87SLM1AVDZU3x6mQv4hvN2L3DmcN
127.0.0.1
0.5 BTC
1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp
7.90905493 BTC
origin
5.9.24.81
5.90520693 BTC
1HZHBnH2FbHNWieMxAh4xBPfgfuxW15UPt
0.503348 BTC
1HhMyY87SLM1AVDZU3x6mQv4hvN2L3DmcN

Anonymity with PK-based Currency

For unspent money: hide any of

– the owner's ID (btw. his Public Key can be a secret, technicality!)

– the "spending" location can be hidden with TOR

=> potentially with state of the art countermeasures,
the potential thief has no way to locate the money!

Bad anonymity when you spend,

- can split larger amounts in many pieces to avoid being seen when you spend.
- still hard to do…

**Anonymity Citations

- Bitcoin is NOT particularly anonymous BUT it is SUPER DENIABLE – Dan Kaminsky

⇒what does he mean???

⇒about creation of unlimited new identities?

⇒one person becomes many pseudonyms…

⇒deniable = I can claim it was not me…

**Anonymity?

Goal: return some money to itself inside the same transaction

- use another fresh address for better anonymity
- transactions also have multiple input addresses,
  - allows perfect mixing in theory…

⇒ in practice we expect that "most of the time" most input addresses belong to the same person as one of the output addresses.

- ⇒ some geographical / side channel information could link them in pairs
- ⇒ unless money is pre-split in standardized amounts like 0.01 BTC and always used as such.
  - ⇒ Then no change is ever returned.

Due to practical and risk management questions, most of the time (?) ALL inputs belong to the same person or to people who know each other.

Also

The secret billionaire syndrome:

- in bitcoin the PK can be secret forever in practice (technicality)!
- (also the payer location can be hidden very well, TOR).
- potentially with state of the art countermeasures,
  the potential thief has no way to locate the money!

- not so good anonymity when you spend,
  - can split in many pieces to avoid being seen when you spend.

Anonymity References:

Robert McMillan: “Sure, You Can Steal Bitcoins. But Good Luck Laundering Them”, August 2013.

Dan Kaminsky: Black ops of TCP/IP, presentation. Black Hat and Chaos Communication Camp, 2011

Fergal Reid and Martin Harrigan: An Analysis of Anonymity in the Bitcoin System, In Security and Privacy in Social Networks, Springer 2013

Hard Or Easy?

Robert McMillan: “Sure, You Can Steal Bitcoins. But Good Luck Laundering Them”, August 2013.

Main points:

- law enforcement has many ways of tracking down a culprit .
- bitcoin network is built in a way that can make it awfully difficult for criminals to spend the digital currency once they steal it

Hard Or Easy?

- you need to provide proof of identity to trade on Mt. Gox or other exchanges
  - they can also hand other information such as IP addresses and bank account numbers to investigators

- UBS 2014 report “Problematic Currency, Interesting Payment System” is positive about legit usage of crypto currencies:
  - "In principle, financial institutions with existing anti-money laundering systems in place (like banks) could adopt a common Bitcoin-like technology to facilitate fast and secure international transfers between end-users…”

S/N question

- while small-scale money laundering “seems quite possible”, but the big fish will have problems
- there simply aren’t enough places to exchange large amounts of money in an anonymous way
  - bad news: look at these two addresses: suspected to have laundered tens/hundreds of millions of dollars…
  - https://blockchain.info/address/135N2nfAkextd6E25quXpM98qLSi2BccCb
  - https://blockchain.info/address/1Facb8QnikfPUoo8WVFnyai3e1Hcov9y8T
- S/N: “the money that’s moving around the system every day is just not enough to disguise large quantities of Bitcoin”
- super disturbing: anyone can setup a bitcoin exchange, lottery, market, etc. on the Internet.

Anonymity Methods

Laundry Services

Like Bitcoin Laundry and Bitmix

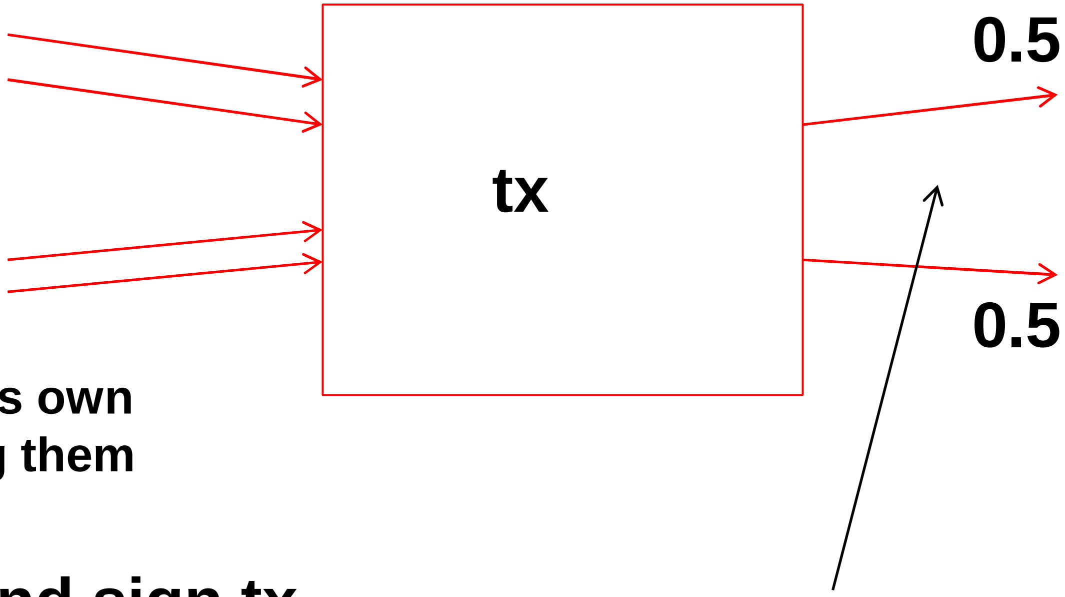
- poor usability
- likely to steal your money

Cooperative Laundering - Main Trick

Known as “CoinJoin” method,
by gmaxwell, August 2013

user A

user B
co-opted
has 0.5 BTC of is own
no risk of losing them



user A
fresh
public key

0.5 BTC

0.5 BTC

user B
fresh
public key

agree and sign tx
independently

which one is user A?

Pb. At any later moment user B can betray himself

Problems with Join Coin

- User A can betray user B

- All inputs must have the same amount
  - ⇒Must return the change to yourself on a fresh address… only to betray your identity later

AltCoins

Each altcoin can be used to exchange to bitcoins and back, hard to trace unless

- you follow all altcoin companies
  - E.g. their network communications,
  - or they cooperate with the police forces
- from public info:
  - timing and amounts of transactions in respective blockchains

- these anonymity services is already a good reason why many “stupid” altcoins exist and have some non-zero market value!

Rented Miners!

You spend BTC from crime on rented miner ASIC.

- Then you produce fresh coins!
- No link (unless the cloud company traces you).

Even less link because of H0…

Classical Ideas

- Run a fake business
- Play a Casino [bitcoin: provably honest casinos]
- Manipulate a market… [use alt-coins] in order to transmit money “wirelessly”:
    - example: inflate some asset on one side, profit from it on the other side.

**Müllerian Mimicry

- Imitate typical patterns of “innocent” bitcoin addresses.
- Cf. David Naccache talk at CECC 2014.

Anonymity Tips / Counter Arguments

• use multiple addresses, new address for each transaction	•no evidence that this helps, these addresses “meet” in the graph of transactions which is not a random graph
• create dummy movements • play lottery, buy/sell shares, exchange against EUR/USD	•must pay fees
• use mixing services, mix small amount at a time	•PERFECT if we cant trust these companies, nobody will now know which addresses belong to you
• avoid EVER connecting your name with any of your Bitcoin addresses	•close to impossible in practice
• Hide you IP address with TOR	•Not a silver bullet

Misconceptions / Counter Arguments

- Bitcoin eliminates identity theft, there is no identity to be stolen [Rosenberg-Anderson]

•On the contrary, it creates new insidious forms of identity theft for the pseudonymous identity:

•Example: steal someone's private keys by a cyber attack, use for money laundering, this creates serious criminal justice problems against which there is no insurance

“Invisible” Recipient? (for the time being)

- Vaguely based on ideas by user=ByteCoin [Bitccoin forum].
- “Untraceable transactions […] are inevitable.”
- Using Diffie-Hellman. Sender =A receiver =B.
- Sender A knows the recipient’s public key g^x mod P
  and B knows A’s public key g^y mod P.
- A computes $S=(g^x)^y$ mod P.
- A computes H(S) as a seed for RNG, generates a deterministic new bitcoin private key **SK_transfer** called the transfer address.
- A sends the money to this address.
- Due to DH magic, B also knows this private key **SK_transfer**.
- B takes the money and transfers them to new addresses.

Remark: This is similar to a theft, the recipient B is anonymous only if he can hide his network presence (e.g. using TOR) and as long as he is not yet spending the money. Requires a lot more work!

- The only real benefit is that nobody can initially associate the recipient B with his public key g^y even though it is in a public directory.

Software and Add-On Solutions

to Make Bitcoin More Anonymous

DarkWallet

Radical nearly-anarchist project

- Software which mixes 2 bitcoin transactions for people who do NOT know each other, mixing by default.
- A lightweight plug-in wallet for Chrome/Firefox.

Anonymity Alt-Coins

DarkCoin

Implementation of Coin-Join with several stages.

Uses blind signatures in order to prove the input belongs to one of the participants.

Has a collateral deposit system: protects against badly behaving users, they may lose money.

Cons: All the issues with CoinJoin.

Zerocoin

Anonymous currency, ZK proofs.

Initially proposed as an extension of bitcoin, now it will be an independent currency.

Another similar proposal: Appecoin.

Zerocoin

S secret serial number I commit to, needed to spend the coin

r random needed to reveal S later on

$C=g^S h^r$

Producing Zerocoins:

In Bitcoin blockchain 1 BTC => C, invalid H(PK), just destroyed 1 bitcoin,

this controls the monetary supply!

Remark: already protected against abuse, nobody wants to destroy bitcoins which cost money…

Now revealing this serial number S will be worth 1 BTC,

like on-time signature mechanism??? ,

PROBLEM; must convince bitcoin developers to accept creation of bitcoins out of thin air!

Breaks bitcoin (or requires permission of bitcoin developers or/and a majority of miners).

Zerocoin Issues

Source: https://bitcointalk.org/index.php?topic=279249.0

Limitations:

- uses cutting-edge cryptography: maybe insecure, understood by relatively few people
- produces large (20kbyte) signatures that would bloat the blockchain (or create risk if in external storage)
- it requires a trusted party to initiate its accumulator. If that party cheats, they can steal coin. (Perhaps fixable with more cutting-edge crypto.)
- validation is very slow (can process about 2tx per second on a fast CPU), which is a major barrier to deployment in Bitcoin as each full node must validate every transaction.
- large transactions and slow validation means costly transactions => will reduce the anonymity set size
- uses an accumulator which grows forever and has no pruning. In practice this means we'd need to switch accumulators periodically to reduce the working set size, reducing the anonymity set size.
- some of these things may improve significantly with better math and software engineering over time.

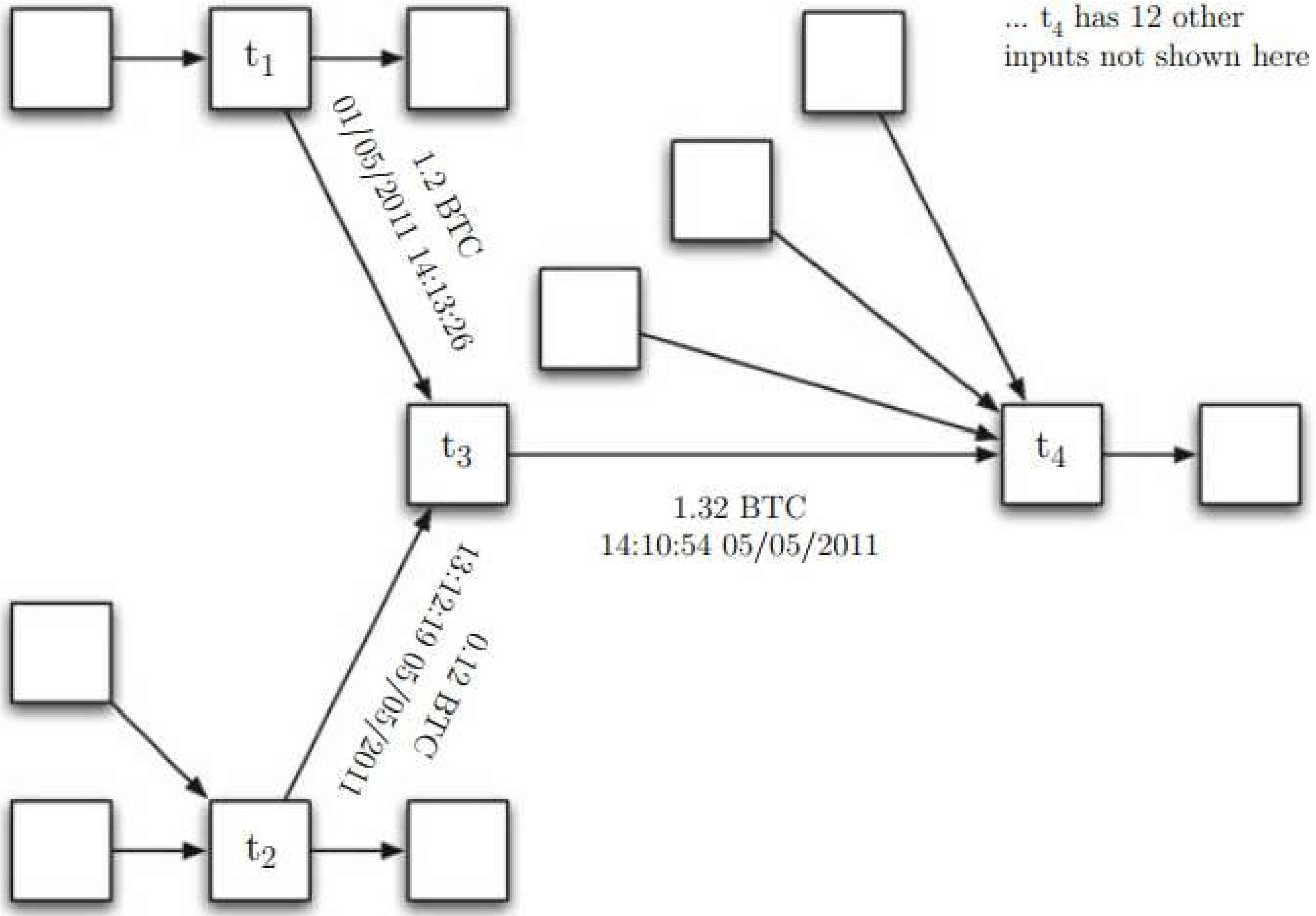
But above all: **Zerocoin requires a soft-forking change to the Bitcoin protocol**, which all full nodes must adopt, which would commit Bitcoin to a particular version of the Zerocoin protocol. Politically contentious, as some developers and Bitcoin businesses are very concerned about being overly associated with "anonymity".

Crime Investigations

Two Graphs

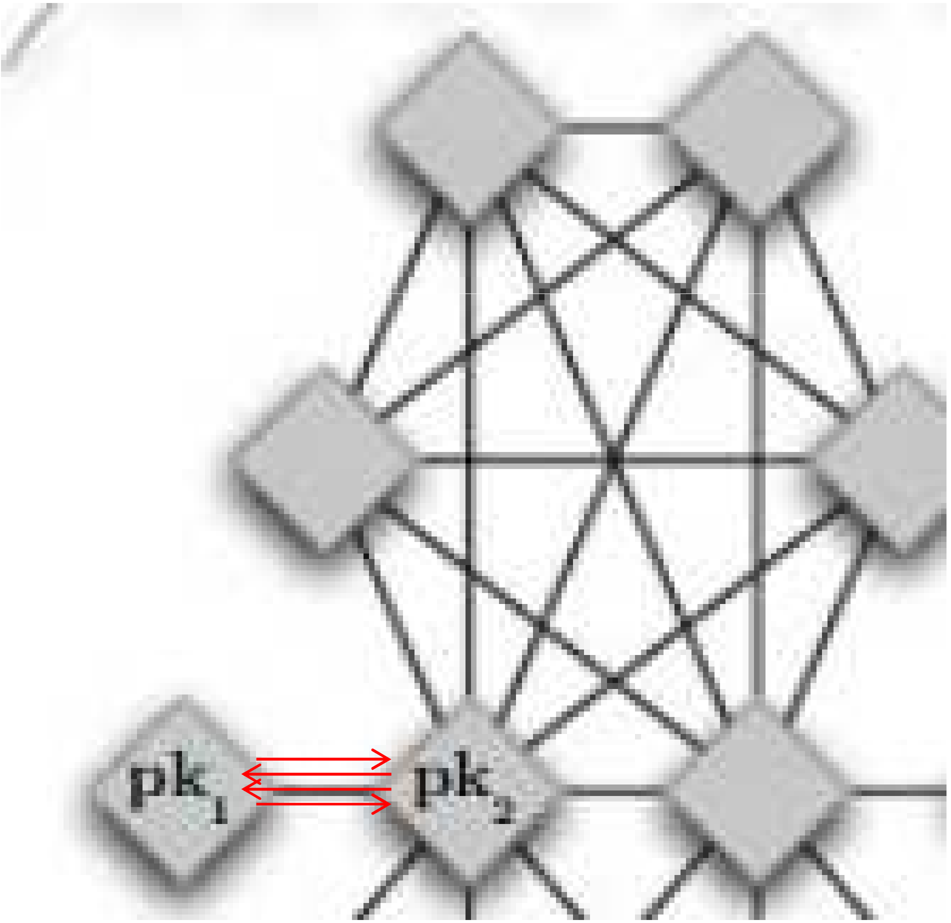
Fergal Reid and Martin Harrigan: An Analysis of Anonymity in the Bitcoin System, In Security and Privacy in Social Networks, Springer 2013

Transactions form a DAG: Directed Acyclic Graph



Second Graph

Public Keys Form A Graph in which money flows potentially in both directions between any pair at various moments



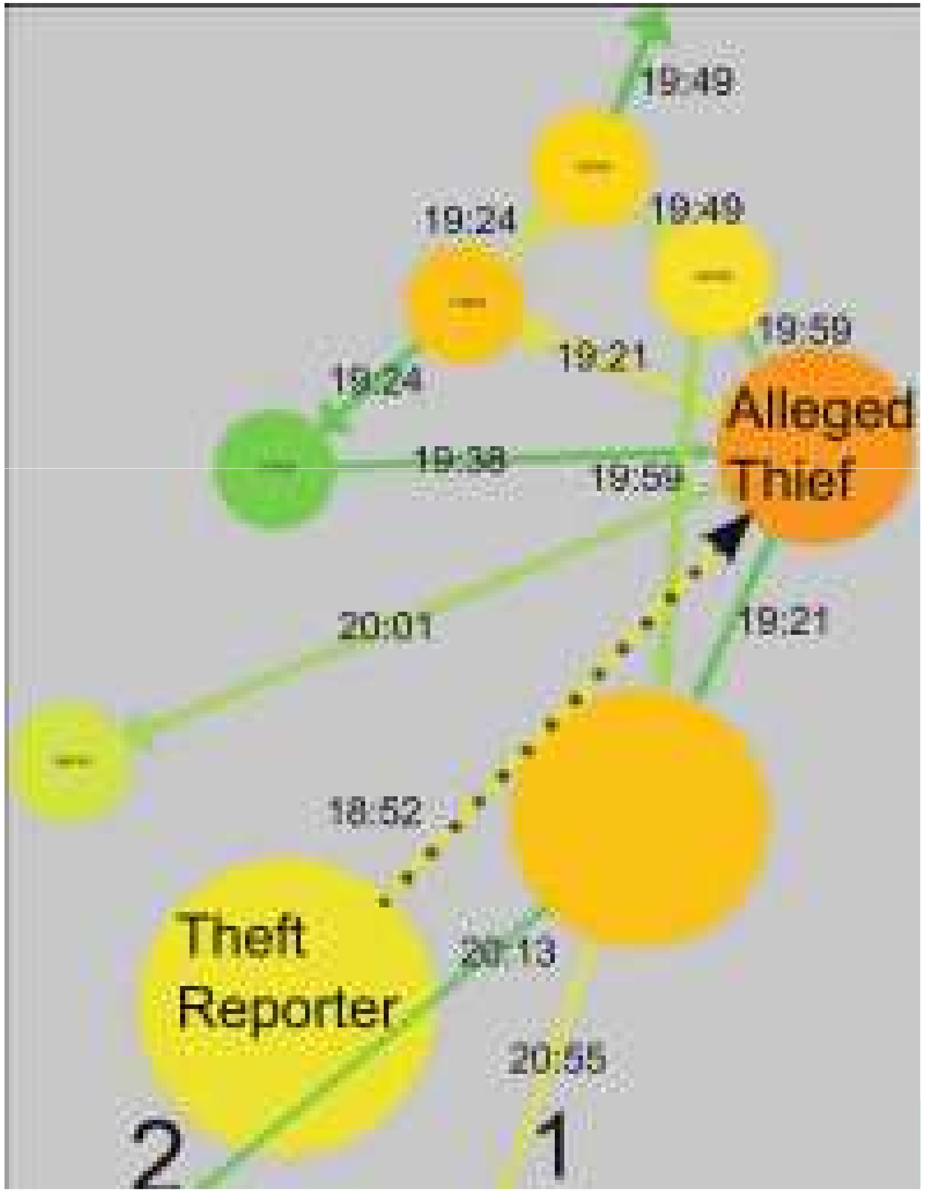
Initial Theft

25,000 BTC

Initial steps:

We can assume that all bitcoin accounts initially involved are related to the thief?

Not quite after the theft, he donated some money to computer hacker group known as LulzSec.

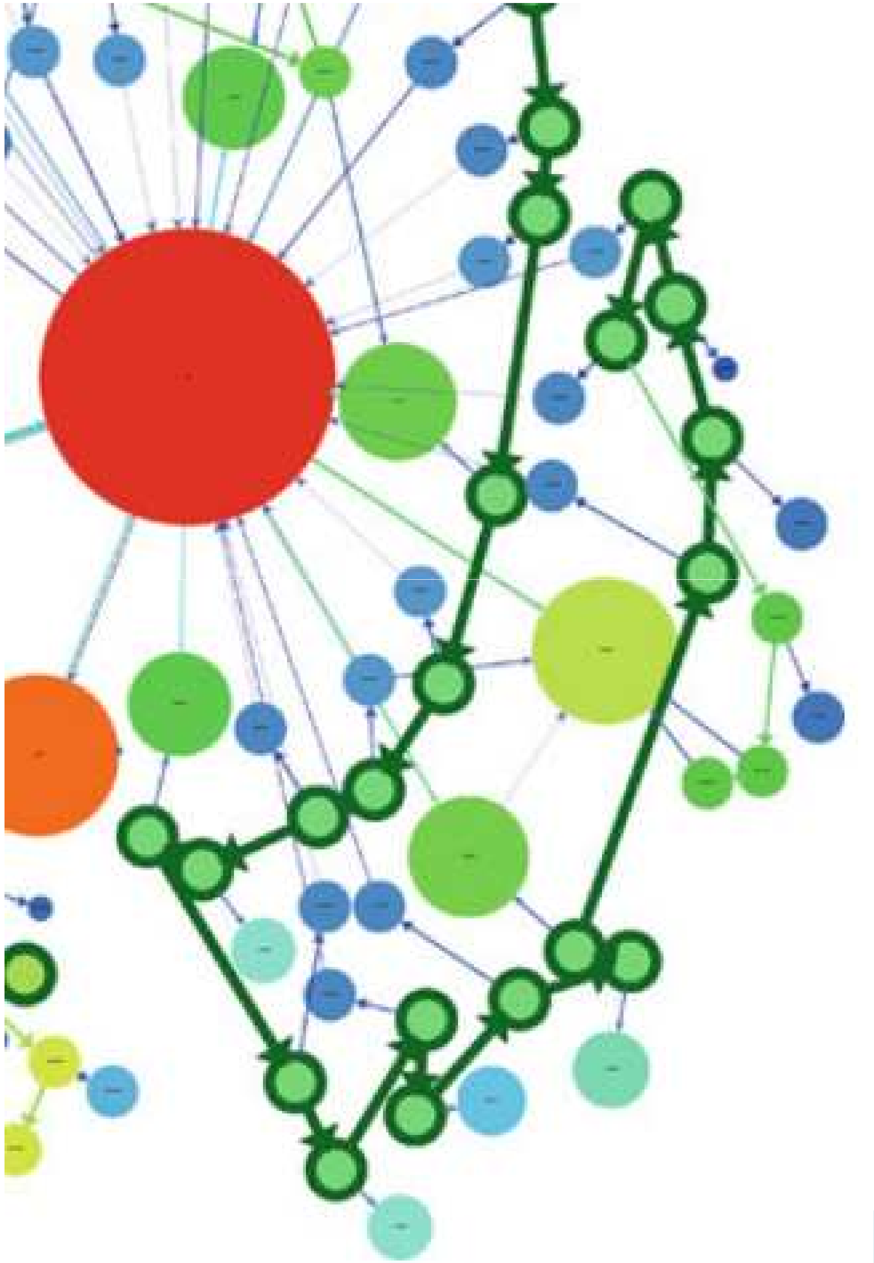


Analysis

- flows split and then merge again
- IP address reporting transactions
- size of inputs/outputs
- speed of transactions
(some are quite fast!)

Other sources of data

- order books with precise amounts from exchanges



Another Example of Actual Crime

A criminal gang promising non-existing miners (Hashblaster.com) run by a non-existing company claimed to be based in Essen, Germany had numerous victims.

Some of these fraudulently obtained sums have transited through

https://blockexplorer.com/address/1Nm1jYHo8WKuJc7Paq1VneAPdNtqcmpm6t

Then they went to (next page).

Bitcoin's most mysterious wallet?

1Facb8QnikfPUoo8WVFnyai3e1Hcov9y8T

Initially it was a great mystery:

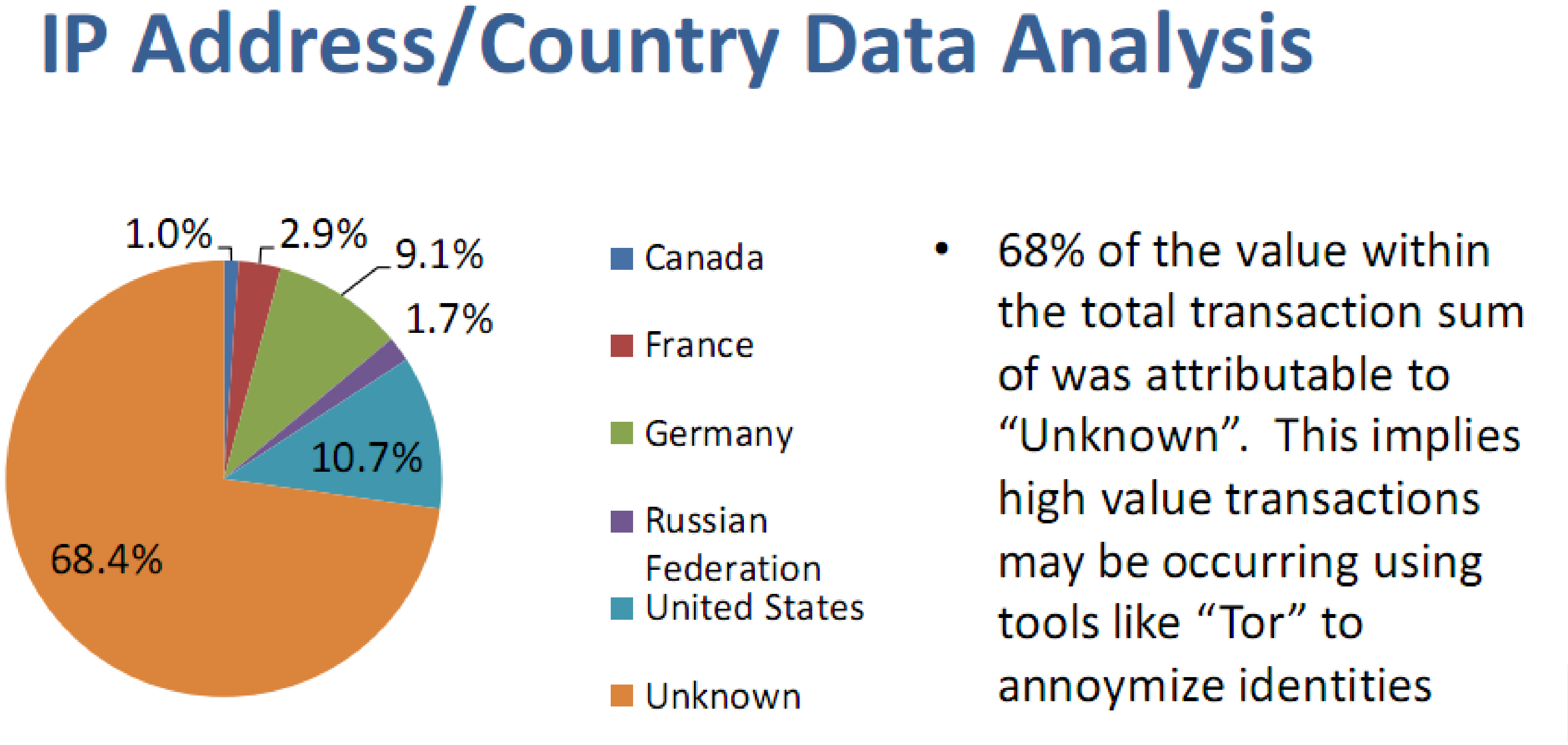
- was active in the period from December 2013
- total funds managed: 219,956 Bitcoins (estimated USD209 million)
- fast growing, suspected to be a major laundry service etc...

Later it was found it belonged to MtGox!
Q: Did MtGox check the identity of their customers?

Tracing Larger Patterns (e.g. Geographic Patterns)

IP Address Per Transaction Reporting

© Bissessar Shiva and Nicolas Courtois, UCL 2013



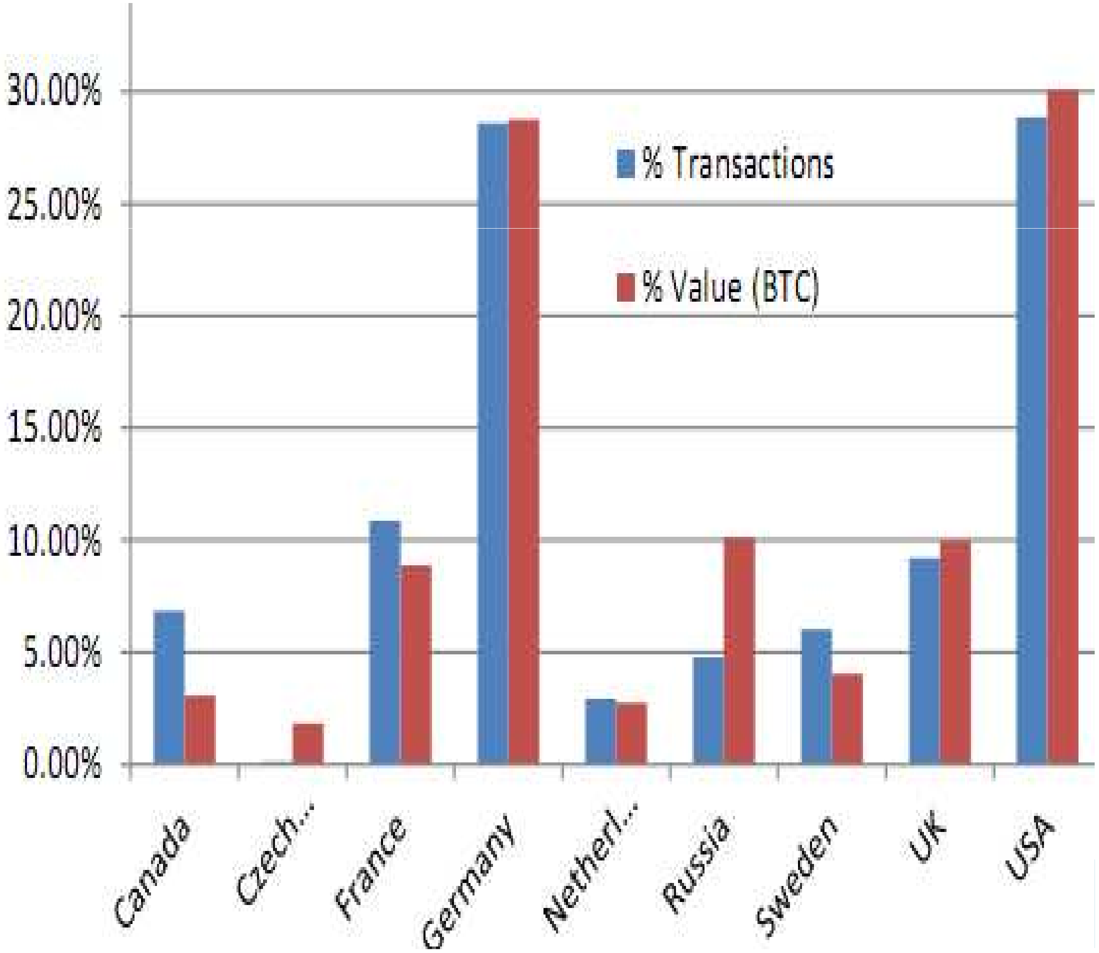
IP Address/Country Data Analysis

- 68% of the value within the total transaction sum of was attributable to “Unknown”. This implies high value transactions may be occurring using tools like “Tor” to annoymize identities

Currency Circulation

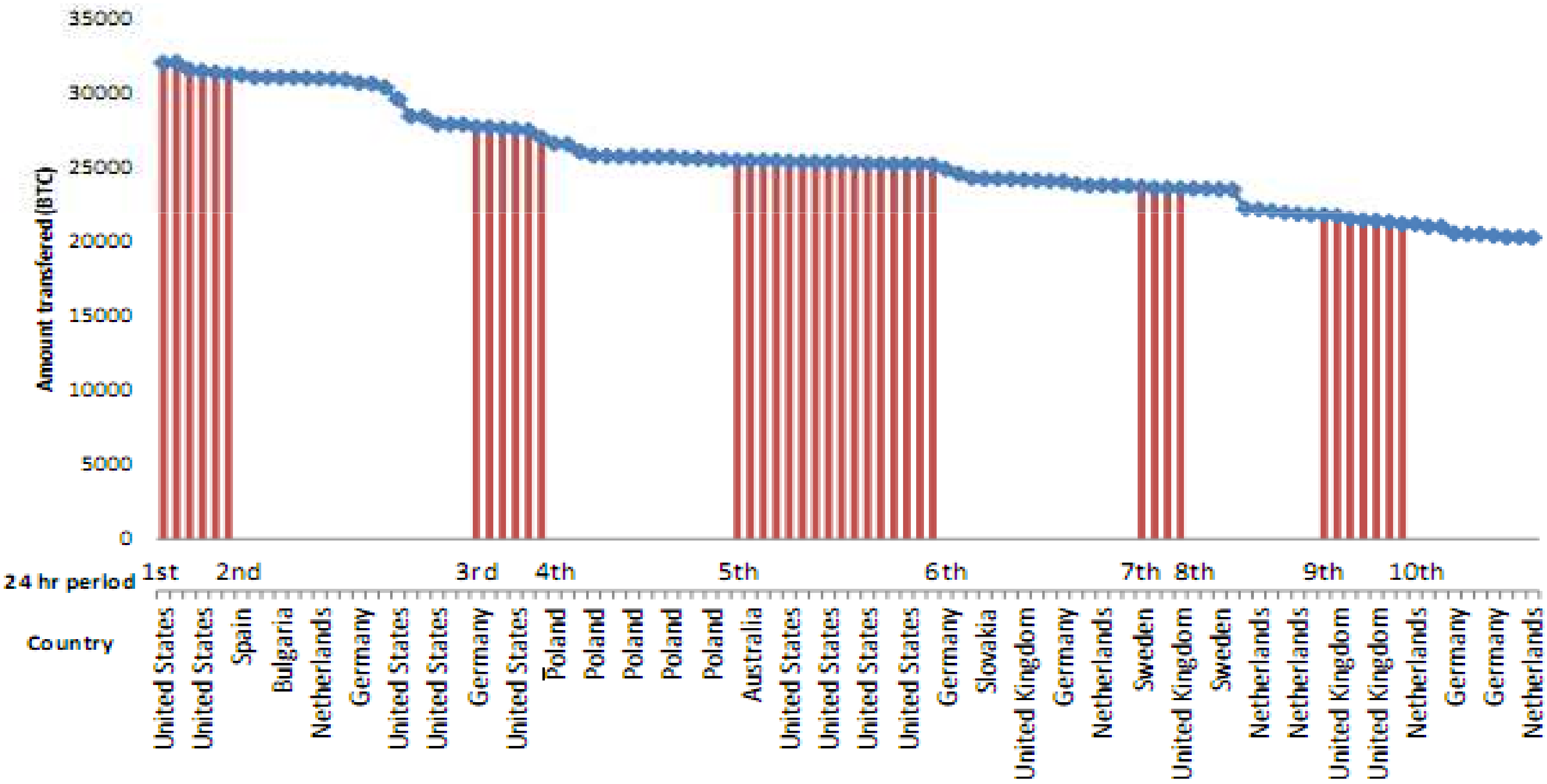
Canada has higher percentage of transactions than Russia, however, Russia has almost 3 times as much transactional value than Canada

US & Germany lead all others in terms of value and volume of transactions



Anonymity??? - Following 3.7 M$ For 24h

© Bissessar Shiva and Nicolas Courtois, UCL 2013



Transparency

Non-Anonymity Is Valuable:

Charity, political party, any publicly managed organization:

- Everybody knows how much money was donated.
- Everybody knows how money was spent.