

Module 5: Privacy and Anonymity

Aron Kondoro & Anthony Kigombola

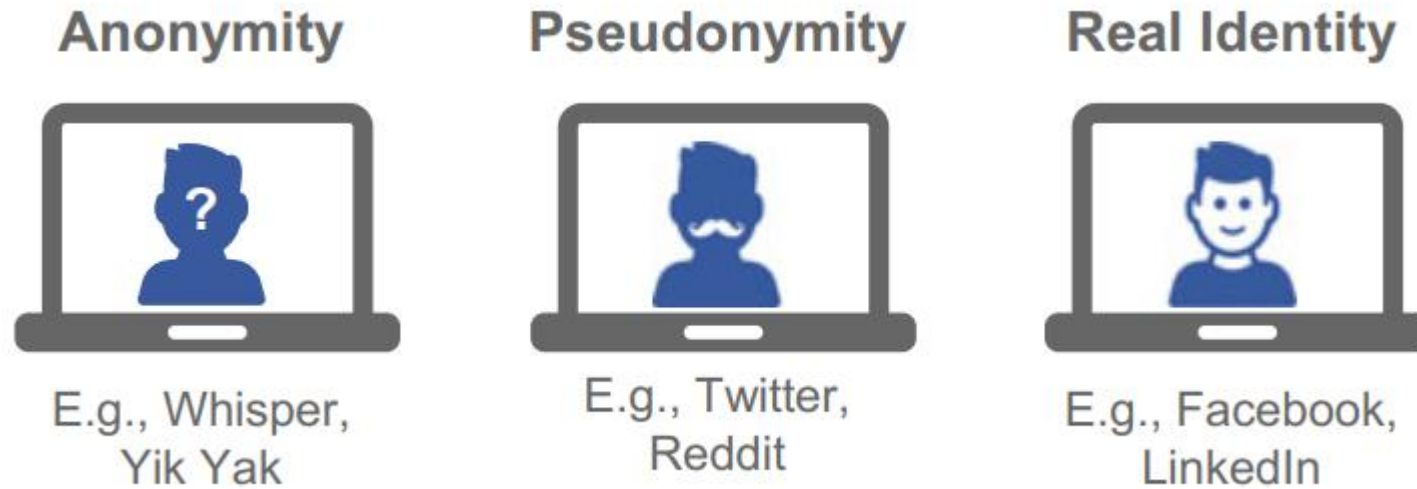
Introduction

- Bitcoin is a pseudonymous currency
 - Any transaction/account is traceable
 - Identity of account owner is a challenge
- Different from real-world financial system which require identity verification

Anonymity vs Pseudonymity

- Anonymity = no name is required
- Pseudonymity = false name can be used
- Bitcoin is pseudonymous because it requires a public address which acts as an identifier
- To make a pseudonymous system like Bitcoin anonymous, linking addresses and transactions to the same originator should be as difficult as possible, so addresses and transactions must be unlinkable
- A Bitcoin user who is concerned about her anonymity wants to ensure that it is not feasible to link a payment's sender and ultimate recipient by examining the blockchain

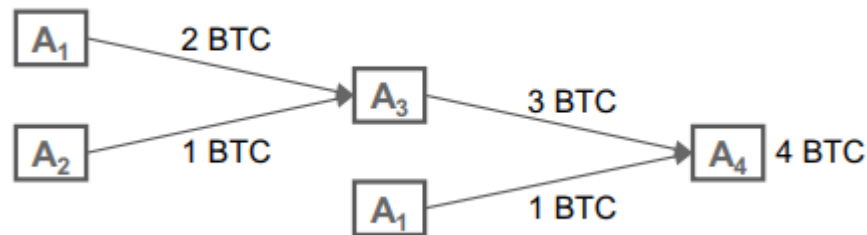
Anonymity vs Pseudonymity



- It is possible to infer information about a user using metadata e.g. time of use, style of language
- For instance, Satoshi Nakamoto frequently published changes to the Bitcoin code repository from UTC 13:00 to UTC 06:00, which suggested that he resided somewhere in the Americas (if he worked during the day)

Taint Analysis

- Taint analysis is one of the measures of anonymity in blockchains
- Calculates the degree to which two addresses are related i.e. one is tainted by another
- The correlation between two addresses as the percentage of bitcoins that originate from the same address in an individual transaction



De-anonymization

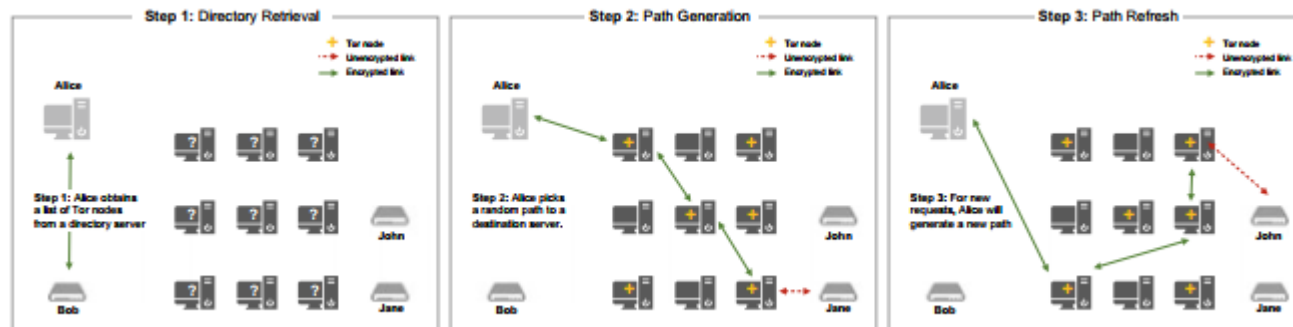
- Transaction Graph Analysis
 - An attacker can analyse the public data on a blockchain to link transactions/addresses
- Network-Layer De-anonymization
 - An attacker who controls enough nodes at various locations can determine the location of the first node that broadcasts a transaction i.e. the transaction originator

Transaction Graph Analysis Tools

- www.blockchain.com
- <https://oxt.me>

The Onion Router (TOR) Network

- A common approach to ensure user anonymity online
- A distributed, anonymous communication service that relies on an overlay network



TOR Components

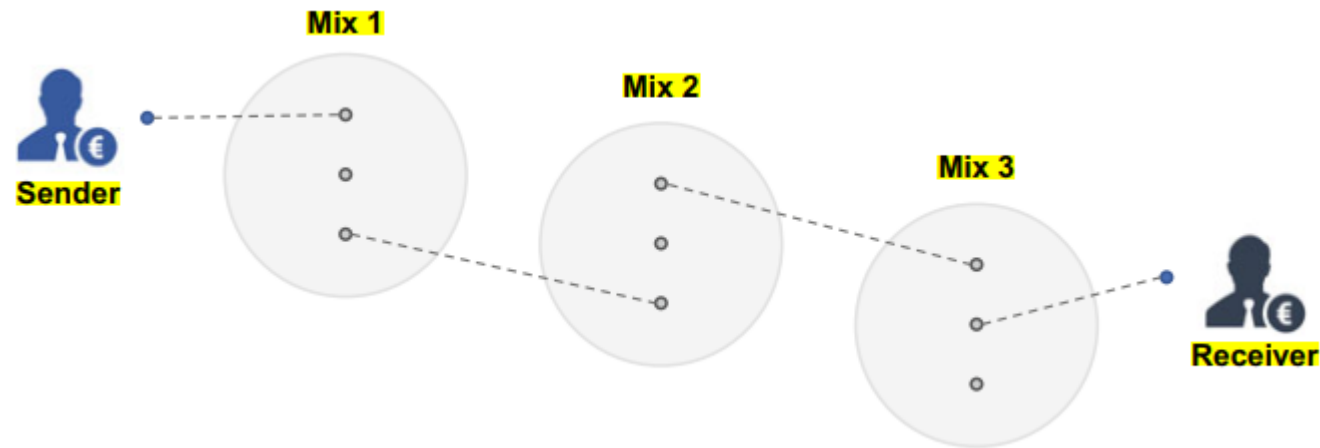
- An overlay Network (ON) that selects and connects a subset of nodes in the network.
- Onion Routers (OR) that route traffic.
- An Onion Proxy (OP) that fetches directories and creates virtual network circuits.
- TOR client software

TOR Features and Limitations

- Anonymity is established because only the user has all the information necessary to reconstruct the full communication path
- None of the relay nodes, the visited website, or even other Internet services used have enough information to know fully who is communicating with whom
- TOR-based solutions for providing end-to-end anonymity for communicating with a blockchain network are not always practical, given the overhead and technical expertise required

Mixing Models

- The most intuitive approach to combating transaction graph analysis is called mixing, which delivers anonymity through an intermediary
- As long as a single mix in the group remains honest and deletes its transaction records, no one will be able to connect the inputs and outputs of the overall process later on



Mixing Services

- <https://blender.io/>

CryptoMixer

Enter CryptoMixer code ?

1

Please enter bitcoin forward to address:

1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xgX

Add address

Set delay

Service fee: **0.5000%** - **0.00%** (discount) ?

Show calculator

CONTINUE

Mix my bitcoins

CryptoMixer

2


Download the [Letter of Guarantee](#) before send us coins

3

Send your coins (min 0.001, max 476.4021 BTC) to:

16MN6q4tfMLavYix7ArXrQWYMqyKJrrpkQ

Add incoming address

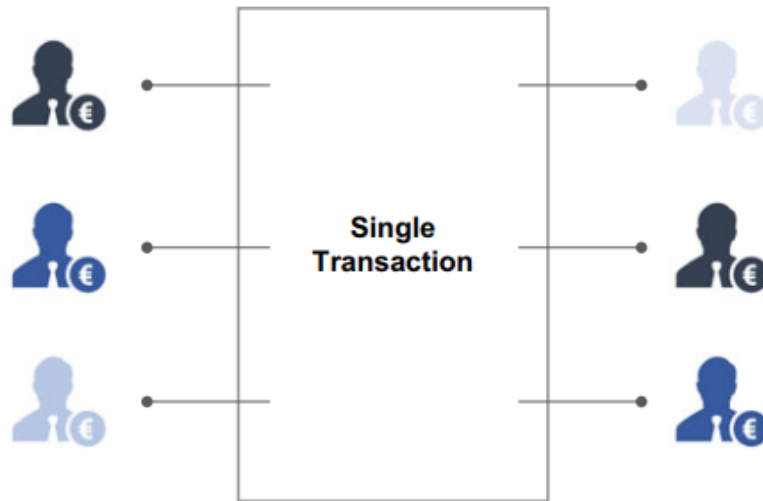


Decentralized Mixing

- Mixing has challenges
 - To execute a mixed transaction, users must first identify each other
 - Given that control of the transactions must be pooled, it is unclear that thefts can be avoided
 - Organizing mixed transactions centrally, one party will still have to obtain all the relevant information
- As a result, various decentralized mixing models have been proposed for both the Bitcoin and the Ethereum ecosystems

Coinjoin Model

- Proposed by core Bitcoin developer Greg Maxwell in 2013
- The model describes a group of Bitcoin users who come together to create a single Bitcoin transaction consisting of input transactions of equal value from each user



Coinjoin Steps

1. Identify several other users to partake in the Coinjoin transactions.
2. Exchange input and output addresses with the other users.
3. Construct a single central aggregated transaction.
4. Distribute the aggregated transaction to all involved users. (All must sign)
5. Post the transaction publicly. (After all signatures are provided)

Coinjoin Anonymity

- To obtain a specific input-output mapping on a de-centralized mixing model, an attacker can infiltrate a Coinjoin transaction by creating many identities, thus obtaining all but one of the input-output mappings; if successful, that one mapping can be identified.
- With decentralized mixing models, the users do not know who their peers are, and for the model to work, all input and output addresses must be communicated to all peers involved.

Zero-Knowledge Proofs

- Zero Knowledge Proofs are mechanisms through which Person A can prove to Person B that Person A knows a secret without revealing any details about the secret to Person B
- Zero proofs criteria
 - Completeness: If the prover's statement is true, it will convince a verifier.
 - Soundness: If the prover's statement is false, it cannot convince the verifier.
 - Zero-knowledge: If the statement is true, the verifier does not learn any information other than that the prover's statement is true
- Zero-knowledge proofs can be used to ensure anonymity

Privacy Coins

- Based on protocols that follow a privacy-first approach unlike Bitcoin, Ethereum
- Designed to address critical weaknesses i.e. privacy guarantees like using cash
- With Bitcoin it is possible to view the history of any payment that has ever occurred

Previous solutions

- Bitcoin laundries i.e. employ mixing models
 - Can be compromised
 - A critical mass of transactions must be pooled together to obscure an individual transaction's origins if they are to operate effectively
- TOR and mixing models
 - are not yet comprehensive or integrated, leaving room for user error and ambiguity

Zero Currencies

- Zerocoin and Zerocash
- They extend the Bitcoin Protocol
- Zerocoin obscure transacting parties by using an inbuilt mixing model
i.e. no need to trust mixes or peers
- Zerocash is similar but also obscures transaction amount
- There is also Monero

Zerocoin

- Initially designed to be part of Bitcoin
- Minting a Zerocoin
- Spending a Zerocoin

Zerocash

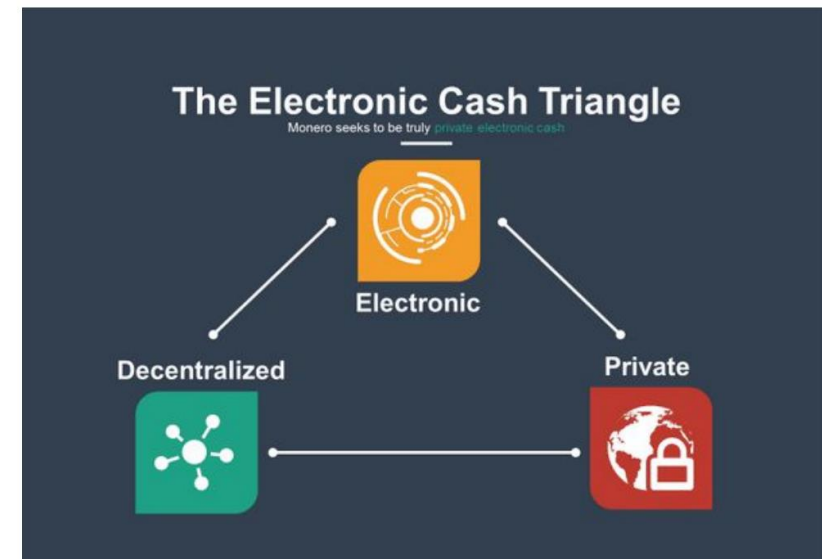
- Provides a privacy-preserving version of Bitcoin (i.e., untraceable e-cash)
- Improves on Zerocoin in that transaction amounts in the Zerocash currency are not public, and both the receiver and the sender can remain anonymous
- Transaction amounts are visible only to the sender and the receiver, as the decentralized ledger traces only the existence of the transactions

Zerocash functionality

- Mint transactions A mint transaction allows a user to convert a specified number of non-anonymous bitcoins from an existing Bitcoin address into the same number of Zerocash coins that belong to a specific Zerocash address
- Pour transactions A pour transaction allows a user to make a private payment by consuming some number of the coins he owns to produce new coins

Monero

- Monero keeps the identity of the sender private through **ring signatures**
- Monero keeps the identity of the receiver private through **Confidential Addresses**
- A “stealth” address is created by the use of two keys (public send and public view)
- Monero keeps the privacy of the transaction through **Ring Confidential Transactions**



Currency of choice for malware



Your documents, photos,
databases and other important files
encrypted



To decrypt your files you need to
buy our special software - **General-
Decryptor**



Follow the instructions below. But
remember that you do not have
much time

General-Decryptor price
the price is for all PCs of your infected network

You have **2 days, 23:38:14**

* If you do not pay on time, the price will be doubled

* Time ends on **Jul 5, 14:15:38**

Current price

24435.5 XMR

≈ 5,000,000 USD

After time ends

48871 XMR

≈ 10,000,000 USD

Monero address:

* XMR will be recalculated in 5 hours with an actual rate.