# Privacy & Zero-Knowledge Proofs

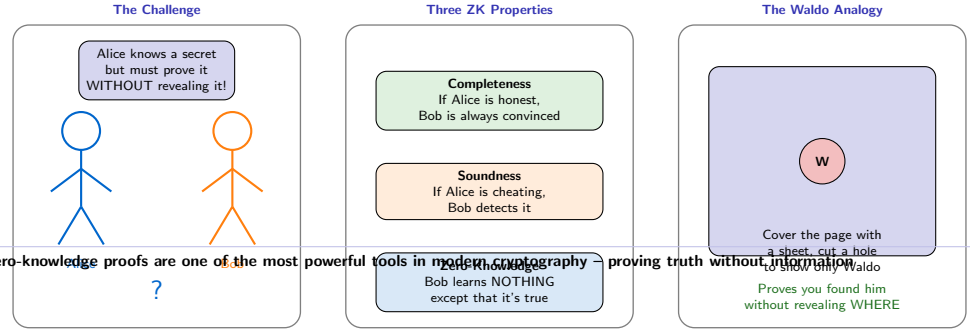
## A Visual Introduction

Prof. Dr. Joerg Osterrieder

University Lecture Series

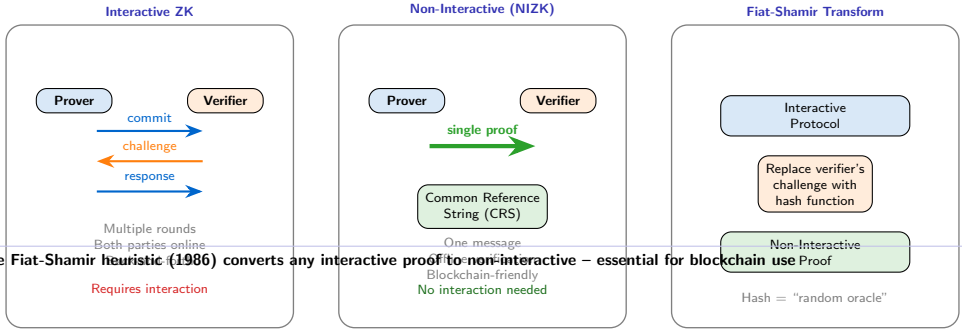
*"Privacy is the power to selectively reveal oneself to the world."*
— Eric Hughes, A Cypherpunk's Manifesto (1993)

# What is a Zero-Knowledge Proof?



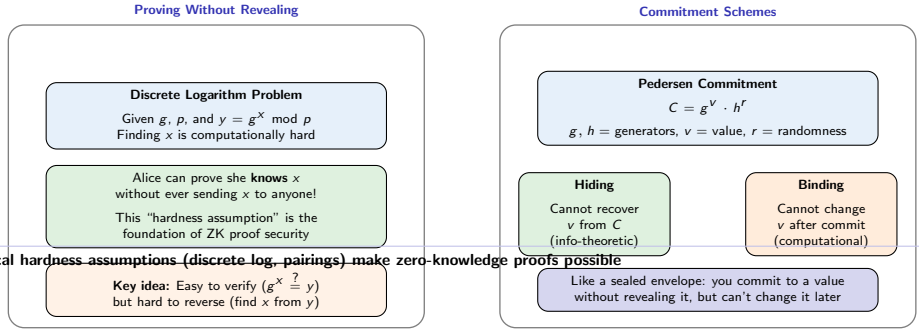

**Zero-knowledge proofs are one of the most powerful tools in modern cryptography – proving truth without information.**

# Interactive vs Non-Interactive Proofs



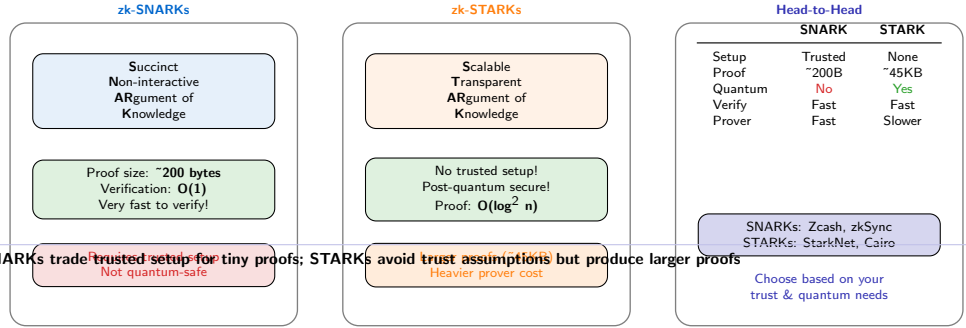

**The Fiat-Shamir heuristic (1986) converts any interactive proof to non-interactive – essential for blockchain use**

# The Math Behind ZK



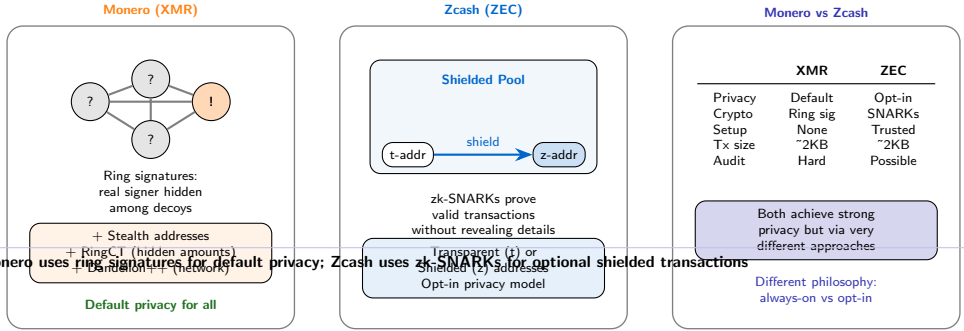

**Mathematical hardness assumptions (discrete log, pairings) make zero-knowledge proofs possible**

# SNARKs vs STARKs



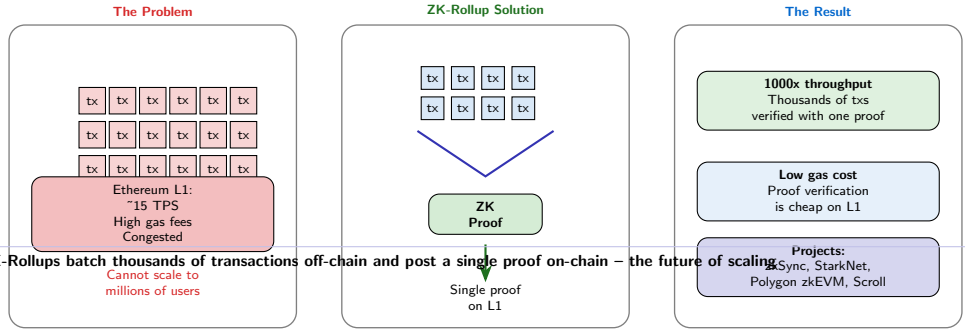

**SNARKs trade trusted setup for tiny proofs; STARKs avoid trust assumptions but produce larger proofs**

# Privacy Coins Overview




**Monero uses ring signatures for default privacy; Zcash uses zk-SNARKs for optional shielded transactions**

# ZK-Rollups Simplified




**ZK-Rollups batch thousands of transactions off-chain and post a single proof on-chain – the future of scaling.**

# Real-World ZK Applications

**Private Voting**

Anonymous but verifiable elections

Prove eligibility without revealing identity
Prevent bribery & coercion (MACI)

**Identity Verification**

Prove age $\geq 18$ without showing ID

Self-sovereign identity (SSI)
Selective disclosure of credentials

**DeFi Privacy**

Private trading (no front-running)
Hidden balances & amounts
Railgun, Aztec, Penumbra

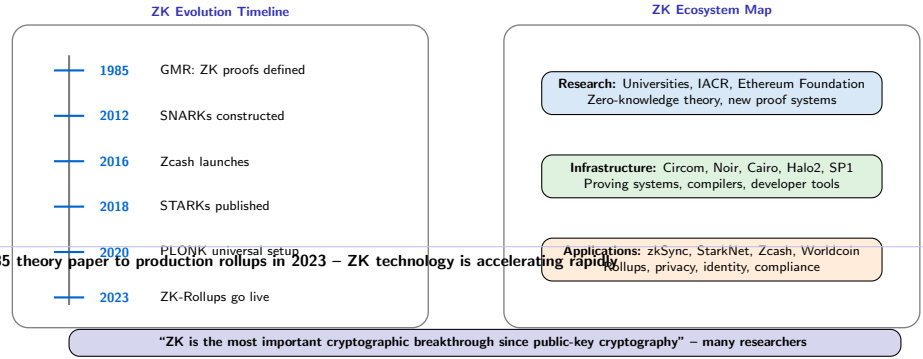
**Supply Chain**

Prove product authenticity

Without exposing trade secrets
Verify compliance privately

**ZK proofs enable "verify without revealing" across voting, identity, finance, and supply chains**

# The ZK Landscape




**From a 1985 theory paper to production rollups in 2023 – ZK technology is accelerating rapidly.**

# Key Takeaways

1. ZK proofs prove knowledge without revealing it – completeness, soundness, zero-knowledge

2. SNARKs are small but need trusted setup; STARKs are transparent and quantum-safe

3. Privacy coins (Monero, Zcash) use different cryptographic approaches to hide transactions

4. ZK-Rollups are scaling Ethereum by orders of magnitude using validity proofs

5. ZK powers private voting, identity verification, DeFi privacy, and supply chain integrity

**Zero-knowledge proofs are transforming blockchain scalability, privacy, and identity – the future is provable**

**Coming Next: Deep dive into proof system math, circuit design, privacy coin internals, and ZK-rollup architecture**