

Wonjae Choi

BLOCKCHAIN RESEARCHER

Seoul, Republic of Korea

✉ wonjae@snu.ac.kr | 🏠 wonj.eth.limo | 📄 0xwonj | 🌐 wonj | 🐦 0xwonj

"In Trustlessness We Trust."

Education

Seoul National University

Seoul, Korea

PH.D. IN ELECTRICAL AND COMPUTER ENGINEERING

Sep. 2024 - Present

- Virtual Machine & Optimization Lab
- Research Area: Blockchain, Protocol Security, Privacy, ZKP, Compiler

Yonsei University

Seoul, Korea

B.S. IN COMPUTER SCIENCE

Mar. 2020 - Aug. 2024

- Scholarship Granted by Wemade (₩ 5,000,000)

Work Experience

Radius

Seoul, Korea

RESEARCH ENGINEER

Oct. 2024 - Mar. 2025

- Architected and led the development of **Lightbulb**, a TEE-based (Intel TDX) block building framework designed to mitigate censorship and toxic MEV.
- Researched and implemented a private & fair transaction ordering mechanism to ensure end-to-end mempool privacy.
- Integrated Linux Security Modules with Intel TDX to harden the trusted computing base (TCB) for secure block construction.
- Engineered high-performance concurrent systems using Rust and Go, optimizing for low-latency block propagation.

Nethermind

London, UK (Remote)

RESEARCH ENGINEER INTERN

June. 2024 - Sep. 2024

- Designed a **FRI-based Data Availability Sampling (DAS)** scheme as a post-quantum secure alternative to KZG commitments.
- Co-developed the initial prototype of a modular DA layer client based on **Reth**, focusing on the execution engine extensions for blob transactions.
- Conducted deep-dive research on cryptographic primitives for scaling Ethereum's data availability layer.

SNU Virtual Machine & Optimization Lab

Seoul, Korea

UNDERGRADUATE RESEARCH INTERN

Feb. 2024 - Aug. 2024

- Conducted **differential fuzzing** on major Ethereum execution clients (Geth, Nethermind) to identify consensus inconsistencies and EVM edge cases.
- Investigated the mathematical and cryptographic foundations of ZK proof systems.
- Conducted research on compiler optimization techniques, specifically on the **LLVM** framework.
- Analyzed Ethereum Core specifications to improve client robustness and security.

XRPL Korea

Seoul, Korea

BLOCKCHAIN DEVELOPER & DEVREL

June. 2023 - Sep. 2023

- Researched and implemented WASM-based smart contracts (Hooks) on XRPL, optimizing instruction gas usage.
- Developed a DEX protocol with novel AMM features and authored technical documentation for the developer community.

Web3Mon

Seoul, Korea

SMART CONTRACT & BACKEND DEVELOPER

Feb. 2023 - May. 2023

- Developed high-performance Solana programs (smart contracts) using Rust and Anchor framework.
- Researched a virtual state channel implementation for trustless cross-chain asset bridging.

Freelance

Remote

QUANTITATIVE RESEARCH ENGINEER

Oct. 2021 - Jan. 2023

- Engineered a low-latency **MEV arbitrage bot** in Rust, handling large-scale mempool data streams.
- Developed algorithmic trading strategies leveraging ML models, managing a data pipeline for real-time market analysis.

Research

DoS-Resistant Complete Mempool Privacy

Seoul National University

EXTENDED ABSTRACT

Jun. 2025 – Present

- Identifying fundamental DoS vulnerabilities in existing encrypted mempool designs and analyzing their structural limitations.
- Proposing a ZK-based DoS-checking mechanism that prevents adversarial spam while preserving mempool privacy guarantees.
- Introducing a new nullifier construction that avoids premature proof invalidation.
- Currently writing paper for submission to a major security conference (expected early 2026).
- Link: [\[Read Extended Abstract\]](#)

ZK Compiler Infrastructure

Seoul National University

RESEARCH PROPOSAL

2025 – Present

- Designing a proof-agnostic intermediate representation (PIR) for arithmetic representations (R1CS, AIR, Plonkish), enabling unified compilation across diverse ZK proving systems.
- Building a compiler pipeline that treats proving as a compiled workload, targeting CPU/GPU/FPGA backends through automated lowering and optimization.
- Exploring graph-based representations of proving systems to enable TVM/XLA-style autotuning and backend-agnostic performance optimization.
- Link: [\[Read Proposal\]](#)

Projects

zkDungeon

Side & Open Source Project

PROJECT LEAD

Sep. 2025 - Present

- A **fully verifiable on-chain gaming protocol** powered by Zero-Knowledge Proof.
- Designed a ZK-optimized game engine from scratch using FSM architecture and separating static assets from dynamic states by committing static assets into oracle and provide merkle path when needed.
- Developed a **hybrid proof mechanism**: ZKP validates every state transition function, while Optimistic Fraud Proofs secure the computationally expensive NPC AI logic.
- Built with Rust, RISC Zero, SP1, Arkworks, Solidity, Move.
- [Github Link](#)

Honors & Awards

Chainlink Constellation Hackathon

Online

TOP QUALITY PRIZE, BEST USE OF SUBGRAPH

Dec. 2023

- Crosschain Lending Protocol
- Implemented crosschain functionalities with CCIP(crosschain interoperability protocol).
- Used DID, graph, oracle services.

Viction Horizon Hackathon

Online

3RD PRIZE

Dec. 2023

- Delta Neutral Stablecoin using Perpetual DEX.
- Implemented crosschain functionality and used native gas paymaster.

XRPL Summer Hackathon | Ripple

Online

GRAND PRIZE

Aug. 2023

- Implemented concentrated liquidity pool.
- Used XRPL hooks which is a Web Assembly based smart contract on XRP Ledger.

Ethereum Global Tokyo Hackathon

Tokyo, Japan

POLYGON TRACK PRIZE

April. 2023

- Federated learning on public blockchain.
- Implemented p2p AI learning protocol.

Additional Activities

Seoul National University

Seoul, Korea

TEACHING ASSISTANT

Sep. 2024 - Present

- Concepts of Computing and Practice (2025-1)
- Practical Applications of Blockchain (2025-2)
- Compiler Design (2025-2)

Decipher (Blockchain Research Group at SNU)

Seoul, Korea

SENIOR RESEARCHER

Sep. 2023 - Present

- Contributed to the **ERC-6900** reference implementation as part of the Open Source contribution team.
- Oversaw various research initiatives including ZKP/Rollup architectures and economic mechanisms like LVR minimization.
- Co-authored a comprehensive 70-page technical report on Bitcoin Scalability, covering BitVM and Data Availability.
- Awarded the "Best Member Prize" (2024) for outstanding research contributions and community engagement.

Academic Paper Seminar Group (NonSafer)

Seoul, Korea

FOUNDER & ORGANIZER

Feb. 2024 - Present

- Founded and organized a weekly academic seminar group dedicated to reviewing top-tier blockchain, cryptography and security papers.

Blockchain at Yonsei

Seoul, Korea

TECH LEAD & INSTRUCTOR

Sep. 2022 - Aug. 2023

- Designed and lectured a 12-week intensive course on Solidity smart contract development and EVM internal architecture.
- Led technical onboarding sessions, fostering an engineering-driven culture within the student society.
- Conducted research on MEV and made an arbitrage bot using cyclic arbitrage method on DEX.