Kaihua Qin

kaihua@qin.ac https://qin.ac

Academic Interests

My academic interests center around designing and building decentralized systems that are secure, stable, and incentive-compatible. The inherent complexity of real-world decentralized systems, with their interdependent and interacting layers, poses a fascinating challenge in achieving this objective. My primary focus is on permissionless blockchains and decentralized finance (DeFi).

In my research, I aim to systematically measure and quantify various problems encountered in the rapidly evolving blockchain and DeFi ecosystems. I also strive to develop real-time offensive and defensive solutions by utilizing advanced program analysis techniques to enhance smart contract security. Furthermore, I intend to devise innovative financial primitives that minimize the systemic risks of DeFi. My research is informed by the fields of security, program analysis, measurement, and finance. I am also actively exploring the application of machine learning and game theory to my research pursuits.

Education

Imperial College London *London, United Kingdom*
PhD in Computer Science 2019 – Present
- Centre for Cryptocurrency Research and Engineering.
- Advisor: Dr. Arthur Gervais.

Imperial College London *London, United Kingdom*
MSc in Communications and Signal Processing (with distinction) 2014 – 2015
- Advisor: Dr. Wei Dai.

Southeast University *Nanjing, China*
BE in Information Engineering 2010 – 2014
- GPA 87 (top 15%).
- Mitsubishi Electric Scholarship, Excellent Award in Innovation Practice, and numerous course scholarships.

Work Experience

University of California, Berkeley
Visiting Researcher 2022.05 – 2022.08
- Host: Prof. Dawn Song

Chainlink Labs *Remote*
Research Intern 2022.02 – 2022.05
- Working on order-fairness protocols.

Cisco *Shanghai, China*
Software Engineer 2016 – 2018
- Responsible for the high-availability features of the cBR-8 and Remote PHY Device product lines.

Publications

Peer-Reviewed

Security'23 The Blockchain Imitation Game. **Kaihua Qin**, Stefanos Chaliasos, Liyi Zhou, Benjamin Livshits, Dawn Song, and Arthur Gervais. *USENIX Security Symposium*. 2023.

FC'23 Mitigating Decentralized Finance Liquidations with Reversible Call Options. **Kaihua Qin**, Jens Ernstberger, Liyi Zhou, Philipp Jovanovic, and Arthur Gervais. *International Conference on Financial Cryptography and Data Security (FC)*. 2023.

WWW'23 On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy. Zhipeng Wang, Stefanos Chaliasos, **Kaihua Qin**, Liyi Zhou, Lifeng Gao, Pascal Berrang, Ben Livshits, and Arthur Gervais. *The Web Conference (WWW)*. 2023.

S&P'23 SoK: Decentralized Finance (DeFi) Attacks. Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, **Kaihua Qin**, Roger Wattenhofer, Dawn Song, and Arthur Gervais. *IEEE Symposium on Security and Privacy (S&P)*. 2023.

FC'22 Speculative Multipliers on DeFi: Quantifying On-Chain Leverage Risks. Zhipeng Wang, **Kaihua Qin**, Duc Vu Minh, and Arthur Gervais. *International Conference on Financial Cryptography and Data Security (FC)*. 2022.

S&P'22 Quantifying Blockchain Extractable Value: How dark is the forest?. **Kaihua Qin**, Liyi Zhou, and Arthur Gervais. *IEEE Symposium on Security and Privacy (S&P)*. 2022.

IMC'21 An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities. **Kaihua Qin**, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. *ACM Internet Measurement Conference (IMC)*. 2021.

CVC'21 CeFi vs. DeFi – Comparing Centralized to Decentralized Finance. **Kaihua Qin***, Liyi Zhou*, Yaroslav Afonin, Ludovico Lazzaretti, and Arthur Gervais (*equal contributions). *Crypto Valley Conference on Blockchain Technology (CVCBT)*. 2021.

S&P'21 On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols. Liyi Zhou, **Kaihua Qin**, Benjamin Livshits, and Arthur Gervais. *IEEE Symposium on Security and Privacy (S&P)*. 2021.

S&P'21 High-Frequency Trading on Decentralized On-Chain Exchanges. Liyi Zhou, **Kaihua Qin**, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. *IEEE Symposium on Security and Privacy (S&P)*. 2021.

FC'21 Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit. **Kaihua Qin**, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. *International Conference on Financial Cryptography and Data Security (FC)*. 2021.

S&B'20 FileBounty: Fair Data Exchange. Simon Janin*, **Kaihua Qin***, Akaki Mamageishvili, and Arthur Gervais (*equal contributions). *IEEE Security and Privacy on the Blockchain (S&B)*. 2020.

CVC'19 Applying Private Information Retrieval to Lightweight Bitcoin Clients. **Kaihua Qin**, Henryk Hadass, Arthur Gervais, and Joel Reardon. *Crypto Valley Conference on Blockchain Technology (CVCBT)*. 2019.

Preprint

- A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. Liyi Zhou, **Kaihua Qin**, and Arthur Gervais. *arXiv preprint arXiv:2106.07371*. 2021.

Report

- An Overview of Blockchain Scalability, Interoperability and Sustainability. **Kaihua Qin** and Arthur Gervais. *EU Blockchain Observatory & Forum.* 2018.

Teaching Experience

Decentralized Finance (*Voluntary Teaching Assistant*) — MOOC
by Dan Boneh, Arthur Gervais, Andrew Miller, Christine Parlour, and Dawn Song — *Autumn'21, Autumn'22*

Decentralized Finance (*Teaching Assistant*) — Imperial College London
by Arthur Gervais — *Spring'22*

Principles of Distributed Ledgers (*Teaching Assistant*) — Imperial College London
by Arthur Gervais — *Spring'20, Spring'21, Spring'22*

Awards and Scholarships

Ph.D. Scholarship	Full Scholarship	2019 – 2022
Meta PhD Research Fellowship	Finalist	2022
AlphaMEV Competition	Ranked the 4th	2021
Scaling Bitcoin Workshop	Subsidy	2019
Mathematical Contest in Modeling	Honorable Mention	2013
National Undergraduate Electronic Design Contest	First Prize	2013

Talks

Quantifying Blockchain Extractable Value: How dark is the forest?
- DRK Lab Web3 Young Scholars Program — 2023/03/09
- University of Surrey — 2022/06/17
- VISA Research — 2022/02/11

An Empirical Study of DeFi Liquidations: Incentives, Risks, and Instabilities
- ACM Internet Measurement Conference — 2021/11/03

DeFi Security
- Blockchain Technology and Cybersecurity Lab at the University of Guelph hosted by Prof. Xiaodong Lin — 2021/10/30

CeFi vs. DeFi – Comparing Centralized to Decentralized Finance
- Crypto Valley Conference on Blockchain Technology — 2021/10/29

On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols
- IEEE Symposium on Security and Privacy — 2021/05/25

Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit
- Theory and Practice of Blockchains — 2021/05/19
- International Conference on Financial Cryptography and Data Security — 2021/03/01
- Open Blockchain – Workshop Series — 2020/06/05

FileBounty: Fair Data Exchange
- IEEE Security & Privacy on the Blockchain — 2020/09/07

Applying Private Information Retrieval to Lightweight Bitcoin Clients
- Crypto Valley Conference on Blockchain Technology 2019/06/25

Projects

SwapSwap https://swapswap.org/
SwapSwap is the first automated arbitrage market maker. Its mission is to promote the decentralized nature of blockchains. By automatically executing optimal routing and arbitrage while swapping crypto-assets, it can save up to an average of 90% on transaction fees. SwapSwap also helps mitigate miner extractable value competition and, as a result, strengthens blockchain consensus security.

Blockchain Workbench https://blockchainworkbench.com
I design, implement, and maintain Blockchain Workbench, a blockchain online learning platform. This platform is designed to provide beginners with fundamental knowledge of blockchains and interactive solidity (the most popular language for developing smart contracts) programming exercises. Notably, Blockchain Workbench has been adopted as the primary solidity educational platform for blockchain and DeFi courses at prestigious institutions such as Imperial College London and ETH Zurich.

Academic Services

- **PC member:** DeFi ('21, '22), CESC ('22)
- **Invited reviewer:** ICIS ('22), IEEE Transactions on Information Forensics and Security, Future Generation Computer Systems, Financial Innovation, Electronic Commerce Research
- **Sub-reviewer:** WWW ('21), WINE ('22)
- **External reviewer:** S&P ('21, '22, '23), CCS ('21, '22), Usenix Security ('21, '22), NDSS ('21, '22, '23), FC ('20, '21, '22, '23), AFT ('21, '22)

Skills

Languages	Chinese – Native Speaker, English – Fluent
Programming	Advanced in Go, Python, C/C++, Familiar with in Javascript, Rust
Operating Systems	Linux, macOS, Windows