Zirui Xu

Email: zx1651@nyu.edu · GitHub: https://github.com/lbrclbrc · Location: New York, USA (open to remote)

Projects

my_coin – Anonymous-but-Accountable Payment Protocol & Single-Node Blockchain Prototype

Independent project · https://github.com/lbrclbrc/my_coin

- Designed and implemented an experimental cryptocurrency protocol, **my_coin**, that supports ZK-proof-backed anonymous payments while allowing users to use their own private keys to reconstruct the anonymous payment chains they initiated, for fund tracing in theft / scam / extortion cases.
- Introduced a **"blue account"** model: only KYC'd accounts (with on-chain color and identity fields) can initiate anonymous payments; ordinary accounts can only perform transparent transfers.
- Defined fund-flow rules between the public account layer and the anonymous pool:
  - **Public → anonymous**: deposits from an account must create anonymous notes controlled by the same private key as the source account, converting "my public balance" into "my anonymous balance" without transferring ownership.
  - **Anonymous pay**: only allows "old anonymous note → public payment + self-owned anonymous change"; the protocol enforces that the change note uses the same key as the spent note so ownership cannot silently change inside the anonymous pool.
- Specified the zero-knowledge statements for public→anonymous and anonymous-pay operations (well-formed notes, value conservation, correctly derived and non-reusable nullifiers, and change bound to the same secret key), designed ZK module interfaces, and integrated them with Halo2 circuits. Circuit code was written with AI assistance; I focused on what to prove, circuit I/O design, and wiring these modules into the prototype.
- Implemented a single-node blockchain prototype in **Python** (account model, anonymous pool, Poseidon-based Merkle tree, transaction validation, block creation, demo scripts) and ZK proof modules in **Rust + Halo2**, exposed to Python via **pyo3**. Wrote tests to accept valid inputs and reject invalid ones (reused nullifiers, wrong keys, broken value conservation). Built end-to-end demos for blue address application, transparent transfers, deposits into the anonymous pool, anonymous payments with change, and "given a private key, enumerating and tracing related anonymous objects on-chain". Documented the design and prototype in a draft whitepaper.

Skills

Programming Languages

- **Python** – Strongest language; used for prototype development, scripting, testing, and implementing the single-node blockchain logic and demos in *my_coin*.

- **Rust** – Familiar with basic syntax; used to implement ZK proof modules (with documentation and AI assistance), design module interfaces, integrate with the Python prototype via FFI, and write tests. Actively learning and improving.
- **Go** – Familiar with basic syntax and the basic ideas of the concurrency model; using it for small tools and learning projects.
- **C++** – Solid fundamentals; used in coursework and for implementing algorithms / data structures.
- **Solidity** – Self-taught; basic understanding of smart contracts and the EVM execution model.

Applied Cryptography & Blockchain

- **Public-key crypto & signatures** – Understands basic principles of ECC, RSA, digital signatures, and key exchange mechanisms.
- **Hash functions & data structures** – Understands hash functions and Merkle trees; in *my_coin*, used Poseidon hash + Merkle tree as the commitment layer for anonymous notes.
- **Privacy & zero-knowledge proofs** – Worked with a Halo2-based ZK-SNARK framework. Circuit code was produced with AI assistance; my main responsibilities were specifying the statements to prove, designing circuit I/O, integrating Rust modules via pyo3, and testing them in the cryptocurrency prototype. Not yet able to independently hand-write complex Halo2 circuits.
- **Blockchain mechanisms** – Understands basic ideas of PoW, PoS, PoI; studied the principles of the Bitcoin Lightning Network and cross-chain atomic swaps.

Other

- Daily development on **Linux / WSL**; comfortable with **Git / GitHub** workflow.

Education

New York University (NYU) – B.Sc. in Computer Science (in progress)
Expected graduation: May 2027

Relevant Coursework & Self-Study

- **Coursework**: Blockchain and Distributed Ledgers, Algorithms and Data Structures, Probability and Statistics, Computer Systems and Low-Level Programming, etc.
- **Self-study**: Applied cryptography, zero-knowledge proofs (primarily Halo2), anonymous payment protocol design, Layer2 / Rollup and other blockchain scalability / privacy mechanisms.