# Anonymity in Cryptocurrencies

**ECON23040**

Emily Willson

January 16, 2019

"The only way to deal with an unfree world is to become so absolutely free that your very existence is an act of rebellion."

*- Albert Camus*

# Does the hype of cryptocurrencies match the anonymity and privacy they provide in practice?

# How Bitcoin Works

Alice

Alice wants to pay Bob 5 BTC.

Bob

## How Bitcoin Works

→ **Address:** *1slkj53ce58ck1359*

pays

**Address:** *1abck50spk59sc20* ←

5 BTC

## How Bitcoin Works

Alice

**Address:** *1slkj53ce58ck1359*

pays

**Address:** *1abck50spk59sc20*

Bob

5 BTC

## Bitcoin: “Anonymity”

*1slkj53ce58ck1359* **= Base58(Alice’s Public Key)**

**This is the only anonymity provided in Bitcoin.**

## Bitcoin: “Anonymity”

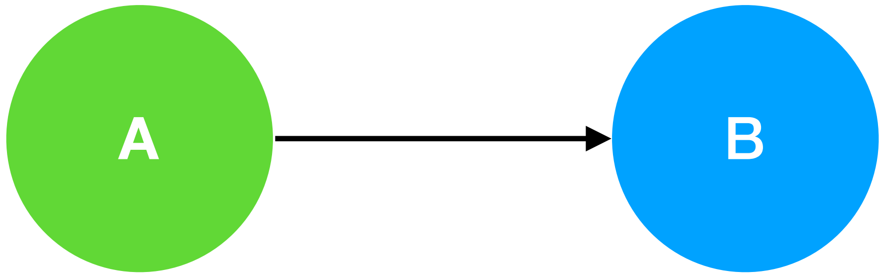
*1slkj53ce58ck1359* **= Base58(Alice’s Public Key)**

**This is the only anonymity provided in Bitcoin.**

**Is this sufficient?**

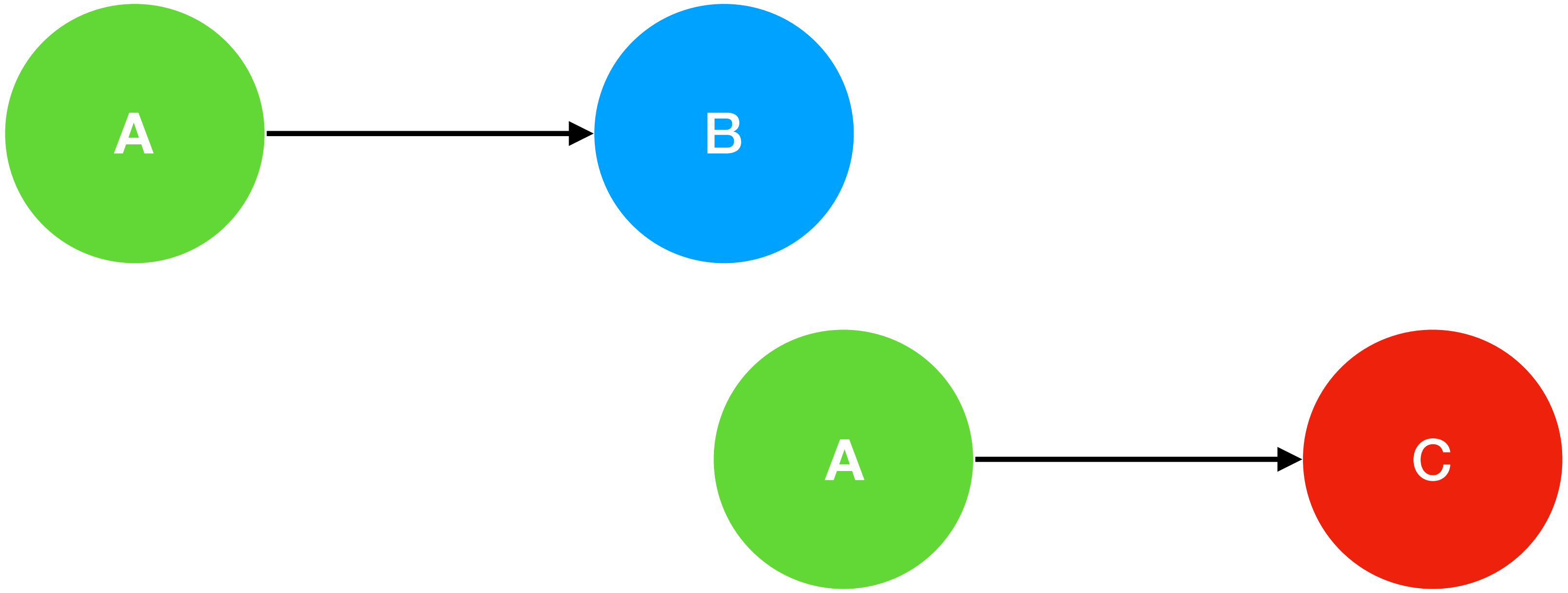
## Bitcoin: Potential Vulnerabilities

*Address reuse*



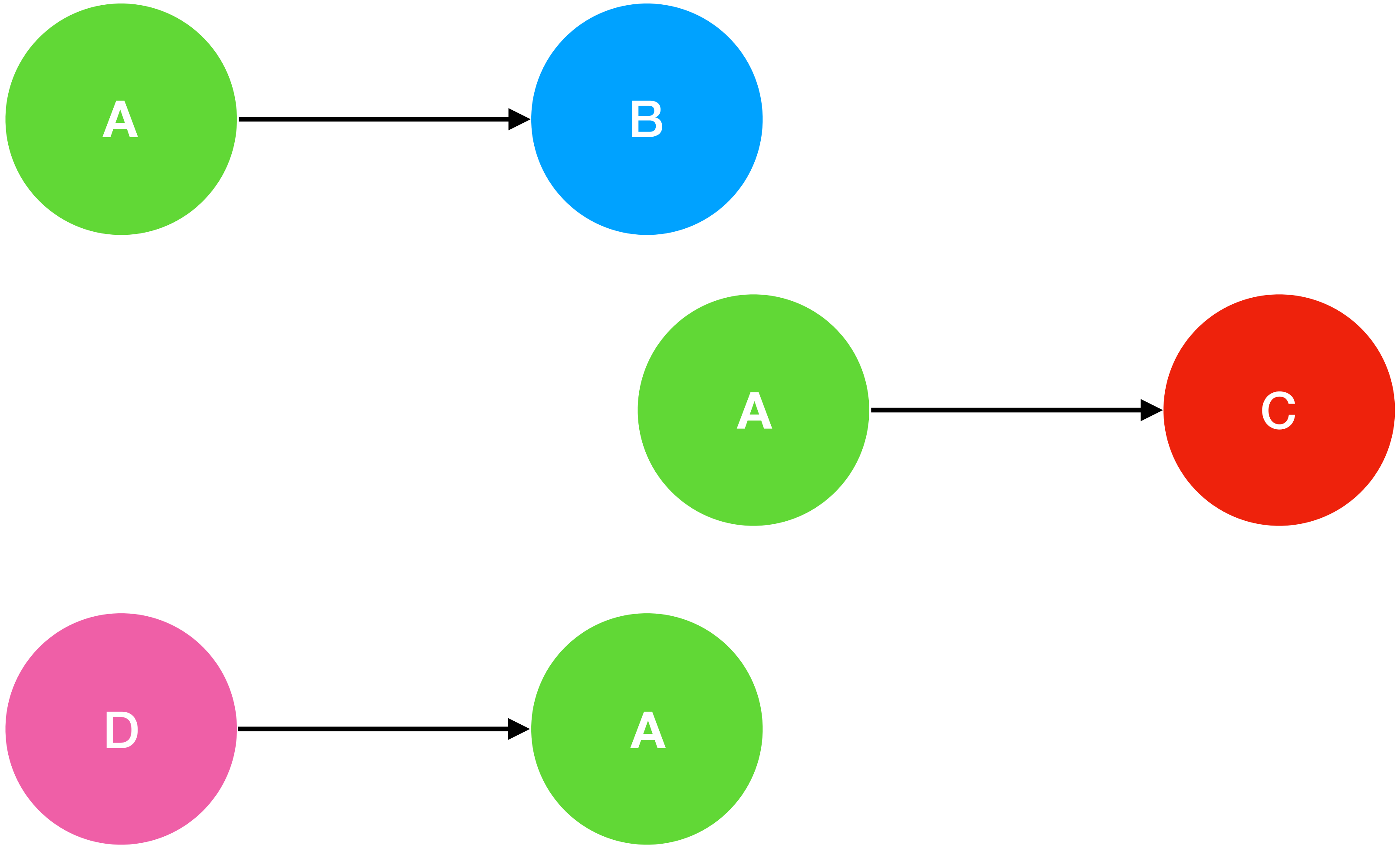
# Bitcoin: Potential Vulnerabilities

*Address reuse*



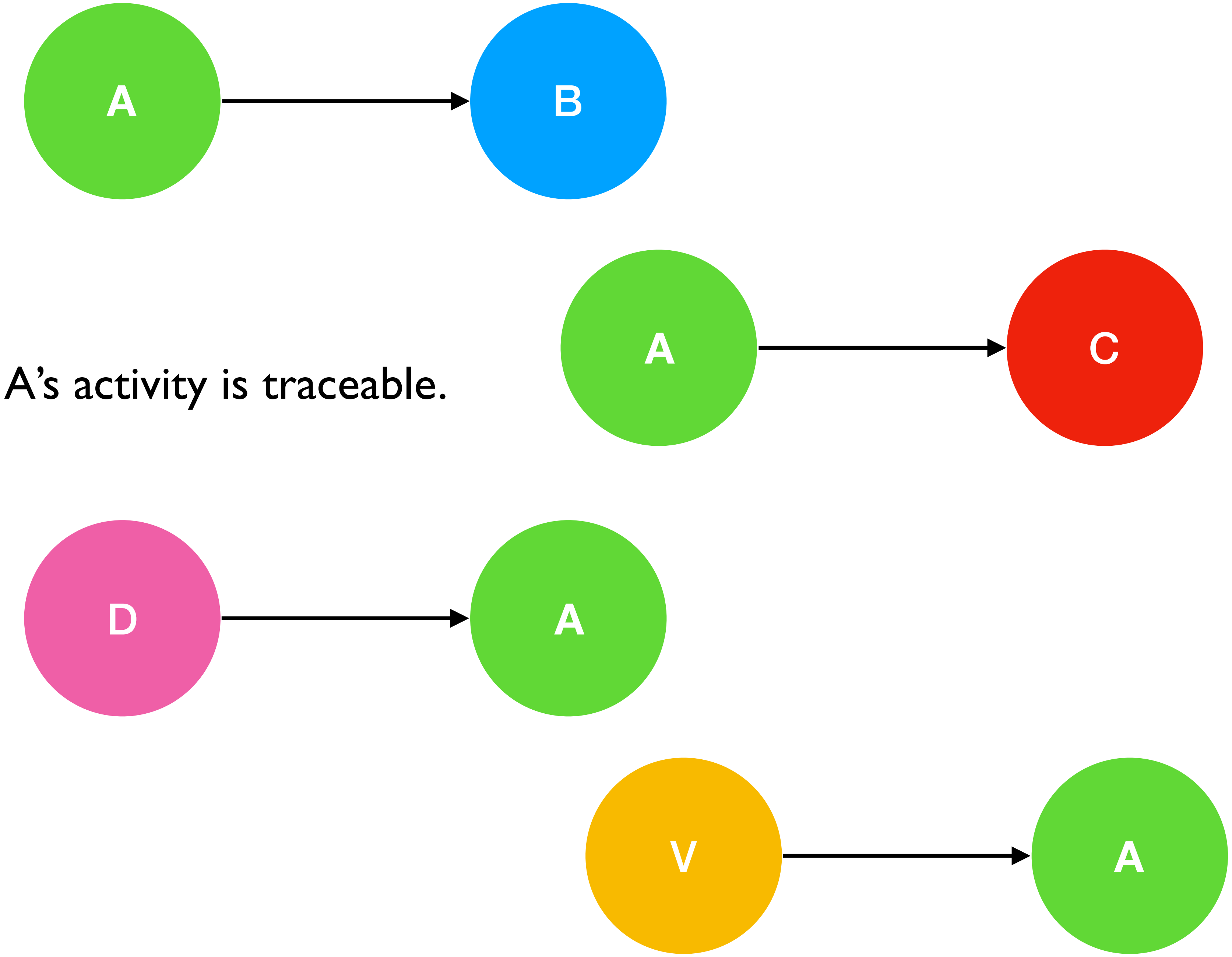
# Bitcoin: Potential Vulnerabilities

*Address reuse*



# Bitcoin: Potential Vulnerabilities

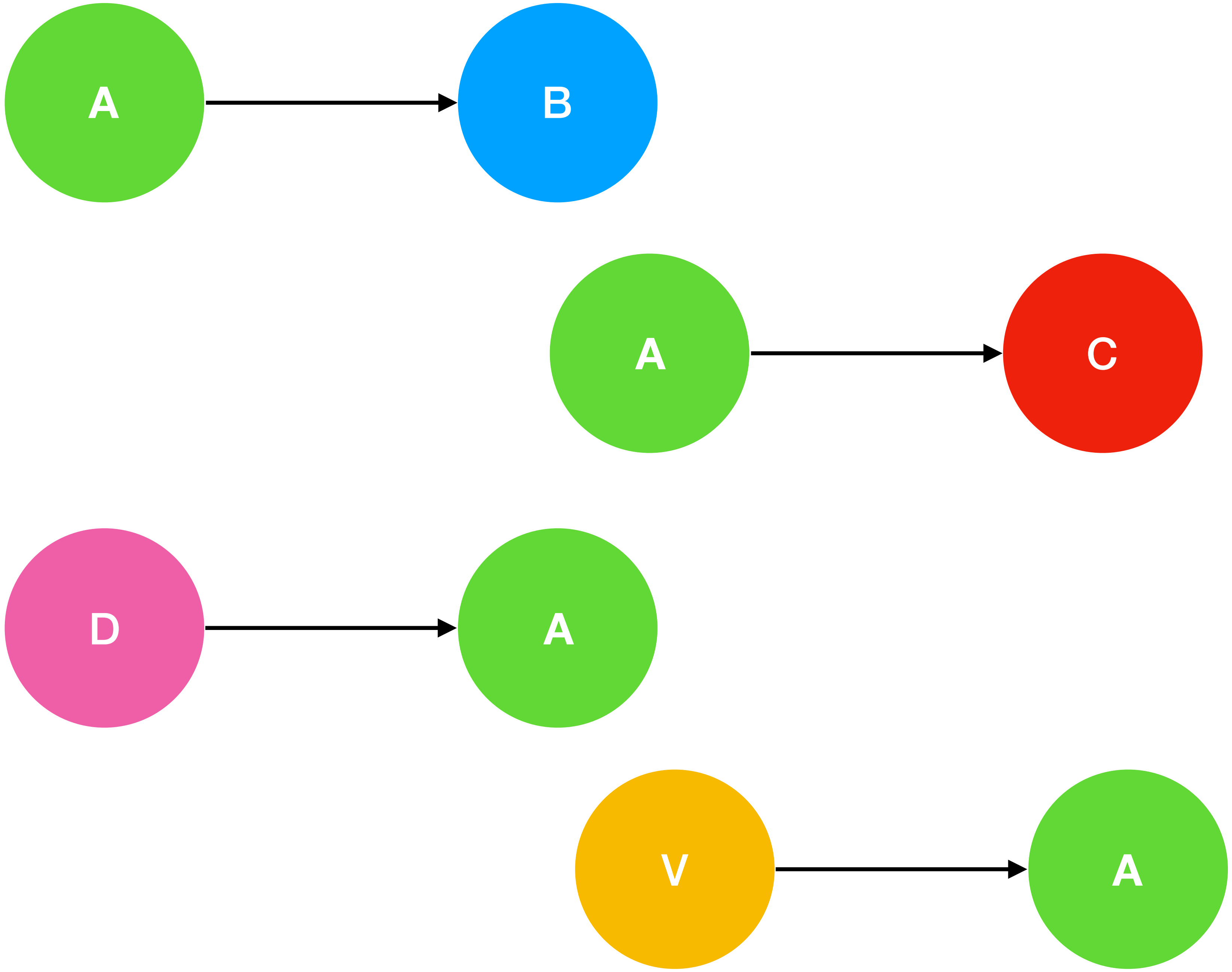
*Address reuse*



**Conclusion:** A's activity is traceable.

## Bitcoin: Potential Vulnerabilities

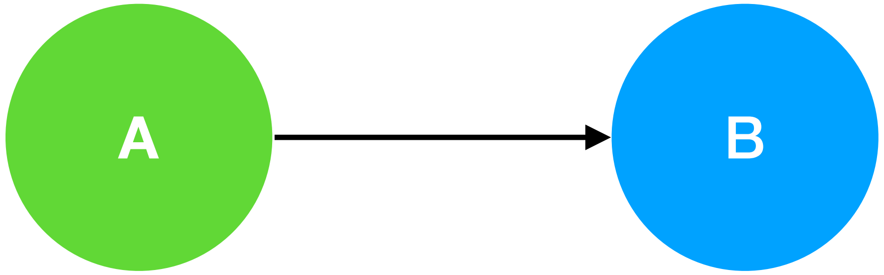
*Address reuse*



# Bitcoin: Potential Vulnerabilities

*Multi-input heuristic*

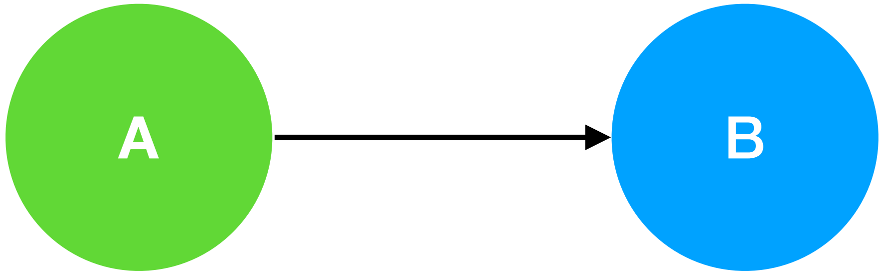
1.



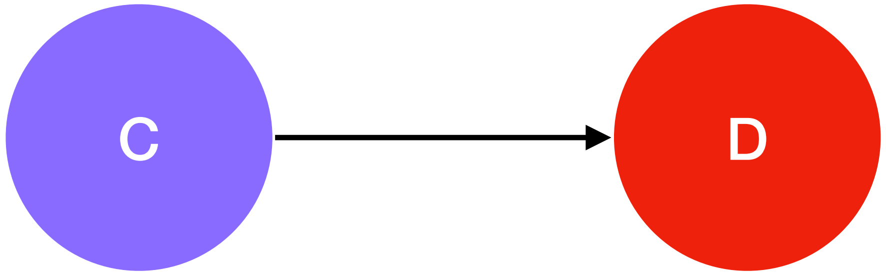
# Bitcoin: Potential Vulnerabilities

*Multi-input heuristic*

1.



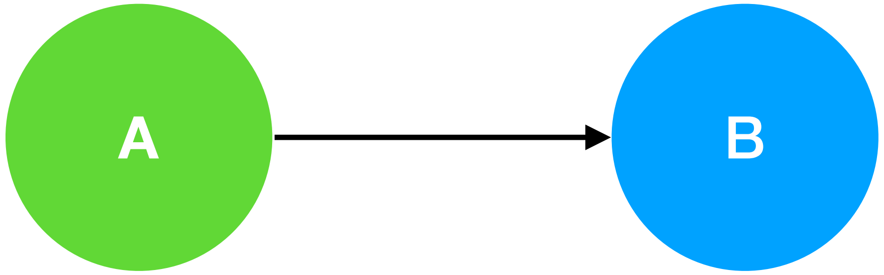
2.



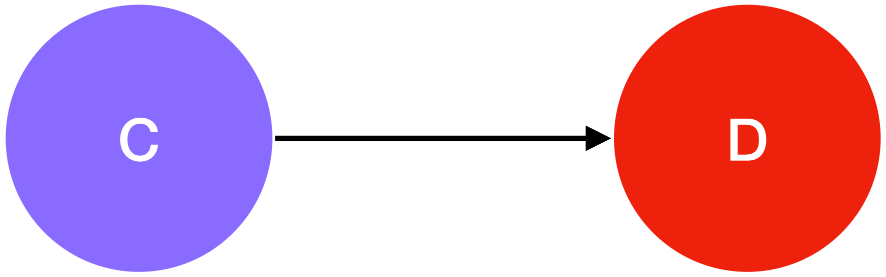
# Bitcoin: Potential Vulnerabilities

*Multi-input heuristic*

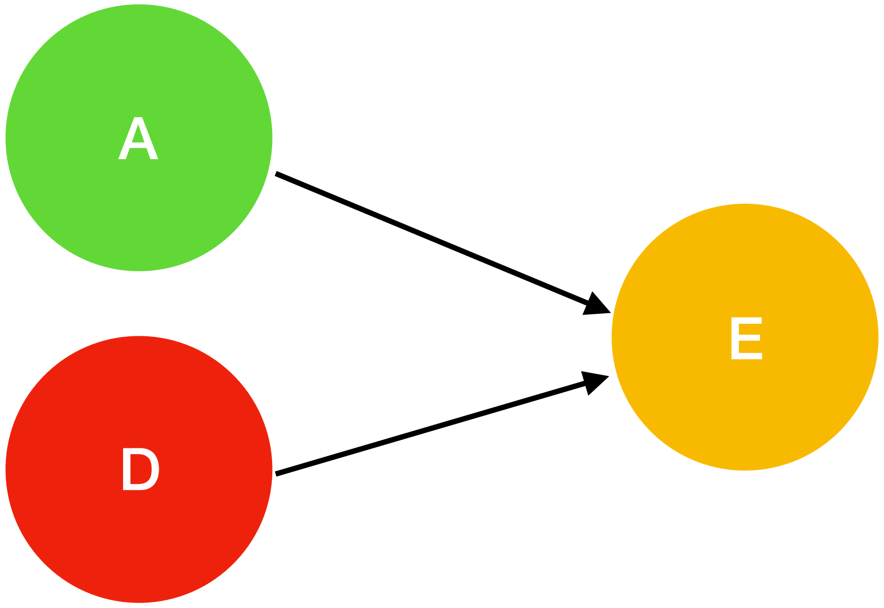
1.



2.



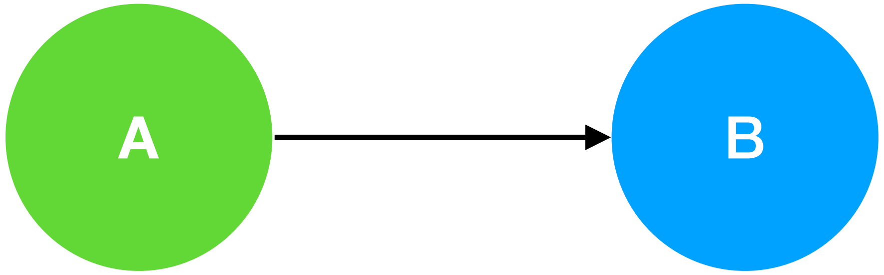
3.



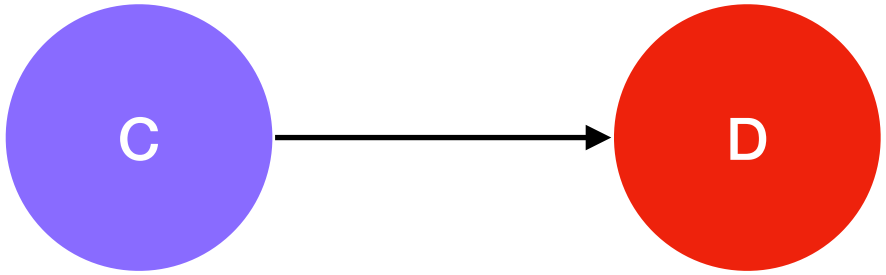
# Bitcoin: Potential Vulnerabilities

*Multi-input heuristic*

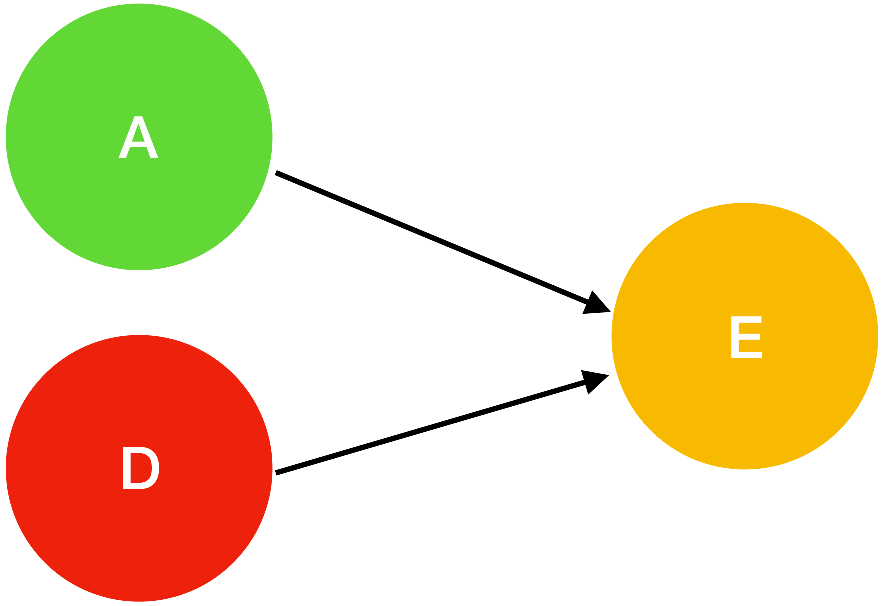
1.



2.



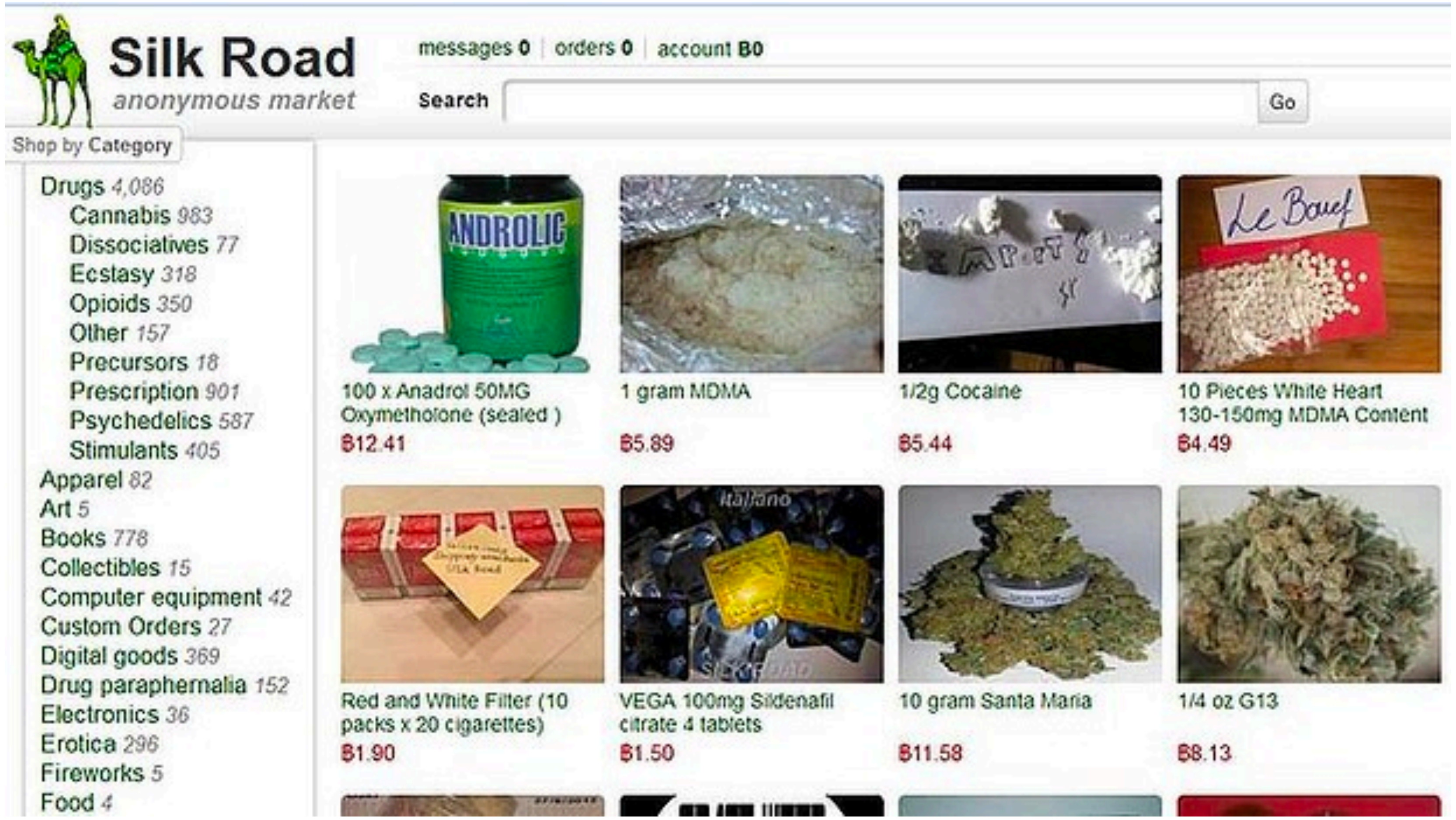
3.



**Conclusion:** A and D are the same person!

## Bitcoin Anonymity in Practice

*The Silk Road**



Drugs 4,086
- Cannabis 983
- Dissociatives 77
- Ecstasy 318
- Opioids 350
- Other 157
- Precursors 18
- Prescription 901
- Psychedelics 587
- Stimulants 405

Apparel 82
Art 5
Books 778
Collectibles 15
Computer equipment 42
Custom Orders 27
Digital goods 369
Drug paraphernalia 152
Electronics 36
Erotica 296
Fireworks 5
Food 4

100 x Anadrol 50MG Oxymetholone (sealed ) ฿12.41

1 gram MDMA ฿5.89

1/2g Cocaine ฿5.44

10 Pieces White Heart 130-150mg MDMA Content ฿4.49

Red and White Filter (10 packs x 20 cigarettes) ฿1.90

VEGA 100mg Sildenafil citrate 4 tablets ฿1.50

10 gram Santa Maria ฿11.58

1/4 oz G13 ฿8.13

Silk Road Address: *1DkyBEKt5S2GDtv7aQw6rQepAvnsRyHoYM*

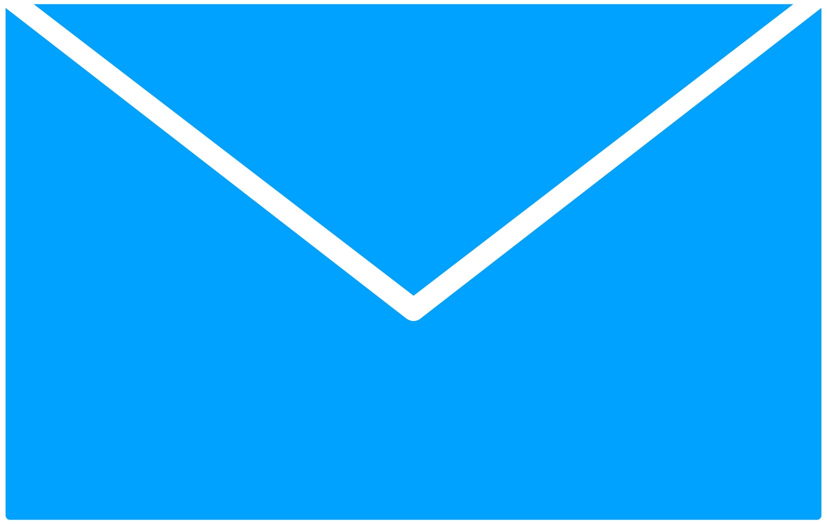
*** Source:** "A Fistful of Bitcoins: Characterizing Payments Among Men With No Names" Meiklejohn et al (2016)

**“Just the place for a snark!”**

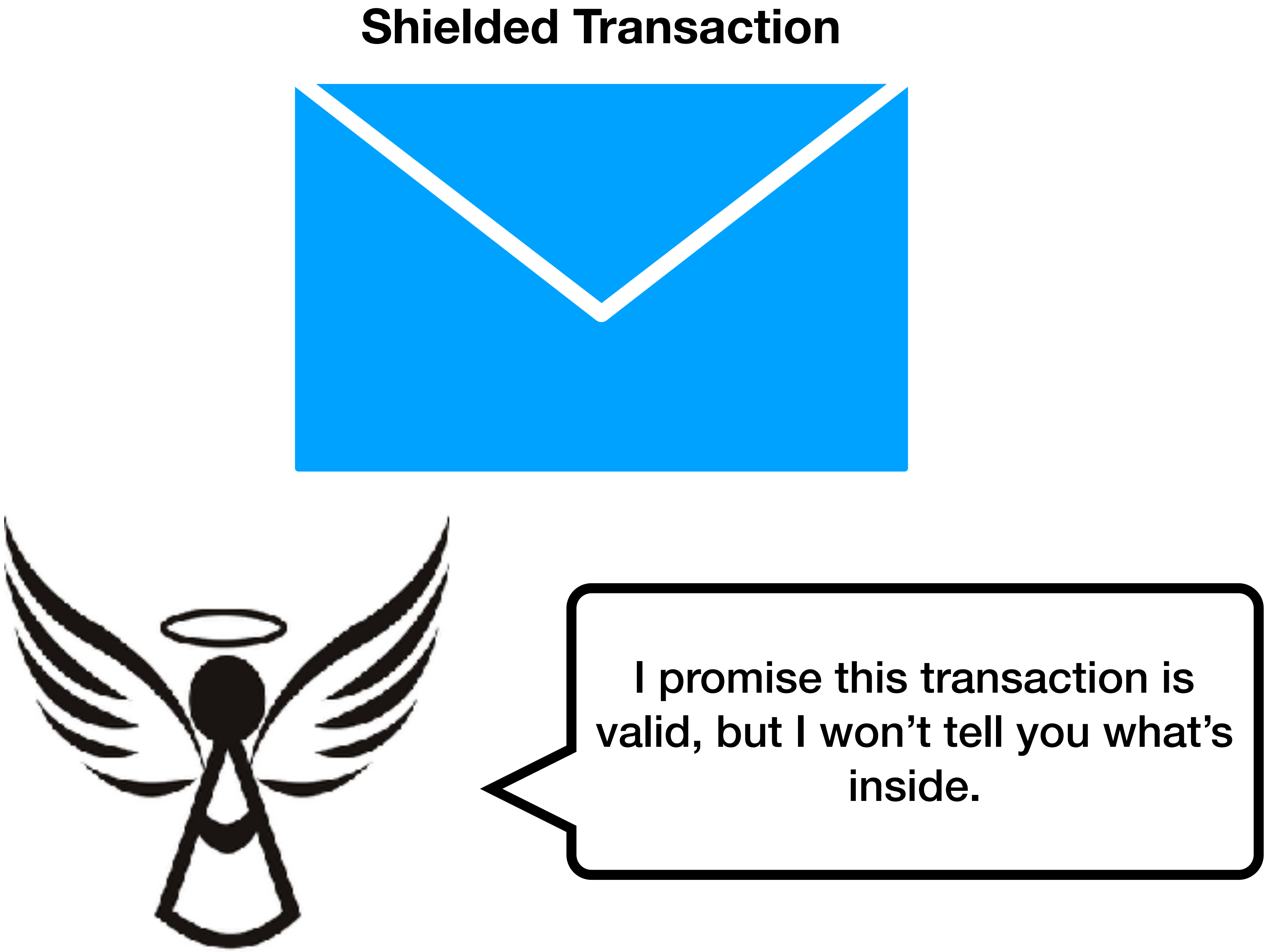
*– Lewis Carroll, “The Hunting of the Snark”*

# ZCash: Angel Model

Shielded Transaction



# ZCash: Angel Model



Shielded Transaction

I promise this transaction is valid, but I won’t tell you what’s inside.

## Zcash: The Basics

Designed to have better **scalability**, **efficiency**, **democracy**, and **secrecy** than Bitcoin.

- **Scalability:** larger block sizes and more frequent block mining.
- **Efficiency:** less compute-intensive proof of work saves electricity.
- **Democracy:** memory-intensive proof of work avoids "elite mining."
- **Secrecy:** shielded transactions designed to provide true blockchain anonymity.

## zk-SNARKs: Definitions

**Snark**: fictional animal species featured in Lewis Carroll's poetry.

**zk-SNARK**: zero-knowledge succinct non-interactive argument of knowledge.

## zk-SNARKs: Definitions

zk-SNARKs are used to verify
**shielded** transactions in Zcash.

↑

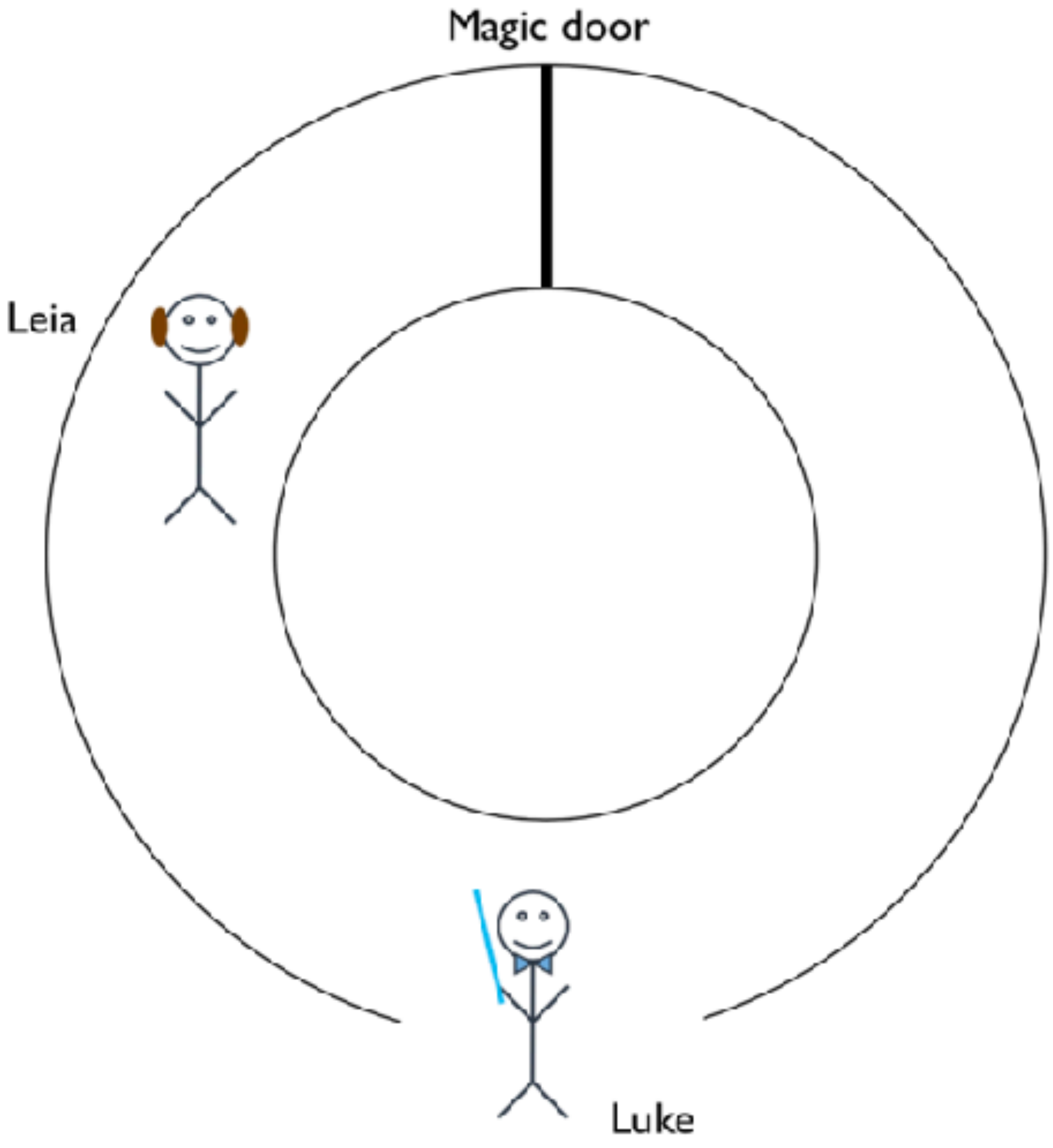
**shielded** transactions: fully
encrypted transactions
stored on the Zcash blockchain.

## zk-SNARKs: Definitions

**zk-SNARK**: zero-knowledge succinct non-interactive argument of knowledge.

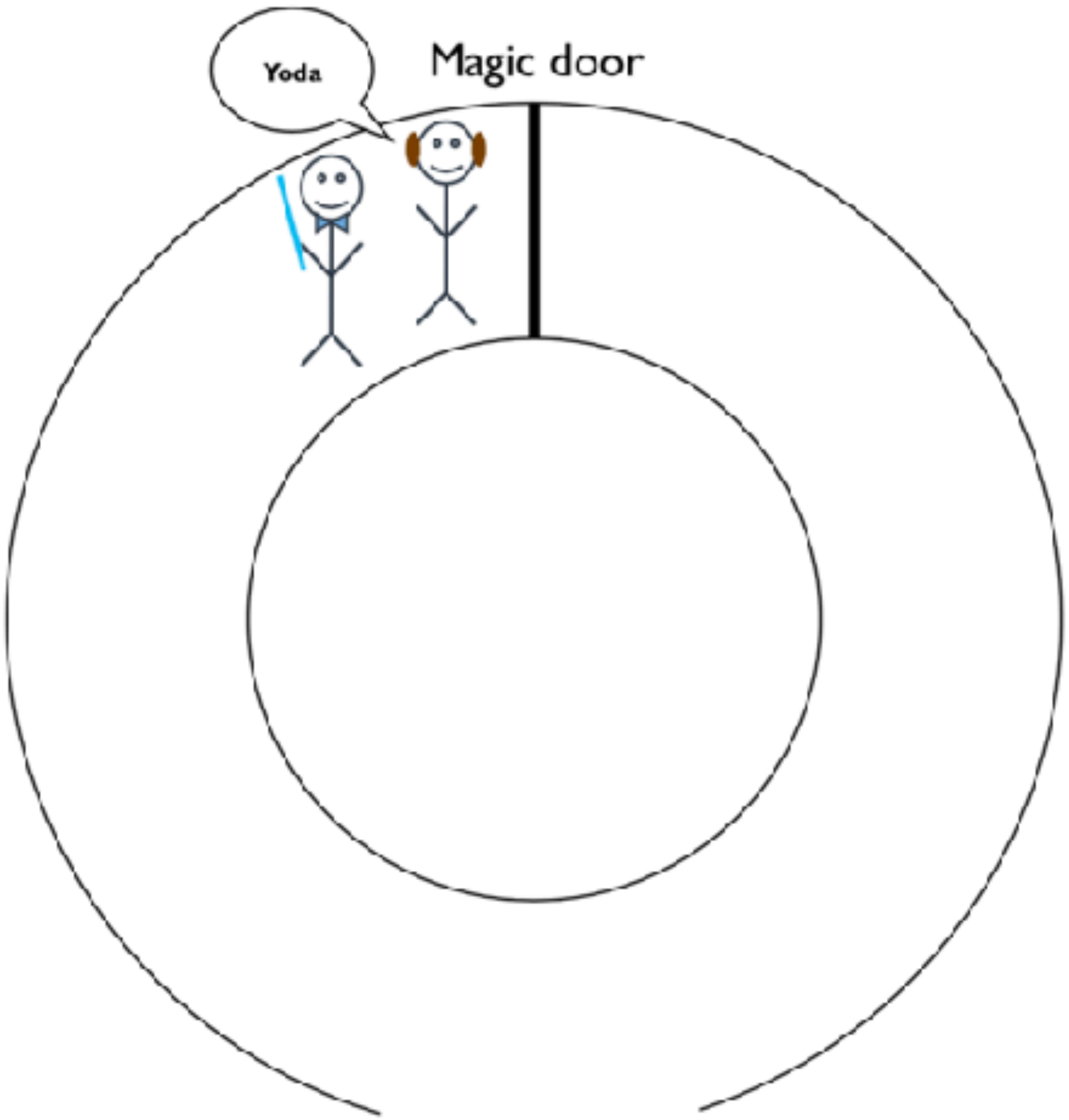
- **Zero knowledge:** transactions don't reveal information about the participants.
- **Succinct:** proofs are (relatively) short and cheap to verify.
- **Non-interactive:** proofs live on blockchain, and anyone can verify them.
- **Argument of knowledge:** anyone can prove transactions are valid.

# The Magic Cave



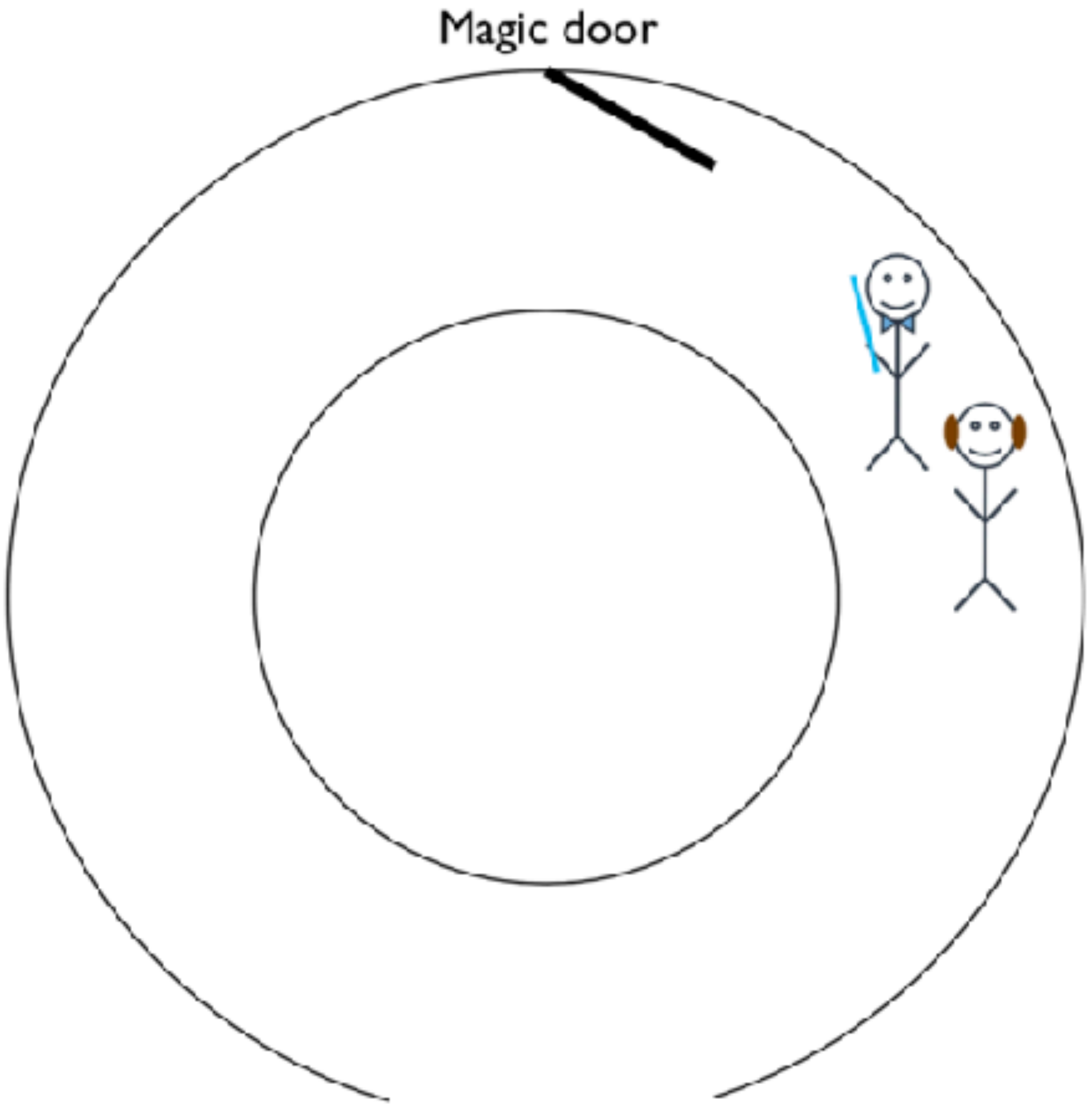
**Goal:** Leia proves to Luke that she knows the magic word to open the magic door.

## The Magic Cave



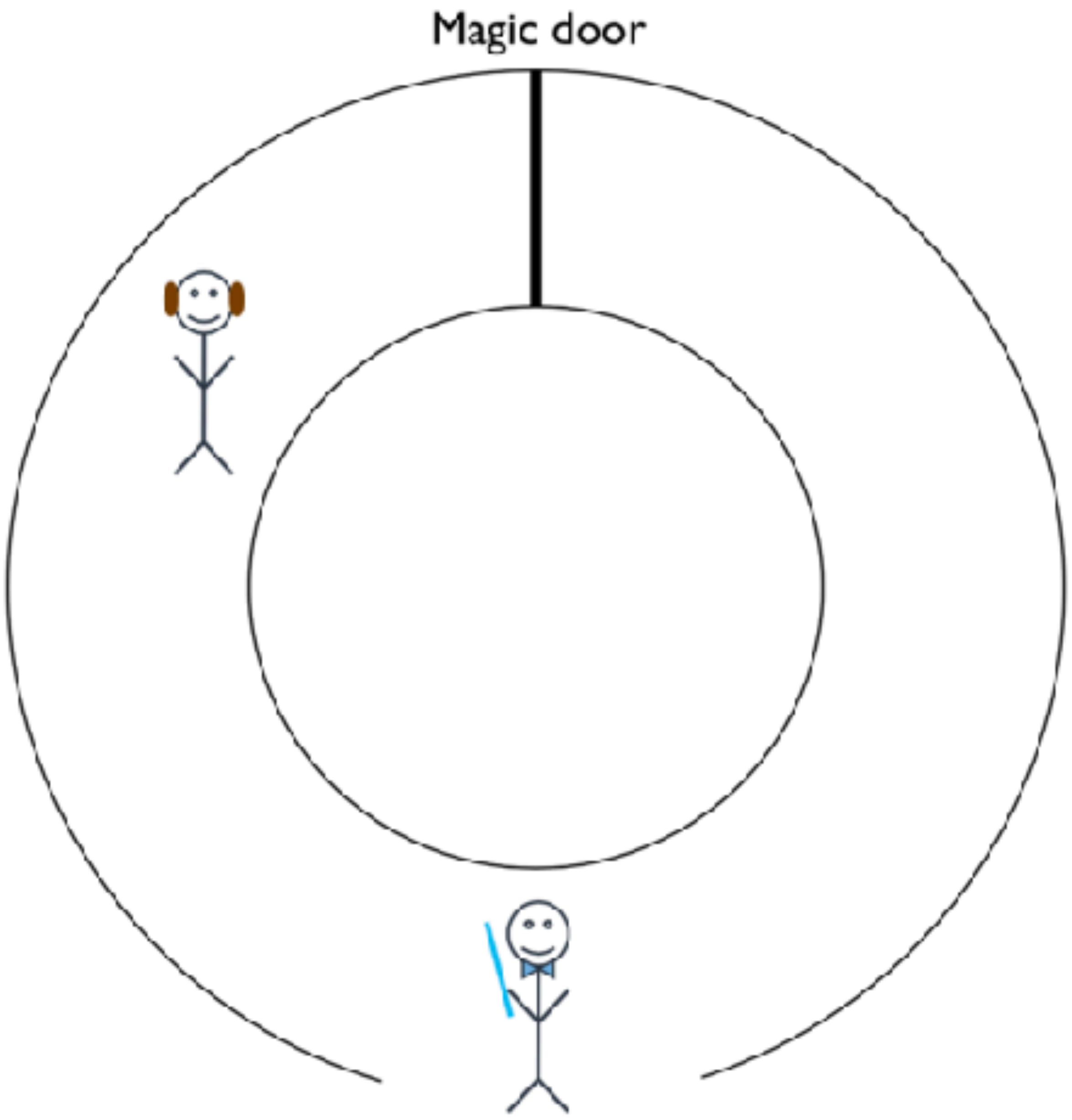
**Attempt 1:** Leia takes Luke to the door and opens it with the magic word.

# The Magic Cave



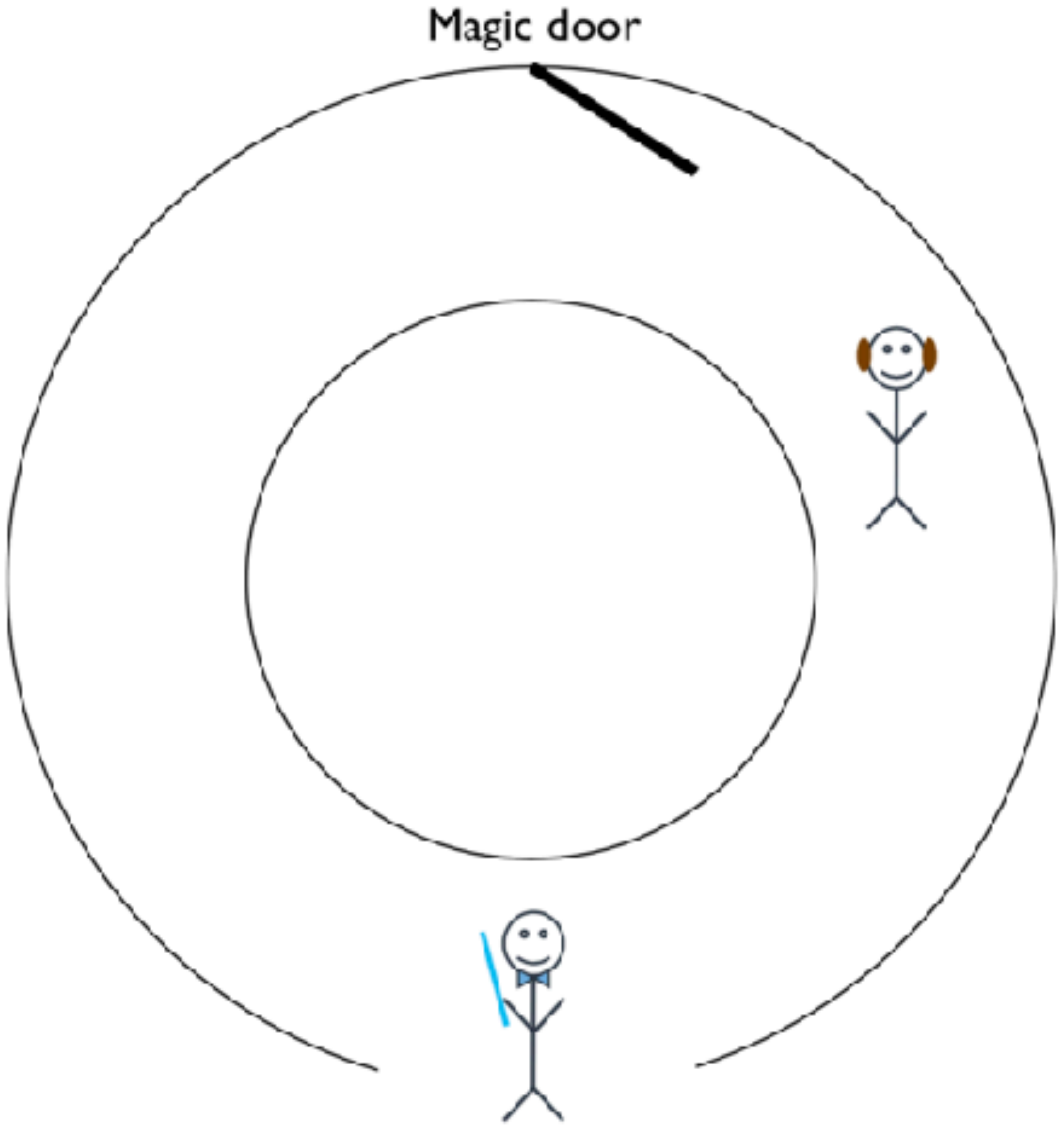
**Bad:** Luke knows that Leia can get through the door, but now Luke knows the magic word.

# The Magic Cave



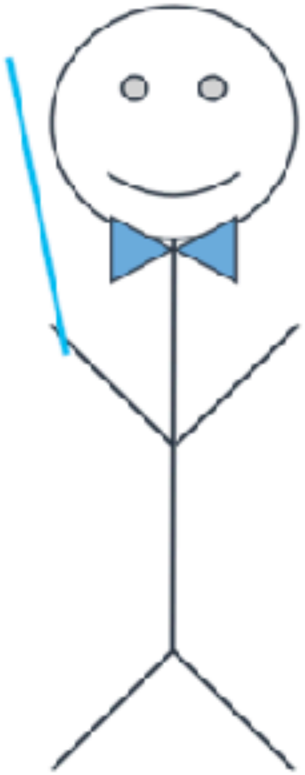
**Attempt 2:** Leia starts on the left side of the cave, while Luke remains outside.

# The Magic Cave

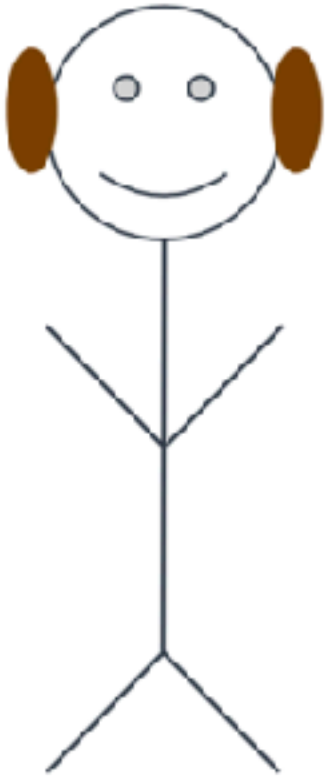


**Good:** Leia appears on the right side of the cave, implying to Luke that she must know the magic word to get through the door.

## The Magic Cave



**Success!** Luke believes that Leia knows how to get through the door, but Leia has not revealed the magic word.



# zk-SNARKs: Overview

## In a nutshell . . .

zk-SNARKs transform the process of proving your transaction is valid into showing you know the solution to a set of algebraic equations without revealing the solution or the equations.

## zk-SNARKs: Overview

### zk-SNARKs show:

1) The sum of transaction inputs matches sum of transaction outputs.

2) Sender holds private spending keys of input notes.

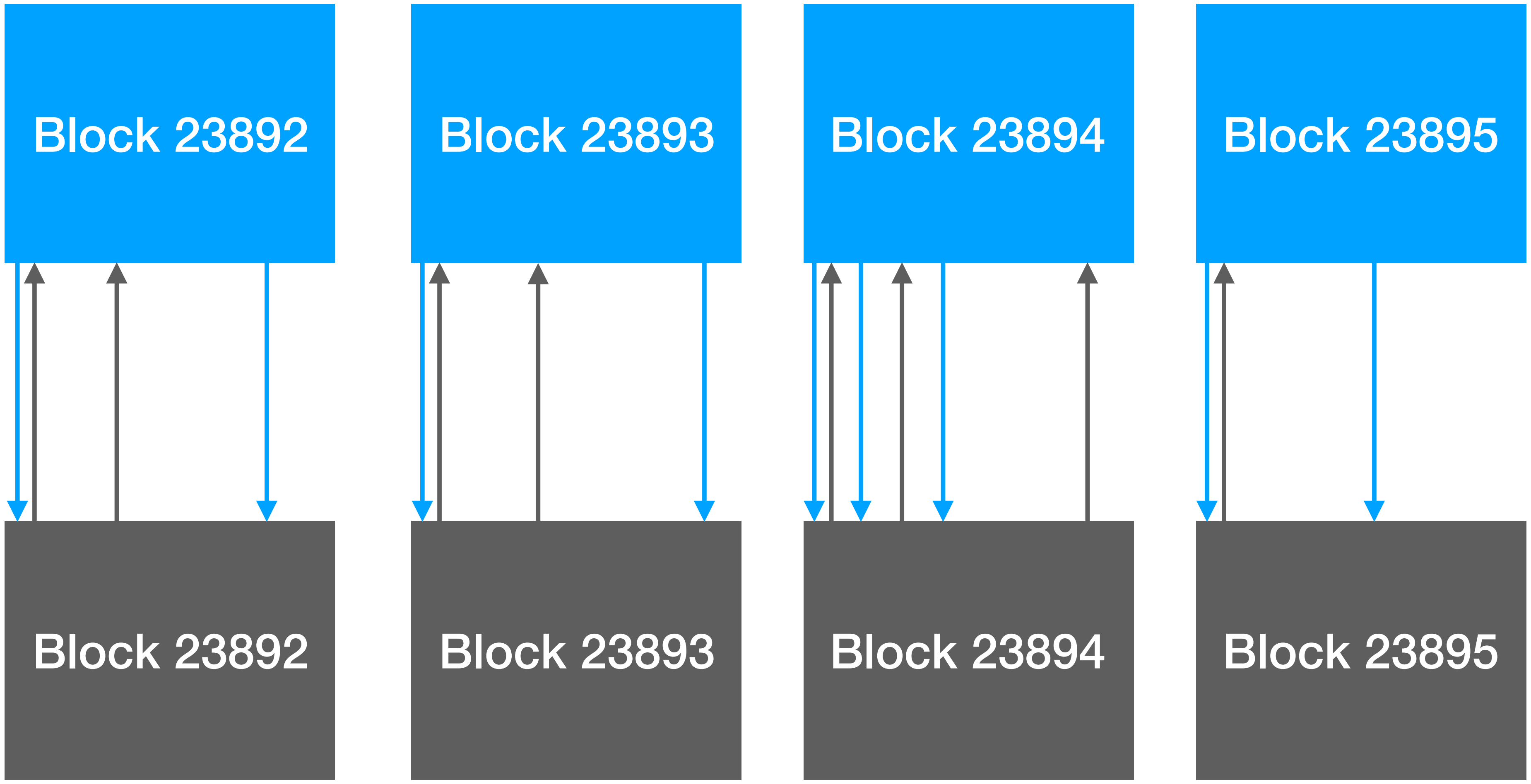
3) Private spending keys can be linked to signature over transaction.

4) For each input note, a revealed commitment* exists.

* Commitment = shows unspent transaction output = HASH(recipient address, amount, ρ, nonce)

# ZCash: How it works

Transparent (t) Transactions - just like Bitcoin



Shielded (z) Transactions - employ zk-SNARKs

# ZCash: How it works

## Types of transactions

- **t-to-t**: completely transparent.
- **t-to-z:** transparent to shielded.
- **z-to-t:** shielded to transparent.
- **z-to-z:** shielded to shielded.

# ZCash: How it works

## Types of transactions

- **t-to-t**: completely transparent. **Everybody sees!**
- **t-to-z:** transparent to shielded. **Everybody sees!**
- **z-to-t:** shielded to transparent. **Everybody sees!**
- **z-to-z:** shielded to shielded. **Everybody sees but nobody understands!**

## ZCash: Potential Vulnerabilities

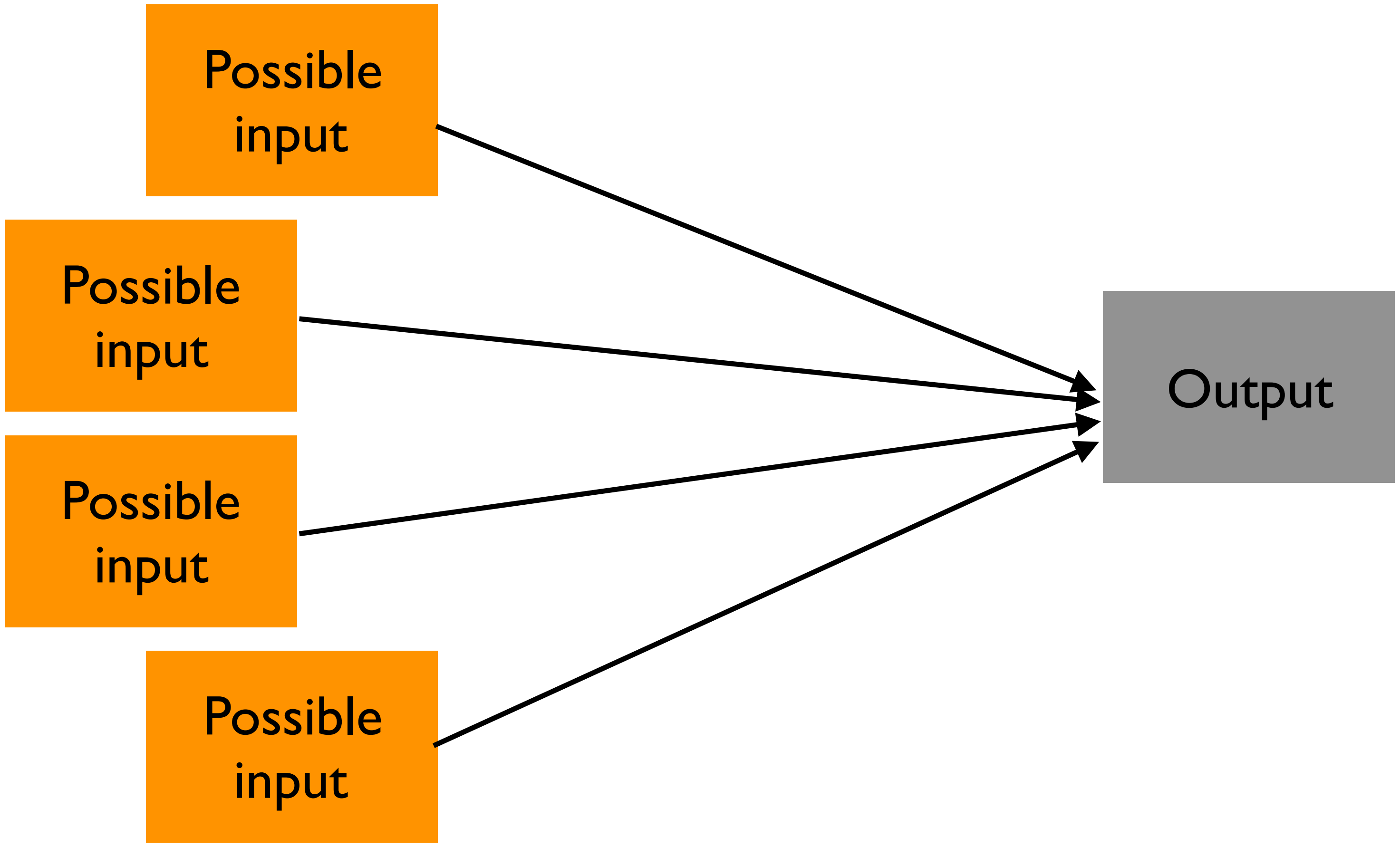
1. Only 15% of ZCash transactions involve the shielded pool.
2. Miners and founders are a huge percentage of shielded pool participants.
3. Putting money into shielded pool and taking it right back out is not anonymous.

* **Source:** "An Empirical Analysis of Anonymity in ZCash" Meiklejohn et al (2016)

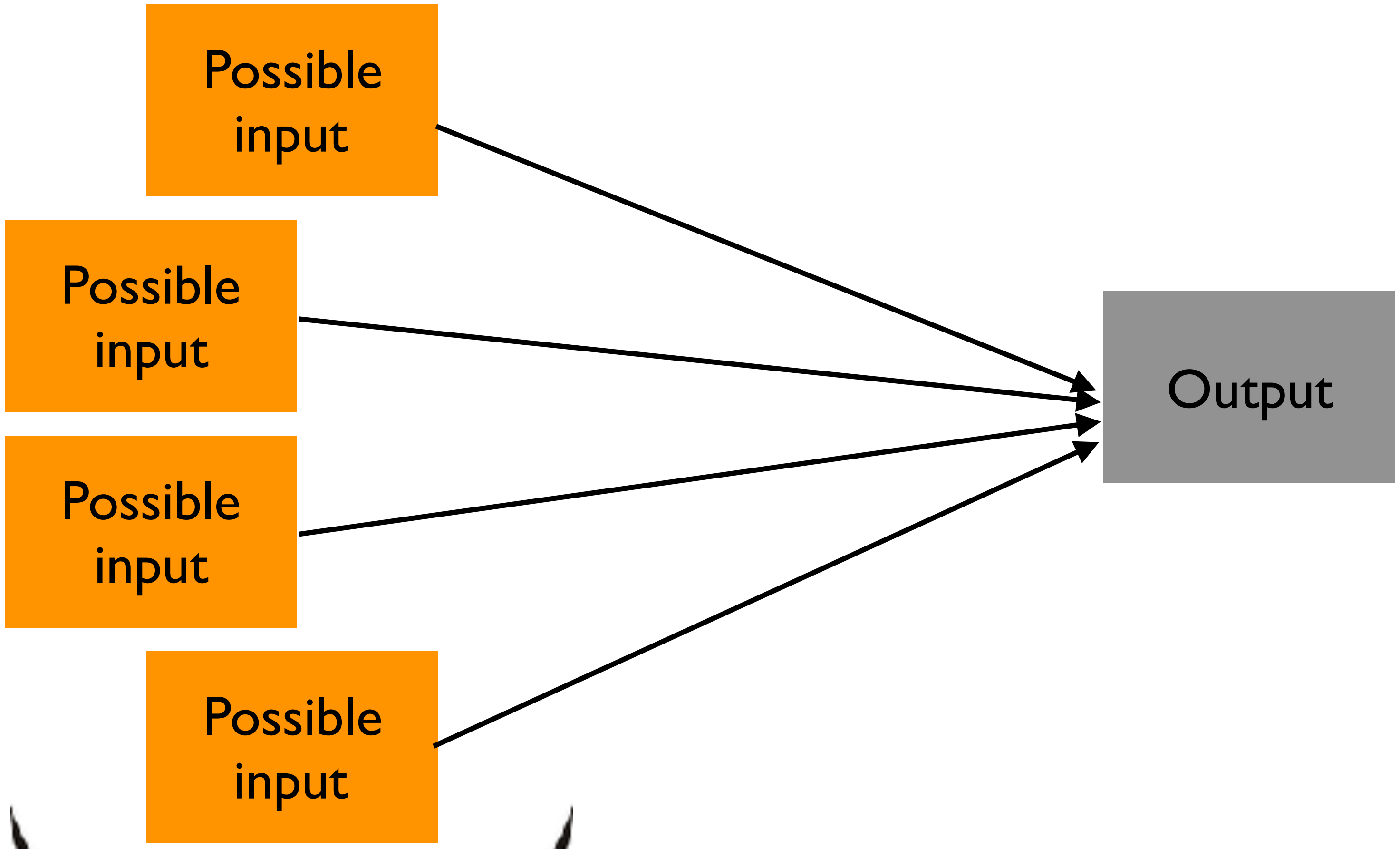
**“TRUST NO ONE.”**

*– User fjbaz on r/monero, 1/13/19*

# Monero: Angel Model



# Monero: Angel Model



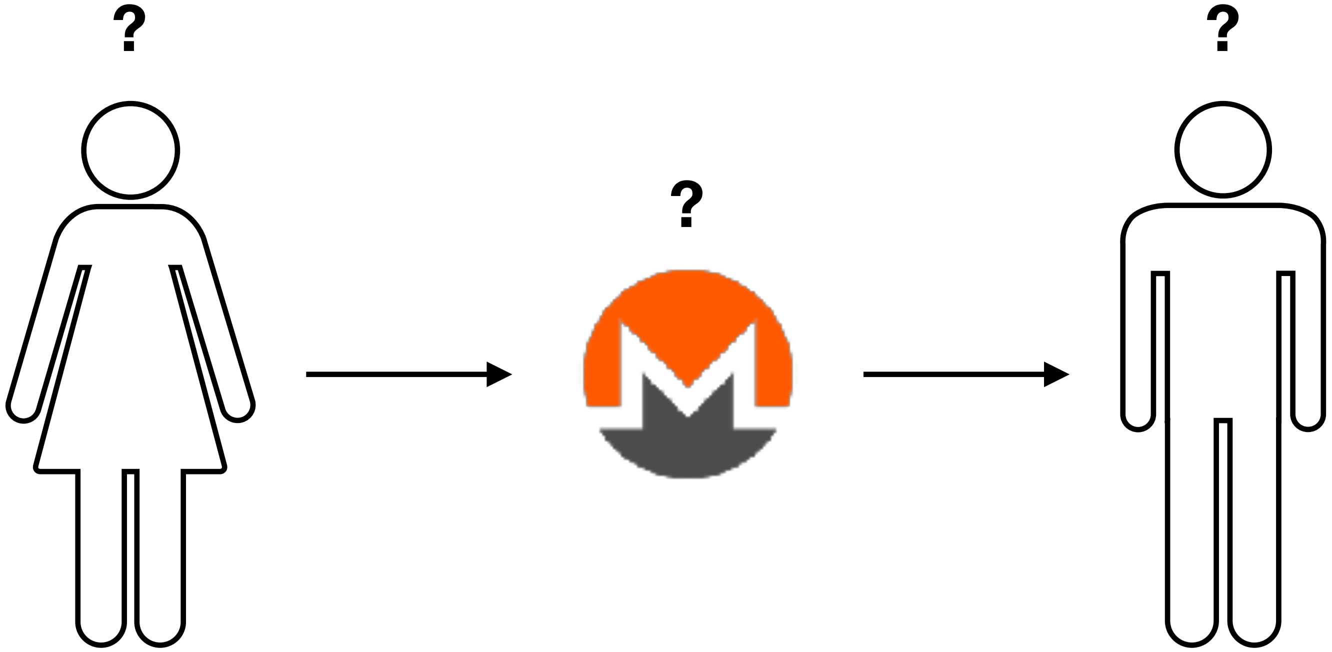
I promise one of the transaction inputs is valid, but I won’t tell you which one.

## Monero: The Basics

Designed to have stronger anonymity guarantees than ZCash and Bitcoin.

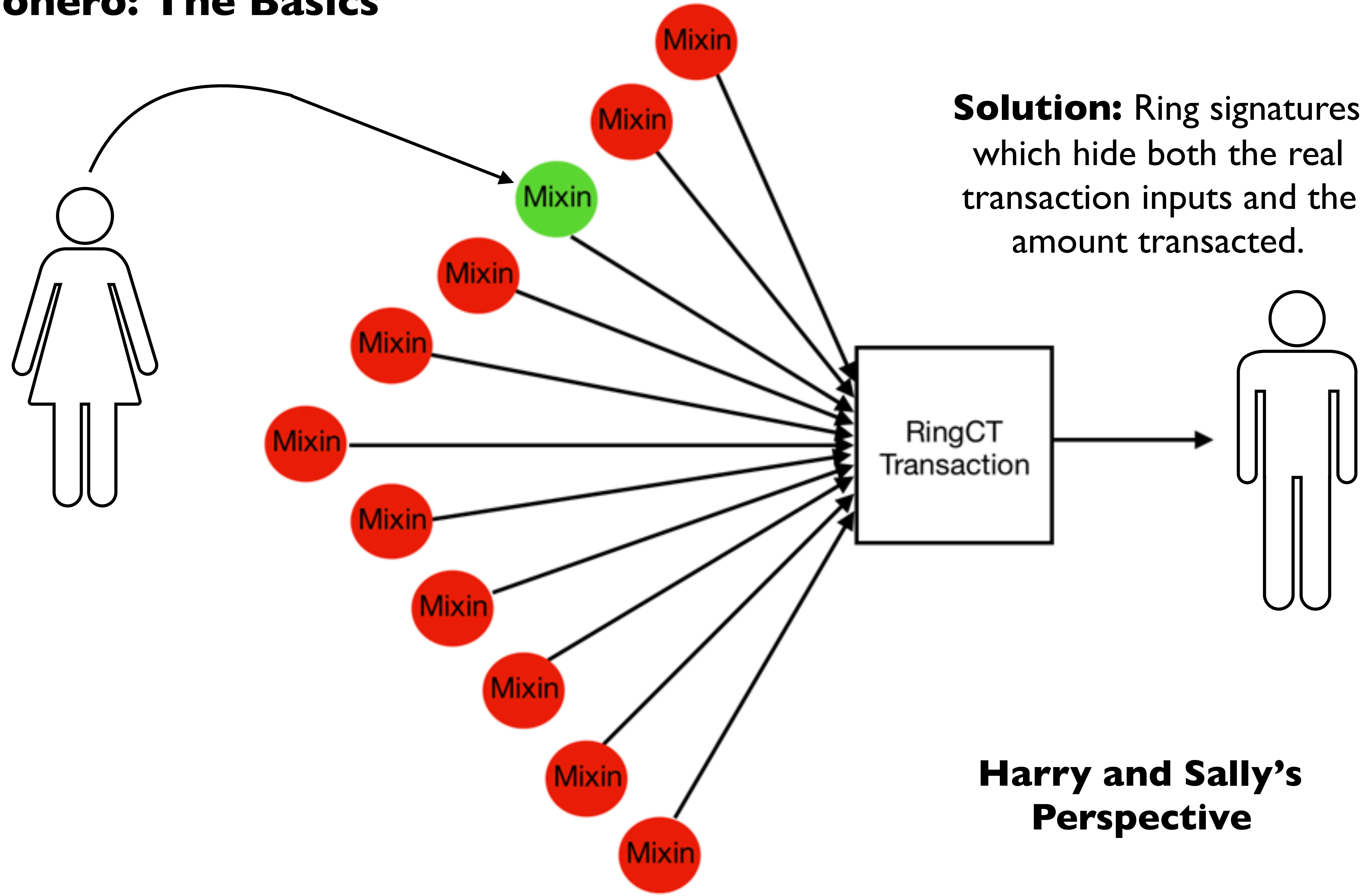
- **Ring Signatures:** guarantee larger anonymity set and provably stronger privacy.
- **Bulletproofs:** short, verifiable proofs enable faster verification.
- **Obscured transaction amounts:** amount transacted hidden from observers.

# Monero: The Basics



**Goal:** Sally pays Harry, but no one knows which address is associate with Sally and how much money was exchanged.

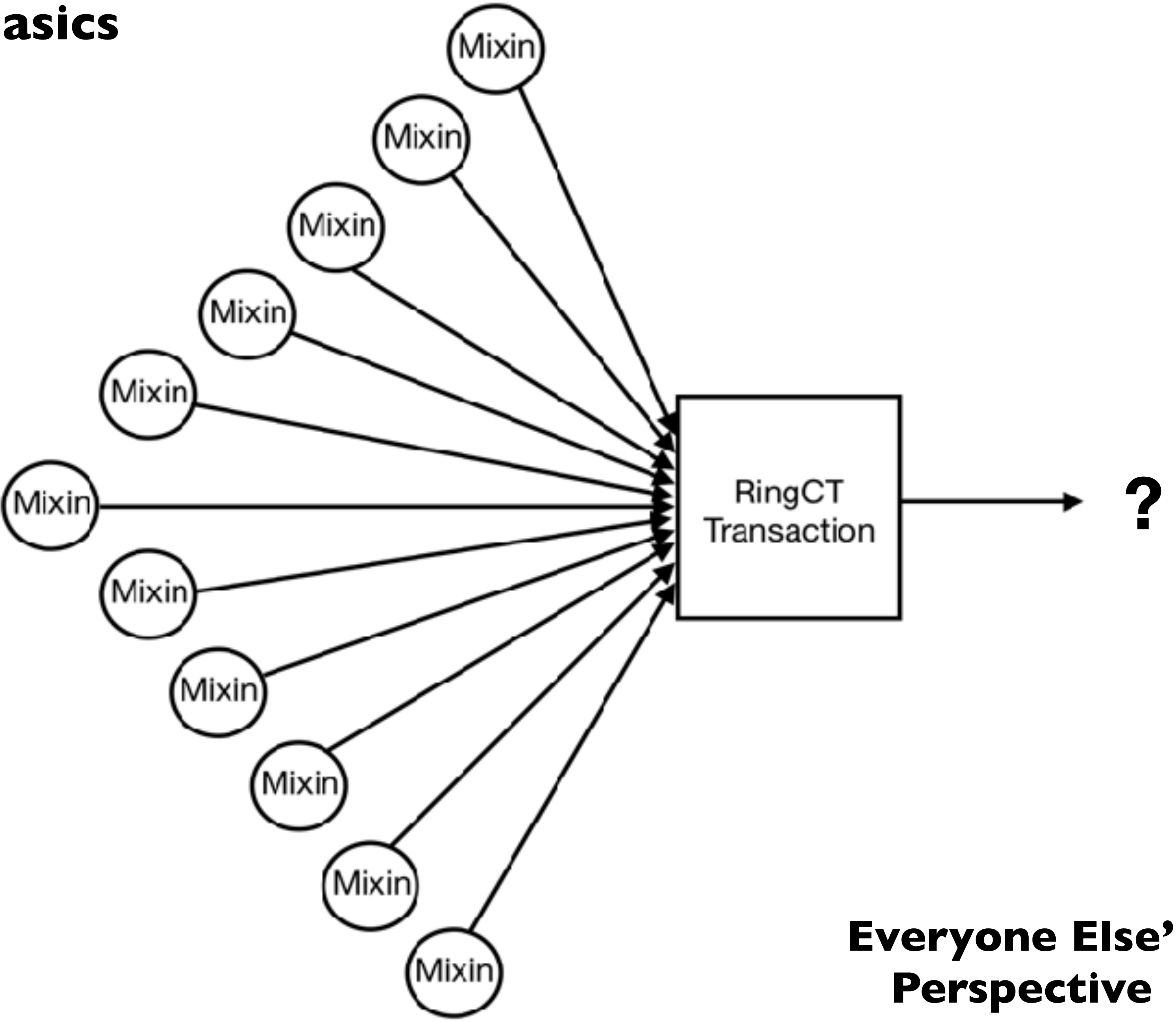
# Monero: The Basics



**Solution:** Ring signatures, which hide both the real transaction inputs and the amount transacted.

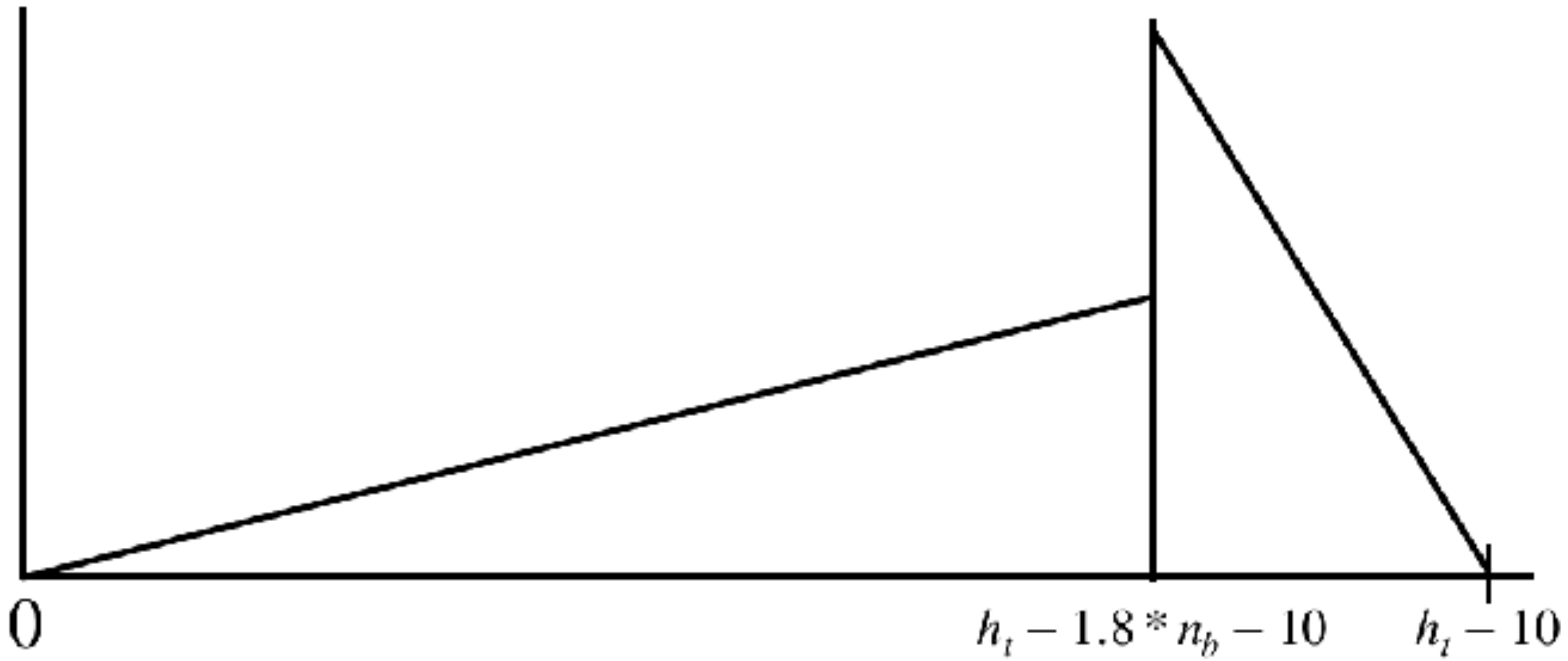
**Harry and Sally's Perspective**

## Monero: The Basics



**Everyone Else's Perspective**

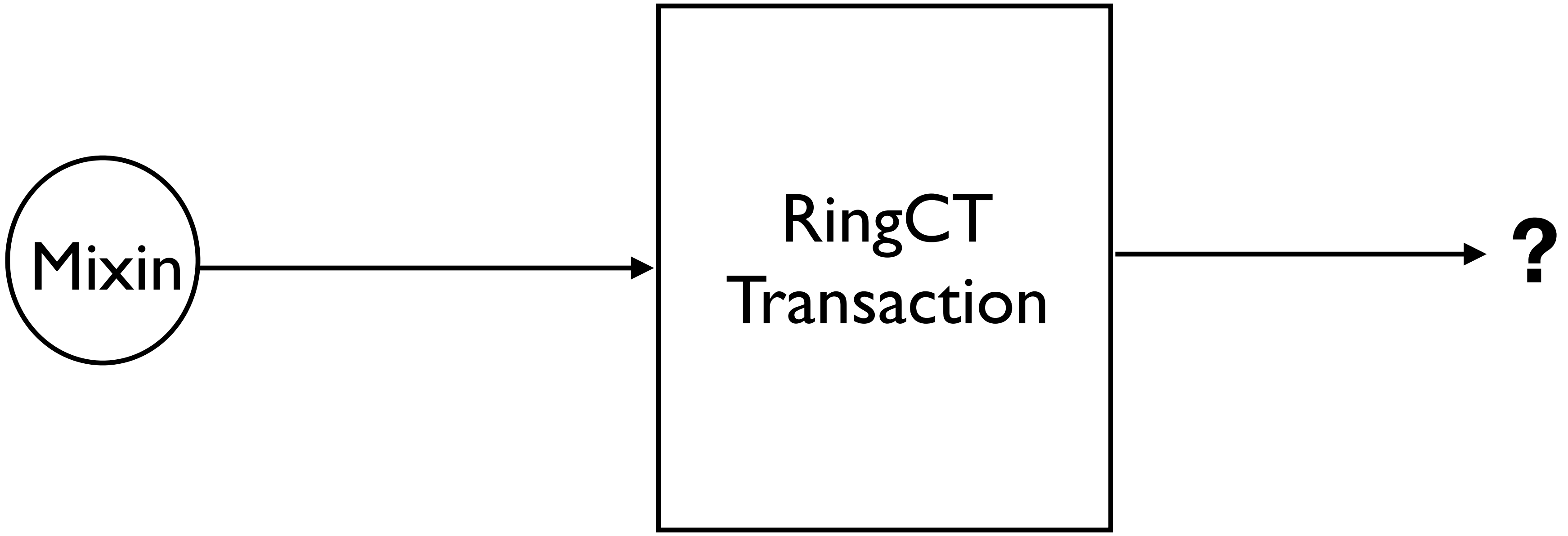
# Monero: The Basics



**Mixin distribution:** half of the mixins are chosen from transactions in the last 1.8 days, half from the rest of the blockchain.

# Monero: Potential Vulnerabilities

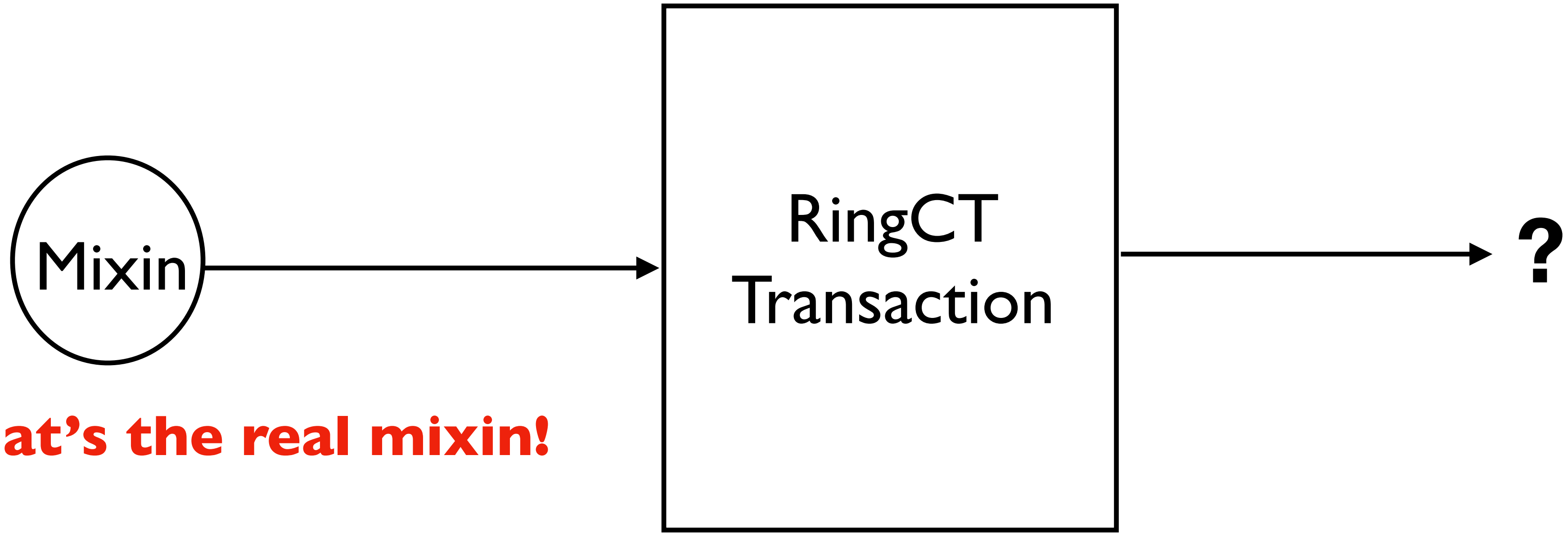
*Single Mixin Deducibility*



*** Source:** "An Empirical Analysis of Traceability in the Monero Blockchain" Miller et al (2018)

# Monero: Potential Vulnerabilities

*Single Mixin Deducibility*

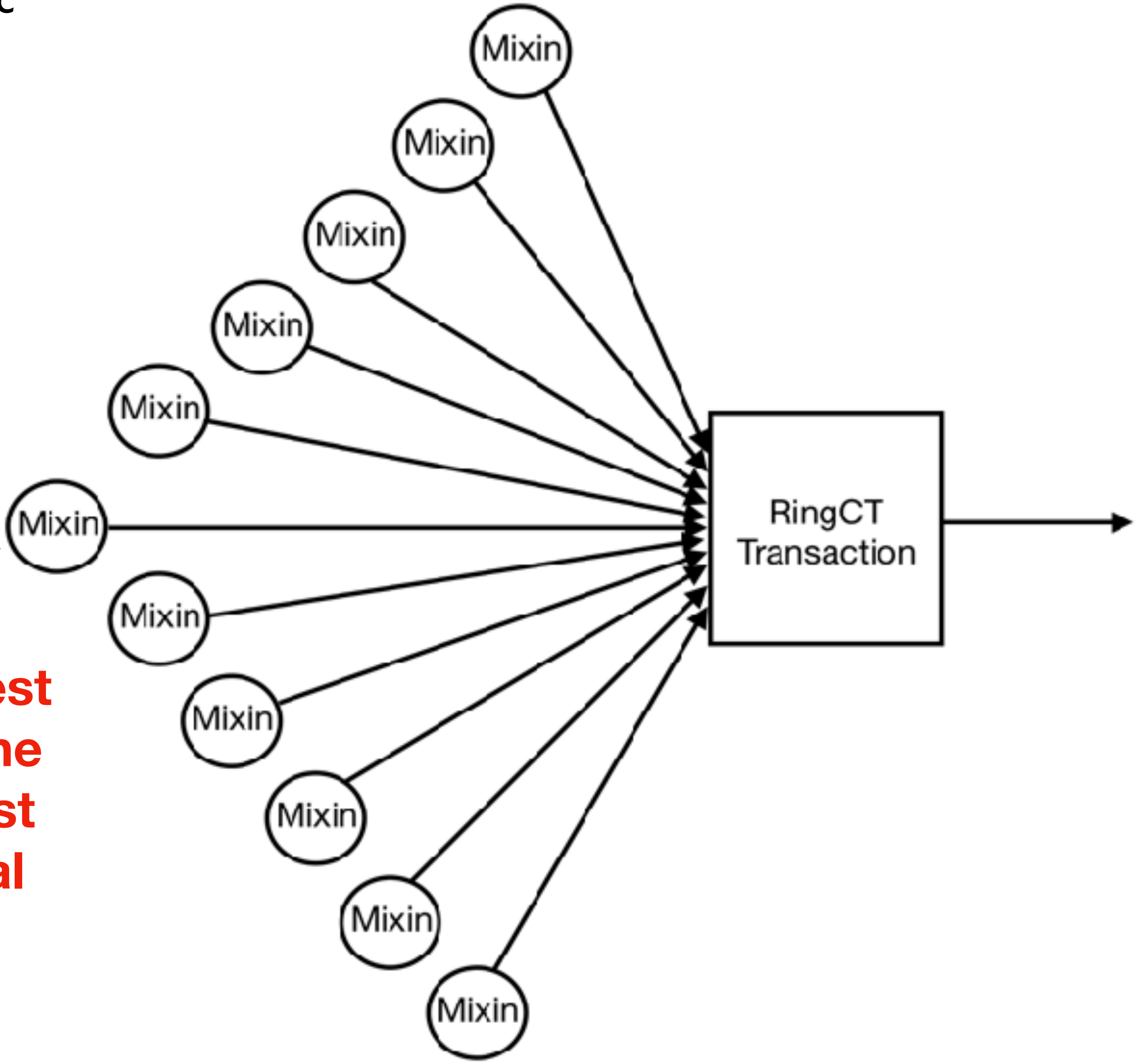


**Hey! That's the real mixin!**

*** Source:** "An Empirical Analysis of Traceability in the Monero Blockchain" Miller et al (2018)

# Monero: Potential Vulnerabilities

*Newest Mixin Heuristic*



**This is the newest mixin! 80% of the time, the newest mixin is the real mixin.**

* **Source:** "An Empirical Analysis of Traceability in the Monero Blockchain" Miller et al (2018)

**Does the hype of cryptocurrencies match the anonymity and privacy they provide in practice?**

Questions?