PRINCIPLE OF BLOCKCHAIN TECHNOLOGY

MONERO (XMR)

Professor: Tumennast Erdenebold
, Group 5

Table of Contents

Points to discuss:

Blockchain

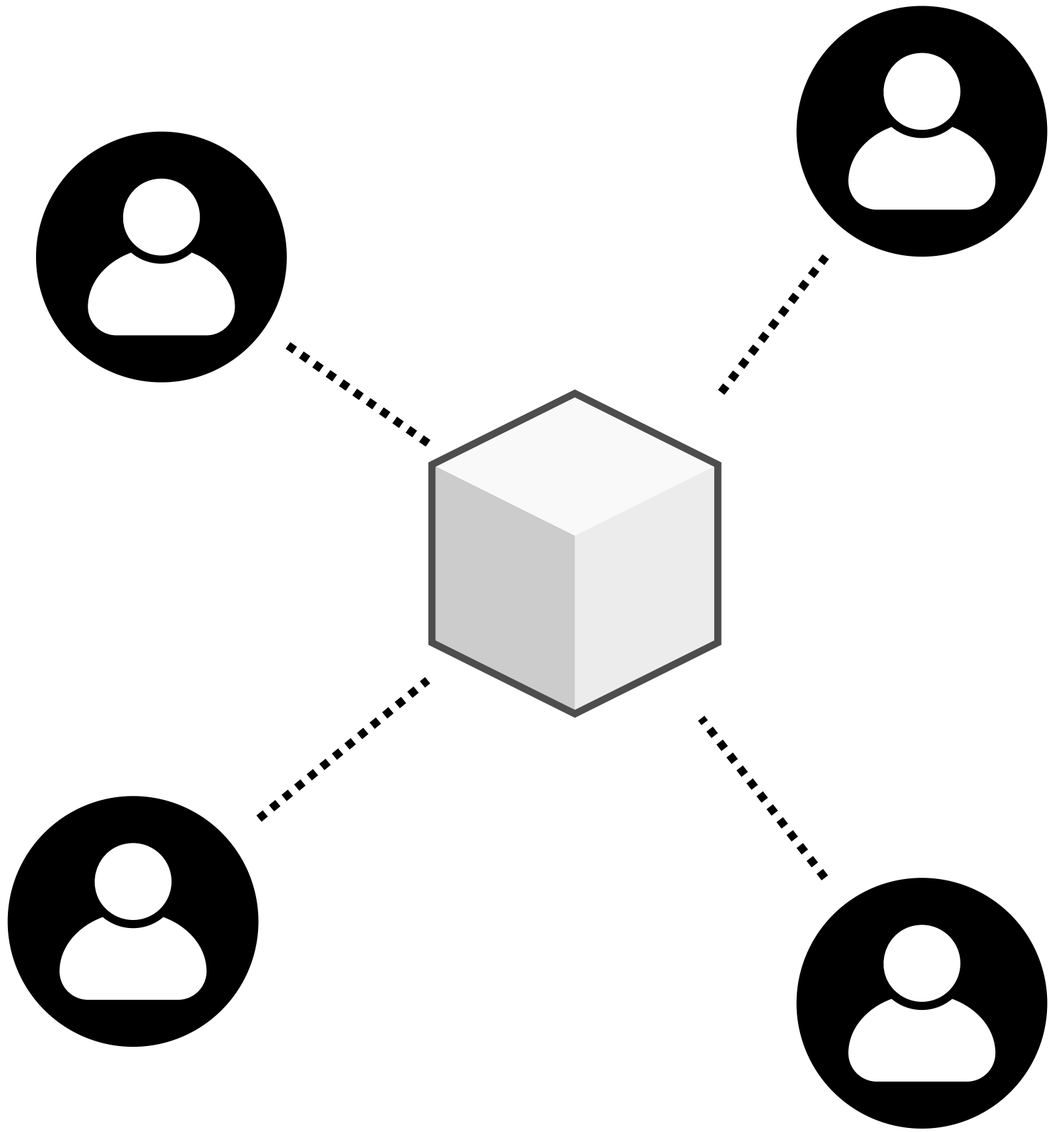
It is a digital ledger of tx in which entries can only be added

These tx are grouped into blocks which are linked together to compose a chain

blocks of record that are being made on the public ledger chaining to each other which distributes to the entire network.

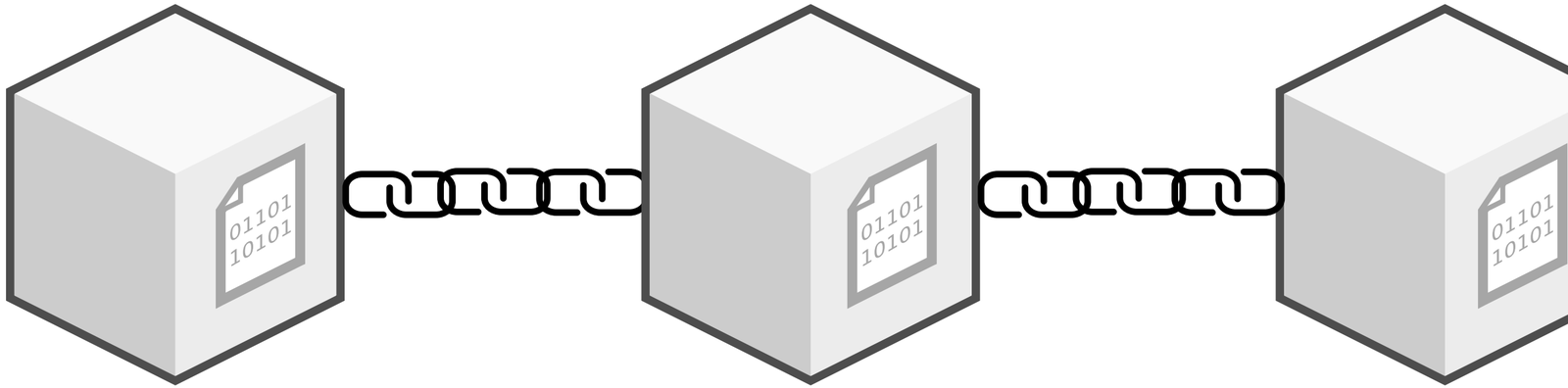
Copies of the ledger are simultaneously maintained by the member of monero

~~Central Authority~~



Adding new block

Miners record tx into block by performing the proof-of-work protocol



prev: **0000000000000000**...
hash: **000005**b65644af...

prev: **00000**5b65644af...
hash: **00000**8j953kf7y...

prev: **00000**8j953kf7y
hash: **00000**s9e8472lw

About Monero (XMR)

Monero = 'Coin' in Esperanto
It means a cryptocurrency based on privacy coin that guarantees privacy protection and anonymity.

- XMR = Monero's Ticker
- Monero Core Team
- C++
- Unlinkability & Untraceablilty

Bitcoin Books

Monero Books

History of Monero

A BitcoinTalk forum user forked tne codebase of Bytecoin under the nave 'BitMonero'	2014
A user group decided that the community need to take over it, changed name to 'Monero'	2014 April
It has continued to develop	After
Chage support services, machanisms, and block time, add features	2015
Monero's anonymity is further. Because of Confiedntial Trading algorithm & Ring CT theory	2017

Why Do People Invest In This Coin?

The most private cryptocurrency to exist

PRIMARY USE CASE

PEER TO PEER TRANSACTIONS

Through the utilization of it’s complicated blockchain ledger. It’s privacy has led to Monero’s developing in cryptography.

PRIVACY OVER SCALABILITY

Monero has placed a higher emphasis on privacy over scalability, focusing on implementing the privacy features before scaling.

IT’S USE IS DRIVEN BY THE USERS

The government officials find Monero’s advanced privacy a problem to track criminals, on the contrary, people find it as a right to transact with each other privately. And as Monero’s community said: “ It’s use is driven by the users themselves, not designed by the developers. "

Why Do People Invest In This Coin?

The most private cryptocurrency to exist

PRIVACY FEATURE

UNTRACEABLE TRANSACTIONS

This allows the transaction to be obfuscated

RING CONFIDENTIAL TRANSACTIONS SCHEME

It was put by the Bitcoin developer Gregory Maxwell, and is one of the primary components that allows transactions to be sent unclear.

NEW LEVEL OF ANONYMITY

It’s for the network as bulletproofs bring benefits of implementing zero-knowledge proofs but are much more efficient and do not require a trust setup.

Why Do People Invest In This Coin?

The most private cryptocurrency to exist

"There are other coins that can provide some level of privacy, but for some reason, Monero is the one that probably has the best crypto and the best means of hiding transactions."

– DAVID DECARY-HETU, PROF. OF UNIVERSITY OF MONTREAL

The Strengths and Weaknesses

Strengths

MULTIPLE KEYS

There are view and Spend keys in which view is for the recipient, and spend is about the sending

DEFAULT PRIVACY AND ANONYMITY

Even though it's a public ledger, all transactions are complicated so it can't be read or tracked

IT IS FUNGIBLE

Unlike bitcoin, the coins don't show where they came or if they are 'tainted' or 'clean' coins

The Strengths and Weaknesses

Weaknesses

MORE POPULAR BLOCKCHAINS

A threat of a more popular blockchain adopting the full privacy technology

DIFFICULT USER EXPERIENCE

It is very complicated to use or invest for new users, it has a very user unfriendly interface

FEWER WALLET OPTIONS

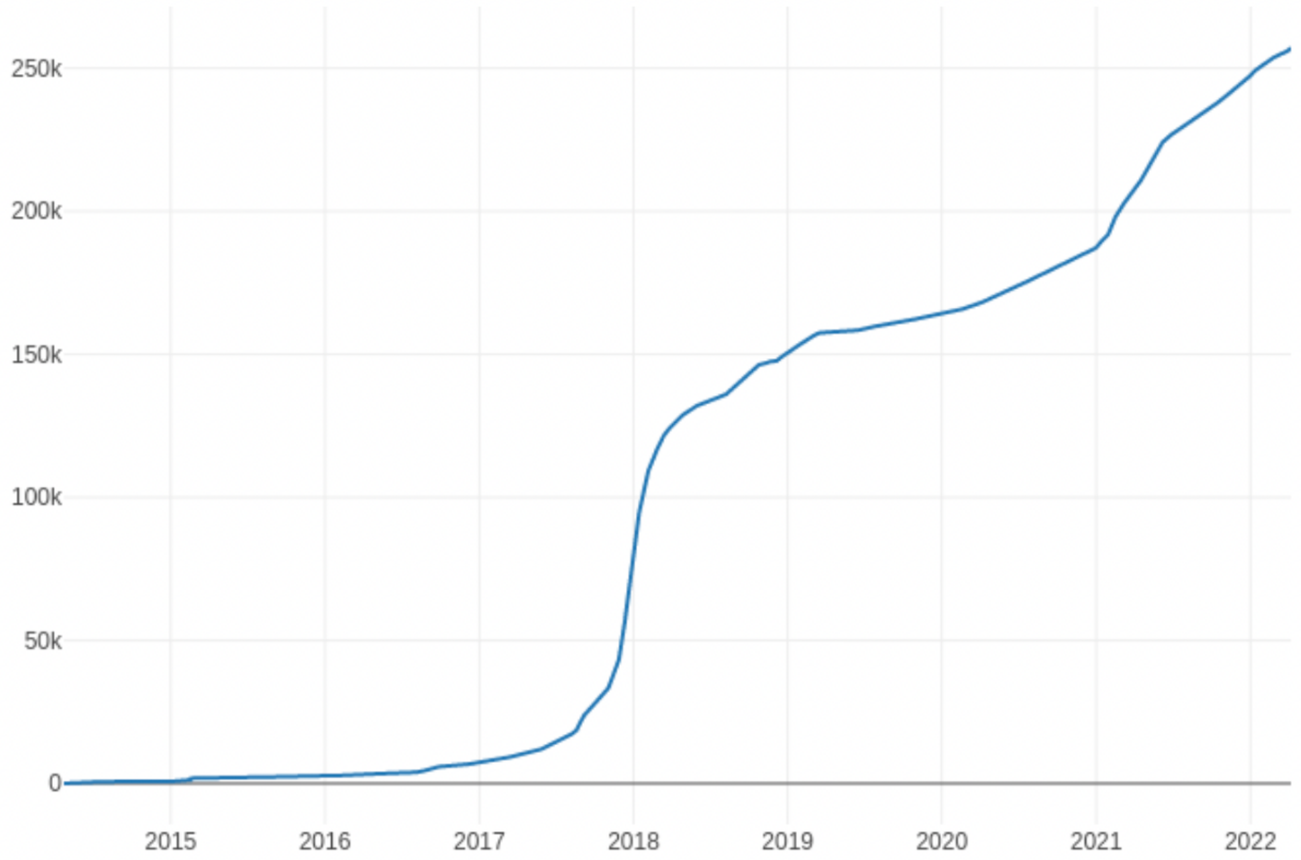
Due to the privacy technology associated with a transaction its harder to find a wallet for it

Market Price

Price predictions in 2022:

There is still hope that the XMR may continue growth until the end of 2022.
At the end of 2022 XMR can have the average rate of $345. It’s range can be $330 to $380.

According to TradingBeasts, XMR may grow about 110% in the next three years.



Market Price

Price predictions in 2023:

Years	Avg Price	Lowest Price	Highest Price
January 2023	$374.73	$348.50	$400.96
February 2023	$383.78	$356.92	$410.65
March 2023	$392.84	$365.34	$420.34
April 2023	$401.89	$373.76	$430.03
May 2023	$410.95	$382.18	$439.72
June 2023	$420.01	$390.61	$449.41
July 2023	$429.06	$399.03	$459.10

Market Price

Price predictions in 2023:

Years	Avg Price	Lowest Price	Highest Price
August 2023	$438.12	$407.45	$468.79
September 2023	$447.17	$415.87	$478.48
October 2023	$456.23	$424.29	$488.17
November 2023	$465.29	$432.72	$497.86
December 2023	$474.34	$441.14	$507.55

HOW DOES IT WORKS?

Let's dive into the difference first

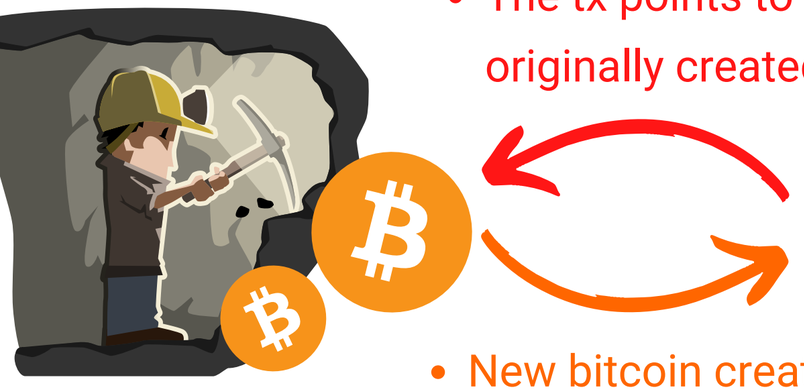
Vs	Monero	Bitcoin
Founder	Group of 7 core developers	Satoshi Nakamoto
Release Date	18 April, 2014	9 Jan 2008
Release Method	Crowdfunded group of 7 core develpers	Genesis Block Mined
Total Coin Supply	18.4 Million XMR + 0.3 XMR/minute	21 Million
Blockchain Protocol	Proof of work	Proof of work
Useage	Digital Currency	Digital Currency
Privacy	Untraceable	Yes
Trackable	No	Yes
Cryptocurrency Used	Monero	Bitcoin(Satoshi)
Cryptocurrency Symbol	(XMR)	(BTC)
Transaction Fee	0.004-0.02 XMR/kB	Varies based on load on blockchain
Algorithm	CrptoNote	SHA-256
Blocks Time	120 seconds	at least 10 minutes
Mining	GPUs, CPU	Pools,ASIC miners
Scalable	Yes	Yes

Bitcoin Vs Monero's img: https://www.google.com/url?sa=i&url=https%3A%2F%2Fcoinsutra.com%2Fmonero-cryptocurrency%2F&psig=AOvVaw0W0jbYpisxdkbWGuq8xY6&ust=1664610275478000&source=images&cd=vfe&ved=0CAwQjRxqFwoTCMDkjNeCvPoCFQAAAAAdAAAAABAO

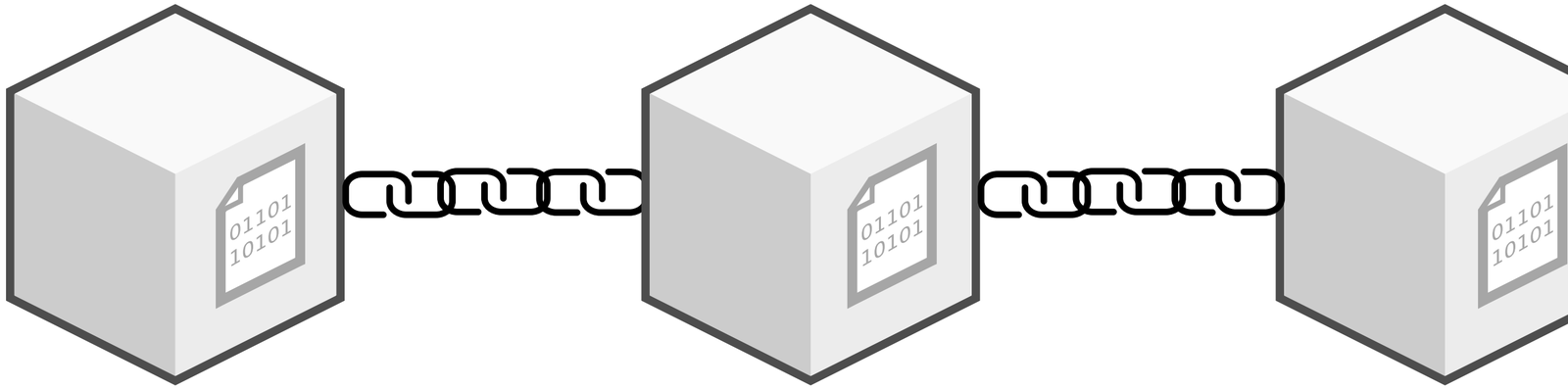
Isn't it pseudonym??

no third party, no bank, you own data & asset?

- You can send bticoin only by pointing to a prev tx in the chain that sent them to you
- The tx points to the previous tx all the way back to the coinbase that it was originally created in,



- New bitcoin create through coinbase transaction
- Proof-of-work: miner recieve reward

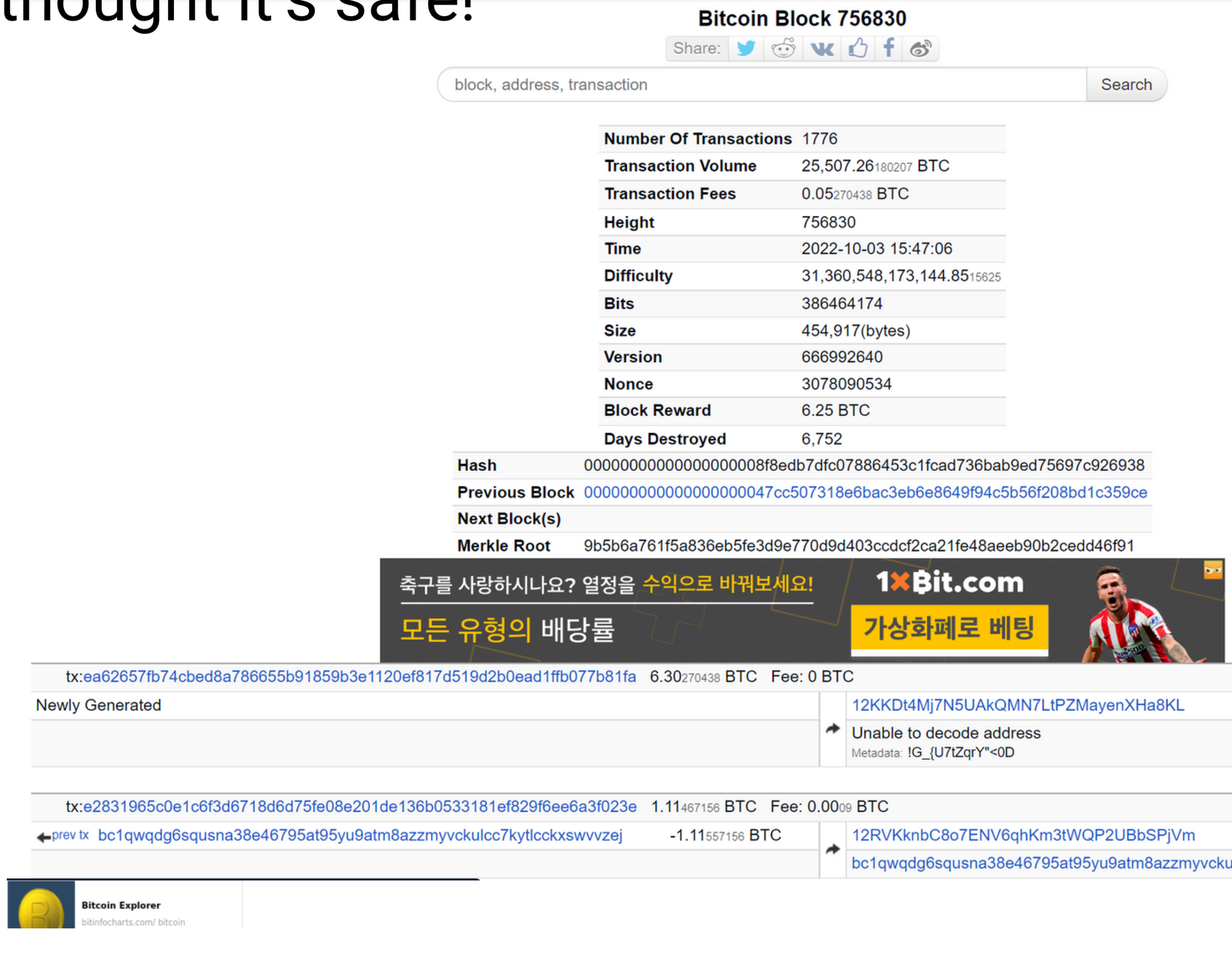


prev: **0000000000000000**...
hash: **00000**5b65644af...

prev: **00000**5b65644af...
hash: **00000**8j953kf7y...

prev: **00000**8j953kf7y
hash: **00000**s9e8472lw

I thought it's safe!



Bitcoin Block 756830

Share:

block, address, transaction — Search

Number Of Transactions	1776
Transaction Volume	25,507.26180207 BTC
Transaction Fees	0.05270438 BTC
Height	756830
Time	2022-10-03 15:47:06
Difficulty	31,360,548,173,144.8515625
Bits	386464174
Size	454,917(bytes)
Version	666992640
Nonce	3078090534
Block Reward	6.25 BTC
Days Destroyed	6,752

Hash	00000000000000000008f8edb7dfc07886453c1fcad736bab9ed75697c926938
Previous Block	00000000000000000047cc507318e6bac3eb6e8649f94c5b56f208bd1c359ce
Next Block(s)	
Merkle Root	9b5b6a761f5a836eb5fe3d9e770d9d403ccdcf2ca21fe48aeeb90b2cedd46f91

tx:ea62657fb74cbed8a786655b91859b3e1120ef817d519d2b0ead1ffb077b81fa 6.30270438 BTC Fee: 0 BTC

Newly Generated	12KKDt4Mj7N5UAkQMN7LtPZMayenXHa8KL	6.30270438 BTC
	Unable to decode address Metadata: !G_{U7tZqrY"<0D	0 BTC

tx:e2831965c0e1c6f3d6718d6d75fe08e201de136b0533181ef829f6ee6a3f023e 1.11467156 BTC Fee: 0.0009 BTC

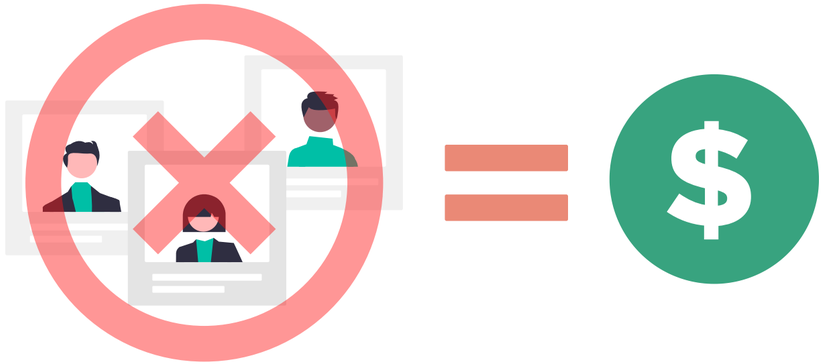
prev tx bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej	-1.11557156 BTC	12RVKknbC8o7ENV6qhKm3tWQP2UBbSPjVm 0.788 BTC
		bc1qwqdg6squsna38e46795at95yu9atm8azzmyvckulcc7kytlcckxswvvzej 0.32667156 BTC

Bitcoin Explorer
bitinfocharts.com/ bitcoin

Monero is baked into the cake

You have to defend your privacy
and "**Monero**"
create all of those for you

You can only protect your data only if it remains anonymous.



Your data is valuable

VALUABLE PRIVACY FEATURE

How does it works?

STEALTH ADDRESS

hide the receiver

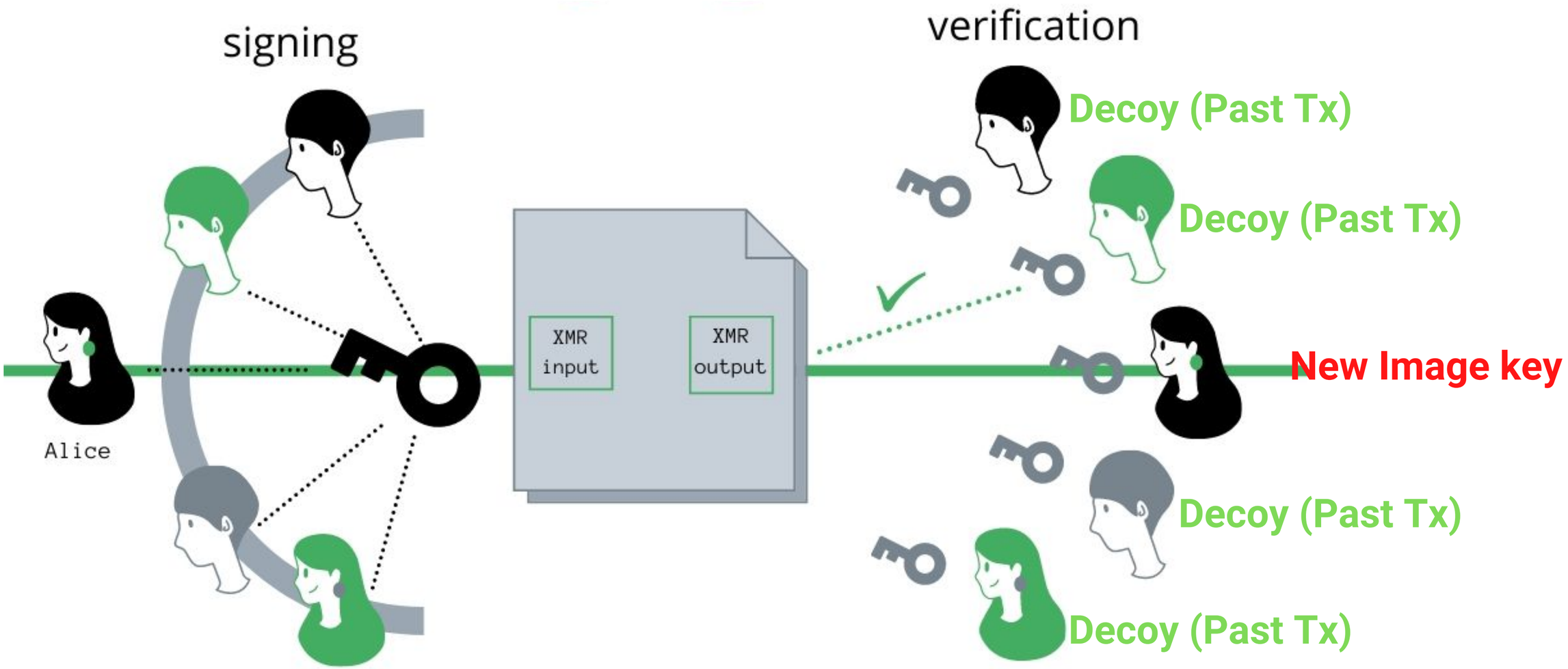
RING SIGNATURE

enable a sender to conceal their identity from other participants in a group. In short, to obscure the true sender

RING CONFIDENTAL TRANSACTIONS (RING CT)

In January 2017, Monero introduced Ring Confidential Transactions (RingCT) which also hides the value of transactions.

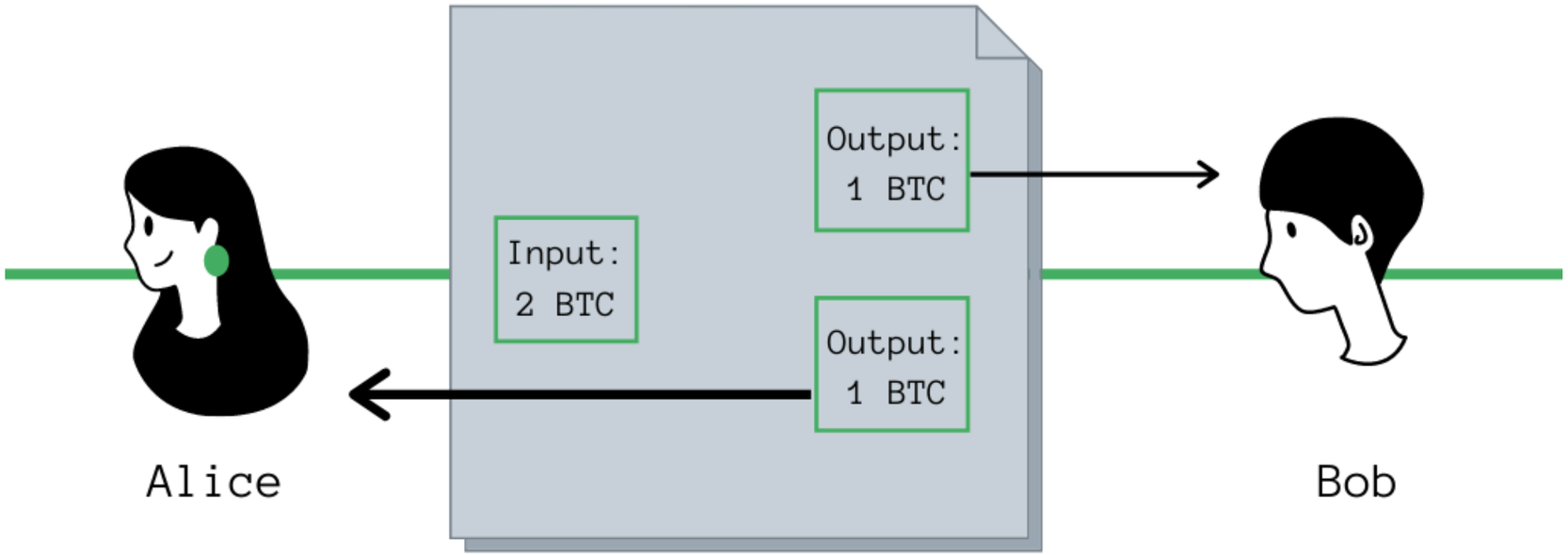
Ring Signature



Alice wants to send XMR. The protocol automatically combines her address with random decoy addresses to form a single ring signature which signs the transaction. Observers cannot tell who initiated the exchange, but can verify the transaction with cryptographic key images.

https://www.google.com/search?q=ring+signature+of+the+monero&tbm=isch&ved=2ahUKEwjGldGBhcT6AhXBCIgKHW9aD-kQ2-cCegQIABAA&oq=ring+sign&gs_lcp=CgNpbWcQARgAMgQIIxAnMgQIIxAnMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgAQyBQgAEIAEMgUIABCABDIFCAAQgARQyBtYtCZgny5oAHAAeACAAYYBiAH5CJIBBDAuMTCYAQCgAQGqAQtnd3Mtd2l6LWltZ8ABAQ&sclient=img&ei=ndI6Y4ZTwZGgBO-0vcgO&bih=809&biw=835&rlz=1C1VDKB_enTH1017KH1018&hl=en#imgrc=EAahitzfhDHoYM

A Simple Bitcoin Transaction

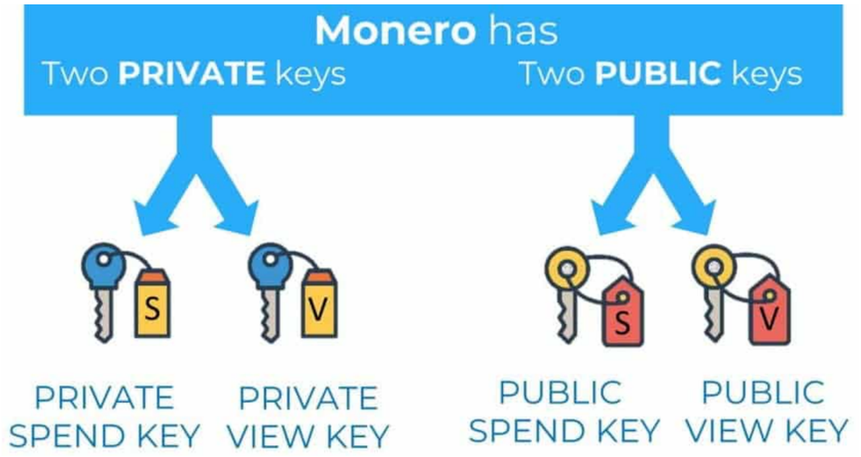


Alice has 2 BTC and she wants to send 1 BTC to Bob.
She initiates a transaction to send 1 BTC from her wallet to Bob's.
She receives 1 BTC back to her wallet as change.

https://www.google.com/search?q=stealth+address+monero&rlz=1C1VDKB_enTH1017KH1018&tbm=isch&sxsrf=ALiCzsbmwV7DnxyVIPW9qsABudKhZZQk2w:1664796132497&source=lnms&sa=X&ved=2ahUKEwjg_ebw-MP6AhXC1GEKHQbzBL0Q_AUoAnoECAEQBA&biw=1707&bih=841&dpr=1.5#imgrc=JYx2Eyj7OPFCIM

Stealth Address

Stealth Address or One-time generate key



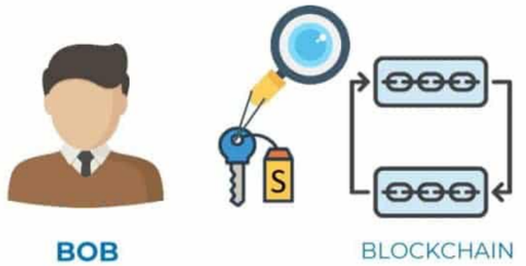
1. Bob's public view key and public spend key together generates a random one-time public key.

2. The one-time public key generates a one-time "stealth address".

3. Alice sends the Monero to the stealth address

#2

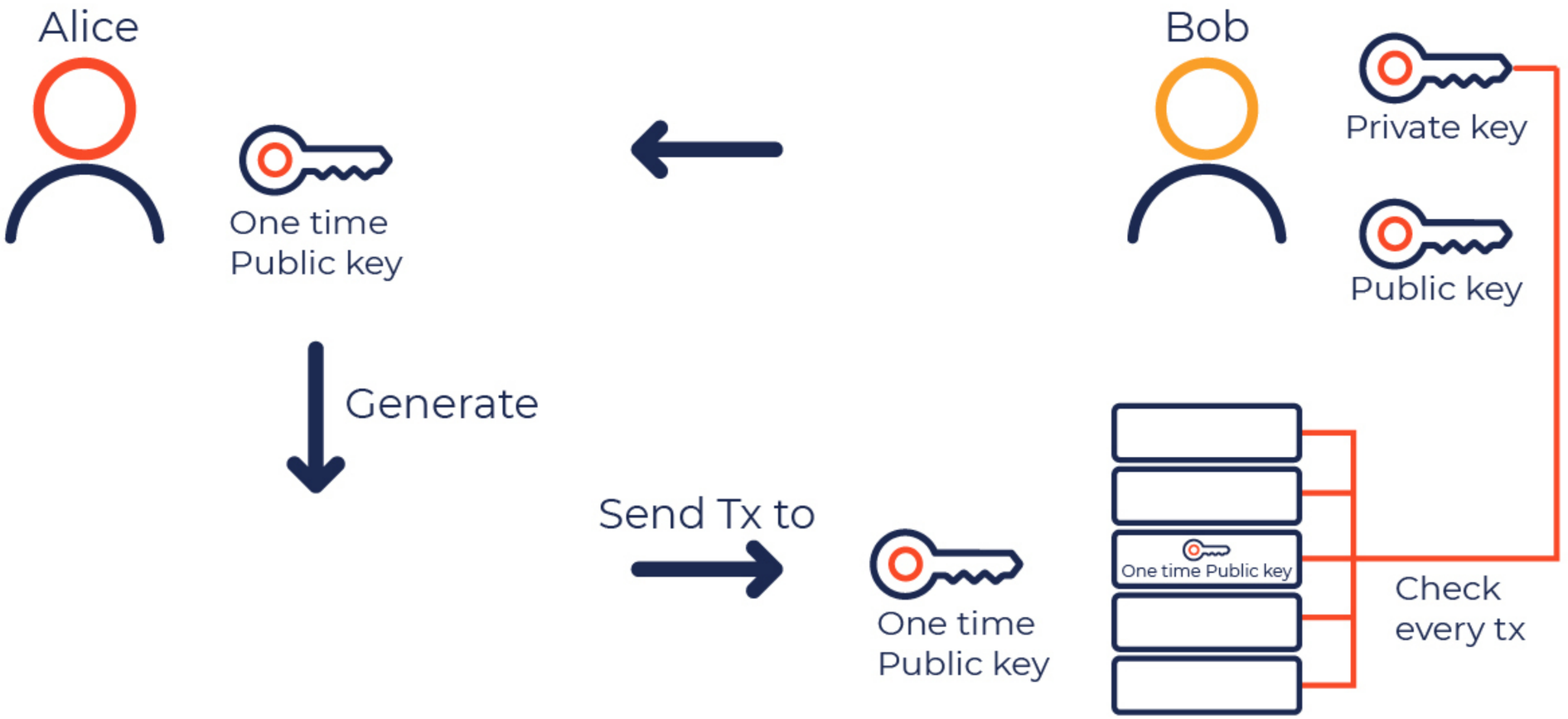
STEALTH ADDRESS protects the receiver's (Bob) identity



4. Bob's private spend key now traces the blockchain to find that transaction.

5. Bob generates a one-time private key corresponding to the one-time public key and retrieves the Monero.

Stealth Address

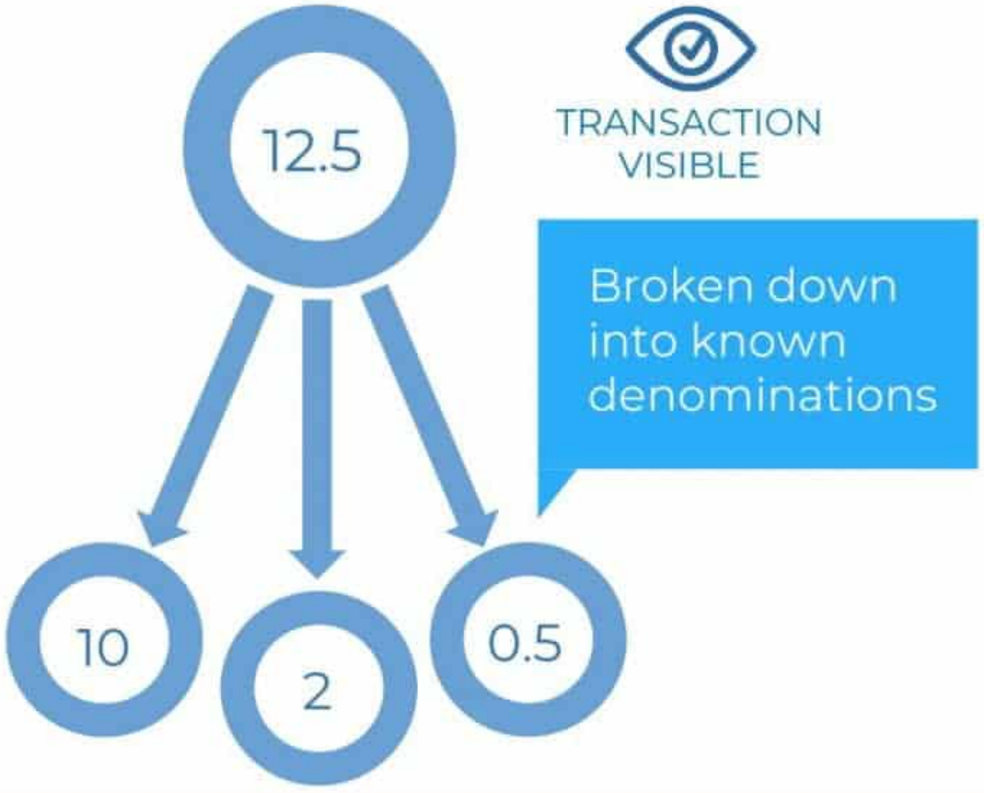


https://www.google.com/search?q=stealth+address+&tbm=isch&ved=2ahUKEwiNp7zx-MP6AhXkTPUHHYJnAGoQ2-cCegQIABAA&oq=stealth+address+&gs_lcp=CgNpbWcQAzIECCMQJ1CEDViEDWD9DWgAcAB4AIABkQGIAZEBkgEDMC4xmAEAoAEBqgELZ3dzLXdpei1pbWfAAQE&sclient=img&ei=5cU6Y82gNuSZ1e8Pgs-B0AY&bih=841&biw=1707&rlz=1C1VDKB_enTH1017KH1018#imgrc=8KULEPrSR-lHjM

Ring Confidential Transactions (Ring CT)

#3 CONFIDENTIAL TRANSACTIONS or RING CT protects the transaction identity

BEFORE RING CT



TRANSACTION VISIBLE

Broken down into known denominations

AFTER RING CT

Any output can link with any other output to create ring signatures

TRANSACTION NOT VISIBLE

Doesn't need to be broken down into known denominations

Monero's privacy and fungibility made it a true electronic cash

When you recieve monero, it is monero.

Key Take away:

- Originally called Bitmonero (2014) hard fork from Bytecoin
- The cryptocurrency that focused on privacy
- Designed to keep the tx completely anonymous including network members, developers, and miners.
- Using "Ring Signature" and "Stealth Address" and "Ring Confidental Transaction"

Please voice your questions out

we will try our best to give explaination!

Reference:

1. https://www.youtube.com/watch?v=cjbHqvr4ffo
2. https://www.youtube.com/watch?v=M6kxtiKKyMQ
3. https://www.youtube.com/watch?v=SSo_EIwHSd4
4. Ring Signature: https://www.youtube.com/watch?v=zHN_B_H_fCs
5. Bitcoin Vs Monero's img: https://www.google.com/url?sa=i&url=https%3A%2F%2Fcoinsutra.com%2Fmonero-cryptocurrency%2F&psig=AOvVaw0W0jbYpisxdkbWGuq8-xY6&ust=1664610275478000&source=images&cd=vfe&ved=0CAwQjRxqFwoTCMDkjNeCvPoCFQAAAAAdAAAAABAO
6. https://www.google.com/search?q=monero&tbm=isch&tbs=rimg:CRMmKfP4C8A4YcGIHoYqYpLs8AEAsgIMCgIIABAAOgQIABAA&rlz=1C1VDKB_enTH1017KH1018&hl=en&sa=X&ved=0CB0QuIIBahcKEwjA5IzXgrz6AhUAAAAAHQAAAAAQaA&biw=835&bih=809#imgrc=k-9_3HYHI_24yM
7. https://www.getmonero.org/get-started/what-is-monero/
8. https://www.cryptoeq.io/corereports/monero-abridged
9. https://www.analyticsinsight.net/monero-price-prediction-is-it-still-a-good-option-why-tama-looks-hotter/
10. https://ambcrypto.com/predictions/monero-price-prediction-2023
11. http://wiki.hash.kr/index.php/%EB%AA%A8%EB%84%A4%EB%A1%9C
12. Check Proof of transaction: https://www.getmonero.org/resources/user-guides/prove-payment.html