Privacy & Anonymity in Blockchain

A Five-Minute Overview

BSc Blockchain Course

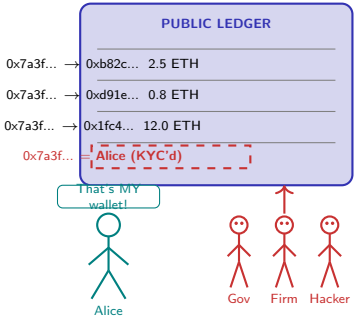
If Blockchain Is Open, Where Is Your Privacy?

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; Chainalysis (2024). "The State of Crypto Crime."

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
- **Anonymous** = no persistent identifier links your transactions to each other or to your identity
- **Fungible** = every coin is identical; no coin carries a traceable history that could cause it to be rejected

Why fungibility matters:

- **Bitcoin's problem:** chain analysis firms flag coins that passed through sanctioned addresses. Exchanges 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.
- **Zcash's compromise:** shielded transactions are optional. Most users stay in the transparent pool, which undermines 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 defeats the purpose.

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.

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."

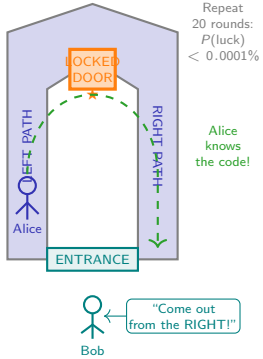
How Can You Prove Something Without Revealing It?

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 randomly picks the left or right path. Both paths 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 – regardless of which path she entered.
4. After 20 rounds, the probability that Alice succeeded by luck alone is $\frac{1}{2^{20}} < 0.0001\%$. Bob is convinced – yet he never learned the code.

In blockchain: zk-SNARKs and zk-STARKs let you prove you own enough funds to send a transaction, or that a computation was performed correctly, without revealing the amounts, the addresses, or the computation inputs.

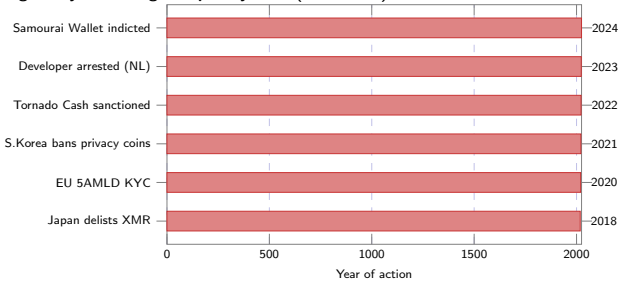


A zero-knowledge proof transfers conviction without transferring knowledge: the verifier learns that the statement is true, but nothing about why it is true.

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 Zero Knowledge for a von Neumann Architecture."

Why Are Governments Cracking Down on Privacy Tools?

Regulatory actions against privacy tools (2019–2024):



Each action escalated the regulatory posture: from delisting coins to arresting individual developers of open-source privacy tools.

What happened at each step:

- **2018 – Japan:** exchanges ordered to delist Monero, Zcash, and Dash after FSA guidance on "anonymous cryptocurrencies"
- **2020 – EU 5AMLD:** extended anti-money-laundering rules to crypto, requiring exchanges to identify all users
- **2022 – Tornado Cash:** US Treasury (OFAC) sanctioned the smart contract addresses, making interaction with the mixer illegal for US persons
- **2023 – Arrest:** Alexey Pertsev, a Tornado Cash developer, was arrested in the Netherlands and later convicted
- **The pattern:** regulators have moved from targeting users to targeting *tool builders* – a fundamental shift in legal exposure for open-source developers

The regulatory trajectory is clear: privacy-preserving tools are increasingly treated not as neutral technology but as potential instruments of money laundering – with developers held personally liable.

Source: US Treasury OFAC (2022). "Sanctions on Tornado Cash." treasury.gov; Fiod (2023). Pertsev arrest announcement; EU Directive 2018/843 (5AMLD).

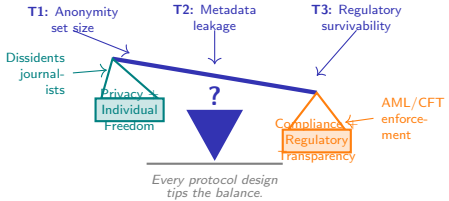
Three Tests That Reveal Any Privacy Protocol's Trade-offs

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 – the opposite of anonymity. 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 (without Tor/I2P integration) 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.



The Privacy Protocol Trilemma:

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

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 three tests expose those trade-offs.

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