BLOCKCHAIN TECHNOLOGY

From Cryptographic Foundations to Zero-Knowledge Proofs

A rigorous, math-heavy course on the primitives, protocols, and proof systems that make modern decentralized infrastructure verifiable.

Cryptography | Distributed Systems | Protocol Security | Zero-Knowledge Proofs

1 Course Features and Highlights

- First-principles cryptography: hash functions, Merkle trees, digital signatures, commitments, and randomness.
- Protocol engineering lens: consensus, finality, state machines, smart-contract execution, and adversarial networks.
- Modern ZK coverage: circuits, arithmetization, polynomial commitments, SNARKs, STARKs, recursion, and rollup proofs.
- Security over hype: assumptions, threat models, attack surfaces, proofs, and performance trade-offs.

2 Core Learning Outcomes

- Compose primitives into ledgers, authenticated data structures, and transaction validity.
- Compare proof-of-work, proof-of-stake, BFT-style consensus, and finality under explicit network assumptions.
- Analyze P2P networking, mempools, execution environments, state transitions, and bridges.
- Reason about ZK: completeness, soundness, zero-knowledge, constraints, witnesses, and verification cost.
- Read specifications and research papers, identify hidden assumptions, and evaluate protocol security claims.

3 Research Directions and Application Domains

- ZK systems: efficient proving, recursive composition, zkVMs, proof aggregation, and proof pipelines.
- Privacy-preserving systems: private identity, selective disclosure, anonymous credentials, and confidential transactions.
- Scalable verification: rollups, data availability, verifiable computation, and proof-carrying data.
- Protocol security: MEV, censorship resistance, consensus attacks, bridge failures, and formal verification.
- Cryptographic engineering: secure implementation, audits, benchmarking, and production-grade tooling.

Recommended preparation: discrete mathematics, algorithms, programming maturity, and comfort with formal reasoning.

Focus: rigorous systems, cryptography, and protocol engineering - not token speculation.