Moving past tribalism to freedom via Monero

Presented by Seth For Privacy

COVERED TODAY

A BRIEF OUTLINE

Why do we need Monero?

A brief history of Monero

Monero Protocol 101

Dispelling Monero myths

- Supply dynamics
- Auditing the supply
- Hard-forks
- Scaling

INFOSEC ENGINEER + SYSADMIN

6+ years in the InfoSec space, focused on cybersecurity engineering

PRIVACY EDUCATOR

Building out pro-privacy education, guides, and resources, including the Opt Out podcast

MONERO CONTRIBUTOR

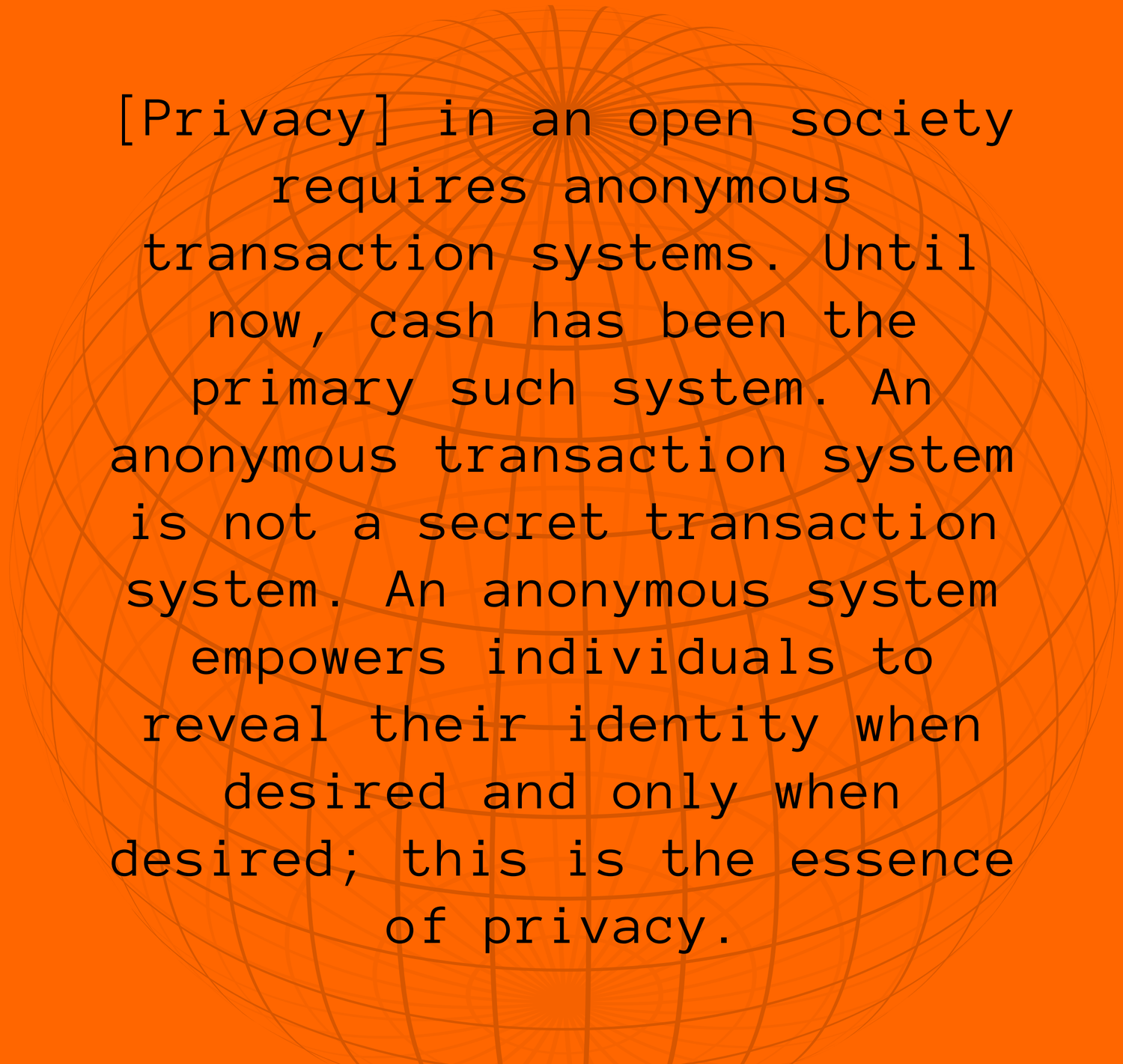
Contributing to Monero for the past 2y

A CYPHERPUNK'S MANIFESTO

“

[Privacy] in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

ERIC HUGHES



"FREEDOM CONVOY"

Bitcoin donated to the “Freedom Convoy” in Canada is blacklisted and frozen at centralized exchanges

RUSSIAN BLACKLISTINGS

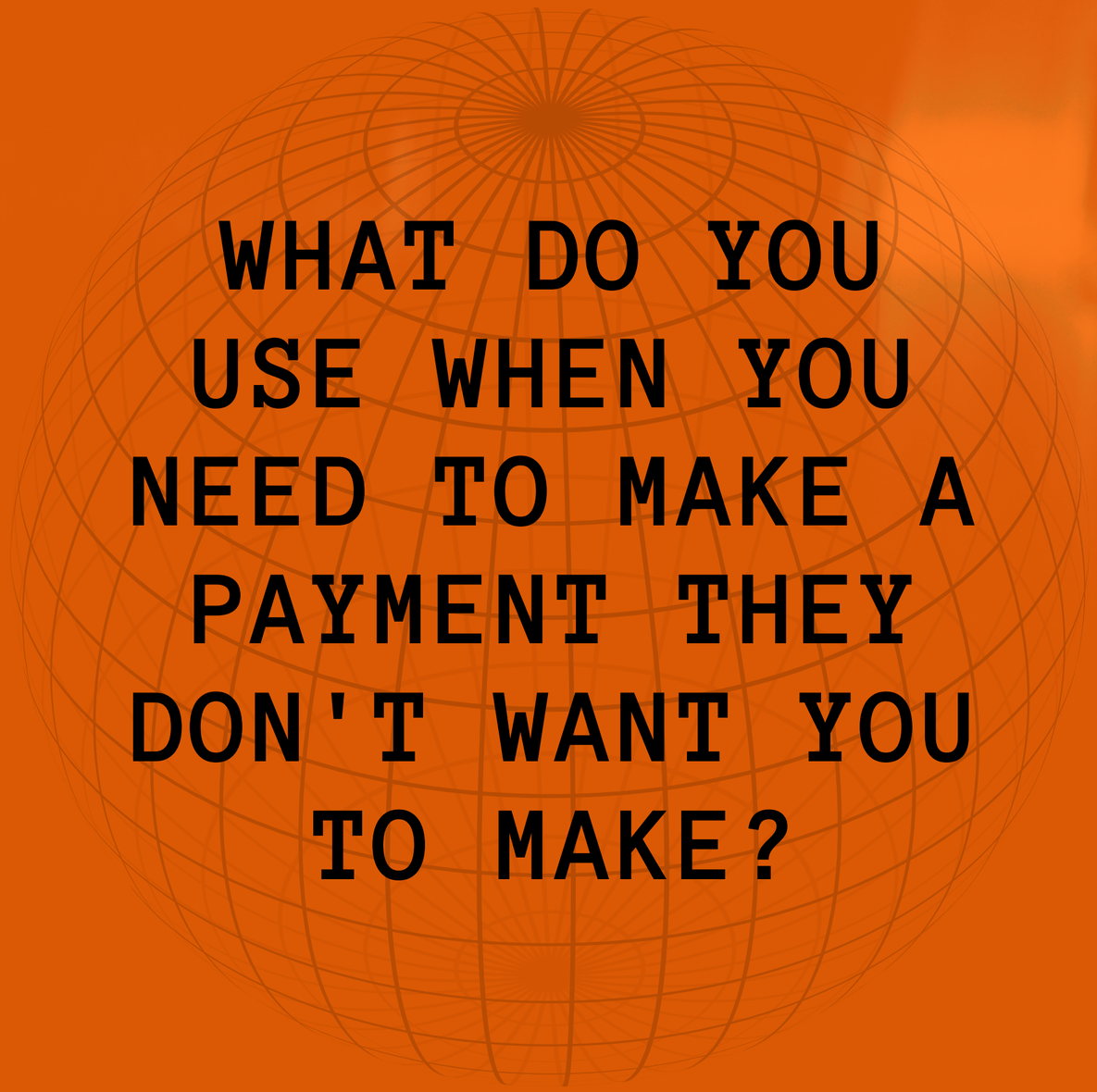
Coinbase proactively traces and blacklists 25,000 addresses connected with Russian users in order to comply with sanctions against Russia

CENSORSHIP OF PRIVACY TOOLS

Wasabi Wallet announces they will start censoring mixing inputs to prevent certain users from mixing their funds using chain analysis

MANY CASES OF CENSORSHIP OF USERS

More cases happening daily of users being prevented from using their Bitcoin as they see fit due to transparency.



WHAT DO YOU USE WHEN YOU NEED TO MAKE A PAYMENT THEY DON'T WANT YOU TO MAKE?

MONERO IS MADE FOR THIS.

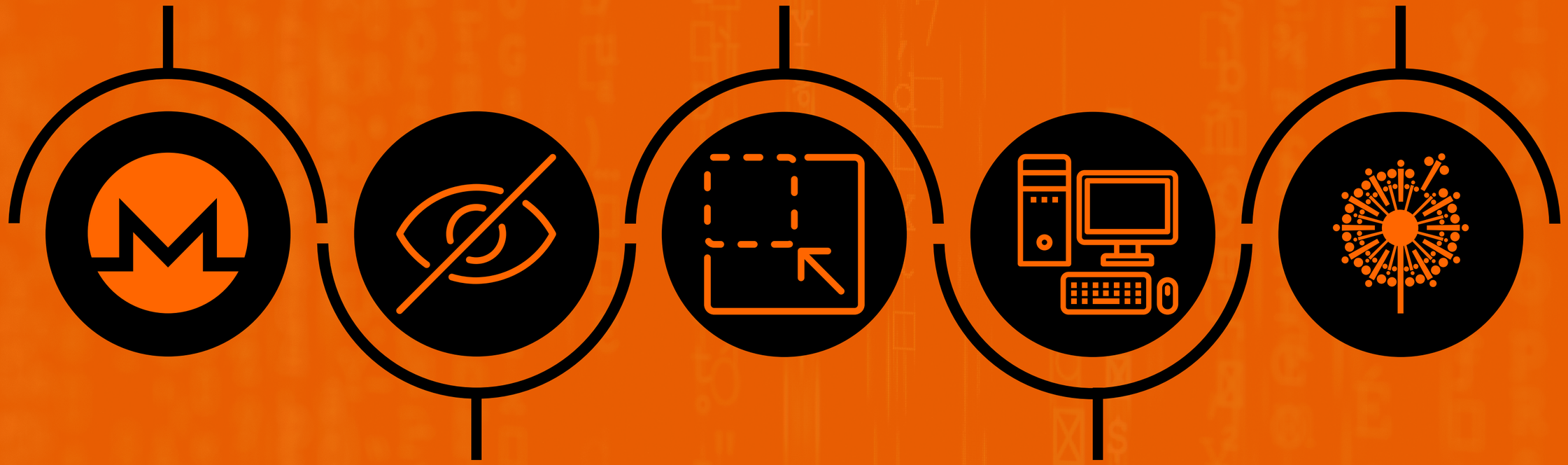
MONERO CREATED FROM CRYPTONOTE PROTOCOL (2014)

MONERO IMPLEMENTS RINGCT, HIDING AMOUNTS (2017)

BULLETPROOFS, 80% DROP IN TX SIZE (2018)

RANDOMX, DECENTRALIZING MINING (2019)

DANDELION++, DEFAULT NETWORK-LEVEL PRIVACY (2020)

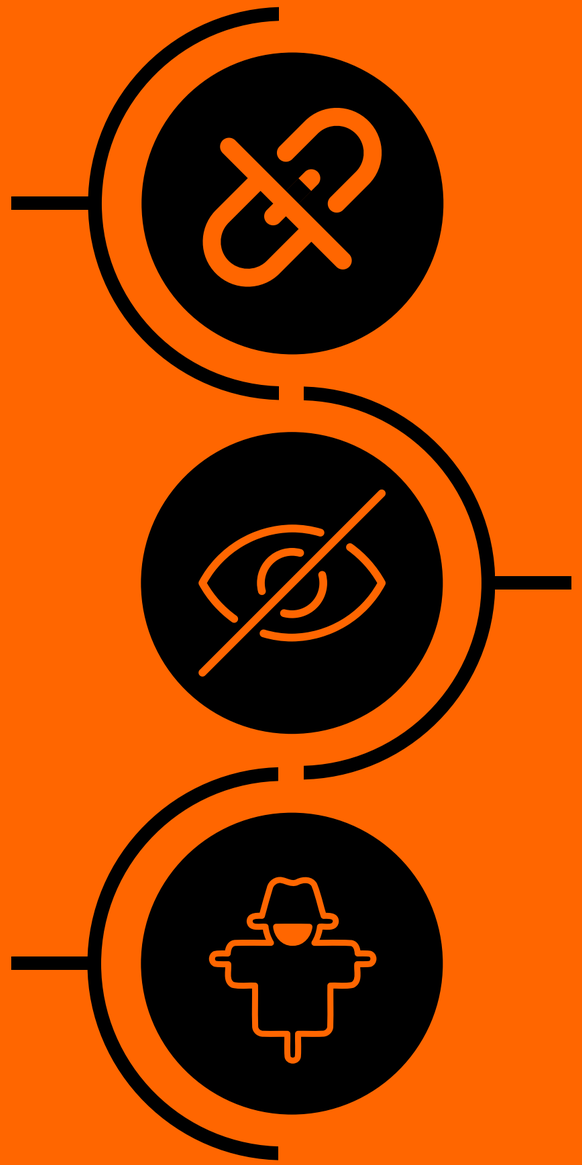


ONE-TIME ADDRESSES

Also known as "stealth addresses", the real address of sender and recipient is never published on-chain.

RING SIGNATURES

Every input to a transaction is combined with 10 "decoy" inputs, any of which could plausibly be the true-spent input to outside observers.



CONFIDENTIAL AMOUNTS

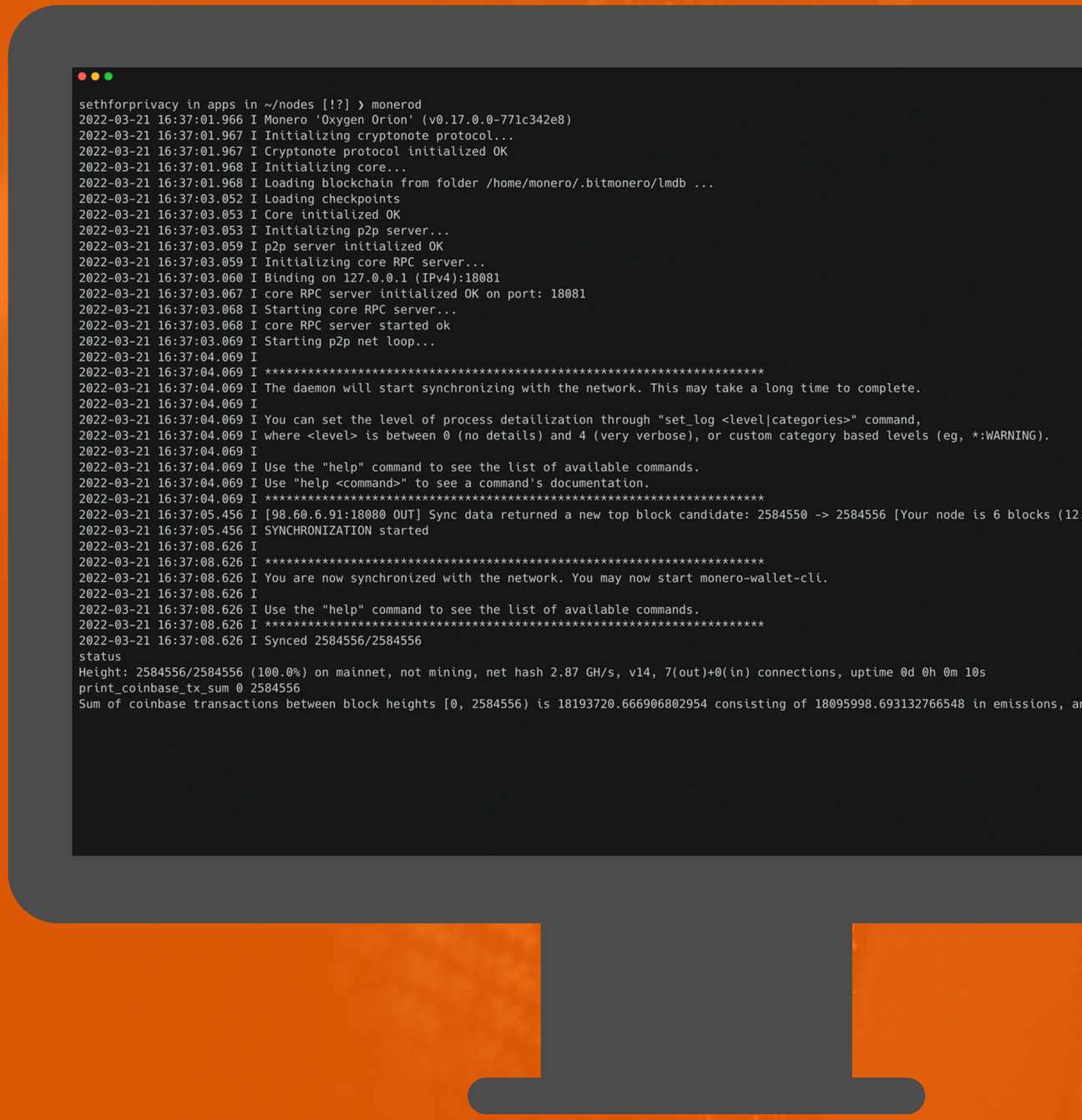
Also known as "Confidential Transactions", the amount in every Monero transaction is cryptographically hidden, and cannot be viewed by outside observers.

MONERO'S SUPPLY DYNAMICS

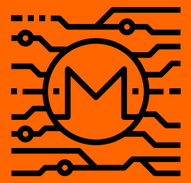
- Disinflationary
- Inflation approaches 0%, lower than gold/Bitcoin today
- Tail-emission of 0.6 XMR/block
- Tail-emission ensures lower bound of network security

AUDITING THE SUPPLY WHILE HIDING AMOUNTS

- Hiding amounts prevents all amount-based heuristics
- Bulletproofs were designed for Bitcoin but never used
- Every transaction is validated by every node to ensure inputs - outputs = 0
- Coinbase outputs are transparent by-design

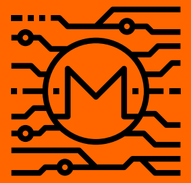


HARD-FORKS



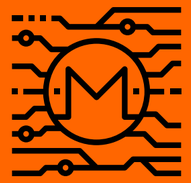
WHY HARD-FORK?

Hard-forks allow the Monero community to enforce sane defaults for privacy, ensure fungibility, and iterate and improve the Monero protocol.



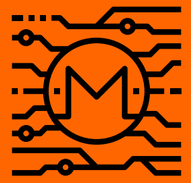
HOW OFTEN DOES MONERO HARD-FORK?

Monero only hard-forks as needed to upgrade the network, which is becoming more rare each year.



WHO IS INVOLVED IN HARD-FORKS?

The entire Monero community has opportunity to engage in discussions, contribute code, and have a say in hard-fork planning.



WHERE CAN I SEE THE PLANNING AROUND HARD-FORKS?

All hard-fork planning occurs in IRC/Matrix during scheduled meetings, or in Github issues.

USE MONERO FOR EVERYTHING

Requires accepting the trade-offs compared to Bitcoin, enables simple privacy and opaque SoV.

SAVE IN BITCOIN, SPEND MONERO

See the proven SoV value prop of Bitcoin, but understand Monero is easier and safer to spend.

USE MONERO FOR TOXIC CHANGE

Leverage Monero as a tool to "clean" or spend "toxic change" from CoinJoining.

USE BITCOIN FOR EVERYTHING

Requires a deep understanding of private usage of Bitcoin in order to spend, i.e. Samourai, post-mix spends, etc.

Conclusion

Monero was made to be a powerful tool for freedom, and should be deeply considered as a part of every freedom-loving person's digital toolkit.

LEARN MORE ABOUT MONERO ->

BLOG

https://sethforprivacy.com

SIGNAL

+1 (616) 326 4079

EMAIL

seth@sethforprivacy.com