

# THE 'WHY'S AND 'HOW'S OF



# MONERO

*Rajarshi Mitra*

# WHAT EXACTLY IS MONERO



# **A CURRENCY SYSTEM**

**SECURE**

**PRIVATE**

**UNTRACEABLE**



**NO.1 FEATURE**



**PRIVACY**



Most of the mainstream cryptocurrencies are open.



Is it bad to want privacy? Is being “open” the way to go?

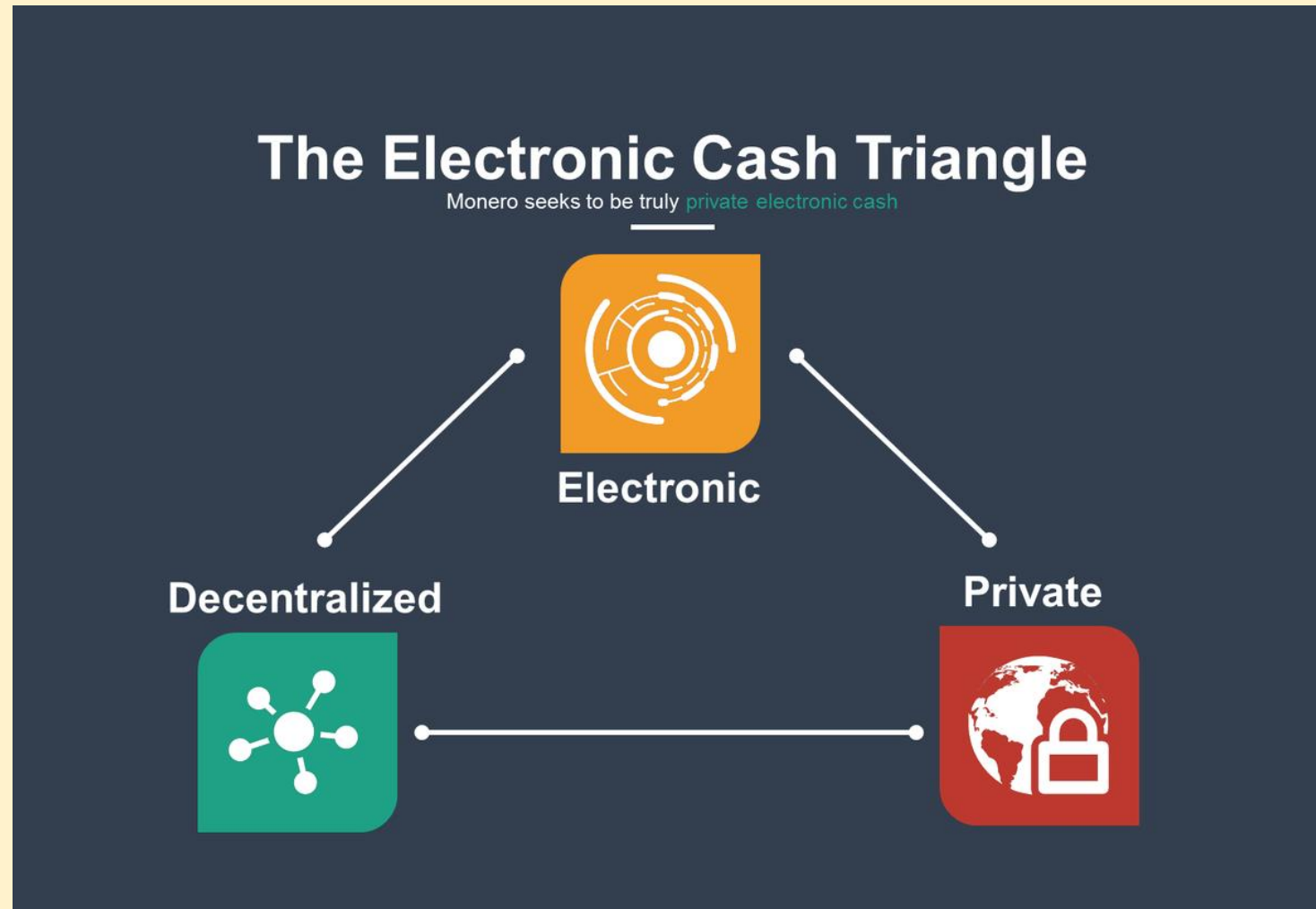


Do only criminals need privacy?

# BITCOIN vs MONERO

	BITCOIN (BTC)	MONERO (XMR)
CONCEPT	Digital money	Untraceable digital money
TRANSACTION DETAILS	Publicly viewable	Concealed from public
TRANSACTION EXAMPLE	Alice sent 1 BTC to Bob	? sent ? XMR to ?
MARKET CAP	~ \$228 billion	~ \$5.7 billion
BLOCK TIME	~ 10 minutes	~ 2 minutes

# THE ELECTRONIC CASH TRIANGLE ACCORDING TO THE MONERO TEAM



# The Case for Bitcoin

**Electronic**



**Decentralized**



**Privacy**

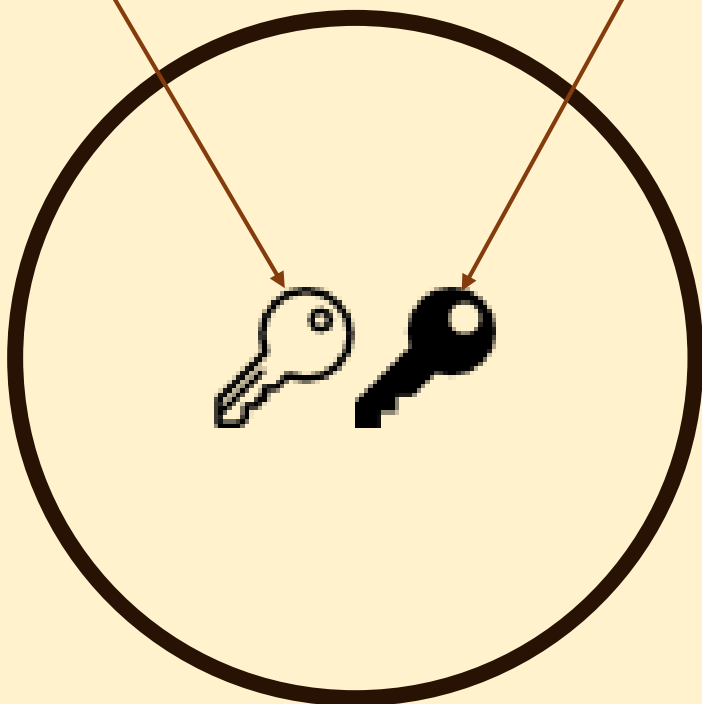


- Bitcoin is on an open ledger, everything is open to the public.
- While it is electronic and decentralized, it fails when it comes to privacy.



**PUBLIC KEY**

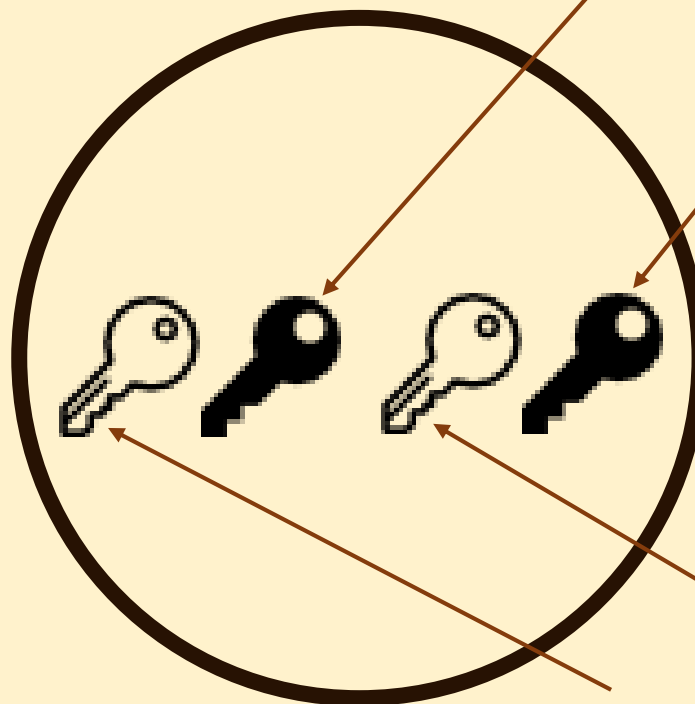
**PRIVATE KEY**



**MOST CRYPTOCURRENCIES**

**PRIVATE (SPEND) KEY**

**PRIVATE (VIEW) KEY**



**PUBLIC (VIEW) KEY**

**PUBLIC (SPEND) KEY**

**MONERO**

# THE 3 PILLARS OF MONERO

**PILLAR #1**

**RING  
SIGNATURES**

**PILLAR #2**

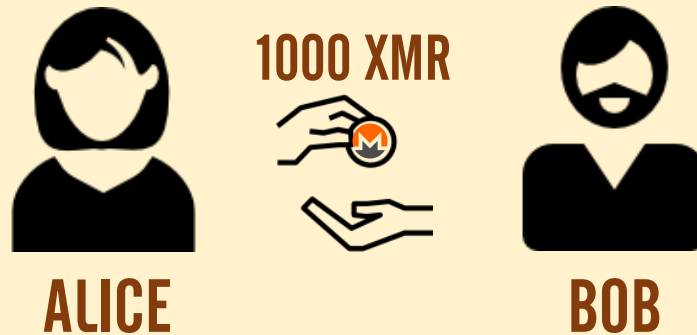
**STEALTH  
ADDRESS**

**PILLAR #3**

**CONFIDENTIAL  
TRANSACTIONS**

## PILLAR #1

## WHAT EXACTLY ARE RING SIGNATURES?



- She first chooses a **ring size**.
- She signs the **outputs** with her **private spend key** and sends it to blockchain.

**DECOY**

**DECOY**

**DECOY**

**DECOY**

**OUTPUT**

**INPUTS OF A  
TRANSACTION**

Suppose Alice chooses a ring size of 5

4 decoy outputs and her own output

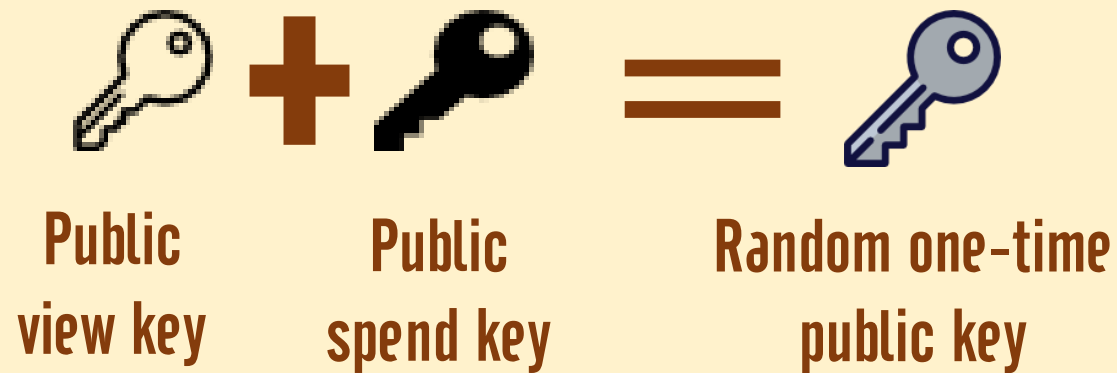
## PILLAR #2

## STEALTH ADDRESS

Q: What is transaction unlinkability?

A: If Alice is sending XMR to Bob, only Alice should know Bob's identity.

## How does Monero ensure Bob's privacy?



Alice uses Bob's public view key and public spend key to generate a random one-time public key.



**Random one-time  
public key**

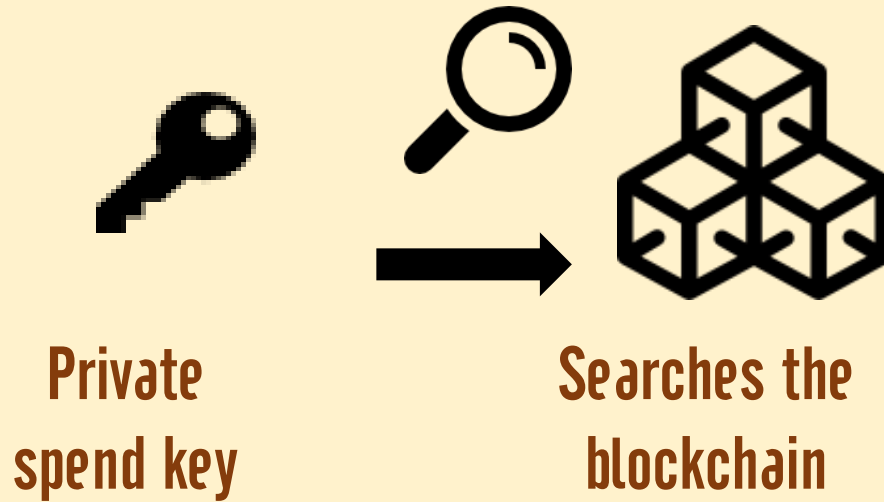


**Stealth address**



**ALICE**

- The one-time public key generates a one-time public address called “stealth address”.
- Alice sends the Monero to the stealth address.



- Bob's private spend key now traces the blockchain to look for that transaction.
- Upon finding it, Bob generates a private key corresponding to the one-time public key and retrieves the Monero.

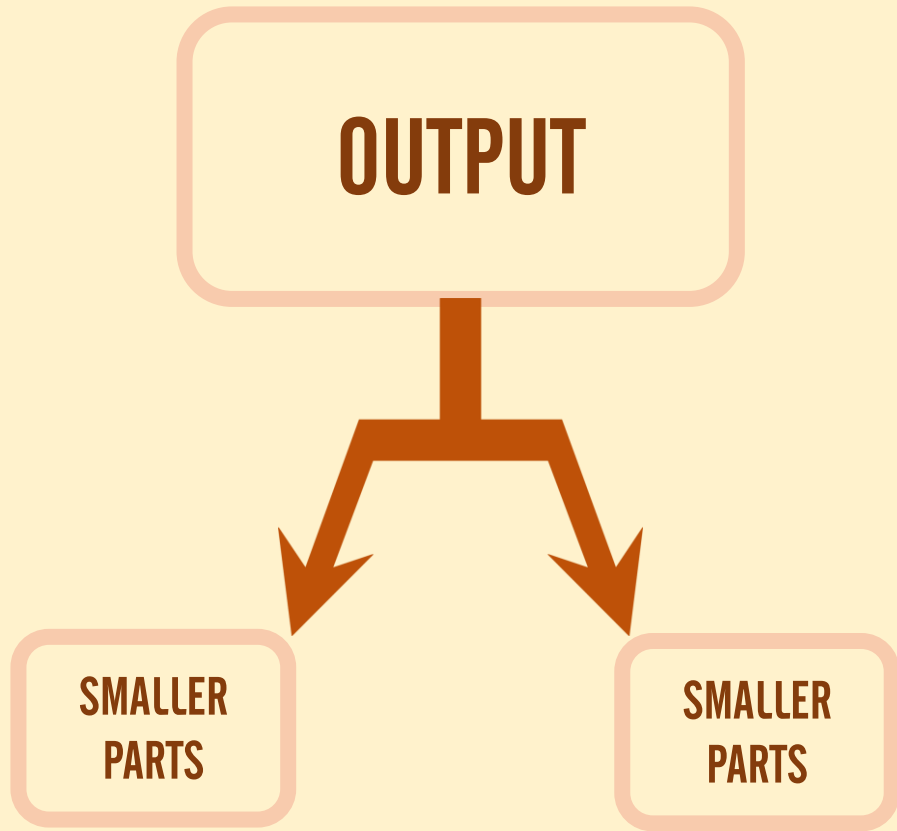


## PILLAR #3

## CONFIDENTIAL TRANSACTIONS

- We have seen how the sender and receiver can remain anonymous.
- How about making the transactions anonymous as well?
- This is where **Ring CT** comes in.

## Before Ring CT Implementation



Eg:



ALICE



BOB

It would break down like this:



- Each part then gets its own ring signature and then gets added to the blockchain.
- However this made the transactions visible to everyone.

## After Ring CT Implementation

- Ring CT hides every transaction in the blockchain.
- This means that every amount doesn't need to be broken down into known denominations.
- Any output can now link with any other output to create ring signatures!

# Meet the MONERO Team

Riccardo "fluffypony" Spagni

ric@getmonero.org



Francisco "ArticMine" Cabañas

articmine@getmonero.org



othe

othe@getmonero.org



smooth

smooth@getmonero.org



tacotime

tacotime@getmonero.org



luigi1111

luigi1111@getmonero.org




NoodleDoodle

noodledoodle@getmonero.org



# MONERO's biggest use case – Privacy Coin

 **Riccardo Spagni** ✓  
@fluffypony Following

Monero is so private that law enforcement can't figure out how much the AlphaBay owner had; not so with the other cryptocurrencies.

22 address. In total, from CAZES' wallets and computer agents took control of approximately \$8,800,000  
23 in Bitcoin, Ethereum, Moreno, and Zcash, broken down as follows: 1,605.0503851 Bitcoin,  
24 millions of dollars in criminal proceeds from AlphaBay. At this time, law enforcement have not  
25 identified a legitimate source for the assets obtained by CAZES and his wife, including any assets held in  
26 CAZES' wife's name. However, the investigation has revealed that between May 2015 and February  
27 2017, Bitcoin addresses associated with AlphaBay conducted approximately 4,023,480 transactions,  
28 receiving approximately 839,087 Bitcoin and sending approximately 838,976 Bitcoin. This equals  
approximately US\$450 million in deposits to AlphaBay. CAZES's 2-4% commission on Bitcoin  
transactions likely conducted with those funds would equal between \$9-18 million, which is consistent  
with the conclusion that his income derived from AlphaBay.  
20  
Verified Complaint for Forfeiture *In Rem*

Case 1:17-at-00557 Document 1 Filed 07/19/17 Page 21 of 27

1 8,309.271639 Ethereum, 3,691.98 Zcash, and an unknown amount of Monero.<sup>7</sup>

2:36 PM - 20 Jul 2017

Is Monero the ultimate “Crime Coin”?

# The Future

- In an increasingly transparent world, Monero's opaqueness is definitely an alluring property.
- It is one of the few non-bitcoin based coins which can make it truly big.
- Hardware wallets need to implement the option of storing Monero.
- Super exciting times ahead!

# Thank You!

You can check out my work here:

- [coinlive.io](https://coinlive.io)
- <https://blockgeeks.com/guides/>
- <https://medium.com/@rajarshimitra>

I hope you gained value from this presentation.