# L10: Privacy Technologies

## BSc Blockchain Course

Digital Finance

# Outline

# Learning Objectives

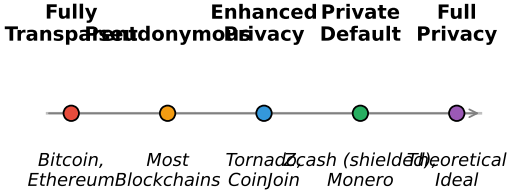
**By the end of this lesson, you will be able to:**

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

---

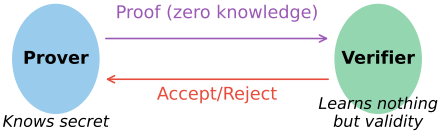
**Privacy is not about hiding wrongdoing – it's a fundamental right.**

# Privacy Spectrum




**Most blockchains are pseudonymous, not anonymous.**

## Zero-Knowledge Proof: Prove Without Revealing



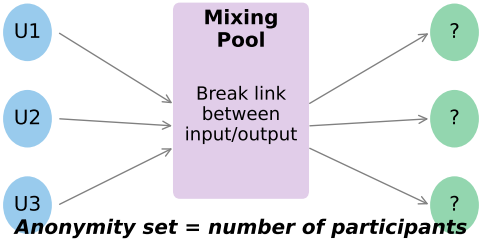

Completeness: valid proofs always accepted

Soundness: invalid proofs rejected

Zero-knowledge: verifier learns nothing

**ZK proofs: prove you know something without revealing it.**

## Mixer/Tumbler: Breaking Transaction Links

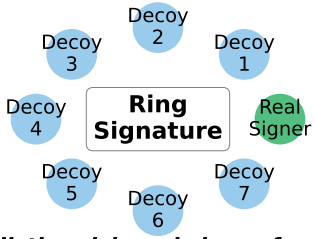



***Anonymity set = number of participants***

Tornado Cash: ZK proofs for withdrawal

**Mixers break the link between deposit and withdrawal addresses.**

## Ring Signatures: Plausible Deniability

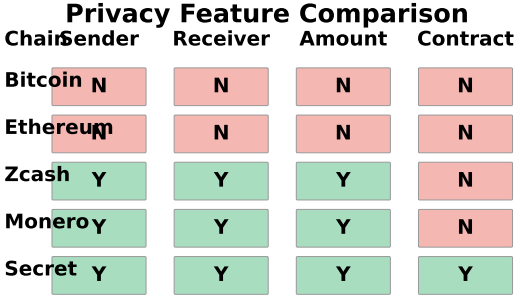



***Cannot distinguish real signer from decoys***

Monero: Ring signatures + stealth addresses + RingCT

**Monero hides sender, receiver, and amount by default.**

# Privacy Comparison




**Zcash and Monero lead in privacy features.**

# ZK-SNARK Mechanics

**How ZK-SNARKs Work:**

- Prover holds a witness (secret input)
- Arithmetic circuit encodes the computation
- Prover generates a short proof without revealing inputs
- Verifier checks the proof in milliseconds

**Properties:**

- **Completeness:** Honest prover always convinces verifier
- **Soundness:** Cheating prover cannot forge proof
- **Zero-knowledge:** Verifier learns nothing beyond truth

---

**ZK-SNARKs power Zcash shielded transactions and ZK-rollups.**

# Privacy vs. Compliance Tradeoff

**The Core Tension:**

- Regulators require AML/KYC on financial flows
- Privacy technologies obscure transaction trails
- Exchanges face legal risk listing privacy coins

**Emerging Approaches:**

- Selective disclosure: reveal to auditor, not public
- View keys: grant read-only access to regulator
- Compliance proofs: ZK proof of AML compliance

---

**Regulatory pressure led to Monero and Zcash delistings on major exchanges.**

# Key Takeaways

**Remember These Points**

1. Most blockchains are pseudonymous, not private
2. ZK proofs enable proving without revealing
3. Mixers break transaction linkability
4. Monero: ring signatures, stealth addresses
5. Zcash: shielded transactions with ZK-SNARKs

**Next Lesson:** DAOs and Governance.