

# Common Prefix

[commonprefix.com](http://commonprefix.com)

We are a scientific blockchain Research & Development company. We combine science and engineering, standing in the intersection of theory and application. We partner with and consult popular L1s, L2s, and DeFi protocols.

## Engineering.

- Unapologetically multichain: Experts in Bitcoin, Ethereum, Solana, Sui, Cosmos, Cardano, building on-chain, off-chain, and cross-chain.
- We audit and implement security-critical components, ranging from cryptographic primitives (ZK, MPC, signatures) to L1 consensus and DeFi.
- Senior engineers with decades of experience in systems, hedge funds, tradfi, and web2 before blockchains, web3, and smart contracts.
- Open contributors to Bitcoin core, Ethereum and Arbitrum light clients, Axelar, XRPL, Sui, pod network and more.

## Science.

- PhDs, professors, post-docs from renowned universities: Stanford, U of Edinburgh, U of Vienna, U of Athens, ETH Zurich, ITU Copenhagen, Imperial College London.
- We design, and formally and rigorously prove protocols secure using pen-and-paper cryptographic-style mathematical proofs (“for all adversaries”).
- Expertise: Cryptography (ZK, MPC, FHE, threshold cryptography), consensus (proof-of-work, proof-of-stake), game theory (incentives, economic security), DeFi (AMMs/CFMMs, tokenomics), light clients, interoperability, channels, scalability, sharding.
- Our scientists co-invented proof-of-stake (Ouroboros), bitVM, NIPoPoWs, checkpointing, proof-of-burn.

Past & present paying partners, customers, and grant issuers

