[An introduction to]

MONERO

Jérémie Dubois-Lacoste – Arne Brutschy

`jeremie|arne@cryptosphere-systems.com`

Bitcoin Meetup Switzerland

Geneva

Who are we?

CRYPTOSPHERE
SYSTEMS

- Three guys with a PhD
- We help you build blockchain-based applicaions
- Specializations
  - cryptocurrencies down to the nuts and bolts
  - scalable algorithms and scalable systems
  - security and dev ops
- Experience: Several crypto apps deployed

Disclaimer

- We own bitcoins and moneros
- We’re geeks and computer scientists, not economists

Outline

Privacy, Fungibility, and Bitcoin

Monero's Privacy Improvements

Summary

XMR.TO

Outline

Privacy, Fungibility, and Bitcoin
- Privacy in Bitcoin
- Fungibility?
- Fungibility in decentralized currencies

Monero's Privacy Improvements

Summary

XMR.TO

Financial Privacy

- Financial privacy is important for a payment system
- Anti-money laundering laws, taxation, etc. are possible even when the payment system ensures privacy

Privacy in Bitcoin

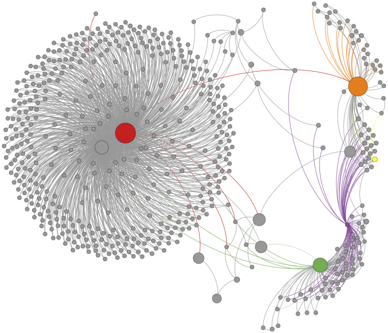
Bitcoin is not anonymous, it is *pseudonymous*. Pseudonymity is very fragile in daily life:

- Linking of transactions reduces privacy;
- Usage leaves traces everywhere on the Internet;
- Privacy-enhancing measures (tumblers/CoinJoin etc.) are costly.

As a result, the analysis of the Bitcoin blockchain can reveal identities.

Practical ways to analyse the blockchain

- Change addresses
- Correlation of transactions
- Addresses of public services (pools, exchanges, merchants, etc.)
- Leaked business records
- Scraping of web resources
- . . .



Bitcoin blockchain analysis: a booming field

- Network-focused blockchain analysis is a thriving research field since a few years already.
- Today, an increasing number of high-level analysis tools are available:
  - https://bitiodine.net/
  - http://coinalytics.co/
  - http://www.quantabytes.com/
  - …
- Permanent nature of blockchain ensures that privacy only ever **decreases**!

What is fungibility?

Formal definition

Fungibility is the property of a good or a commodity whose individual units are capable of mutual substitution.
That is, it is the property of essences or goods which are "capable of being substituted in place of one another."

TL;DR: Fungibility means that units are **interchangable.**

Why do we care?

Fungibility is a **fundamental property** of currencies.

- In centralized currencies, fungibility is guaranteed by the government.
- . . . and in decentralized currencies?

The formal description of Bitcoin:

Information exchange protocol, that allows the transfer of units of account; These units behave like the money we are used to, having these properties:

- Durability
- Portability
- Divisibility
- Relatively rare
- **Fungibility**

Is Bitcoin really fungible?

- Social pressure not to accept *tainted* coins (theft/fraud. . .)
- If privacy can be broken, fungibility is **voluntary.**

The lack of privacy in Bitcoin threatens its fungibility.

Services that track taint render bitcoins non-fungible, eg.:

- http://www.coinvalidation.com/
- http://coinalytics.co/
- https://chainalysis.com/

What can we learn from Bitcoin?

- Voluntary fungibility does not work.
- Fungibility in cryptocurrencies requires privacy.
- People becoming more aware of the fungibility issue in Bitcoin.
- Many approaches to fix this exist nowadays.

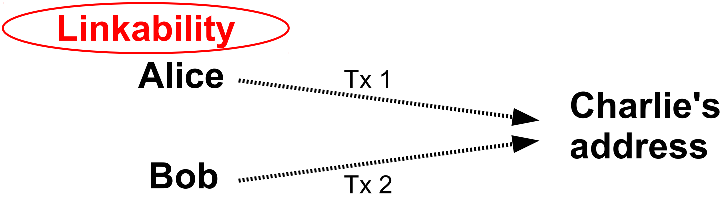
Outline

Privacy, Fungibility, and Bitcoin

Monero's Privacy Improvements
- Unlinkability and Untraceability
- Stealth Addresses
- Ring Signatures
- Viewkeys

Summary

XMR.TO



Linkability

Alice

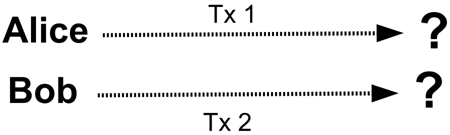
Tx 1

Charlie's address

Bob

Tx 2

The world: "*Tx 1 and Tx 2 are going to the same address!*"



Alice

Tx 1

?

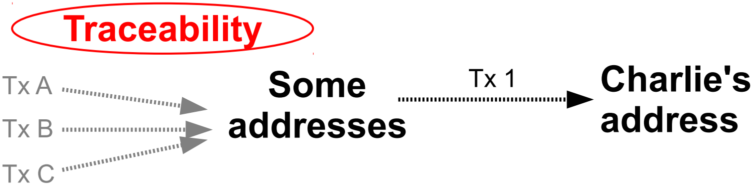
Bob

?

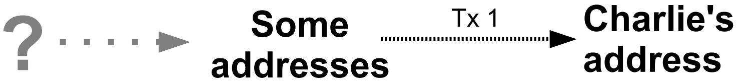
Tx 2

The world: "*No idea where the transactions are going!*"

Unlinkability



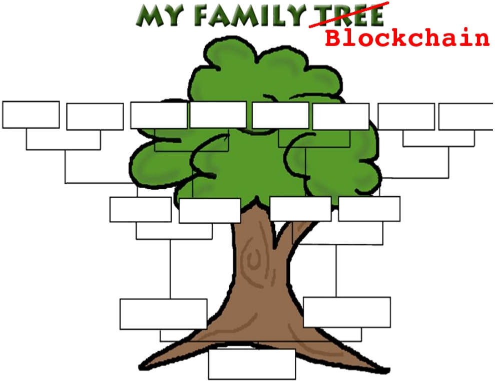
The world: "*Tx 1 is spending funds received in Txs A, B and C!*"



The world: "*No idea which funds are spent in Tx1*"

Untraceability

Simple analogy



- Unlinkability: I don't know who are the children of X
- Untraceability: I don't know who are the parents of X

Monero's approach

- Unlinkability: I don't know who are the children of X

  → Monero uses stealth addresses

- Untraceability: I don't know who are the parents of X

  → Monero uses ring signatures

Outline

Privacy, Fungibility, and Bitcoin

Monero's Privacy Improvements
- Unlinkability and Untraceability
- Stealth Addresses
- Ring Signatures
- Viewkeys

Summary

XMR.TO

Stealth addresses (1)

- The “destination” for each output is derived from the Monero address, it is different everytime
- Only the owner of the Monero address knows that an output is for him

Stealth addresses (2)

Now Charlie can give his Monero address to everybody:

- Each output sent to Charlie will look to observers as having different destinations
- Nobody can tell these outputs are going to Charlie
- Nobody can even tell these outputs are going to the same person

Stealth addresses (3)

Side remark:

- Stealth addresses discussed and proposed for Bitcoin too.
- Feasible but not very practical: requires exchange of information beforehand (either with a secure channel or an elaborated use of OP_RETURN).

Outline

Privacy, Fungibility, and Bitcoin

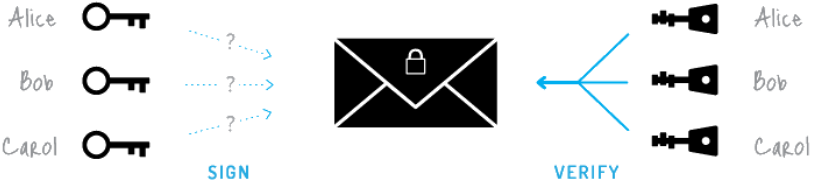
Monero's Privacy Improvements
- Unlinkability and Untraceability
- Stealth Addresses
- Ring Signatures
- Viewkeys

Summary

XMR.TO

A ring signature

- A group of cryptographic signatures with at least one real participant, but no way to tell which in the group is the real one as they all appear valid.



Real world analogy

"Say some unpopular military attack has to be ordered, but nobody wants to go down in history as the one who ordered it. If 10 leaders have private keys, one of them could sign the order and you wouldn't know who did it."

Real world analogy

> *"Say some unpopular military attack has to be ordered, but nobody wants to go down in history as the one who ordered it. If 10 leaders have private keys, one of them could sign the order and you wouldn't know who did it."*

- Can you find the author of this quote?

Brilliant idea: apply it to cryptocurrencies!

> *"Crypto may offer a way to do "key blinding". I did some research and it was obscure, but there may be something there. "group signatures" may be related."*

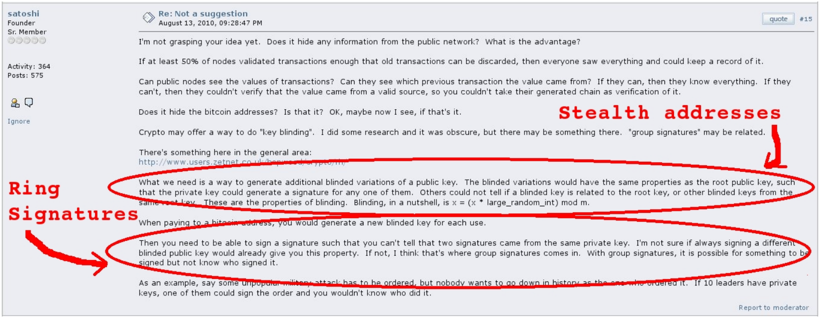
Brilliant idea: apply it to cryptocurrencies!

> *"Crypto may offer a way to do "key blinding". I did some research and it was obscure, but there may be something there. "group signatures" may be related."*

- And now, can you find the author of the quotes?

Foreseen in 2010 by... Satoshi Nakamoto!

Satoshi on ring signatures, 13/08/2010:



satoshi
Founder
Sr. Member

Activity: 364
Posts: 575

Ignore

Re: Not a suggestion
August 13, 2010, 09:28:47 PM

quote #15

I'm not grasping your idea yet. Does it hide any information from the public network? What is the advantage?

If at least 50% of nodes validated transactions enough that old transactions can be discarded, then everyone saw everything and could keep a record of it.

Can public nodes see the values of transactions? Can they see which previous transaction the value came from? If they can, then they know everything. If they can't, then they couldn't verify that the value came from a valid source, so you couldn't take their generated chain as verification of it.

Does it hide the bitcoin addresses? Is that it? OK, maybe now I see, if that's it.

Crypto may offer a way to do "key blinding". I did some research and it was obscure, but there may be something there. "group signatures" may be related.

There's something here in the general area:
http://www.users.zetnet.co.uk/hopwood/crypto/rh/

What we need is a way to generate additional blinded variations of a public key. The blinded variations would have the same properties as the root public key, such that the private key could generate a signature for any one of them. Others could not tell if a blinded key is related to the root key, or other blinded keys from the same root key. These are the properties of blinding. Blinding, in a nutshell, is x = (x * large_random_int) mod m.

When paying to a bitcoin address, you would generate a new blinded key for each use.

Then you need to be able to sign a signature such that you can't tell that two signatures came from the same private key. I'm not sure if always signing a different blinded public key would already give you this property. If not, I think that's where group signatures comes in. With group signatures, it is possible for something to be signed but not know who signed it.

As an example, say some unpopular military attack has to be ordered, but nobody wants to go down in history as the one who ordered it. If 10 leaders have private keys, one of them could sign the order and you wouldn't know who did it.

Report to moderator

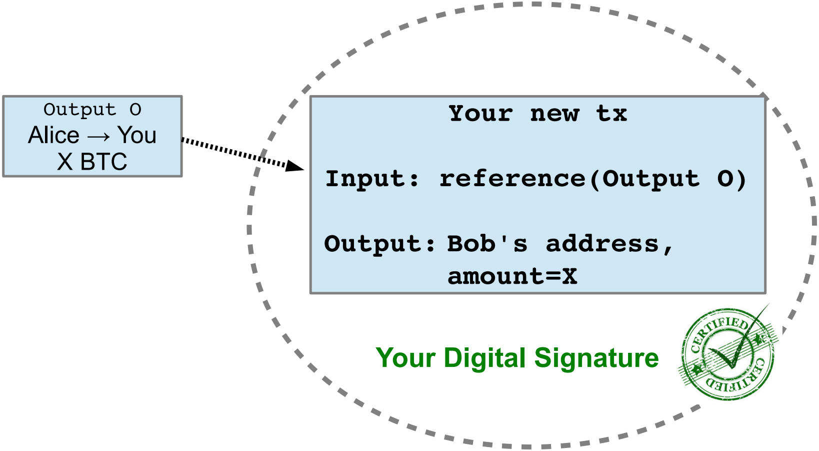
Source: https://bitcointalk.org/index.php?topic=770#msg9074

Ring signatures to achieve untraceability?

You want to spend output O of amount X, and send it all to Bob.

- In Bitcoin:
  - You construct a transaction saying “I use output O, and create a new output going to Bob's address”
  - You sign this transaction with the private key of the address that received the output O
- In Monero:
  - You find some outputs in the blockchain with the same amount X as your output O
  - You construct a transaction saying “I use one of these outputs, and create a new output going to <stealth destination>”
  - You sign this transaction using a ring signature

Usual Bitcoin signature



Output O
Alice → You
X BTC

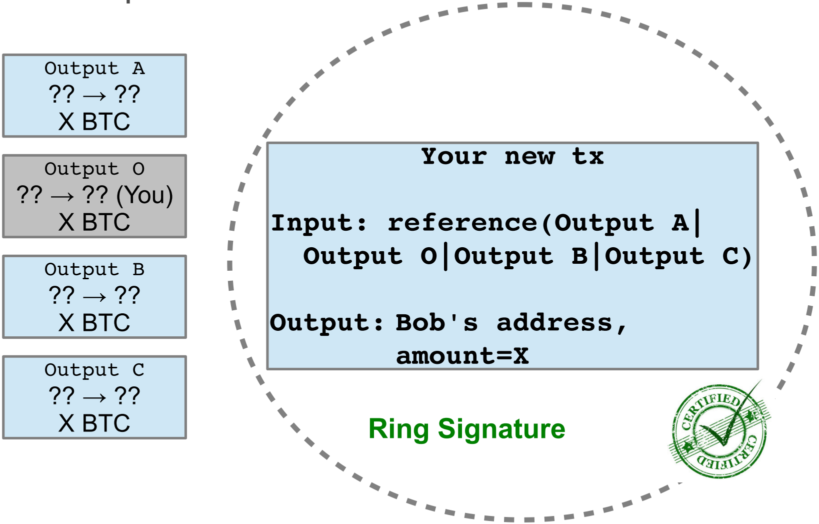
Your new tx

Input: reference(Output O)

**Output: Bob's address,
amount=X**

Your Digital Signature

Monero equivalent



Output A
?? → ??
X BTC

Output O
?? → ?? (You)
X BTC

Output B
?? → ??
X BTC

Output C
?? → ??
X BTC

```
Your new tx

Input: reference(Output A|
  Output O|Output B|Output C)

Output: Bob's address,
        amount=X
```

Ring Signature

Ring signatures achieve untraceability

- Not only you are “mixing” your output when actually spending it: everybody is constantly using other people's output in ring signatures, they will use yours too
- No need for people controlling the other outputs in the ring signature to be online or active
- Combinatorial explosion kicks in very quickly and render impractical forensic analysis of the blockchain

Ok, ring signatures are cool! But...

- Output spent using ring signature is not “spent for sure”: how to prevent double-spend?

Ok, ring signatures are cool! But...

- Output spent using ring signature is not “spent for sure”: how to prevent double-spend?
  - Signatures are deterministic, so spending the same output twice can be detected easily

Ok, ring signatures are cool! But...

- Output spent using ring signature is not “spent for sure”: how to prevent double-spend?
    - Signatures are deterministic, so spending the same output twice can be detected easily
- To spend my output of amount X using a ring signature, I must find other outputs with the same amount X! Isn't it difficult?

Ok, ring signatures are cool! But...

- Output spent using ring signature is not "spent for sure": how to prevent double-spend?
  - Signatures are deterministic, so spending the same output twice can be detected easily
- To spend my output of amount X using a ring signature, I must find other outputs with the same amount X! Isn't it difficult?
  - Outputs are automatically broken down into common denominations. For instance, sending 11.5 XMR actually creates an output of 10, plus another one of 1, plus another one of 0.5.
    Thus, always plenty of outputs with proper amount. And all of them use their own ring sig!

Summary of privacy aspects

- Monero hides destination of transactions
- Monero hides origin of transactions
- Monero hides precise amount being transferred
- There is no "rich list": nobody can see the amount associated to each address

Ok, privacy is cool. But?...

- Having a fully-private decentralized ledger is useful, but also problematic
  - No way to comply in many tax jurisdictions
  - No way to prove a transaction was made in case of dispute
  - No way to be transparent about donations for a non-profit
  - No way to prove certain holding to ask for loans, etc.

Outline

Privacy, Fungibility, and Bitcoin

Monero's Privacy Improvements

- Unlinkability and Untraceability
- Stealth Addresses
- Ring Signatures
- Viewkeys

Summary

XMR.TO

Viewkeys

A clever cryptographic mechanism, the "viewkey". For each address, you have:

- A spend key ($\approx$ Bitcoin private key)
- Plus a viewkey
  - Give viewkey to somebody: they can see which outputs you control (= what you received, and your balance).

Viewkey mechanism exists also for one single transaction only.

Viewkey: transparency or privacy, user's choice!

- With optional, voluntary use of viewkeys, Monero transparency becomes close to Bitcoin's one
- Monero provides high privacy by default whilst still providing opt-in full transparency when desired
- It does all of this at the (very elegant) cryptographic layer

Outline

Privacy, Fungibility, and Bitcoin

Monero's Privacy Improvements

Summary

XMR.TO

More Cool Tech Stuff

Example: Monero has an adaptive block size.

- Bitcoin: the maximum block size is hardcoded
(Ever heard of 1MB vs. 20MB debate?...)
- Monero adapts the maximum block size with a simple rule (very similar to mining difficulty adjustments).

  Idea is that the size is determined by free market mechanism.

Monero: a great future?

- Demand for more fungible/private cryptocurrencies
  - Bitcoin is a decentralized fully transparent public ledger
  - We now have a technology for a decentralized private-by-default/transparent-on-demand public ledger
- Monero is the best contender currently for that role

```
- Electronic cash is easy.  Facebook could do it.
- Private electronic cash is harder, but Chaum
  figured out how to do it in the early 90s.
- Decentralized electronic cash is even harder.
  That's Bitcoin.
- Decentralized private electronic cash is even
  harder.  That's the next step.
```

– pdtmeiwn on /r/bitcoin

Ressources

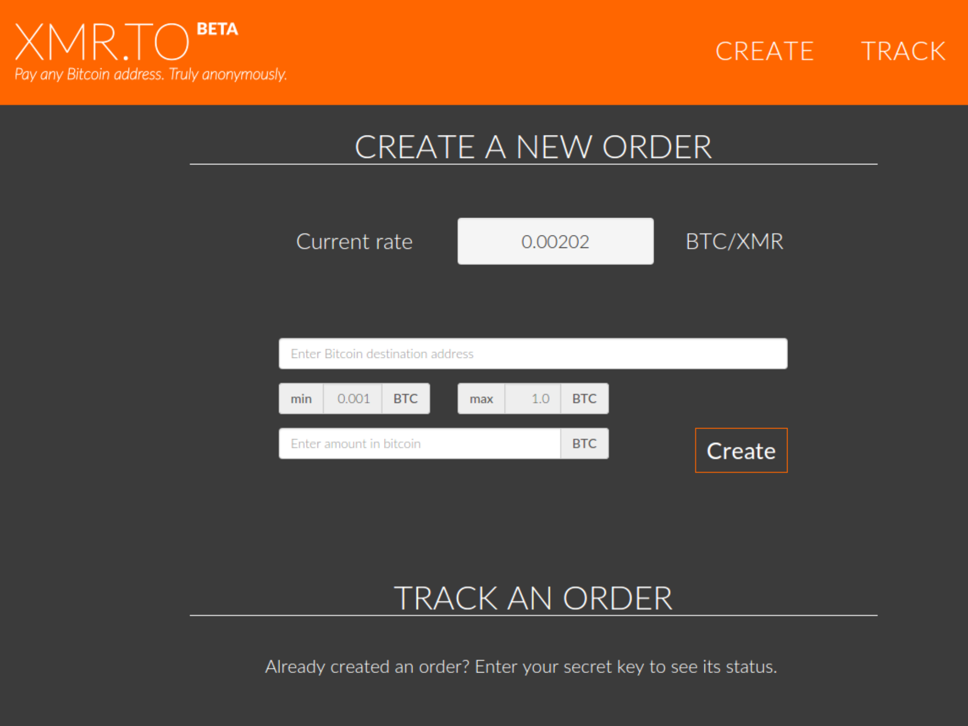
- Online: `http://getmonero.org`
- In real life, upcoming Monero meetups in Europe:
  - Brussels – 19th of May
  - Paris – 21th of May
  - Amsterdam – 23th of May
  - Berlin – 24th of May

Main problem of Monero

- Theory, usage practices and software are quite different from Bitcoin
- Few merchants support Monero
- Few Monero-specifc services exist
- Getting started is difficult

Our goal

- Make Monero usable in many places
- Low barrier of entry
- Maintain primary advantage of Monero (privacy)



XMR.TO BETA

Pay any Bitcoin address. Truly anonymously.

CREATE A NEW ORDER

Current rate 0.00202 BTC/XMR

Enter Bitcoin destination address

min 0.001 BTC

max 1.0 BTC

Enter amount in bitcoin BTC

TRACK AN ORDER

Already created an order? Enter your secret key to see its status.