L10: Privacy Technologies

Extended Slides – BSc Blockchain Course

Digital Finance

Outline

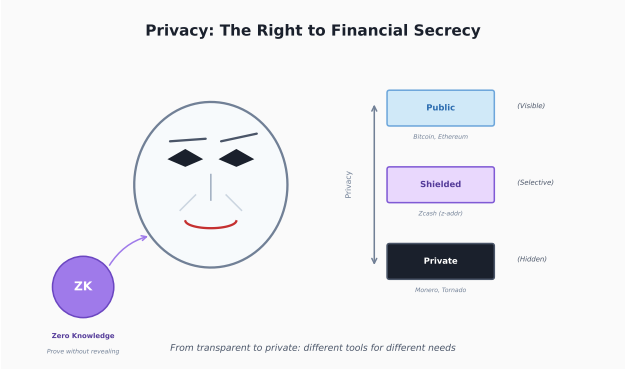
Learning Objectives

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

1. Understand the blockchain privacy spectrum
2. Explain zero-knowledge proofs conceptually
3. Describe mixer and tumbler mechanisms
4. Analyze privacy features of Monero and Zcash
5. Evaluate privacy-preserving technologies

Prerequisites: L02 Cryptography, L05 Ethereum.

The Privacy Dilemma



Purpose: Public blockchains expose all transactions. Privacy technologies balance transparency with confidentiality—a critical tension in blockchain design.

Financial privacy vs. regulatory compliance: the ongoing challenge.

Why Privacy Matters

Legitimate Privacy Needs:

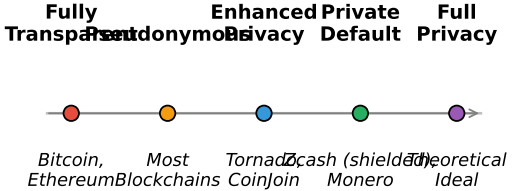
- Financial confidentiality
- Business competitive secrets
- Personal safety (no stalking via blockchain)
- Fungibility of money

The Paradox:

- Transparency enables trustless verification
- But also enables surveillance

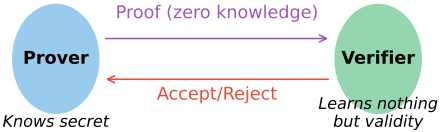
Privacy is not about hiding crimes – it's about freedom.

Privacy Spectrum



Pseudonymity is not anonymity – addresses can be linked.

Zero-Knowledge Proof: Prove Without Revealing



Completeness: valid proofs always accepted

Soundness: invalid proofs rejected

Zero-knowledge: verifier learns nothing

ZK proofs are foundational to privacy and scaling.

ZK-SNARKs vs ZK-STARKs

ZK-SNARKs:

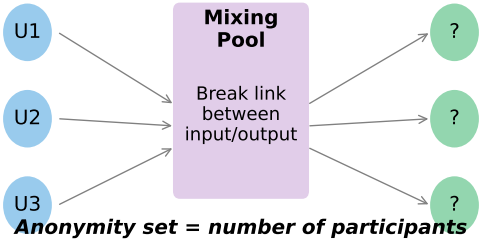
- Succinct Non-interactive Arguments of Knowledge
- Small proofs, fast verification
- Traditional SNARKs need trusted setup; newer (Halo2, Plonky2) do not
- Used by Zcash, Tornado Cash

ZK-STARKs:

- No trusted setup (transparent)
- Larger proofs but quantum-resistant
- Used by StarkNet

Both enable proving computation without revealing inputs.

Mixer/Tumbler: Breaking Transaction Links

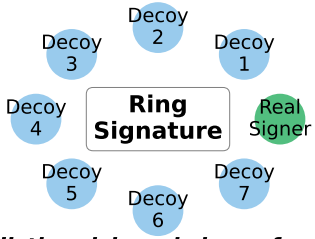


Anonymity set = number of participants

Tornado Cash: ZK proofs for withdrawal

Larger anonymity set = better privacy.

Ring Signatures: Plausible Deniability



Cannot distinguish real signer from decoys

Monero: Ring signatures + stealth addresses + RingCT

Monero uses mandatory privacy for all transactions.

Monero Privacy Stack

Three Layers:

- **Ring Signatures:** Hide sender among decoys
- **Stealth Addresses:** One-time receive addresses
- **RingCT:** Confidential transaction amounts

Result:

- Sender hidden
- Receiver hidden
- Amount hidden
- All mandatory

Privacy by default, not optional.

Zcash Shielded Transactions

Two Pool Types:

- **Transparent:** Like Bitcoin, fully visible
- **Shielded:** ZK-SNARK protected

Shielded Features:

- Prove you own funds without revealing
- Prove correct state transitions
- Optional (unlike Monero)

Zcash pioneered ZK-SNARKs in cryptocurrency.

Privacy Comparison

Privacy Feature Comparison

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

Secret Network adds private smart contracts.

Regulatory Challenges

Tension Points:

- OFAC sanctions (Tornado Cash)
- AML/KYC requirements
- Exchange delistings of privacy coins

Ongoing Debate:

- Privacy as a right vs crime prevention
- Code as speech (First Amendment)
- International regulatory differences

Privacy tools face increasing regulatory scrutiny.

Ring Signatures: Technical Detail

How Ring Signatures Work:

- Sender picks n decoy public keys from the blockchain
- Signature is valid for any member of the "ring"
- Observer cannot determine actual signer
- Ring size in Monero: 16 (mandatory)

Key Image:

- Unique value derived from true signing key
- Prevents double-spending without revealing sender
- Same key image appearing twice flags double-spend

Larger ring sizes improve privacy at the cost of transaction size.

Stealth Addresses

Problem Solved:

- Reusing public addresses links all incoming transactions
- Anyone can watch a known address for payments

Stealth Address Protocol:

- Receiver publishes a public spend and view key pair
- Sender generates a one-time address per transaction
- Receiver scans blockchain with view key to find payments
- Only receiver can spend, only receiver knows the link

Result: On-chain, all payments appear to go to unrelated addresses.

Monero uses stealth addresses by default; EIP-5564 brings them to Ethereum.

Privacy Coin Comparison

Feature Matrix:

- **Monero:** Ring signatures + stealth + RingCT; all mandatory; strongest default privacy
- **Zcash:** ZK-SNARKs (Sapling/Orchard); optional shielded; widely delisted due to compliance risk
- **Dash:** CoinJoin-based PrivateSend; optional; weakest of the three
- **Grin:** MimbleWimble; cut-through removes old outputs; no amounts or addresses on-chain

Tradeoffs:

- Mandatory privacy (Monero) vs. opt-in (Zcash, Dash)
- Proof size: SNARKs (small) vs. STARKs (larger, no trusted setup)

Fungibility requires that all coins appear identical – Monero achieves this most fully.

ZK Proofs Beyond Privacy Coins

ZK-Rollups (Scaling):

- Batch thousands of transactions off-chain
- Submit a single ZK proof to Layer 1
- Full security of Ethereum with 100× throughput
- Used by: zkSync, StarkNet, Polygon zkEVM

Other Applications:

- Identity proofs: prove age without revealing birthdate
- Credential verification: prove degree without transcript
- Compliance: prove tax payment without income details

ZK proofs are becoming a general-purpose cryptographic tool, not just for privacy coins.

Privacy vs. Compliance Tradeoff

Regulatory Pressure Points:

- FATF Travel Rule: exchanges must share sender/receiver data
- OFAC sanctions: Tornado Cash smart contract sanctioned (2022)
- MiCA (EU): requires issuer identification for asset-referenced tokens

Technical Mitigations:

- **View keys:** Allow auditor read-only access to transactions
- **Selective disclosure:** ZK proof of compliance without full disclosure
- **Compliance proofs:** Prove funds are not from sanctioned sources

---

Privacy and compliance may be reconcilable through cryptographic selective disclosure.

Key Takeaways

Remember These Points

1. Blockchains are pseudonymous, not anonymous
2. ZK proofs: prove without revealing
3. Mixers break transaction graphs
4. Monero: mandatory privacy (ring sigs + stealth)
5. Zcash: optional shielded transactions
6. Privacy tools face regulatory challenges

Next Lesson: DAOs and Governance.