

Privacy & Anonymity in Blockchain

A Standalone Overview

BSc Blockchain Course

If Blockchain Is Open, Where Is Your Privacy?

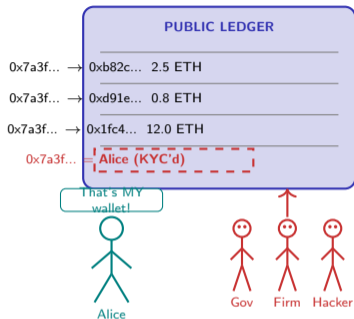
Blockchains are celebrated for transparency: every transaction is recorded on a public ledger that anyone can read, verify, and trace. That transparency is the source of trustlessness – and also its greatest privacy liability.

Three uncomfortable facts about public ledgers:

- **Every transfer is permanent** – your entire financial history lives on-chain, forever searchable by anyone with a block explorer
- **Addresses are pseudonymous, not anonymous** – once a single address is linked to your identity (exchange KYC, ENS name, social media), every connected transaction is deanonymised
- **Chain analysis firms profit from tracing you** – Chainalysis, Elliptic, and others sell deanonymisation as a service to governments and corporations

If your bank statement were public, would you still use the same bank?

Blockchain transparency is a feature for auditability and a vulnerability for privacy: every transaction is a permanent, public, linkable data point.



Source: Meiklejohn, S. et al. (2013). "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names." IMC '13.

Open a Block Explorer – Can You Find Your Own Transactions?

Most people who own cryptocurrency have never actually looked at their own transactions on a block explorer. The experience is revealing – and uncomfortable. Your wallet address, every transfer you have made, every amount, every counterparty address: all of it is there, indexed and searchable, forever.

Quick Exercise – Try This Before We Continue

- 1 **Open a block explorer** (e.g., `etherscan.io` for Ethereum, `mempool.space` for Bitcoin). Search for any well-known address – a public donation wallet, a DeFi protocol treasury, or your own address if you have one. What can you learn about the owner from the transaction history alone?
- 2 **Follow the money:** pick any large transaction and click through to the receiving address. Click again. How many hops does it take before you lose the trail – or does it never end?
- 3 **Now imagine this is your salary:** every payday, your employer's address sends ETH to your address. Anyone who knows either address can see your income, your spending patterns, which DeFi protocols you use, and which NFTs you bought. Would you accept these terms from a bank?
- 4 **The core tension:** transparency enables trustless verification (you can prove reserves without auditors). But it also enables mass surveillance without a warrant. Where should the line be drawn?

Keep your answer to question 4 in mind. We will revisit it when we discuss regulatory trade-offs later.

Block explorers make the abstract transparency of blockchain viscerally real. Privacy is not theoretical when your salary is one click away.

What Makes Anonymous Different from Pseudonymous?

Four payment systems – four levels of privacy:

Property	Cash	Bitcoin	Monero	Zcash
Identity	Anonymous	Pseudonymous	Anonymous	Optional
Traceability	None	Full graph	Obscured	Shielded
Fungibility	Perfect	Tainted coins	Enforced	Mixed
Sender hidden	Yes	No	Ring sigs	zk-SNARKs
Amount hidden	Yes	No	RingCT	zk-SNARKs
Receiver hidden	Yes	No	Stealth addr	zk-SNARKs
Regulatory risk	Low	Moderate	High	Moderate

Key distinctions:

- **Pseudonymous** = you use a consistent identifier (address) that is not your name, but can be linked to you via metadata, exchange records, or social connections
- **Anonymous** = no persistent identifier links your transactions to each other or to your real-world identity
- **Fungible** = every unit is interchangeable; no coin carries a traceable history that could cause it to be rejected or discounted

Pseudonymity gives you a mask; anonymity removes you from the crowd entirely. The difference determines whether your financial history is public record or genuinely private.

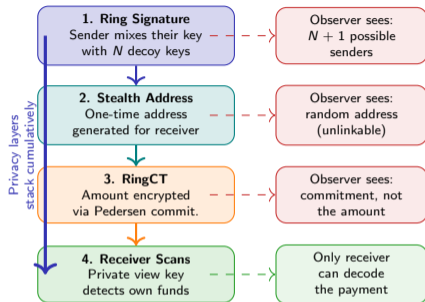
Why fungibility matters in practice:

- **Bitcoin's problem:** chain analysis firms flag coins that passed through sanctioned addresses. Exchanges may refuse deposits of "tainted" BTC. Two bitcoins are not equal if one has a criminal history.
- **Monero's approach:** every transaction is private by default – ring signatures, stealth addresses, and confidential amounts make tracing impractical. All XMR are interchangeable by design.
- **Zcash's compromise:** shielded transactions are optional. Most users stay in the transparent pool, reducing the anonymity set for those who do shield.

Privacy is only as strong as the crowd you hide in. Optional privacy means a small anonymity set – which often defeats the purpose.

Source: Narayanan, A. & Möser, M. (2017). "Obfuscation in Bitcoin." IEEE S&P; Möser, M. et al. (2018). "An Empirical Analysis of Traceability in the Monero Blockchain."

Follow One Monero Transaction – Who Can See What?



What each layer hides:

- 1. Ring Signature:** the sender's real key is mixed with decoys from the blockchain. An observer cannot determine which of the $N + 1$ possible signers authorised the transaction.
- 2. Stealth Address:** the sender generates a one-time address derived from the receiver's public key. This address appears on-chain only once, breaking the link to the receiver's identity.
- 3. RingCT:** the amount is hidden using a Pedersen commitment – miners verify inputs equal outputs without seeing the actual numbers.
- 4. Receiver Scan:** only the receiver, using their private view key, can detect and decode which outputs belong to them.

All four layers are mandatory in Monero. This is what "privacy by default" means in practice.

Monero's privacy is not one mechanism but four interlocking layers: ring signatures hide the sender, stealth addresses hide the receiver, RingCT hides the amount, and mandatory application ensures a large anonymity set.

Source: Noether, S. et al. (2016). "Ring Confidential Transactions." Ledger Journal; van Saberhagen, N. (2013). "CryptoNote v2.0." cryptonote.org

How Can You Prove Something Without Revealing It?

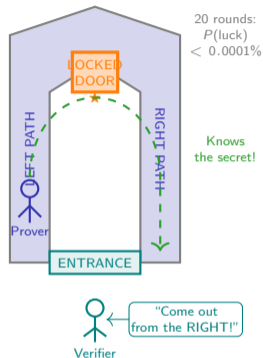
A zero-knowledge proof lets a prover convince a verifier that a statement is true – without revealing *any* information beyond the truth of the statement itself.

The cave analogy (Quisquater et al., 1989):

- 1 Alice enters a cave with a fork. She picks the left or right path. Both meet at a locked door deep inside.
- 2 Bob, standing outside, shouts: “Come out from the LEFT” or “Come out from the RIGHT.”
- 3 If Alice knows the secret (the door code), she can always emerge from whichever side Bob requests.
- 4 After 20 rounds, $P(\text{luck}) = \frac{1}{2^{20}} < 0.0001\%$. Bob is convinced – yet he never learned the code.

Blockchain applications:

- **zk-SNARKs** (Zcash): prove a valid transaction without revealing sender, receiver, or amount
- **zk-STARKs** (StarkNet): prove computation correctness without revealing inputs – no trusted setup
- **zk-Rollups** (zkSync, Scroll): prove thousands of transactions valid in one on-chain proof



A zero-knowledge proof transfers conviction without transferring knowledge: the verifier learns that the statement is true, but nothing about why.

Source: Quisquater, J.-J. et al. (1989). “How to Explain Zero-Knowledge Protocols to Your Children.” CRYPTO '89; Ben-Sasson, E. et al. (2014). “Succinct Non-Interactive ZK for a von Neumann Architecture.”

What Happened When Tornado Cash Got Sanctioned?

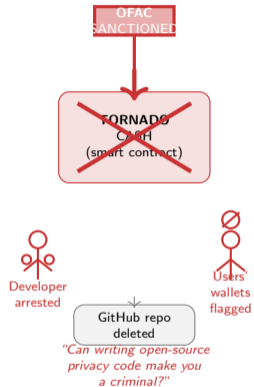
The Tornado Cash Crisis (2022–2024)

Tornado Cash was an Ethereum smart contract that mixed deposits to break the on-chain link between sender and receiver – the most widely used privacy tool on Ethereum.

August 2022: The US Treasury (OFAC) sanctioned the smart contract addresses themselves – not a person, not a company, but immutable code. This was unprecedented.

The cascading consequences:

- **Developer arrested:** Alexey Pertsev was detained in the Netherlands; convicted in 2024 for facilitating money laundering via open-source code
- **Users frozen:** wallets that had interacted with Tornado Cash were flagged; DeFi protocols auto-blocked these addresses
- **GitHub repo deleted:** the source code was removed within hours of the sanctions announcement
- **Chilling effect:** privacy tool developers worldwide reconsidered whether writing privacy software could make them personally liable

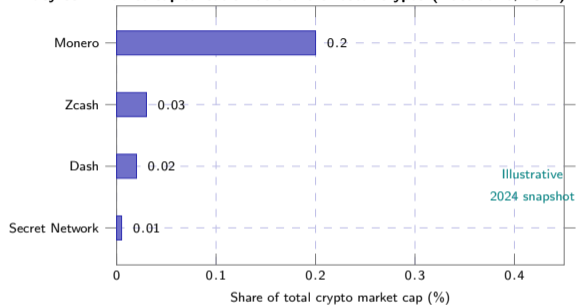


Tornado Cash established that governments can sanction immutable smart contracts and hold developers personally liable for how others use open-source privacy tools.

Source: US Treasury OFAC (2022). "Tornado Cash Sanctions." [treasury.gov](https://www.treasury.gov); Dutch FIOD (2023). Pertsev indictment; 5th Circuit Court (2024). *van Loon v. Treasury* (partial reversal).

How Many People Actually Use Privacy Tools?

Privacy coin market capitalisation as share of total crypto (illustrative, 2024):



privacy coins combined represent under 0.5% of total crypto market capitalisation. The vast majority of crypto users transact on fully transparent chains.

Why adoption remains low:

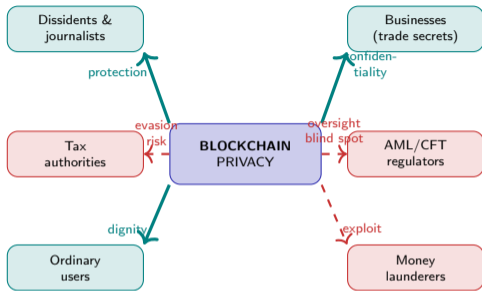
- **Exchange delistings:** Monero has been delisted from Binance, OKX, Huobi, and most regulated exchanges in the EU and Asia. Users cannot easily buy or sell XMR through normal channels.
- **Usability:** privacy tools add complexity – stealth addresses, key management, longer confirmation times – that mainstream users will not tolerate.
- **Network effects:** Ethereum and Bitcoin have dominant developer ecosystems, DeFi integrations, and institutional infrastructure. Privacy coins lack this ecosystem depth.
- **Stigma:** regulators and media associate privacy coins with illicit finance, creating a perception problem that discourages legitimate adoption.

The paradox: privacy tools need large adoption to provide strong anonymity sets, but regulatory pressure suppresses the adoption needed to make them effective.

Privacy coins occupy a tiny fraction of the crypto market. Regulatory hostility, exchange delistings, and the usability gap create a vicious cycle: low adoption weakens privacy, which discourages further adoption.

Source: CoinGecko market data (2024). Illustrative figures; actual values fluctuate. Binance delisted Monero in February 2024 for EU compliance.

Who Benefits from Privacy – And Who Gets Hurt?



Stakeholder perspectives:

Dissidents: Activists in authoritarian regimes use privacy tools to receive donations without government surveillance. Privacy is a matter of physical safety.

Businesses: Companies need transaction privacy to protect trade secrets – supplier payments and M&A activity should not be visible to competitors.

Ordinary users: Most people do not want their salary, medical payments, or charitable donations on a public ledger.

Criminals: The same tools that protect dissidents enable money laundering, ransomware payments, and sanctions evasion.

Regulators: Without tracing capability, regulators cannot enforce AML rules or tax compliance.

Privacy tools do not distinguish between the dissident and the criminal. The policy challenge is designing systems that protect legitimate privacy without providing a permanent safe harbour for illicit finance.

Source: Chainalysis (2024). "Crypto Crime Report."; Human Rights Foundation (2023). "Bitcoin and Human Rights." hrf.org

Three Tests That Reveal Any Privacy Protocol's Trade-offs

Before evaluating any privacy protocol, apply these three tests in order:

Test 1 – Anonymity Set Size:

How large is the crowd you hide in?

A privacy tool is only as strong as the number of users whose transactions look identical. If only 2% of Zcash transactions are shielded, those shielded users stand out. Monero's mandatory privacy means every transaction contributes to the anonymity set. **Test 2 – Metadata Leakage:**

What does the protocol reveal besides the payment itself?

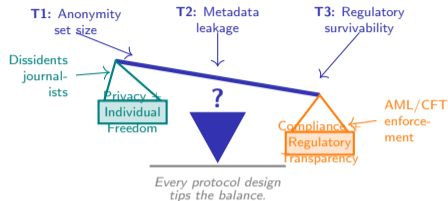
Even if amounts and addresses are hidden, timing, IP addresses, transaction size, and interaction patterns can deanonymise users. A protocol that hides amounts but leaks IP addresses provides false confidence.

Test 3 – Regulatory Survivability:

Can the protocol function if exchanges delist it?

Privacy coins delisted from all major exchanges lose liquidity and on-ramps. A protocol must either achieve sufficient peer-to-peer adoption or offer a compliance mode that lets users selectively disclose to regulators. *Strong on all three? Genuinely private. Weak on any one? A false sense of security.*

Privacy is not binary. Every protocol makes trade-offs between the size of the anonymity crowd, the metadata it leaks, and its ability to survive regulatory pressure.



The Privacy Protocol Trilemma:

No protocol simultaneously maximises anonymity set size, metadata resistance, and regulatory survivability. Every design chooses a point on this balance.

Source: Bonneau, J. et al. (2014). "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." IEEE S&P; Buterin, V. (2023). "Some thoughts on privacy." vitalik.eth.limo

Your Challenge: Evaluate a Privacy Protocol's Design

Choose one protocol from the table below. Apply all three tests from the previous slide.

Activity: Privacy Protocol Evaluation (15 minutes)

Step 1 – Pick your protocol:

Protocol	Mechanism	Privacy Default	Status (2024)
Monero (XMR)	Ring sigs + stealth addr + RingCT	Mandatory	Delisted from most exchanges
Zcash (ZEC)	zk-SNARKs (shielded pool)	Optional	Listed but <5% shielded use
Tornado Cash	Mixer (ETH smart contract)	Mandatory per tx	Sanctioned (OFAC)
Aztec / Railgun	zk-Rollup with private txns	Opt-in layer	Active on Ethereum

Step 2 – Apply the three tests:

Test	Rating (Strong / Weak)	Evidence (one sentence)
T1: Anonymity set size
T2: Metadata leakage
T3: Regulatory survivability

Step 3 – Discuss (5 min): Compare protocols with your neighbour. Which scores best overall? Which has the most dangerous false sense of security? Could any redesign to improve their weakest test?

The three tests are a permanent toolkit: apply them to any privacy technology you encounter – in crypto, in messaging, in identity systems.