Monero (XMR)

A Privacy Oriented Cryptocurrency

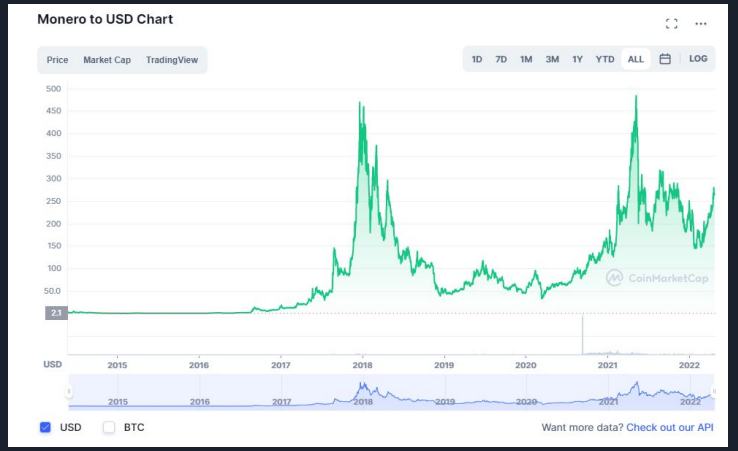
Origins of Monero

Bitcoin’s transparency was called a “critical flaw”

Deployed in 2014 with true anonymity being the goal

Forked from CryptoNote

Currently has a 4.1 billion dollar market-cap



All time Monero to USD graph. Source: https://coinmarketcap.com/currencies/monero/

Monero vs Bitcoin

Similarities:

- Decentralised nodes operate the same way
- Both are fungible (One unit is exactly the same as another unit)

Differences:

- Monero transactions are entirely private (bitcoin has an open ledger)
- Dynamically scalable block
- Monero ASIC resistant

What actually is Monero (Overview)

Privacy, privacy, privacy!!

Unique pseudo identities for each transaction

Monero is fungible - intended as a currency

“One-vote-per-person”

ASIC resistant

Peer-to-peer network

More on these systems shortly

Mining of Monero

ASIC Resistant Mining

Monero uses hash algorithms designed to be inefficient on GPU, FPGA and ASIC architectures

RandomX algorithm

Mining is accessible to regular people using regular hardware

Still will need to join a mining pool to reap any profits

Issues with Mining

MineXMR control close to 40% of hashrate

78% of hashrate controlled by top 5 mining pools

Many individual miners making up this large pool

Can be solved by evenly distributing individual miners

Monero Pool List

Home FAQ About Chat

The Monero pools list is currently tracking 25 different mining pools to help you pick a pool before you start mining!

Check the frequently asked questions or join our chat if you need any help.

№	Pool	Location	Payout	Min. Payout (ɱ)	Fee (%)	Miners	Hashrate (kH/s)	Hashrate (%)
1	MineXMR	Global	PPLNS	0.004	1.000	12,351	1,126,198	39.215
2	SupportXMR	Global	PPLNS	0.100	0.600	7,394	440,284	15.331
3	nanopool	Global	PPLNS	1.000	1.000	3,742	387,762	13.502
4	XMRPOOL.EU	NL	PPLNS	0.100	0.900	1,827	126,941	4.420
5	p2pool	P2P	PPLNS	0.000	0.000	453	97,198	3.384
6	MoneroOcean	Global	PPLNS	0.003	0.000	5,177	96,572	3.363
7	Skypool	CN	PPS+	0.020	1.000	379	47,872	1.667
8	2Miners	UK	PPLNS	0.010	1.000	2,963	44,147	1.537
9	HashVault	Global	PPLNS	0.001	0.900	1,849	37,459	1.304
10	p2pool mini	P2P	PPLNS	0.000	0.000	249	12,749	0.444

Monero's top 10 pool list. Source: https://pools.xmr.wiki/

What Makes Monero Private?

Distribution and Transactions

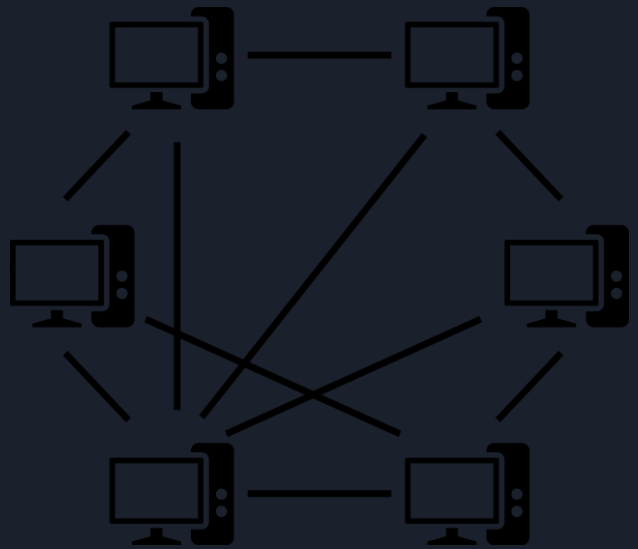
Peer-to-peer consensus network to record transaction outputs

Transactions are the transformation of old outputs into new outputs

Transactions are confidential and untraceable

Uses Stealth Addresses, Ring Signatures, RingCT

More on these now…



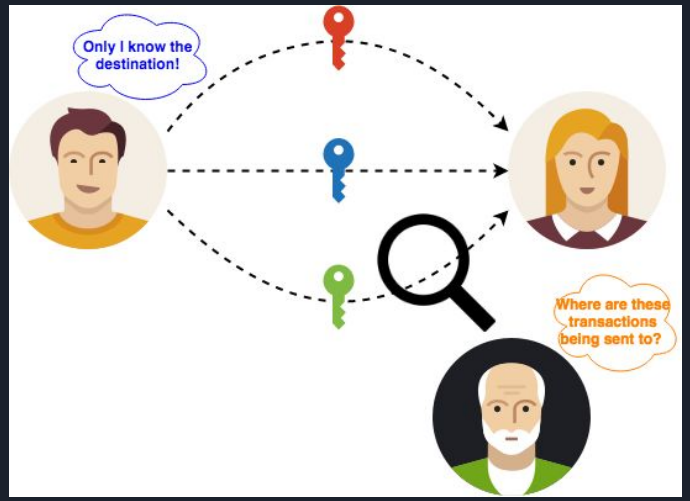
Stealth Addresses

New one-time destination public key for each transaction

Monero wallet: 95 character string consisting of a public view key and public spend key

Outsiders unable to distinguish individuals in transactions

Wallet addresses never appears on the blockchain



Ring Signatures

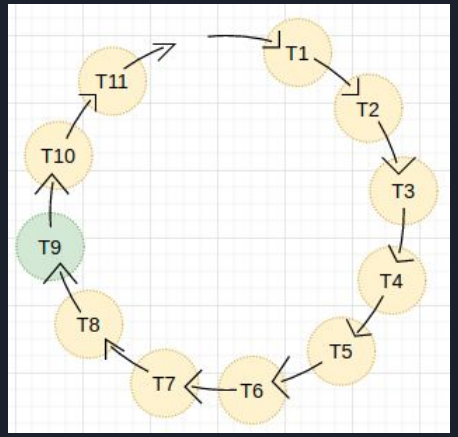
Algorithm creates an anonymity set of possible singers

Makes all inputs indistinguishable from each other

Ring size of 11 - 1 real transaction and 10 decoy transactions

Plausible deniability: can prove that the signature is real, just not which one

Key images used to prevent Monero spent more than once



RingCT

“Ring Confidential Transactions”

Implemented in 2017

When newly mined Monero is transferred, masked amount outputs are generated

Will disclose just enough information to prove input funds is equal to output

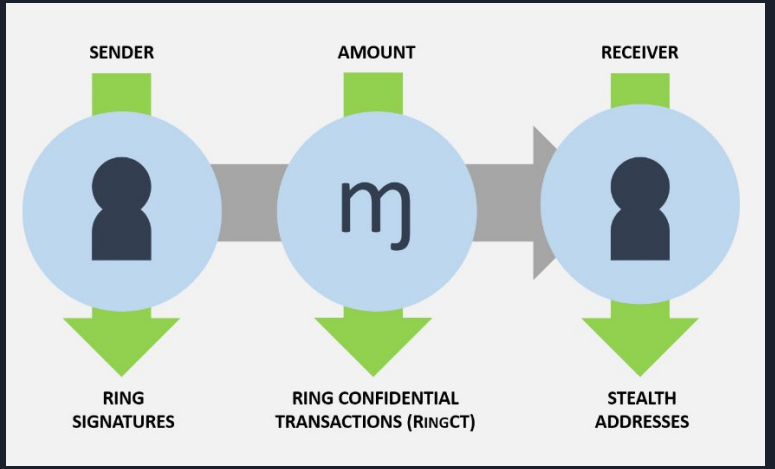
Anyone can confirm a transaction is legit without seeing the value: Pederson commitment

Range Proof to prevent negative values

Summarising Transaction Privacy

Stealth Addresses + Ring Signatures + RingCT

= anonymous transactions



Problems with Monero

Anonymity too far?

SUS!

Powers individual and strips it away from governments, organisations and banks

Circumvents traceable forms of currency transactions, allowing criminal activity to go undetected

However, Monero is not the preferred finance option for criminal activities

$1.5 to $4 trillion dollars in money laundering, $10 billion in criminal financing

(United Nations, 2021)

If they use an exchange, the transaction is transparent and traceable anyway

Tax Evasion

Share money without the use of a central authority

Large percentage of population using would hurt government funding

Measures could be put into place to avoid these

- Namely allowing merchants to accept Monero
- Government provides an XMR-to-Cash swap system
- Allows private transactions to be secure, whilst also keeping people in the tax system

Issues Solved by Monero

Political targets/refugees/protection from tyrannical government

- Protects the individual against reckless governments
- Allows people fleeing their homes to preserve some wealth
- Empowers developing nations' citizens to engage in global economies
    - Allows outside investment to circumvent corrupt central banks and economies to persevere, despite corrupt authorities.
- Provides the decentralisation of Bitcoin, but allows the user to remain private, preserving the last shred of privacy that is available in Australia.
- Empowers the individual and rips financial authority from central bodies.

Conclusion

Coin focused on privacy!

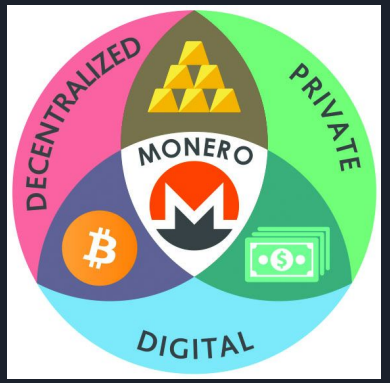
Uses stealth addresses and ring signatures to mask users

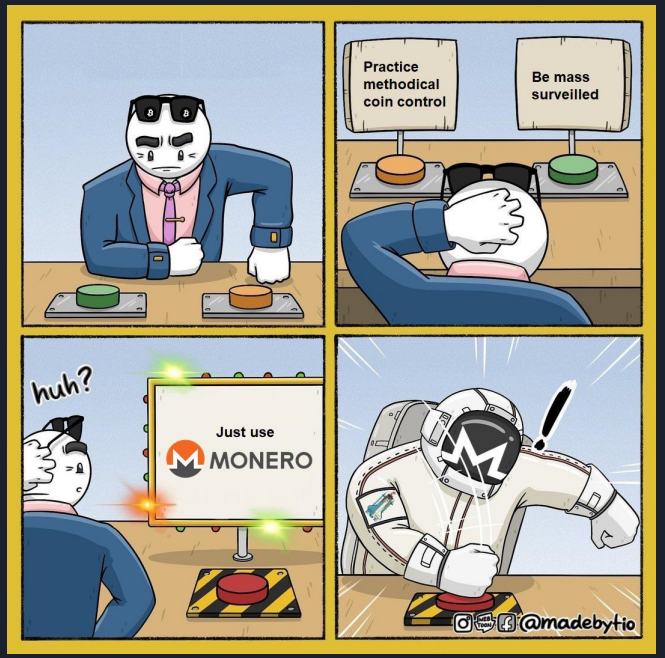
RingCT hides the amount being transferred

Gives power back to the individual

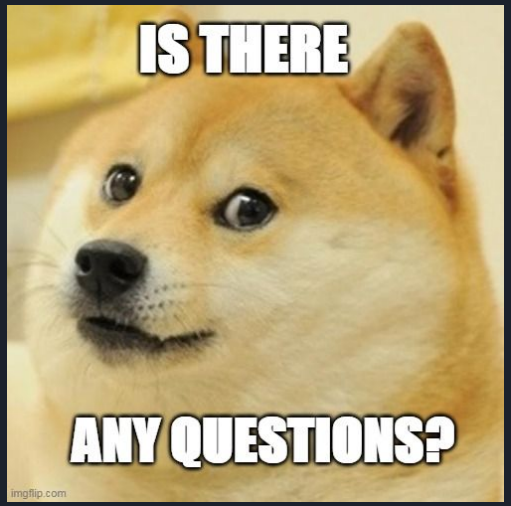
Dynamically scalable

Issues with mining pools but only short term issue





Any Questions?



References

CoinMarketCap, 2022. Monero. [Online]

Available at: https://coinmarketcap.com/currencies/monero/

[Accessed 10 April 2022].

Monero, 2022. Home | Monero. [Online]

Available at: https://www.getmonero.org/

[Accessed 10 April 2022].

Seth, S., 2021. Monero (XMR) Cryptocurrency. [Online]

Available at: https://www.investopedia.com/tech/introduction-monero-xmr/

[Accessed 10 April 2022].

XMR Wiki, 2022. Monero. [Online]

Available at: https://pools.xmr.wiki/

[Accessed 25 April 2022].

Bambrough, B., 2021. Warning: The FBI Has Issued A Serious Bitcoin And Crypto Alert. [Online]

Available at: https://www.forbes.com/sites/billybambrough/2021/07/14/the-fbi-has-issued-a-serious-bitcoin-and-crypto-alert-warning/?sh=1502e67148f8

[Accessed 30 March 2022].

Image References

https://www.getmonero.org/

https://www.computerworld.com/article/3545530/ultimate-guide-to-privacy-on-android.html

https://www.digminecraft.com/materials/images/diamond_ore_pickaxe.png

https://www.bitdegree.org/crypto/tutorials/monero-mining

https://pools.xmr.wiki/

https://upload.wikimedia.org/wikipedia/commons/thumb/9/9e/P2P_network.svg/640px-P2P_network.svg.png

https://www.rambus.com/blogs/the-importance-of-hardware-based-security-solutions/

https://hackernoon.com/blockchain-privacy-enhancing-technology-series-stealth-address-i-c8a3eb4e4e43

https://medium.com/coinmonks/mapping-ring-signatures-and-stealth-addresses-in-monero-a5543a434684#:~:text=Transaction%20Receiver,addresses%20visible%20on%20the%20blockchain

https://medium.com/@crypto_ryo/on-chain-tracking-of-monero-and-other-cryptonotes-e0afc6752527

http://assets.stickpng.com/images/61d183263a856e0004c6334a.png

https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6

https://www.inventiva.co.in/stories/tax-evasion-leads-loss/

https://www.reddit.com/r/Monero/comments/mklzyw/decentralized_private_digital/

https://mobile.twitter.com/moneromemes

https://thicc.mywaifulist.moe/waifus/38922/cbb686f837e1b05238a7a0d95437a134bab2abe0ca177628aa1a6d394d56fdc4_thumb.png

https://comfymetro.com/data/2c2eef38c87a4e143f31398a94cb83a9.png

https://medium.com/@harrypotter0/how-does-monero-work-17f18ea37652

https://securityweekly.com/wp-content/uploads/2021/06/43759104674_fd09fe32fa_o.jpg