Lulu Zhou

Email: zhoululu789@gmail.com | **Phone:** (919)-638-1614 | **LinkedIn**

EDUCATION

Yale University *New Haven, CT* Expected Dec 2024

M.A. in Computer Science

Coursework: Operating System (Honor), Secure Decentralized System (Honor), Zero Knowledge Proof (Honor)

Fudan University *Shanghai, China* Sep 2015 - Jun 2020

B.S. in Statistics and Data Science

Coursework: Artificial Intelligence, Data Mining in Finance and Economics, Statistical and Machine Learning, Operations Research, Stochastic Processes, Convex Optimization, Advanced Big Data Analytics, Large-Scale Distributed System, Biostatistics.

Awards: Cargill Global Scholarship 2018; 1st prize in China University Physics Tournament (National Level)

TECHNICAL SKILLS

Methods: Blockchain consensus, Zero-Knowledge proof, Trusted hardware. **Programming:** Python, JavaScript, C.

PROFESSIONAL EXPERIENCE

Graduate Researcher | *Yale University, New Haven, CT* Sep 2022 - Present

- Lead and contribute to projects on Blockchain Consensus, Trusted Hardware, Mechanism Design and Zero-Knowledge proofs, advised by professor Fan Zhang.
- Published papers in *Advances in Financial Technologies (AFT) 2024*, *Science of Blockchain Conference (SBC) 2023* and *USENIX Security Symposium 2024*.

Intern | *Circle, Boston, MA* May 2024 - Aug 2024

- Led the project of Ethereum Fast Confirmation Rule. Provided weekly progress updates to the principal engineer (mentor) and presented the final outcomes to cross-functional teams, receiving high commendations for the project's impact.
- Collaborated with industry experts from a16z, Ethereum Foundation, and Stanford University, incorporating their insights and receiving positive feedback on the approach and outcomes.

Researcher | *Shanghai Qizhi Institute, Shanghai, China* Jun 2020 - Jun 2021

- Contributed to projects about payment channel. Published a paper on payment-channel routing algorithm in *20th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt)*.

Undergraduate Researcher | *Fudan University, Shanghai, China* Jan 2020 - Jun 2020

- Conducted PoW Consensus Attack Analysis by integrating selfish mining and blockchain withholding strategies, utilizing Markov Decision Processes (MDP) for optimal attacker strategy determination.

SELECTED PROJECTS

Ethereum Fast Confirmation Rule | *Blockchain Consensus at Circle* June 2024 - August 2024

- Implemented the Ethereum Fast Confirmation Rule, tested its security and performance using real Ethereum data collected from the Beacon API, and authored blog posts to explain the rule and test results clearly.
- Advanced research and promoted the adoption of the Fast Confirmation Rule, enhancing the security of Ethereum.

ZK Proof Accelerator | *Zero-Knowledge proof, collaborate with Mysten Labs* April 2024 - May 2024

- Modified the snarkjs and ffjavascript packages to implement dynamic caching for ZK-Login.
- Accelerated the MSM process in ZK proof by 15% and reduced the total proof generation time by 3%.

TEE Wallet | *Trusted Hardware, incentives, paper published in AFT 24'* Sep 2021 - May 2024

- Developed a Trusted Execution Environment (TEE)-based wallet for secure secret key management, employing OAuth to ensure an accountable authorization process.
- Enhanced security using insurance and bounty incentives, and evaluated the solution's effectiveness using a MDP model.

Sprints | *Layer1, blockchain consensus* Jan 2021 - Mar 2022

- Developed "Sprints," a blockchain protocol combining PoW and PoD to reduce ecological impact while maintaining security.
- Validated its security through performance testing with patched Bitcoin clients.

Transaction Relay Strategy | *Payment Channel* Jun 2020 - Jun 2021

- Analyzed optimal transaction relaying in Payment Channel Networks (PCNs) using MDP to optimize relay policies.
- Developed an algorithm for optimal relay strategies in PCNs, assessing the impact on network performance.

SERVICE & LEADERSHIP EXPERIENCE

Reviewer | *IEEE Internet of Things Journal*

Sub-reviewer | *33rd USENIX Security Symposium, 44th IEEE Symposium on Security and Privacy, 20th International Conference on Autonomous Agents and Multiagent Systems*

Founder | *Joint-young club in School of Management in Fudan University, for career experience sharing.*

PUBLICATION

- **Lulu Zhou**, Zeyu Liu, Fan Zhang, and Michael K. Reiter. "CrudiTEE: A Stick-and-Carrot Approach to Building Trustworthy Cryptocurrency Wallets with TEEs." Advances in Financial Technologies 2024 (AFT'24).
- Wang, Wenhao, **Lulu Zhou**, Aviv Yaish, Fan Zhang, Ben Fisch, and Benjamin Livshits. "Mechanism Design for ZK-Rollup Prover Markets." arXiv preprint arXiv:2404.06495 (2024).
- Mirkin, Michael, **Lulu Zhou**, Ittay Eyal, and Fan Zhang. "Sprints: Intermittent Blockchain PoW Mining." The Science of Blockchain Conference 2023 (SBC'23).
- Liu, Jiayuan, Canhui Chen, **Lulu Zhou**, and Zhixuan Fang. "Real-Time Recursive Routing in Payment Channel Network: A Bidding-based Design." In 2022 20th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt), pp. 193-200. IEEE, 2022.