Monero

an anonymous altcoin

Dionysis Zindros

ATHECRYPT 2016

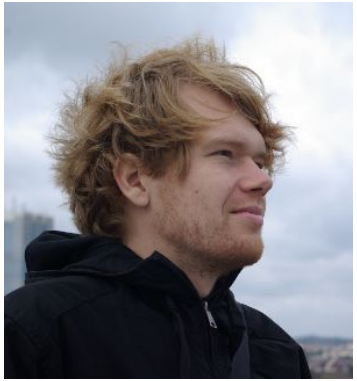
Overview

- Bitcoin’s problems
- Monero’s solutions
- Fungibility
- Anonymity
- Unlinkability
- Untraceability

Acknowledgments

Bitcoin Genève, Université Libre de Bruxelles

Jérémie Dubois-Lacoste

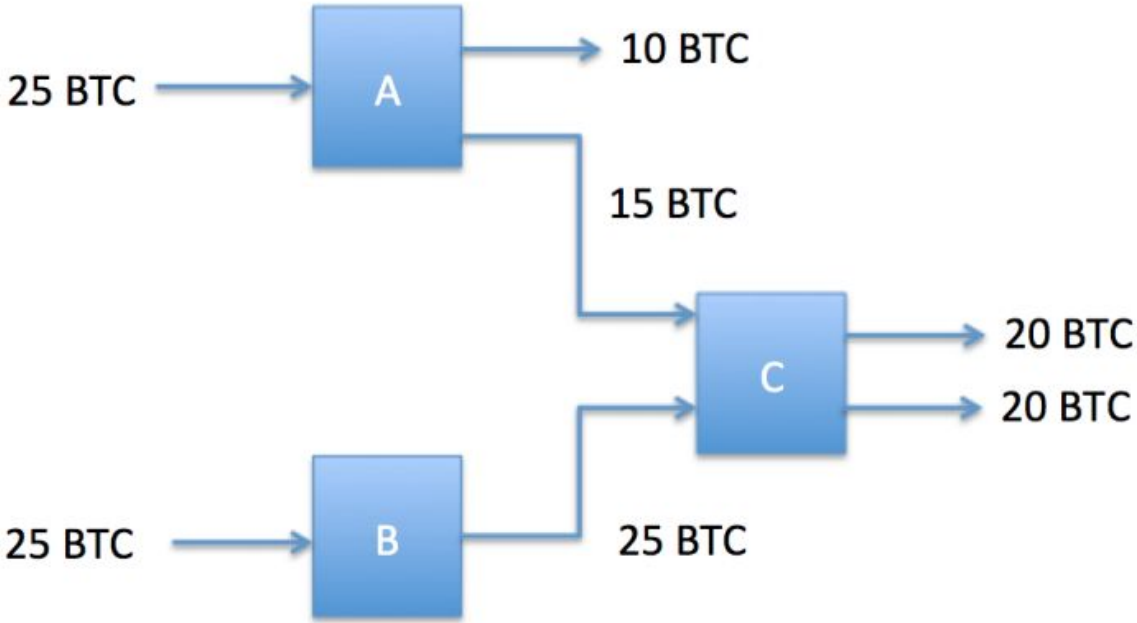


Arne Brutschy

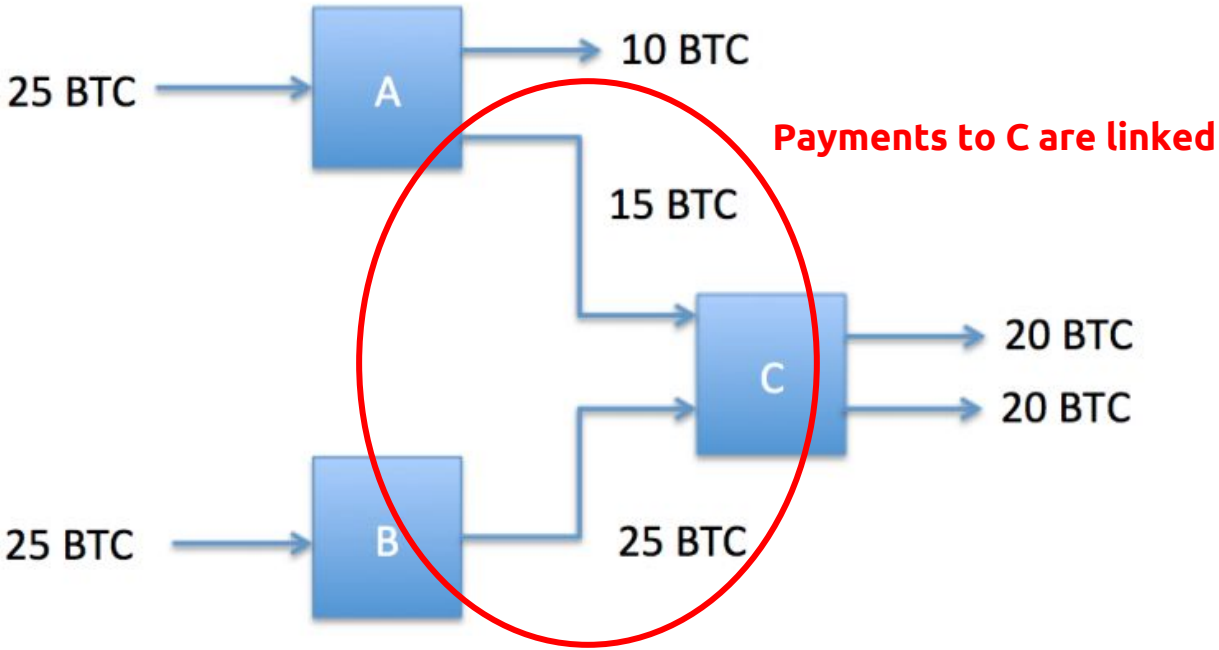
Bitcoin

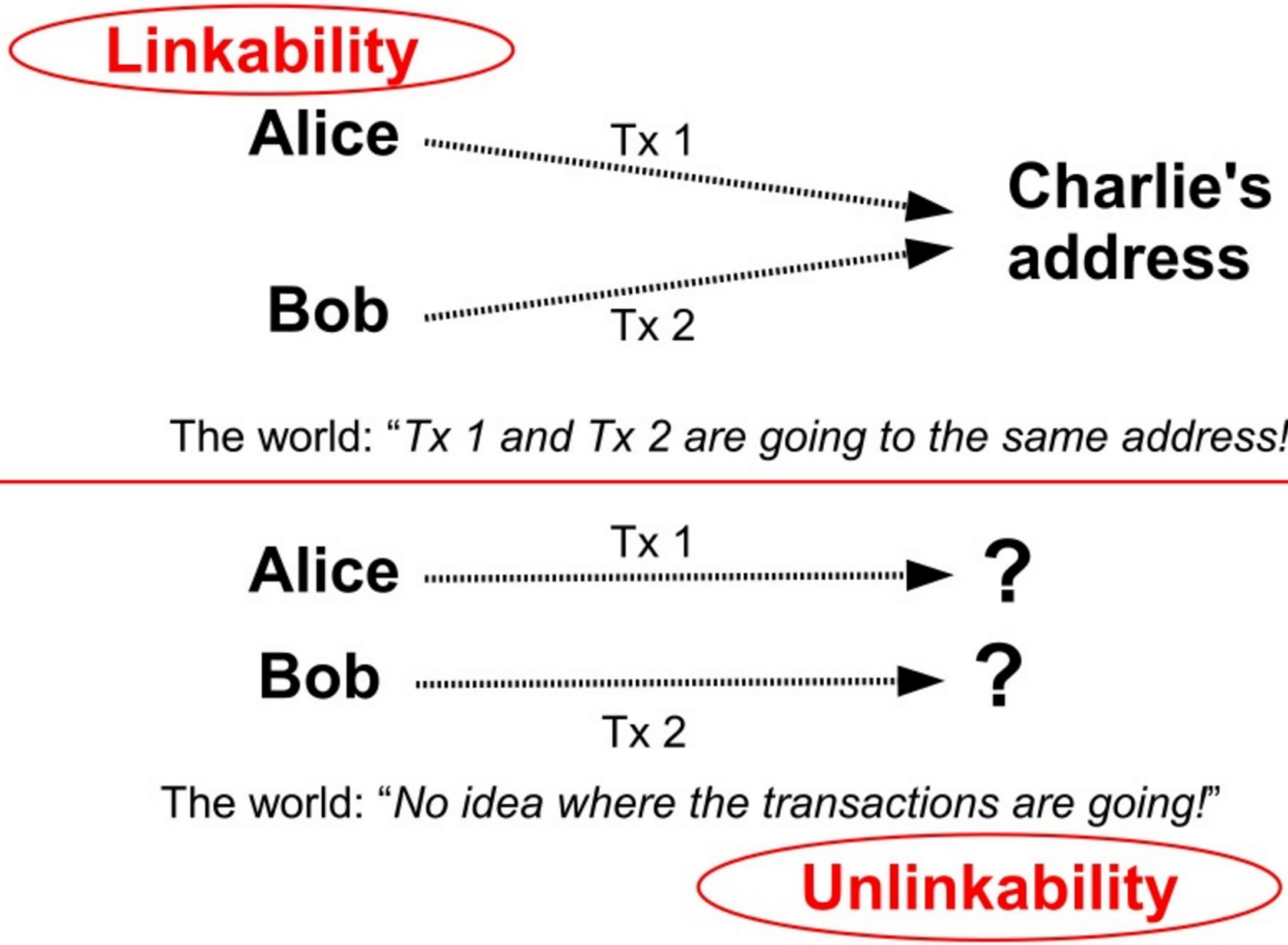
- The first decentralized cryptocurrency
- But it has problems
- It is not **fungible**
- It is not **anonymous**
- It’s **linkable**
- It’s **traceable**

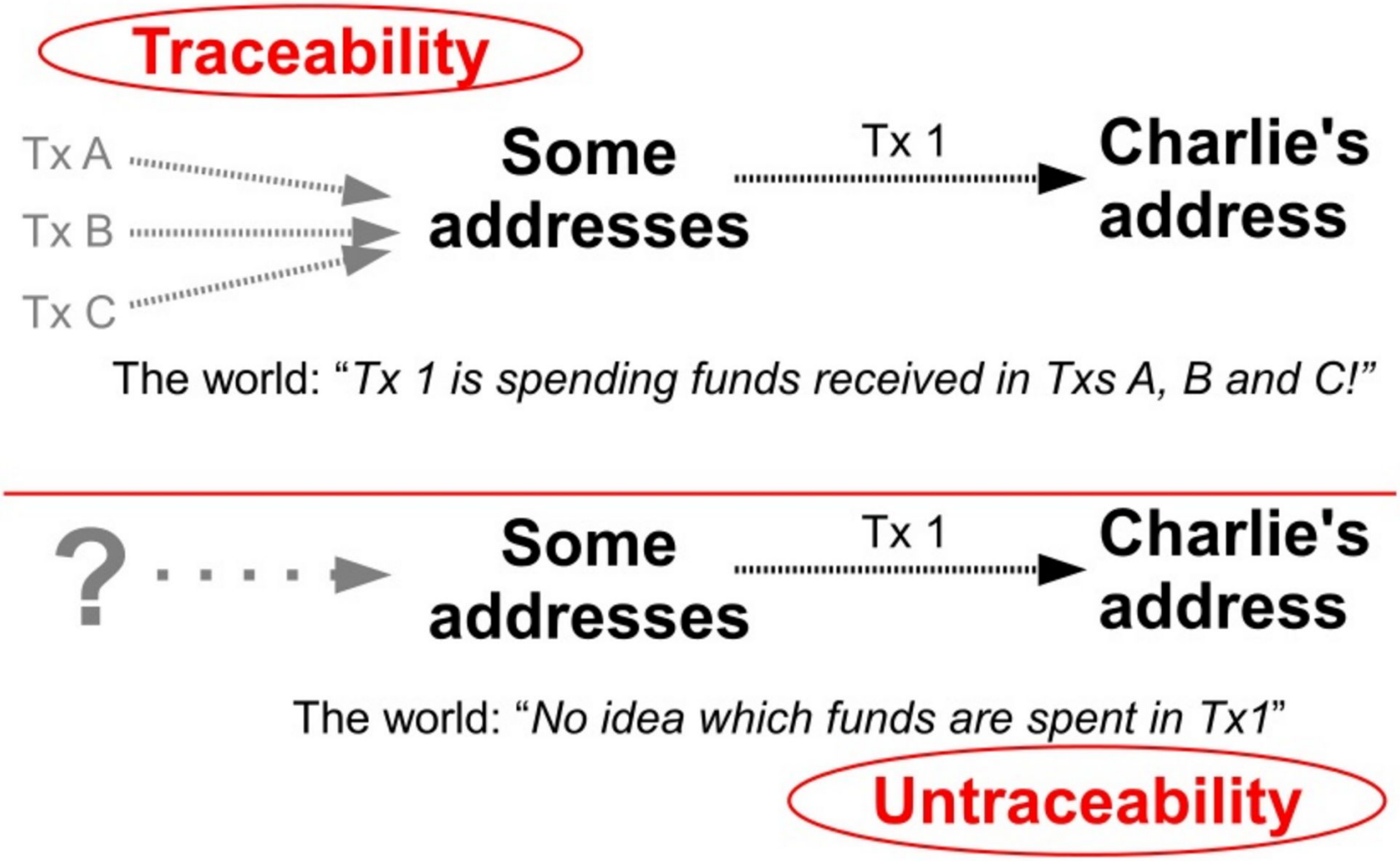
Bitcoin’s graph


25 BTC
A
10 BTC
15 BTC
C
20 BTC
20 BTC
25 BTC
B
25 BTC

Linkability




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


Traceability
Tx A
Tx B
Tx C
Some addresses
Tx 1
Charlie's address
The world: "Tx 1 is spending funds received in Txs A, B and C!"
?
Some addresses
Tx 1
Charlie's address
The world: "No idea which funds are spent in Tx1"
Untraceability

Forensic analysis of blockchains

Forensic analysis of bitcoin **reveals identities**

What can we use to forensically analyze the bitcoin blockchain?

- **Change** addresses
- Transaction **correlation**
- **Public** service addresses (pools, shops)

Blockchain forensic analysis services

- Booming new field
  - bitiodine.net
  - coinalytics.co
  - quantabytes.com
- Blockchain is **permanent**
- Privacy can only decrease with time

Why do we need financial privacy?

- Supported by long-history of cypherpunk philosophy
- Private crypto currencies will dominate
- Evidence illustrates privacy benefits the honest
- Needed if we want to achieve **true decentralization**
- Otherwise centralization can be forced upon us through courts of law

“Those people who do not have power, we mustn't reduce their power even more by making them yet more transparent.”

Julian Assange

Fungibility

Fungibility is the property of a commodity whose individual units are capable of **mutual substitution**.

Fungible cryptocurrencies have units that are **interchangeable**.

Bitcoin’s lack of fungibility

- All bitcoins are equal, but some bitcoins are **more equal** than others
- Coins are traceable
- **Colored** coins
- **Tainted** coins
- Privacy can be broken, so fungibility is **voluntary**
- coinvalidation.com
- Social pressure exists to break fungibility in bitcoin

Why do we want fungibility?

- **Fundamental** property of currencies
- If I get paid, I need to know that I can spend my money
- We know from bitcoin voluntary fungibility does not work
- Lack of fungibility **centralizes** nature of coins
    - Who is the **authority** to determine tainting?

Achieving blockchain untraceability

- Tumblers (bitcoin)
  - Centralization
- Coinjoin (bitcoin)
  - Opt-in, off by default
  - Anonymity set is too small
- Zerocash
  - Large proofs
  - Costly fees
  - Slow
- **Monero**

Achieving bitcoin unlinkability

- Bitcoin **stealth** addresses
  - Requires interactivity
  - Or exchange of information beforehand
  - Or elaborate use of OP_RETURN
- **Renew** addresses every time
  - Impractical

Monero

- Altcoin
- Rewritten from scratch, not a fork
- Created April 2014
- Based on **CryptoNote** protocol

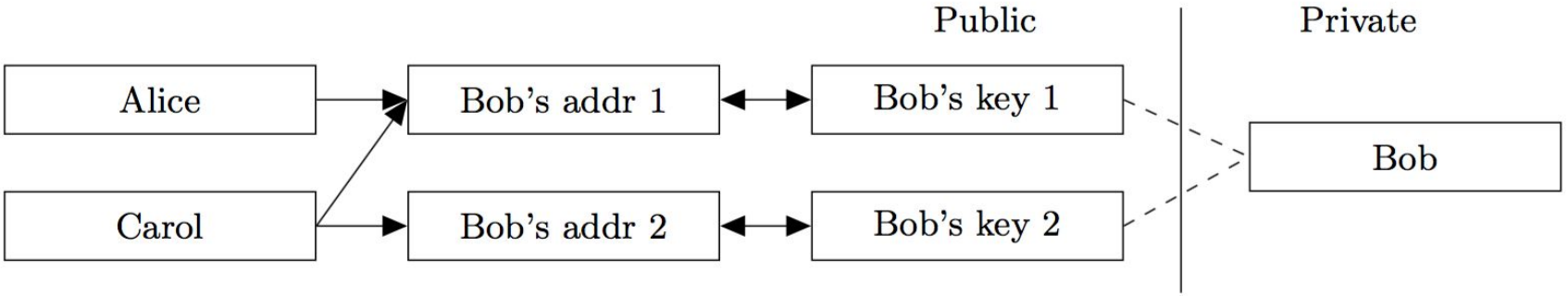
Monero overview

- **Stealth addresses** achieve **unlinkability**
- **Ring signatures** achieve **untraceability**

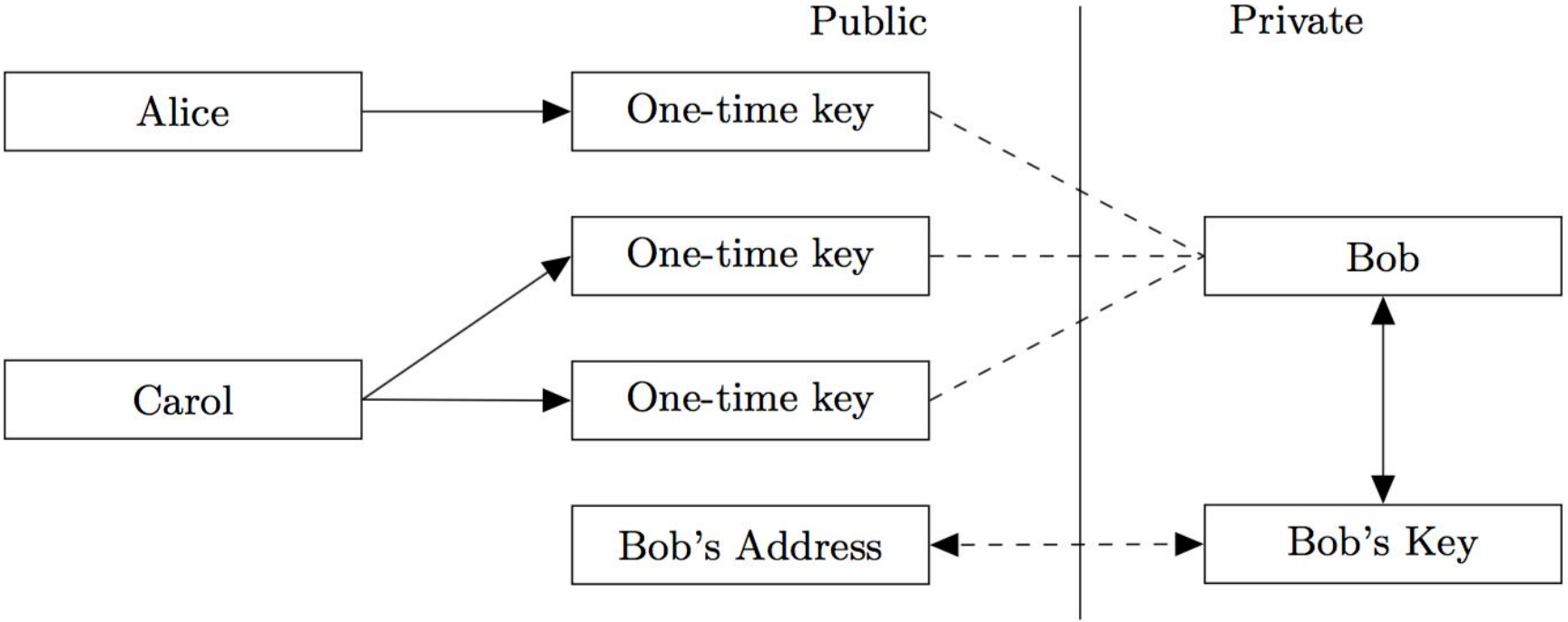
Monero’s unlinkability

- Monero uses **stealth** addresses

Bitcoin address model



CryptoNote address model



Stealth addresses

- Bob maintains **one** pre-generated **public** address
- To send money to Bob, Alice generates a **one-time** key based on Bob's public address
- Bob monitors the blockchain for payments
- Bob can recognize payments to one-time keys from his address using his private key
- Only the **owner** of a monero address knows the output is for him
- Mallory cannot distinguish whether a payment belongs to Bob

Stealth addresses

- Bob can now **publish** his stealth address to everybody
- Each output sent to Bob will look to observers as having different destinations
- Nobody can tell these outputs are going to Bob
- Nobody can tell these outputs are going to **the same person**

Stealth addresses

- Bob creates two EC key pairs **(A, a)** and **(B, b)**
- **(a, b)** is his private key
- **a** is the *view key* (or tracking key)
- **b** is the *spending key*
- **(A, B)** is his public key and can be encoded into an *address*

Send money to stealth address

G is elliptic curve base point
H is hash function

- Alice wants to pay bob to **(A, B)**
- She generates random **r** and publishes **R = rG**
- Computes one-time key **P = H(rA)G + B**

Viewing money on stealth address

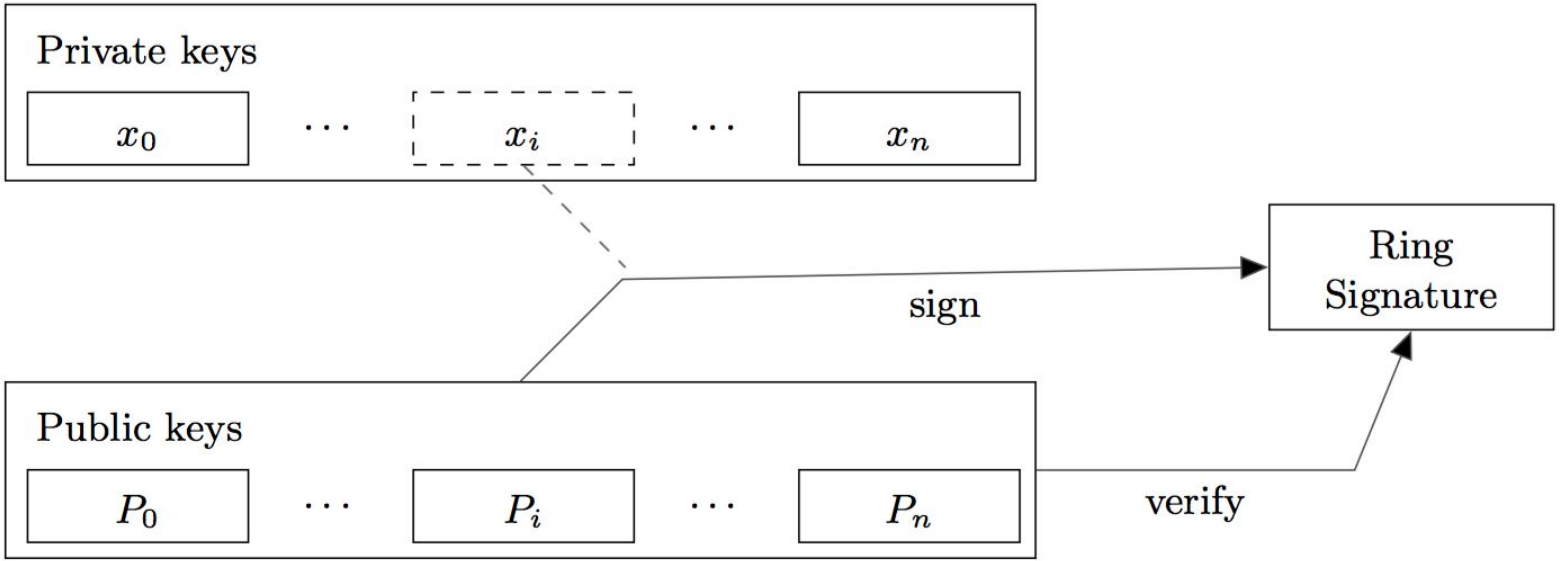
- For every transaction on the blockchain, Bob computes **P’ = H(aR)G + B**
- Bob checks if **P = P’**
- **P’ = H(aR)G + B**
  = H(arG)G + B
  = H(raG)G + B
  = H(rA)G + B
  = P
- Only **a** is needed to view money; **a** is a *view key*

Spending money from stealth address

- Bob can compute **x = H(aR) + b** such that **P = xG**
- **xG = (H(aR) + b)G**
  = H(aR)G + bG
  = H(aR)G + B
  = P
- Bob can spend by signing with **x**
- **b** is needed to spend money; **b** is a *spending key*

Ring signatures

Ring signatures



Ring signature

- We control key (P_S, x_S)
- Pick an anonymity set:

  $S' = \{ P_1, P_2, \ldots, P_N \}$

- Augment the public key set with our own key

  $S = S' \cup \{ P_S \}$

- Sign message **m** using **S** and x_s and output signature **σ**

Ring signatures terminology

GEN: Produces key pair **(P, x)** where **P** is public, **x** is private and an associated public key image **I** (such that $\mathbf{P} \rightarrow \mathbf{I}$ is one-way and masked with **x**)

SIG: Takes message **m**, an anonymity set $\mathbf{S' = \{ P_i \}_{i \neq s}}$ and a pair $\mathbf{(P_s, x_s)}$, outputs a signature **σ** and a set $\mathbf{S = S' \cup \{ P_s \}}$

VER: Takes message **m**, public key set **S**, signature **σ** and outputs "*true*" or "*false*"

LNK: Takes a signature **σ** and a public key image set $\mathcal{I} = \mathbf{\{ I_i \}}$ and outputs "*linked*" or "*independent*"

Ring signature

- **Correctness**: **VER(m, S, SIG(m, x_S, S' U {P_S}))** is *true*

If a message is signed with a private key from a set of public keys, the signature can be verified with this set of public keys.

Ring signature

- **Unforgeability**: Given only a public key set **S**, it is impossible to produce a valid signature

Ring signature

- **Linkability**: The same private key cannot be used to sign two different messages

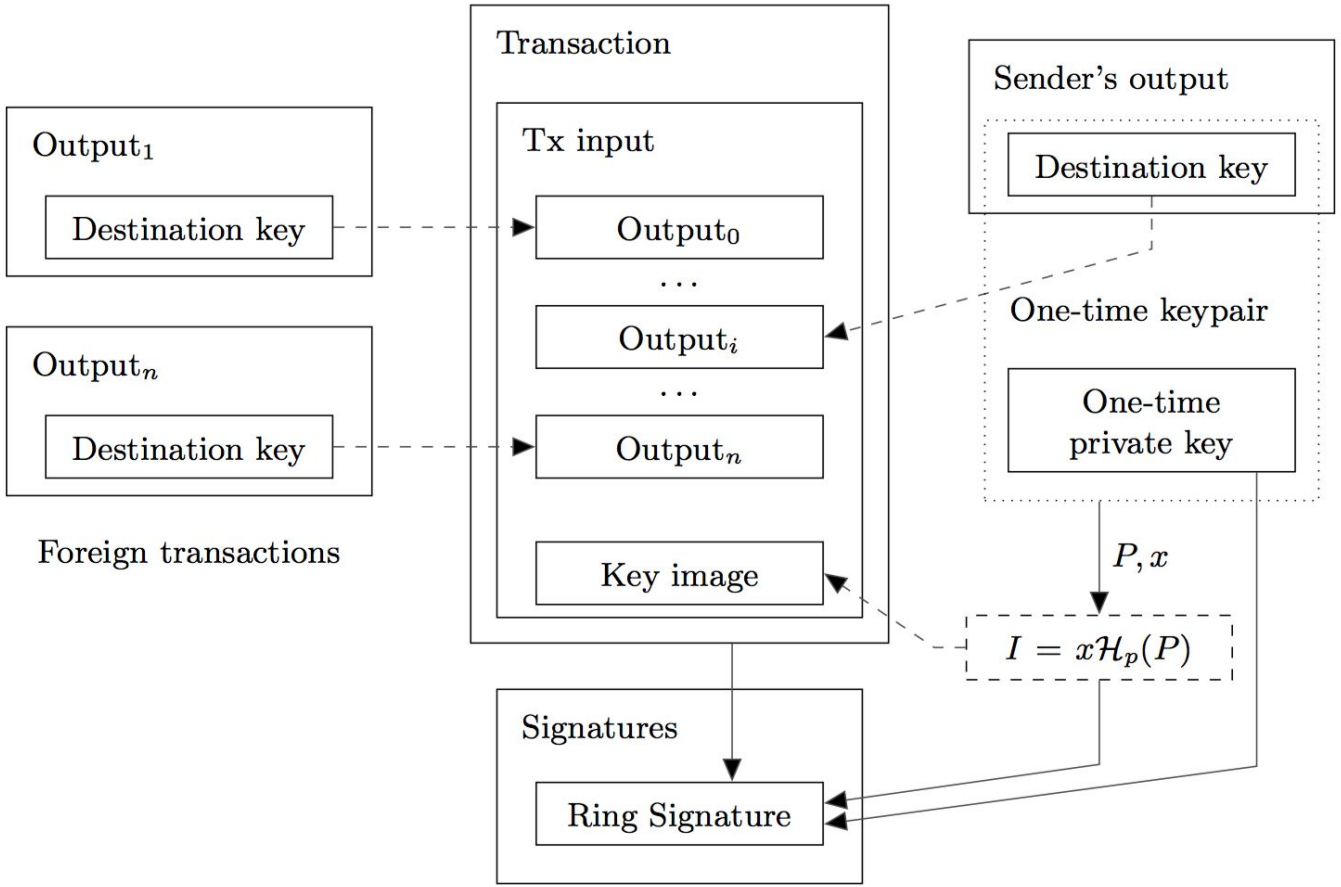
Given all the secret keys $\{ x_i \}$ for a set of public keys **S**, it is impossible to produce $n + 1$ distinct signatures $\sigma_1, \sigma_2, \ldots, \sigma_{n+1}$

Ring signature

- **Anonymity**: Given a signature **σ** and a set **S**, it is impossible to determine the public key associated with the signer (with probability **1/n + non-negl**)

Monero’s untraceability

- Monero uses **ring signatures**
- To make a payment, Alice picks an **anonymity set S** from the **utxo**
- She ring-signs as **σ** the anonymity set **S** with her private key $\mathbf{x}_s$
- Alice gives key image **I** of her public key $\mathbf{P}_s$ to Bob
- Alice proves to Bob that the ring signature was made using some private key associated with some public key whose image is **I**
- Bob receives payment and validates ring signature **σ**
- Bob cannot distinguish which private key from the anonymity set was used
- Transaction graph becomes **non-deterministic**


Transaction
Tx input
Output$_0$
...
Output$_i$
...
Output$_n$
Key image
Output$_1$
Destination key
Output$_n$
Destination key
Foreign transactions
Sender's output
Destination key
One-time keypair
One-time private key
P, x
$I = x\mathcal{H}_p(P)$
Signatures
Ring Signature

Spending money

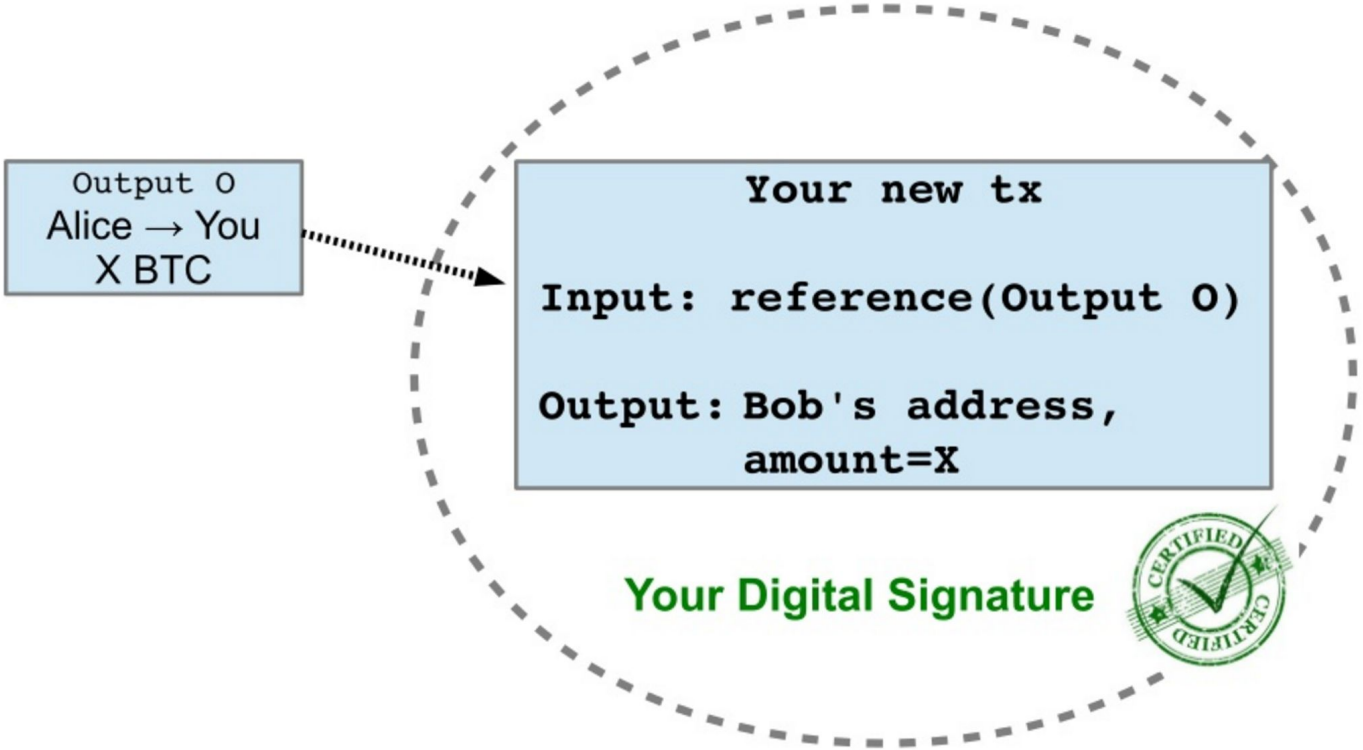
In bitcoin:

- Sign your utxo **O** of amount **X** using the private key corresponding to the public key you used for receiving **O**

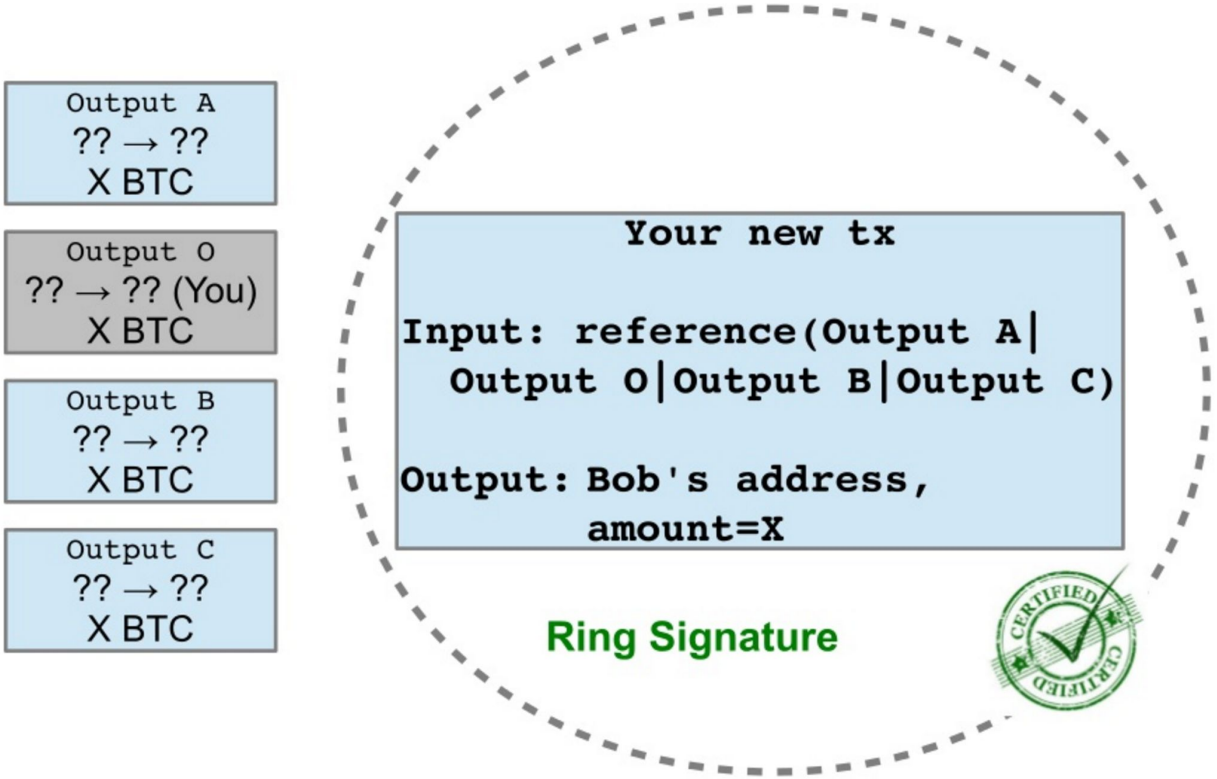
In monero:

- Find anonymity set from utxo* with same amount **X** as **O**
- Sign using anonymity set and the private key corresponding to the public key you used for receiving **O**

Bitcoin TX

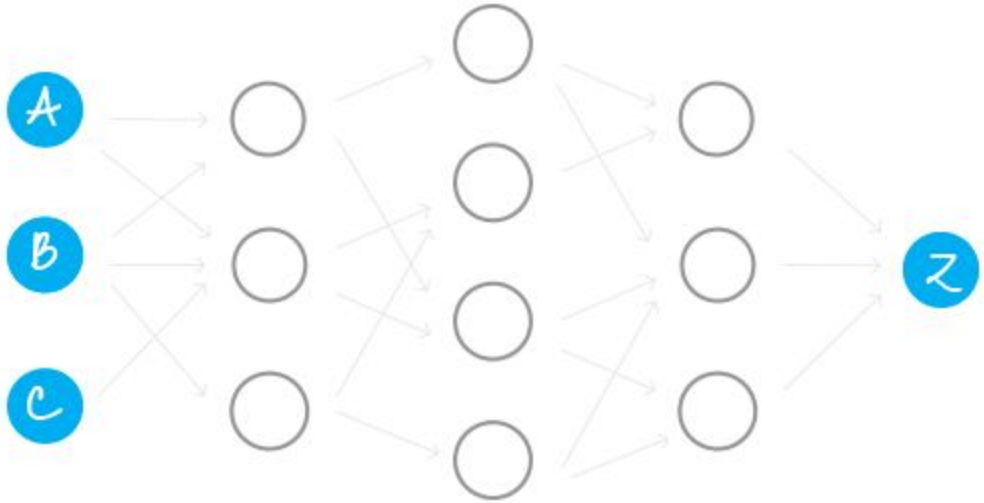

Output 0
Alice → You
X BTC
Your new tx
Input: reference(Output 0)
Output: Bob's address,
amount=X
Your Digital Signature
CERTIFIED
CERTIFIED

Monero TX


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
CERTIFIED
CERTIFIED

Ring signatures

- You’re mixing your outputs with others’
- Others are mixing your output with theirs constantly too!
- No need for interactivity or consent from others in your anonymity set
- Forensic analysis impossible due to combinatorial explosion


A
B
C
Z

Double spend avoidance

- Possible due to LNK function
- For each utxo, keep list of public key images **I**
- When we wish to validate new transaction:
  - Take its input anonymity set **S**
  - For each input public key **P** ∈ **S** verify independence
  - Find list of public key images **I** associated with plausible spendings of **P**
  - Run **LNK** on **σ** against list
- Spending the same output twice is easily detected

Spending money

In bitcoin:

- Sign your utxo **O** of amount **X** using the private key corresponding to the public key you used for receiving **O**

In monero:

- Find anonymity set from utxo* with **same amount X** as **O**
- Sign using anonymity set and the private key corresponding to the public key you used for receiving **O**

Denominations

- Monero outputs are split into decimal denominations
- Similar to bank notes
- To send **11.5 XMR**, we send **10 XMR + 1 XMR + 0.5 XMR**
- Each denomination is sent to stealth address by reapplying stealth algo

Monero achievements

- Hides transactions destination (stealth)
- Hides transactions origin (ring)
- Hides precise amounts (denominations)
- There is no “rich list” like in bitcoin

View keys

- View keys can be used to comply with taxation if we want
- Can be used to prove transaction was made in case of dispute
- Can be used to achieve transparency in case of non-profits
- Could be used in solvency proofs
- The user can choose privacy or transparency as they wish
- Transparency is opt-in only

Real-world statistics

- Market capitalization: $5,222,000
- 1 XMR = 1 mBTC

Bonus

- **CryptoNight mining** achieves **egalitarian** proof-of-work
- 60 seconds expected block generation time for **fast confirmation**
- **Adaptive** block size
- **Smooth emission**

thanks ♥

 @dionyziz

45DC 00AE FDDF 5D5C B988 EC86 2DA4 50F3 AFB0 46C7

References

CryptoNote whitepaper:

https://cryptonote.org/whitepaper.pdf