# Privacy & Zero-Knowledge Proofs: Course Preview

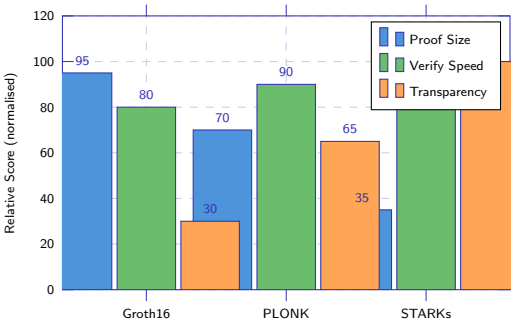
## INTRO Preview

Prof. Dr. Joerg Osterrieder

University Lecture Series

March 1, 2026

# Why Zero-Knowledge Proofs Matter

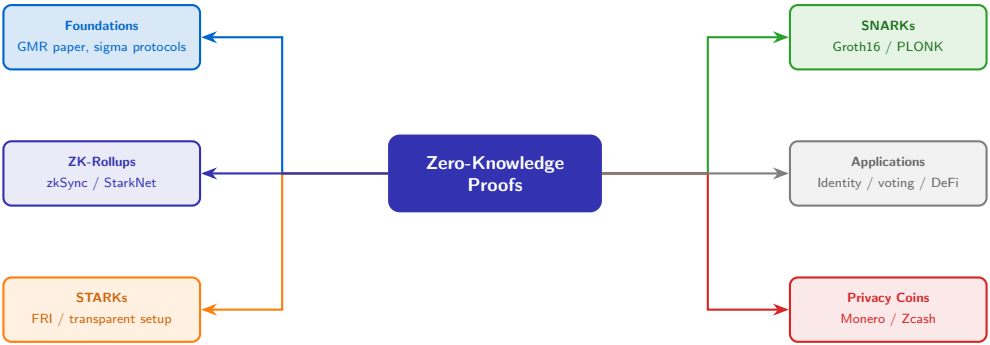



## Key Metrics

- ✓ **$10B+** ZK-rollup TVL in 2025
- ✓ **<10ms** proof verification on-chain
- ✓ **$3B+** privacy coin market cap
- ✓ **100x** throughput via ZK-rollups

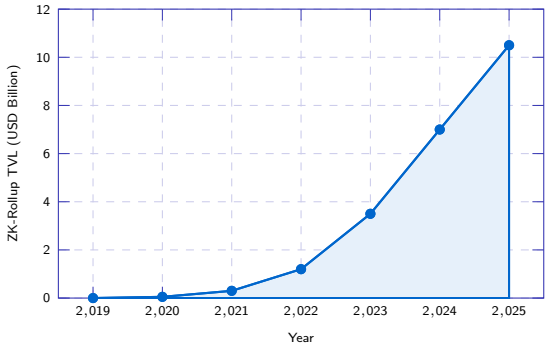
**ZK proof systems trade proof size, verification speed, and trusted-setup requirements: Groth16 is compact, PLONK is universal, STARKs are transparent.**

# ZK Proof Landscape




**The ZK landscape spans foundational cryptography, proof system families, privacy coins, ZK-rollup scaling, and emerging applications in identity and DeFi.**

# ZK Ecosystem Growth




## Growth Drivers

- ✓ **DeFi privacy** demand rising sharply
- ✓ **Hardware acceleration** of proof generation
- ✓ **Recursive proofs** enabling new architectures
- ✓ **Regulatory pressure** boosting privacy tech

**ZK-rollup TVL grew from near zero in 2019 to over $10B by 2025, driven by hardware advances, recursive proving breakthroughs, and rising privacy demand.**

# Course Coverage


## Prerequisites

- ✓ Basic cryptography and hash function knowledge
- ✓ Introductory blockchain and Ethereum concepts

## Outcomes

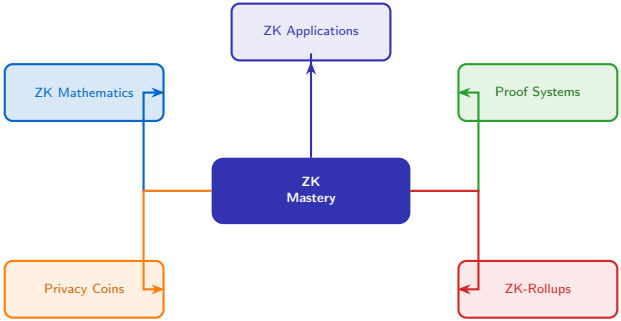
- ✓ Construct and verify ZK proof arguments
- ✓ Evaluate privacy coin and ZK-rollup trade-offs

**Five modules progress from foundational ZK theory through SNARKs and STARKs to privacy coins, ZK-rollups, and the frontiers of zkML and zkEVM.**

# What You Will Learn

## Learning Outcomes

- ✓ **Proof system mathematics** — completeness, soundness, zero-knowledge, polynomial commitments
- ✓ **SNARKs vs. STARKs** — trusted setup, proof size, verification cost trade-offs
- ✓ **Privacy coins** — ring signatures, stealth addresses, shielded pools in Monero and Zcash
- ✓ **ZK-rollups** — zkSync, StarkNet architecture, sequencers, validity proofs
- ✓ **ZK applications** — private identity, on-chain voting, confidential DeFi




**By the end you will be able to reason rigorously about ZK proof systems, privacy coins, and ZK-rollup architectures from first principles to production applications.**