

# L10: Privacy Technologies – Technical Deep Dive

BSc Blockchain Course

Digital Finance

- 1 Privacy Fundamentals
- 2 Zero-Knowledge Proofs
- 3 Mixers and Tumblers
- 4 Privacy Coins
- 5 Privacy Architecture
- 6 Regulation and Adoption
- 7 Future and Synthesis

By the end of this lesson you will be able to:

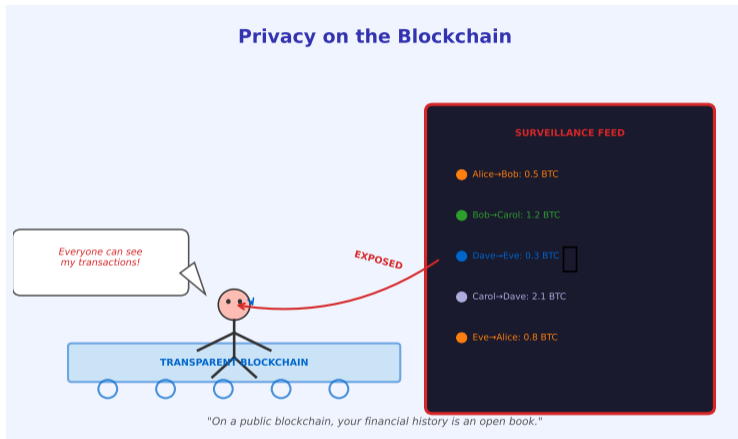
- 1 **Explain** why public blockchains are pseudonymous, not anonymous, and identify the privacy risks this creates. *[Understand]*
- 2 **Describe** the core idea behind zero-knowledge proofs (proving something is true without revealing it). *[Understand]*
- 3 **Compare** ZK-SNARKs (small proofs, fast verification, trusted setup) and ZK-STARKs (no trusted setup, quantum-resistant, larger proofs). *[Analyze]*
- 4 **Analyze** how mixers, ring signatures, and stealth addresses break the link between sender and receiver. *[Analyze]*
- 5 **Evaluate** the tension between financial privacy and regulatory compliance (AML/KYC vs individual rights). *[Evaluate]*

**Bloom's levels covered:** Understand, Analyze, Evaluate

---

**Prerequisites:** L02 Cryptography (hash functions, digital signatures), L05 Ethereum (smart contracts, transactions).

# What If Every Purchase You Ever Made Was Published on a Billboard?



Imagine every coffee, every rent payment, every donation you make is recorded on a public ledger visible to anyone with an internet connection. That is the reality of public blockchains like Bitcoin and Ethereum today. Privacy technologies aim to preserve the benefits of decentralization – trustless verification, censorship resistance – while restoring the confidentiality that traditional bank accounts take for granted.

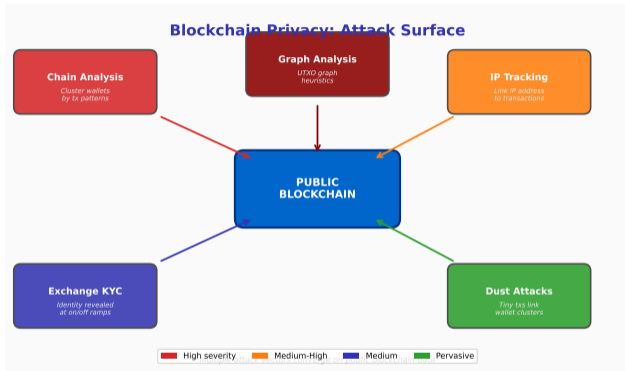
# Why Does Privacy Matter on Public Blockchains?

Public blockchains publish every transaction for anyone to see. This transparency enables trustless verification – but it also enables surveillance.

## Legitimate privacy needs:

- **Financial confidentiality:** Your employer, landlord, or ex-partner should not see your spending habits.
- **Business secrets:** A company paying suppliers on-chain reveals its cost structure to competitors.
- **Personal safety:** A publicly visible large balance makes you a target for extortion or physical theft.
- **Fungibility:** If coins can be “tainted” by past transactions, they lose equal value – breaking a core property of money.

**The paradox:** Transparency enables trust, but it also enables tracking. Privacy technologies try to preserve the first while preventing the second.



- **What you see:** A threat model showing who can observe what on a public blockchain.
- **Key pattern:** Blockchain explorers, chain analysis firms, and even casual observers can link addresses to identities.
- **Takeaway:** Without privacy tools, pseudonymity is a thin veil – one data link connects your wallet to your name.

# Where Does Your Blockchain Fall on the Privacy Spectrum?

Not all blockchains handle privacy the same way. They exist on a spectrum from fully transparent to fully private.

## Three levels:

- 1 **Transparent (Bitcoin, Ethereum):** Every transaction amount, sender address, and receiver address is publicly visible. Anyone can trace the flow of funds.
- 2 **Optional privacy (Zcash):** Users can choose between transparent transactions (like Bitcoin) and shielded transactions (hidden behind zero-knowledge proofs). Most users choose transparent.
- 3 **Mandatory privacy (Monero):** Every transaction is private by default. Sender, receiver, and amount are always hidden. There is no “opt out” of privacy.

**Key insight:** Optional privacy is weaker than mandatory privacy. When only 5% of transactions are shielded, those transactions stand out as “something to hide.” When 100% are private, everyone blends in.

## Blockchain Privacy Spectrum

Fully Transparent      Pseudonymous      Enhanced Privacy      Private by Default      Full Privacy



Bitcoin, Ethereum      Most Blockchains      Tornado Coinjoin      Zcash (shielded), Monero      Theoretical Ideal

Privacy <-----> Transparency

- **What you see:** Blockchains arranged along a transparency-to-privacy spectrum.
- **Key pattern:** Most mainstream blockchains cluster at the transparent end. Only a few offer strong privacy guarantees.
- **Takeaway:** “Pseudonymous” (using a random-looking address instead of your name) is not the same as “anonymous.”

Pseudonymous means your real name is hidden, but your address is permanent and linkable. One slip – a KYC exchange, a public donation – and the link

# Pseudonymity Is Not Anonymity: How Chain Analysis Works

Bitcoin addresses look random (e.g., 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa), but they are **permanent pseudonyms**, not anonymous identifiers. Chain analysis companies exploit three weaknesses.

## Three attack vectors against pseudonymity:

- 1 **Address reuse:** If you use the same Bitcoin address twice, both transactions are linked. An observer can build your complete transaction history from a single address.
- 2 **Transaction graph analysis:** When multiple inputs (addresses) are combined into one transaction, they likely belong to the same person. Firms like Chainalysis cluster addresses using this heuristic to identify wallets.
- 3 **Off-chain data leaks:** When you withdraw crypto from Coinbase (which has your passport), that withdrawal address is now linked to your identity. Every subsequent transaction from that address – and every address it sends to – is traceable.

**Real-world example:** In 2013, the FBI traced the Silk Road marketplace operator (Ross Ulbricht) by connecting his Bitcoin transactions to a single exchange withdrawal. The “anonymous” cryptocurrency was the key evidence in his conviction.

---

Chainalysis claims to have mapped over 1 billion Bitcoin addresses into ownership clusters as of 2024.

# How Can You Prove Something Without Revealing It?

A **zero-knowledge proof** (ZK proof) lets one party (the prover) convince another party (the verifier) that a statement is true – **without revealing any information beyond the truth of the statement.**

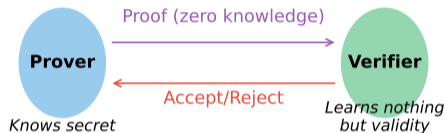
The classic analogy – Ali Baba's cave:

- 1 A cave has two paths (A and B) that meet at a locked door in the middle. Only someone with the secret word can pass through.
- 2 You enter one path while I wait outside. I shout which path I want you to exit from.
- 3 If you know the secret, you can always exit the correct path. If you do not, you succeed only 50% of the time.
- 4 After 20 rounds, chance of faking =  $(0.5)^{20}$  = one in a million.

Three properties of a ZK proof:

- **Completeness:** If  $x \in L$ , an honest prover convinces the verifier with probability 1
- **Soundness:** If  $x \notin L$ , any cheating prover succeeds with probability  $\leq \epsilon$  (soundness error)
- **Zero-knowledge:** The verifier's view is simulatable without the witness  $w$

## Zero-Knowledge Proof: Prove Without Revealing



Completeness: valid proofs always accepted

Soundness: invalid proofs rejected

Zero-knowledge: verifier learns nothing

- **What you see:** The zero-knowledge proof concept illustrated through an interactive protocol.
- **Key pattern:** The prover demonstrates knowledge through repeated challenges, not by revealing the secret itself.
- **Takeaway:** ZK proofs are the foundation of both privacy coins (Zcash) and scaling solutions (zkRollups).

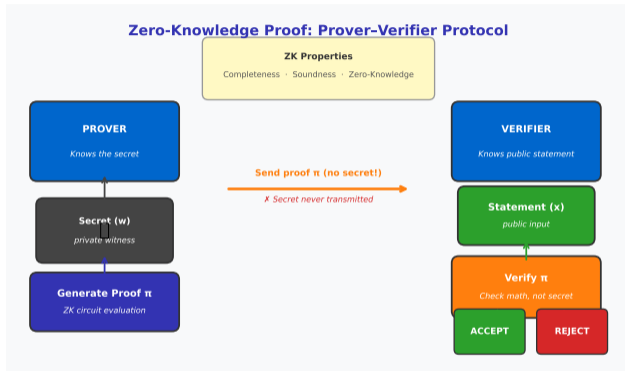
# How Do ZK Proofs Work in Practice on a Blockchain?

On a blockchain, ZK proofs serve a specific purpose: prove that a transaction is valid (correct amounts, authorized sender) without revealing the transaction details (who sent how much to whom).

## The process:

- 1 **Prover (sender):** Constructs a mathematical proof that their transaction satisfies all rules – inputs equal outputs, no double-spend, valid signature.
- 2 **Proof generation:** The prover runs a computation that encodes the transaction into a proof (a short string of data, typically 200–300 bytes for SNARKs).
- 3 **Verifier (network):** Every node checks the proof in milliseconds – far faster than re-executing the transaction.
- 4 **Result:** The network is convinced the transaction is valid, but no node learns the sender, receiver, or amount.

**Analogy:** Imagine a sealed envelope containing your tax return. A ZK proof is like a stamp on the outside that says “verified correct by the IRS” – without anyone ever opening the envelope.



- **What you see:** The mechanics of proof generation and verification in a blockchain transaction.
- **Key pattern:** Proof generation is computationally expensive (seconds to minutes), but verification is cheap (milliseconds).
- **Takeaway:** This asymmetry is what makes ZK proofs practical – one heavy computation secures the entire network.

# ZK-SNARKs: Small Proofs, Fast Verification, One Catch

**SNARK** stands for **S**uccinct **N**on-interactive **A**rgument of **K**nowledge. Each word matters:

- **Succinct:** The proof is tiny (a few hundred bytes) regardless of how complex the computation being proved.
- **Non-interactive:** The prover sends one message – no back and forth between prover and verifier (unlike the cave analogy).
- **Argument of Knowledge:** The proof demonstrates that the prover actually *knows* the secret input, not just that a valid input exists.

## The catch – the trusted setup:

Traditional ZK-SNARKs (as used in Zcash's original Sprout protocol) require a one-time “trusted setup ceremony” that generates cryptographic parameters. If the secret randomness from this ceremony is not destroyed, anyone who kept it could forge proofs and create fake coins undetectably.

## The pairing-based verification equation (Groth16 scheme):

$$e(\pi_A, \pi_B) = e(\alpha, \beta) \cdot e(\pi_C, \delta)$$

where  $\pi_A, \pi_B, \pi_C$  are proof elements and  $\alpha, \beta, \delta$  are trusted-setup parameters. A valid proof satisfies this bilinear pairing identity; forging one requires breaking the discrete logarithm assumption.

**Zcash's solution:** They ran a multi-party computation ceremony with 6 participants. As long as *at least one* participant destroyed their secret, the system is secure. Newer SNARKs (Halo 2, Plonky2) eliminate the trusted setup entirely.

---

Zcash launched in 2016 as the first cryptocurrency to use ZK-SNARKs in production. It was founded by cryptographer Zooko Wilcox.

# ZK-STARKs: No Trusted Setup, Quantum-Resistant, Larger Proofs

**STARK** stands for **S**calable **T**ransparent **A**RGument of **K**nowledge. The key difference from SNARKs is the word “transparent” – no trusted setup required.

Property	ZK-SNARKs	ZK-STARKs
<b>Trusted setup</b>	Required (traditional) or eliminated (Halo 2)	Never required
<b>Proof size</b>	Small (288 bytes for Groth16)	Larger (tens of KB)
<b>Verification time</b>	Very fast (milliseconds)	Fast (slightly slower)
<b>Prover time</b>	Moderate	Faster for large computations
<b>Quantum resistance</b>	No (relies on elliptic curves)	Yes (uses hash functions only)
<b>Used by</b>	Zcash, Tornado Cash, zkSync	StarkNet, StarkEx (dYdX)

## Why does quantum resistance matter?

SNARKs rely on the difficulty of the “discrete logarithm problem” on elliptic curves. A sufficiently powerful quantum computer (estimated by 2035–2040) could solve this problem, breaking SNARK security. STARKs rely only on hash functions, which remain secure even against quantum computers.

**Key insight:** Neither system is strictly better. SNARKs win on proof size (important when storing proofs on-chain). STARKs win on transparency and future-proofing.

---

**Eli Ben-Sasson, co-inventor of STARKs, co-founded StarkWare (now valued at over \$8 billion). STARKs were published in 2018.**

# How Do SNARKs and STARKs Compare Visually?

The choice between SNARKs and STARKs depends on the application's priorities.

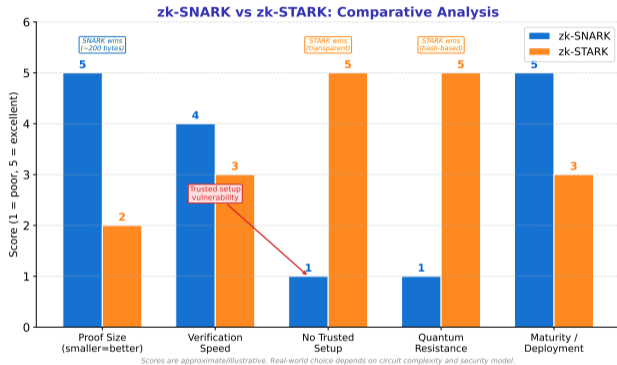
## Choose SNARKs when:

- On-chain storage cost matters (smaller proofs mean lower gas fees)
- You need the smallest possible verification footprint
- You can accept a trusted setup (or use newer setup-free variants)

## Choose STARKs when:

- Transparency is non-negotiable (no trusted party)
- Long-term quantum resistance is required
- The computation being proved is very large (STARKs scale better for complex computations)

**Convergence trend:** Both technologies are evolving rapidly. Newer SNARK systems (Halo 2) eliminate the trusted setup. Newer STARK systems compress proof sizes. The gap is narrowing.



- **What you see:** A multi-dimensional comparison of SNARKs and STARKs across key properties.
- **Key pattern:** SNARKs and STARKs have complementary strengths – neither dominates on all dimensions.
- **Takeaway:** The best ZK system depends on the specific use case. Privacy coins favor SNARKs; scaling solutions increasingly use STARKs.

# How Do Mixers Break the Transaction Trail?

A **mixer** (also called a **tumbler**) is a service that pools funds from many users and redistributes them, breaking the on-chain link between the original sender and the final recipient.

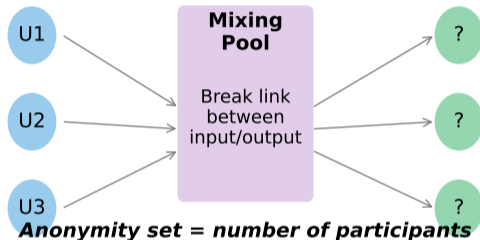
## How it works:

- 1 **Deposit:** Multiple users send the same fixed amount (e.g., 1 ETH each) to the mixer's smart contract.
- 2 **Pool:** All deposits are combined into a single pool. An observer sees many inputs but cannot match them to outputs.
- 3 **Withdraw:** Each user withdraws the same fixed amount to a *new, unlinked* address after a random time delay.
- 4 **Result:** The connection between deposit address and withdrawal address is broken.

**Critical concept – anonymity set:** The number of users in the pool at any time. A pool with 1,000 depositors gives each user 1-in-1,000 anonymity. A pool with 10 gives only 1-in-10.

**Mixing entropy:** The information-theoretic privacy of a mixer with  $n$  participants is quantified by Shannon entropy

## Mixer/Tumbler: Breaking Transaction Links



Tornado Cash: ZK proofs for withdrawal

- **What you see:** The flow of funds through a mixer – deposits enter, get pooled, and exit to new addresses.
- **Key pattern:** Fixed deposit amounts are essential. If Alice deposits 1.37 ETH and someone withdraws 1.37 ETH, the link is obvious.
- **Takeaway:** Larger anonymity sets provide stronger privacy. This is why Tornado Cash used standardized denominations (0.1, 1, 10, 100

# What Makes a Mixer Pool Effective or Ineffective?

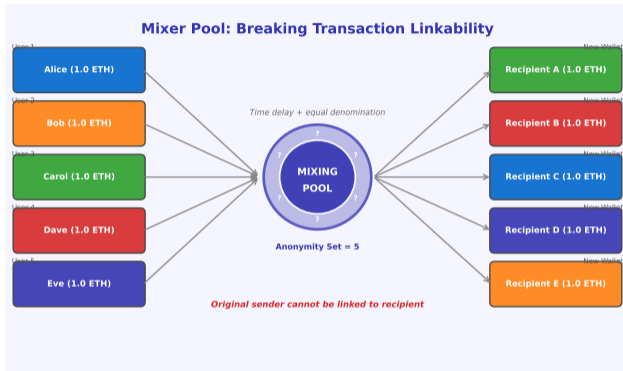
A mixer is only as strong as its **anonymity set** – the number of indistinguishable participants in the pool at any given time.

## Factors that weaken mixer privacy:

- **Small pool size:** If only 5 people use the mixer, an observer reduces the suspect list to 5 – not anonymous enough.
- **Timing correlation:** If you deposit at 3:01 PM and withdraw at 3:02 PM, the timing link is obvious.
- **Amount correlation:** Depositing 7.3 ETH and withdrawing 7.3 ETH defeats the purpose, even through a mixer.
- **Behavioral patterns:** Withdrawing to an address that then interacts with your known address re-links the trail.

**Best practice:** Use the most popular denomination, wait hours or days between deposit and withdrawal, and never send the withdrawn funds to any address connected to your identity.

**Anonymity set size:** Formally, the anonymity set  $A$  is the set of possible senders indistinguishable to an adversary. Privacy is meaningful only when  $|A| = k > 2$ ; strong



- **What you see:** How anonymity set size affects privacy strength over time.
- **Key pattern:** Larger pools and longer wait times exponentially increase the difficulty of tracing funds.
- **Takeaway:** Privacy is a collective good – each additional user in the pool makes everyone more private.

# Tornado Cash: The Mixer That Changed the Regulatory Landscape

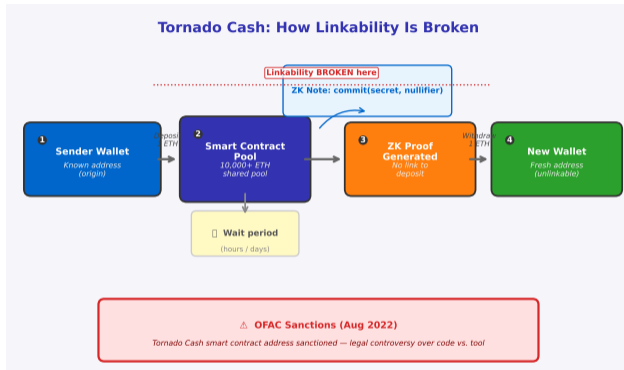
**Tornado Cash** was the most widely used Ethereum mixer from 2019 to 2022, processing over \$7 billion in deposits.

## How Tornado Cash worked:

- 1 Deposit a fixed amount (0.1, 1, 10, or 100 ETH) into a smart contract.
- 2 Receive a cryptographic “note” – a secret key proving your deposit.
- 3 Later, present a ZK proof (derived from the note) to withdraw to a new address. The proof shows you are a depositor without revealing *which* depositor.

## What happened:

- August 2022: US Treasury (OFAC) sanctioned Tornado Cash’s smart contract addresses – the first time a piece of *code* was sanctioned.
- Developer Alexey Pertsev was arrested in the Netherlands.
- Circle froze \$75,000 in USDC held in Tornado Cash addresses.



- **What you see:** The architecture and flow of Tornado Cash, including the ZK proof mechanism.
- **Key pattern:** The smart contract is immutable – even after sanctions, the code remains deployed on Ethereum and can still be used.
- **Takeaway:** Tornado Cash exposed a fundamental question: can governments sanction autonomous code, or only the people who

# How Do Ring Signatures Hide the Sender?

A **ring signature** lets one member of a group sign a message so that an observer knows *someone in the group* signed it, but cannot determine *who*.

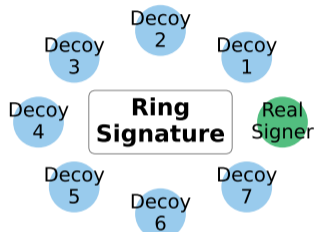
**Analogy:** Imagine 11 people in a room, each with a key to the same lock. One person locks a box. An observer knows the box was locked by someone in the room, but cannot determine which of the 11 did it.

## In Monero:

- 1 When Alice sends XMR (Monero's currency), her transaction includes her real input mixed with 15 "decoy" inputs pulled from the blockchain.
- 2 All 16 inputs look equally likely to be the real one.
- 3 A ring signature proves that *one* of the 16 inputs is real – without revealing which one.

**Key property:** Unlike mixers, ring signatures do not require a separate mixing step or a pool of users. Privacy is built into every transaction automatically.

## Ring Signatures: Plausible Deniability



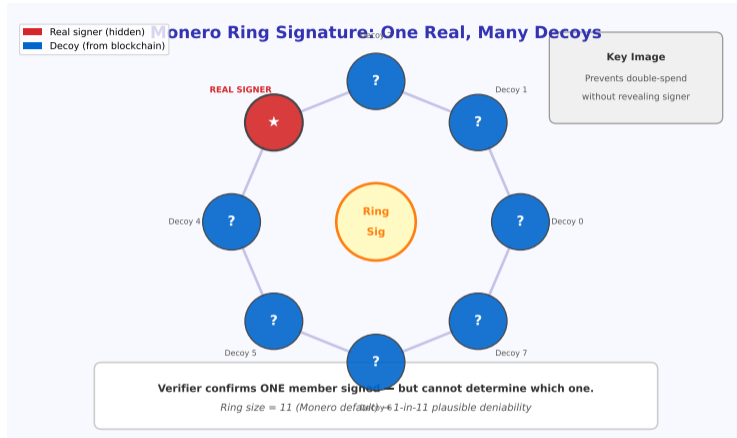
**Cannot distinguish real signer from decoys**

Monero: Ring signatures + stealth addresses + RingCT

- **What you see:** How a ring signature mixes the real signer with decoy signers to hide the true origin.
- **Key pattern:** The real input is indistinguishable from decoys. More decoys = larger anonymity set = stronger privacy.
- **Takeaway:** Ring signatures provide sender privacy without requiring any interaction between users – a significant advantage over mixers.

Monero increased its mandatory ring size from 7 to 16 in 2022, making each transaction blend with 15 decoys instead of 6.

# What Happens Inside a Monero Transaction?



## Anatomy of a ring signature transaction:

- 1 **Real input:** The actual coins Alice is spending
- 2 **Decoy inputs:** 15 randomly selected outputs from previous transactions on the blockchain
- 3 **Key image:** A unique cryptographic tag  $I = x \cdot H_p(P)$  derived from Alice's private key  $x$  – prevents double-spending without

# Monero: Three Layers That Hide Sender, Receiver, and Amount

Monero combines three privacy technologies, each hiding a different piece of transaction information. All three are **mandatory** – there is no way to send a transparent Monero transaction.

Layer	Technology	What It Hides	How It Works
1. <b>Sender</b>	Ring Signatures	Which input is real	Mix real input with 15 decoys
2. <b>Receiver</b>	Stealth Addresses	Destination address	Generate one-time address per transaction
3. <b>Amount</b>	RingCT (Ring Confidential Transactions)	Transaction amount	Pedersen commitments (cryptographic hiding)

## Stealth addresses explained:

When Bob publishes his Monero address, it is a “master public key,” not a receiving address. When Alice sends to Bob, her wallet generates a unique one-time address derived from Bob’s key. Even if Alice sends to Bob 100 times, each transaction goes to a different on-chain address – no observer can link them.

## RingCT explained:

Transaction amounts are hidden using Pedersen commitments. For value  $v$  and blinding factor  $r$ , the commitment is  $C = g^v \cdot h^r$ . The network verifies balance without decryption:

$$\sum C_{in} = \sum C_{out} + C_{fee}$$

**Analogy:** Imagine sealed envelopes containing numbers. The envelopes can be “added” to prove the sum is correct, but nobody can open them.

---

**Monero’s privacy is mandatory by default since 2017 (RingCT) and has been continuously upgraded since. It is widely considered the strongest privacy coin.**

# Zcash: Optional Privacy Through Shielded Transactions

Zcash takes a fundamentally different approach from Monero: privacy is **optional**. Users choose between transparent transactions (like Bitcoin) and shielded transactions (protected by ZK-SNARKs).

**Four transaction types:**

Type	From	To	What's Hidden
Transparent	t-address	t-address	Nothing (same as Bitcoin)
Shielding	t-address (public)	z-address (shielded)	Amount and receiver
Deshielding	z-address (shielded)	t-address (public)	Amount and sender
Fully shielded	z-address	z-address	Sender, receiver, and amount

**Shielded mechanics:** When Alice sends a shielded transaction, her wallet generates a ZK-SNARK proof that: (1) she owns the coins, (2) the amounts balance (no inflation), (3) no double-spend. The proof is posted on-chain; the transaction details are encrypted.

# Zcash: Optional Privacy Through Shielded Transactions

Zcash takes a fundamentally different approach from Monero: privacy is **optional**. Users choose between transparent transactions (like Bitcoin) and shielded transactions (protected by ZK-SNARKs).

Four transaction types:

Type	From	To	What's Hidden
Transparent	t-address	t-address	Nothing (same as Bitcoin)
Shielding	t-address (public)	z-address (shielded)	Amount and receiver
Deshielding	z-address (shielded)	t-address (public)	Amount and sender
Fully shielded	z-address	z-address	Sender, receiver, and amount

**Shielded mechanics:** When Alice sends a shielded transaction, her wallet generates a ZK-SNARK proof that: (1) she owns the coins, (2) the amounts balance (no inflation), (3) no double-spend. The proof is posted on-chain; the transaction details are encrypted.

**The adoption problem:** As of 2024, less than 15% of Zcash transactions use shielded addresses. Because shielded transactions are rare, they stand out – a chain analyst can flag them as “potentially suspicious.” This is the **optional privacy paradox**: when privacy is a choice, choosing it becomes a signal.

---

Zcash's Sapling upgrade (2018) reduced shielded transaction time from 40 seconds to under 3 seconds, yet adoption remains low.

# How Do Privacy Technologies Compare Across Blockchains?

Different blockchains implement privacy at different layers and with different trade-offs.

## Comparison dimensions:

- **Default privacy:** Is privacy on by default (Monero) or opt-in (Zcash)?
- **Sender hiding:** Ring signatures (Monero) vs ZK proofs (Zcash) vs none (Bitcoin)
- **Amount hiding:** RingCT (Monero) vs ZK proofs (Zcash) vs none (Bitcoin, Ethereum)
- **Smart contract support:** Secret Network offers private smart contracts; Monero and Zcash are payment-focused
- **Regulatory status:** Monero and Zcash have been delisted from exchanges in Japan, South Korea, and Australia

**Key insight:** No single blockchain excels on all dimensions. Monero leads on mandatory privacy; Zcash pioneered ZK-SNARK deployment; Secret Network extends privacy to programmable contracts.

Chain	Sender	Receiver	Amount	Contract
Bitcoin	N	N	N	N
Ethereum	N	N	N	N
Zcash	Y	Y	Y	N
Monero	Y	Y	Y	N
Secret	Y	Y	Y	Y

*Y = Private by default, N = Public/Transparent*

- **What you see:** A feature comparison of privacy approaches across major blockchains.
- **Key pattern:** Mandatory privacy (Monero) provides the strongest guarantees but faces the most regulatory resistance.
- **Takeaway:** Privacy technology choice involves a three-way trade-off: privacy strength, regulatory acceptance, and smart contract capability.

# How Have Privacy Coin Market Caps Evolved?

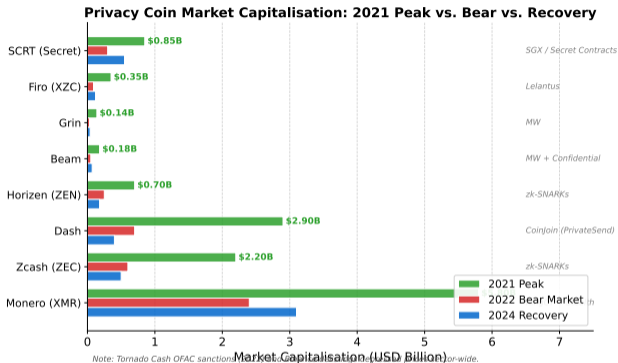
Privacy coin valuations reflect both technical merit and regulatory pressure – the two are inseparable in this sector.

## Market dynamics:

- **Monero dominates:** XMR holds the largest market cap among pure privacy coins, driven by mandatory privacy and genuine transactional use.
- **Regulatory discount:** Coins delisted from major exchanges trade at a structural discount – reduced liquidity suppresses price regardless of technology quality.
- **Bear-to-recovery patterns:** Privacy coins lost 60–80% in 2022, broadly in line with the wider crypto market. Recovery has been partial, constrained by exchange delistings.

**Technology-valuation link:** Coins using stronger cryptography (RingCT, zk-SNARKs) tend to retain more value through bear markets than those relying on simpler mixing (CoinJoin). The market implicitly prices cryptographic robustness.

Monero's market cap of  $\approx$ \$3B (2024) is roughly 6 $\times$  that of Zcash, despite Zcash's arguably stronger ZK-SNARK cryptography – a reminder that adoption drives value.



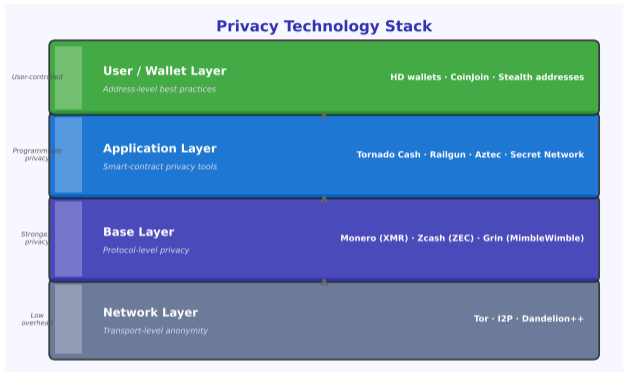
# Where Does Privacy Fit in the Blockchain Stack?

Privacy can be implemented at multiple layers of the blockchain stack. Each layer offers different trade-offs between privacy strength, performance, and compatibility.

## Five privacy layers:

- 1 **Network layer:** Hide your IP address when broadcasting transactions (Tor, Dandelion++ protocol)
- 2 **Protocol layer:** Privacy built into the blockchain itself (Monero, Zcash) – strongest guarantees, but requires a separate chain
- 3 **Smart contract layer:** Privacy via on-chain contracts (Tornado Cash, Aztec) – works on existing chains like Ethereum
- 4 **Layer 2:** Privacy channels or rollups (Aztec Network) – transactions happen off-chain with only proofs posted on-chain
- 5 **Application layer:** Privacy-preserving dApps, encrypted messaging, private DeFi

**Key insight:** The most robust privacy combines multiple layers. Using Monero (protocol-level privacy) over Tor (network-level privacy) provides much stronger anonymity than either alone.



- **What you see:** The privacy technology stack showing where each solution operates.
- **Key pattern:** Lower layers provide stronger guarantees but are harder to change. Upper layers are more flexible but easier to bypass.
- **Takeaway:** Defense in depth – just as cybersecurity uses multiple layers, blockchain privacy is strongest when applied at multiple levels.

# Confidential Transactions: Proving Amounts Balance Without Revealing Them

**Confidential Transactions (CT)** hide the monetary value of a transaction while still allowing the network to verify that no coins are created from nothing.

## The core tool – Pedersen commitments:

A commitment to value  $v$  with blinding factor  $r$  is

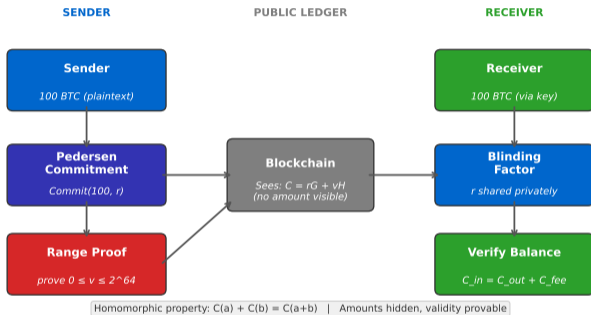
$$C = g^v \cdot h^r$$

where  $g$  and  $h$  are independent generator points on an elliptic curve. Publishing  $C$  hides  $v$  (computationally binding) yet lets anyone verify the homomorphic identity  $C_{in} = C_{out} + C_{fee}$  without learning any amount.

**Range proofs:** The sender also provides a zero-knowledge *range proof* showing  $0 \leq v < 2^{64}$ , preventing negative amounts that would inflate supply.

**Used by:** Monero (RingCT), MimbleWimble (Grin, Beam), and proposed for Bitcoin via the Elements sidechain.

## Confidential Transactions: Hiding Amounts on a Public Ledger



The homomorphic property of Pedersen commitments –  $C(a) + C(b) = C(a + b)$  – is the key that allows balance verification without decryption.

# Stealth Addresses: One-Time Receiving Addresses That Only the Recipient Can Find

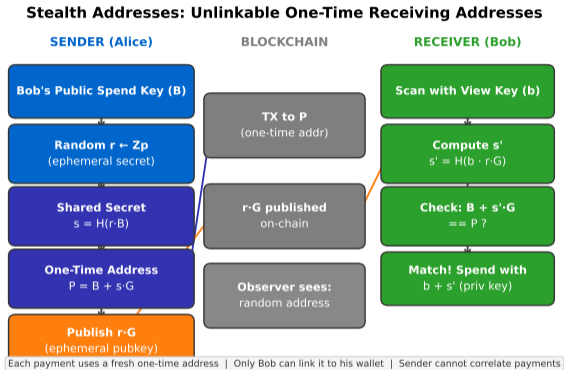
A **stealth address** generates a fresh, unlinkable on-chain address for every payment – even when the sender pays the same receiver repeatedly.

## Protocol (Diffie–Hellman key exchange on-chain):

- 1 Bob publishes spend key  $B = bG$  and view key  $V = vG$ .
- 2 Alice picks random  $r$ , computes shared secret  $s = H(r \cdot B)$ , and sends to one-time address  $P = B + s \cdot G$ .
- 3 Alice posts ephemeral pubkey  $R = rG$  on-chain.
- 4 Bob scans with view key  $b$ : computes  $s' = H(b \cdot R)$  and checks whether  $B + s' \cdot G = P$ .

**Privacy guarantee:** An observer sees only random-looking addresses. Only Bob can link  $P$  to his wallet. Anonymity set size  $|A| = k$  grows with every stealth address ever generated on the chain – typically  $k \geq 10^4$  in practice.

ERC-5564 (2023) proposes a standard stealth address scheme for Ethereum. Vitalik Buterin's blog estimated it would increase Ethereum privacy significantly with minimal UX change.



# Can Ethereum Become Private Without Changing Its Protocol?

Ethereum is fully transparent by default – every transaction, balance, and smart contract interaction is public. Several projects are building privacy on top of Ethereum without modifying the base protocol.

## Privacy solutions on Ethereum:

- 1 **Aztec Network (ZK rollup):** A Layer 2 that processes transactions off-chain using ZK proofs. Users get privacy *and* lower gas fees. Supports private DeFi (lending, swaps) natively.
- 2 **Railgun:** A smart contract system that shields ERC-20 tokens and NFTs directly on Ethereum. Uses ZK-SNARKs to prove transaction validity without revealing details.
- 3 **Stealth addresses (ERC-5564):** A proposed standard that brings Monero-style stealth addresses to Ethereum. Vitalik Buterin advocated for this in a January 2023 blog post.
- 4 **Private mempools:** Services like Flashbots Protect submit transactions directly to block builders, bypassing the public mempool (the waiting room where pending transactions are visible).

**Key insight:** Privacy on Ethereum is evolving from “breaking the link” (mixers) to “never creating the link in the first place” (stealth addresses, private rollups). This shift is both technically superior and potentially more regulatory-friendly.

---

Vitalik Buterin's January 2023 blog “An incomplete guide to stealth addresses” proposed a practical path to Ethereum privacy without protocol changes.

# Privacy-Preserving DeFi: Trading Off Privacy, Functionality, and Regulatory Risk

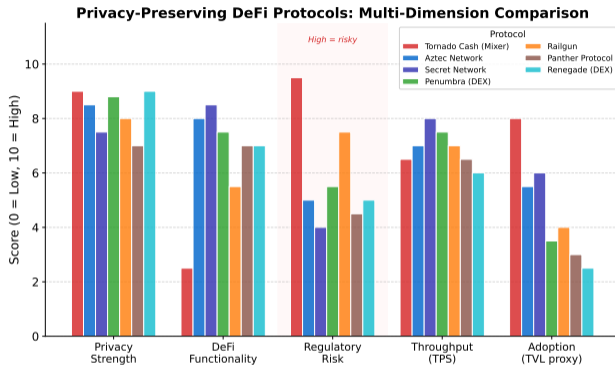
DeFi amplifies the privacy problem: every swap, loan, and liquidity position is permanently on-chain. A new wave of protocols aims to add confidentiality without sacrificing composability.

## Key protocols compared:

- **Tornado Cash:** Highest privacy strength (score 9/10) but maximum regulatory risk (9.5/10 on risk axis). Sanctioned by OFAC in 2022.
- **Aztec Network:** Balanced trade-off – strong privacy (8.5) with moderate regulatory risk (5.0) and full DeFi functionality (8.0). Uses ZK rollup architecture.
- **Secret Network:** TEE-based private smart contracts; broadest DeFi surface (8.5) with lower regulatory risk (4.0).
- **Railgun:** On-chain shielding for ERC-20 tokens using ZK-SNARKs; simpler scope than Aztec but production-ready.

**Key insight:** High privacy and low regulatory risk are currently anti-correlated. Aztec is the closest to threading this needle.

Aztec Network paused its rollup in 2024 to rebuild as a fully programmable privacy layer – a sign of how rapidly the architecture is evolving.



# Who Actually Uses Privacy Technologies – and How Much?

Despite strong cryptographic foundations, privacy technology adoption remains a small fraction of overall blockchain activity.

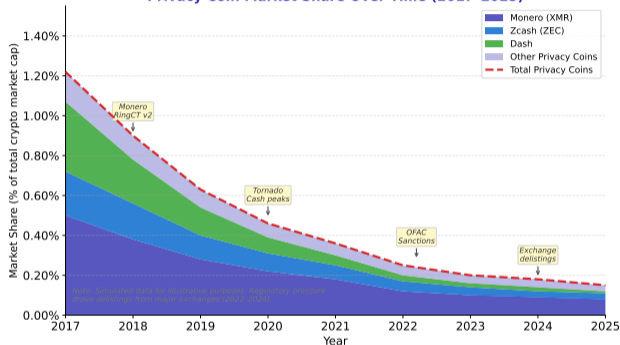
## Adoption statistics (2024):

- **Monero:** Approximately 25,000–30,000 daily transactions (vs Bitcoin's 400,000+)
- **Zcash shielded:** Less than 15% of all ZEC transactions use shielded addresses
- **Tornado Cash:** Processed \$7+ billion before sanctions, but activity dropped 90%+ after the OFAC action
- **Railgun:** Growing but still under \$500M in total volume

## Why so low?

- UX complexity (generating proofs, managing keys)
- Higher transaction costs (ZK proofs consume more compute)
- Exchange delistings reduce liquidity
- Regulatory fear (“will I get flagged?”)

Privacy Coin Market Share Over Time (2017–2025)



- **What you see:** Privacy technology adoption metrics over time, showing usage volumes and market share.
- **Key pattern:** Regulatory events (exchange delistings, sanctions) cause sharp drops in privacy coin usage.
- **Takeaway:** Technical capability far exceeds actual adoption. Privacy technologies are available but underused – mostly due to

# Privacy vs Compliance: An Unresolved Tension

Governments and privacy advocates hold fundamentally opposing positions on blockchain privacy. Neither side is entirely wrong.

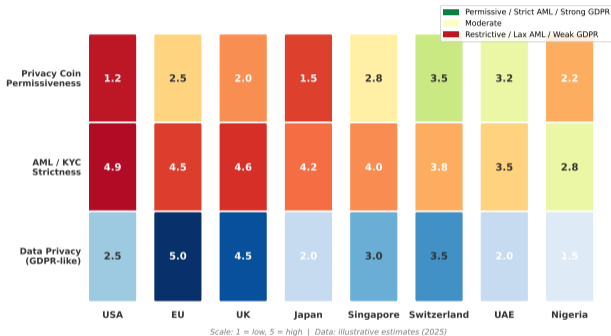
## The compliance argument:

- Anti-money laundering (AML) laws require financial institutions to track the flow of funds
- Know Your Customer (KYC) regulations require identity verification
- Privacy tools can be used for ransomware payments, sanctions evasion, and tax fraud
- The FATF "Travel Rule" requires exchanges to share sender and receiver information for transactions above \$1,000

## The privacy argument:

- Financial privacy is a human right (UDHR Article 12)
- Surveillance disproportionately harms dissidents, journalists, and minorities in authoritarian regimes
- Cash is already anonymous – blockchain privacy merely restores the status quo
- Code is speech (First Amendment in the US)

Regulatory Tension Map: Privacy vs. Compliance



- **What you see:** A map of regulatory positions across jurisdictions, from permissive to restrictive.
- **Key pattern:** There is no global consensus. Some jurisdictions ban privacy coins entirely; others protect them as free speech.
- **Takeaway:** The regulatory landscape is fragmented and rapidly

# How Effective Is Chain Analysis Against Each Privacy Technology?

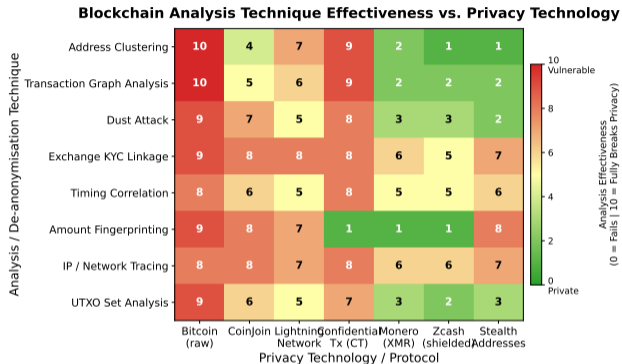
Chain analysis firms deploy a portfolio of techniques. Their effectiveness varies dramatically across privacy technologies.

## Reading the heatmap:

- **Red cells (score 8–10):** The analysis technique largely defeats that privacy technology. Raw Bitcoin scores 9–10 on nearly every row.
- **Green cells (score 0–2):** The privacy technology resists that attack. Monero scores 1–2 on address clustering and transaction graph analysis.
- **Exchange KYC linkage (row 4)** is the universal weakness: even Monero scores 6/10 because on-ramps require identity verification.

**Key finding:** Confidential Transactions (CT) completely defeats amount fingerprinting (score 1) but leaves other vectors open. No single privacy technology scores green across all rows – defense in depth is necessary.

Chainalysis publishes an annual “Crypto Crime Report” documenting which privacy technologies were most successfully bypassed by law enforcement that year.



# OFAC Sanctions: Can a Government Ban a Smart Contract?

In August 2022, the US Office of Foreign Assets Control (OFAC) sanctioned Tornado Cash – adding its Ethereum smart contract addresses to the Specially Designated Nationals (SDN) list. This was unprecedented: for the first time, *code* – not a person or company – was sanctioned.

## The chain of events:

- 1 **OFAC justification:** North Korea's Lazarus Group used Tornado Cash to launder over \$455 million stolen from DeFi hacks.
- 2 **Immediate effects:** Circle froze \$75K in USDC. GitHub removed the Tornado Cash repository. Infura and Alchemy (Ethereum API providers) blocked access to the contract.
- 3 **Developer arrested:** Alexey Pertsev was arrested in the Netherlands in August 2022 and convicted of money laundering in May 2024.
- 4 **Legal challenge:** Coin Center and six Tornado Cash users sued OFAC, arguing that sanctioning immutable code exceeds OFAC's statutory authority.
- 5 **Court ruling (Nov 2024):** The Fifth Circuit ruled that immutable smart contracts are not “property” of a foreign national and therefore cannot be sanctioned under IEEPA (International Emergency Economic Powers Act).

**Key question:** If the code is legal but using it is sanctioned, who bears responsibility – the developer, the user, or the code itself?

---

The Tornado Cash contract remains deployed on Ethereum. Immutable smart contracts cannot be “taken down” – they run as long as the blockchain exists.

# Is There a Middle Ground Between Privacy and Compliance?

The binary framing – “total privacy” vs “total surveillance” – is false. Several emerging approaches attempt to provide privacy for legitimate users while allowing compliance when legally required.

## Four approaches to selective disclosure:

- 1 **View keys (Monero, Zcash):** Users can share a special “view key” that lets a third party (e.g., a tax auditor) see their transactions without being able to spend their coins. Privacy by default, transparency by choice.
- 2 **Compliance pools (Aztec Connect):** Separate mixing pools where all participants have passed KYC. Privacy within the group, identity known to the verifier.
- 3 **ZK proofs for compliance:** Prove you are not on a sanctions list without revealing your identity. Projects like Chainway and Proof of Innocence explore this approach.
- 4 **Privacy-preserving analytics:** Allow regulators to detect suspicious patterns (e.g., sudden large flows) without seeing individual transaction details – similar to how encrypted email can be flagged by volume without reading content.

**Key insight:** ZK proofs may ultimately *resolve* the privacy-compliance tension rather than perpetuate it. You can prove “I am not on the OFAC list” without revealing “I am Alice.”

---

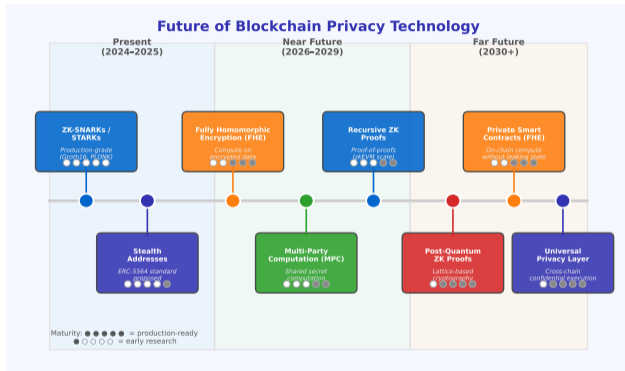
**Proof of Innocence, launched in 2023, uses ZK proofs to let Tornado Cash users prove their funds are not from sanctioned sources – compliance without deanonymization.**

# What Privacy Technologies Are Coming Next?

Privacy technology is evolving rapidly. The next generation aims to make privacy cheaper, faster, and more compatible with existing blockchains.

## Five technologies to watch:

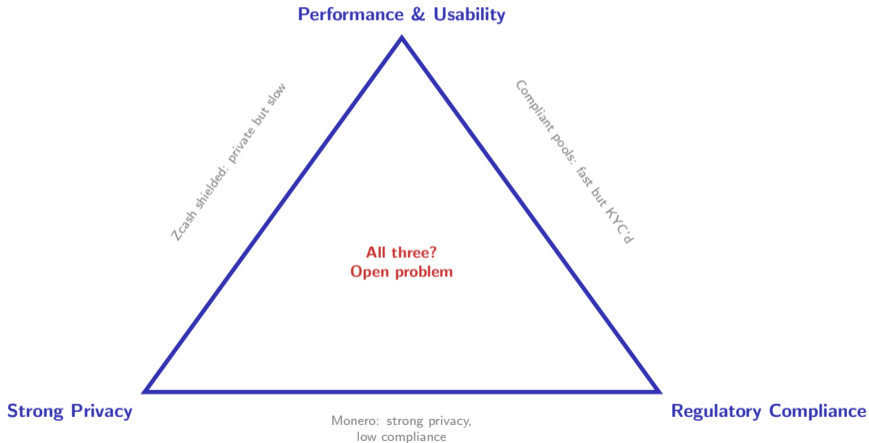
- 1 **FHE (Fully Homomorphic Encryption):** Perform computations on encrypted data without ever decrypting it. A holy grail for private smart contracts – but still 1,000x slower than unencrypted computation.
- 2 **MPC (Multi-Party Computation):** Multiple parties jointly compute a result without any party seeing the others' inputs. Used for private auctions and voting.
- 3 **ZK rollups with privacy:** Aztec and Polygon Miden combine scaling (cheap transactions) with privacy (hidden details) in a single Layer 2.
- 4 **Account abstraction + privacy:** ERC-4337 wallets that automatically route transactions through privacy-preserving paths.
- 5 **Recursive ZK proofs:** Proofs that verify other proofs, enabling infinite composability without growing proof size.



- **What you see:** A timeline and readiness map of emerging privacy technologies.
- **Key pattern:** Technologies move from research to production over 3–7 years. ZK proofs took 30+ years from invention (1985) to mass deployment (2020s).
- **Takeaway:** The privacy tools of 2030 may make today's debate

# The Privacy Trilemma: Can You Have All Three?

Every privacy system on a blockchain faces a three-way trade-off. You can optimize for two of the three properties, but achieving all three simultaneously remains an open challenge.



Evaluation framework – three questions for any privacy system:

# Five Questions to Evaluate Any Privacy Tool

Before using or investing in a privacy technology, walk through these five evaluation questions. They apply to any system – from Monero to Tornado Cash to the next privacy protocol that launches.

## The Five Questions:

- 1 **Is privacy mandatory or optional?** Mandatory privacy (Monero) protects all users equally. Optional privacy (Zcash) creates a two-tier system where private users stand out.
- 2 **How large is the anonymity set?** A mixer with 10 users provides trivial privacy. A mixer with 10,000 provides meaningful protection. Bigger is always better.
- 3 **What trust assumptions exist?** Does the system require a trusted setup (original SNARKs), trusted hardware (Secret Network's TEEs), or a trusted third party (centralized mixer)?
- 4 **What is the regulatory status?** Is the technology banned, restricted, or legal in your jurisdiction? Can you comply with tax reporting obligations while using it?
- 5 **What are the costs?** Privacy is not free. Higher gas fees, slower transactions, limited exchange support, and reduced composability with other protocols are real trade-offs.

**Decision rule:** If a privacy tool scores poorly on questions 2 and 3 (small anonymity set, strong trust assumptions), its privacy guarantees are likely weaker than advertised.

---

Apply these five questions to both Monero and Zcash as an exercise. How does each score?

# What Comes Next: DAOs and Governance

Today you learned how privacy technologies protect individual users on public blockchains. In Lesson 11, we shift from individual rights to collective decision-making: how do blockchain communities govern themselves without a central authority?

## Lesson 11 will cover:

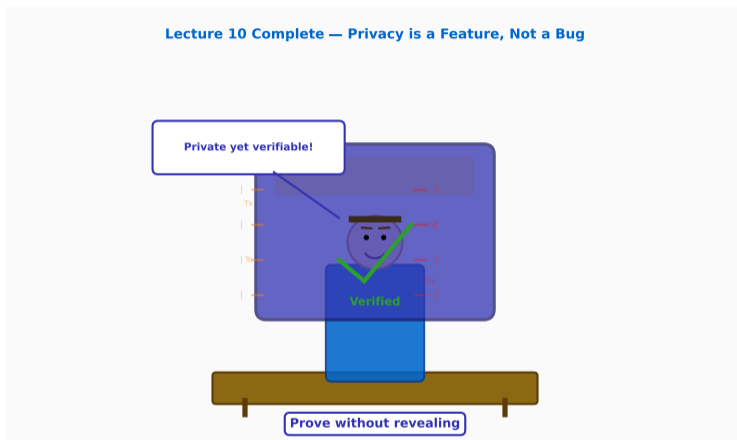
- **DAOs (Decentralized Autonomous Organizations):** Smart contract-based organizations where rules are encoded in code and decisions are made by token holders through on-chain voting.
- **Voting mechanisms:** Token-weighted voting, quadratic voting (where the cost of additional votes rises quadratically), and conviction voting (votes gain weight over time).
- **Governance attacks:** Flash loan governance attacks (borrowing tokens to vote, then returning them), voter apathy, and plutocracy (rule by the wealthiest token holders).
- **The DAO hack:** The 2016 attack that drained \$60 million and led to the Ethereum/Ethereum Classic split.

**Bridge:** Privacy is about protecting the individual. Governance is about empowering the collective. Both require careful cryptographic design to prevent abuse.

**Preparation:** Think about how decisions are made in organizations you belong to (clubs, companies, student groups). Who votes? Who can propose changes? What prevents one person from dominating?

---

Lesson 11 builds on the smart contract concepts from L05 and the token economics from L08.



Now you understand the core tension: public blockchains need transparency for trust but privacy for freedom. Zero-knowledge proofs, ring signatures, and mixers each offer a different way to balance this trade-off – and each comes with its own costs. The technology exists to make blockchain transactions private. The open question is whether society will allow it.

**The best privacy tools make privacy the default, not the exception. When everyone is private, nobody stands out.**

## Key Takeaways

- 1 **Pseudonymity is not anonymity:** Public blockchains expose every transaction. Chain analysis firms can link addresses to identities through exchange data, transaction patterns, and address reuse.
- 2 **ZK proofs:** Prove a statement is true without revealing the underlying data. ZK-SNARKs offer small proofs; ZK-STARKs eliminate the trusted setup and resist quantum computers.
- 3 **Mixers:** Break the link between sender and receiver by pooling and redistributing funds. Effectiveness depends on anonymity set size and user discipline.
- 4 **Monero vs Zcash:** Monero enforces mandatory privacy (ring signatures, stealth addresses, RingCT). Zcash offers optional privacy (ZK-SNARKs). Mandatory privacy provides stronger guarantees but faces harsher regulatory pushback.
- 5 **Privacy layers:** Privacy can be built at the network, protocol, smart contract, L2, or application layer. Defense in depth combines multiple layers.
- 6 **Regulatory tension:** Governments want transaction visibility for AML/KYC. Individuals want financial confidentiality as a right. ZK proofs for compliance (proving innocence without revealing identity) may bridge this gap.

---

Review question: Using the five evaluation questions from Frame 29, compare Monero and Zcash on privacy strength, compliance, and usability.

## Summary / Next Lesson Preview

Public blockchains are transparent by design – every transaction is visible to everyone. Privacy technologies restore confidentiality through cryptographic techniques: zero-knowledge proofs let you prove facts without revealing data; mixers break the link between sender and receiver; ring signatures hide the real signer among decoys. Monero implements mandatory privacy through three layers (ring signatures, stealth addresses, RingCT), while Zcash offers optional shielded transactions using ZK-SNARKs. The OFAC sanctions on Tornado Cash in 2022 revealed the unresolved tension between financial privacy and regulatory compliance – a tension that ZK proofs for selective disclosure may eventually resolve.

### Key Vocabulary:

- Zero-Knowledge Proof (ZK Proof)
- ZK-SNARK / ZK-STARK
- Trusted Setup
- Mixer / Tumbler
- Anonymity Set
- Ring Signature
- Stealth Address
- RingCT (Ring Confidential Transactions)
- Shielded Transaction
- Chain Analysis

**Next lesson:** *DAOs and Governance* – how blockchain communities make collective decisions through on-chain voting, and what happens when governance is attacked.

---

Try this before Lesson 11: visit a blockchain explorer ([etherscan.io](https://etherscan.io)) and look up any Ethereum transaction. Notice how much information is publicly visible.