

KAIHUA QIN

✉ kaihua@qin.ac 🌐 <https://qin.ac>

ACADEMIC INTERESTS

My academic interests center around building secure, stable, and incentive-compatible decentralized systems, with an emphasis on permissionless blockchains and decentralized finance. The foundation of my research draws upon diverse disciplines, including information security, program analysis, measurement, machine learning, game theory, and finance.

EDUCATION

- | | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Imperial College London
<i>PhD in Computer Science</i>
• Advisor: Dr. Arthur Gervais . | <i>London, United Kingdom</i>
2019 – 2024 |
| Imperial College London
<i>MSc in Communications and Signal Processing</i>
(with distinction)
• Advisor: Dr. Wei Dai . | <i>London, United Kingdom</i>
2014 – 2015 |
| Southeast University
<i>BE in Information Engineering</i>
• GPA 87 (top 15%).
• Mitsubishi Electric Scholarship, Excellent Award in Innovation Practice, and numerous course scholarships. | <i>Nanjing, China</i>
2010 – 2014 |

ACADEMIC APPOINTMENTS

- | | |
|--------------------------------------------------------------------------------------------------------|-------------------|
| Yale University
<i>Affiliated Researcher</i>
• Host: Prof. Fan Zhang and Prof. Zhong Shao | 2024.02 – Present |
| University of California, Berkeley
<i>Visiting Researcher</i>
• Host: Prof. Dawn Song | 2022.05 – 2022.08 |

INDUSTRY EXPERIENCE

- | | |
|-----------------------------------------------------------------------------------------------------------|----------------------------------|
| Decentralized Intelligence
<i>Co-founder</i>
• https://d23e.ch | Switzerland
2022.12 – Present |
| Chainlink Labs
<i>Research Intern</i>
• Working on order-fairness protocols | 2022.02 – 2022.05 |
| Cisco
<i>Software Engineer</i> | Shanghai, China
2016 – 2018 |


TEACHING EXPERIENCE

Cryptocurrencies <i>Guest Lecturer</i>	University College London <i>Autumn'23</i>
Introduction to Blockchains, Cryptocurrencies, and Smart contracts <i>Guest Lecturer</i>	Yale University <i>Autumn'23</i>
Decentralized Finance <i>Voluntary Teaching Assistant</i>	MOOC by Stanford, UCL, UIUC, and UC Berkeley <i>Autumn'21, Autumn'22</i>
Decentralized Finance <i>Teaching Assistant</i>	Imperial College London <i>Spring'22</i>
Principles of Distributed Ledgers <i>Teaching Assistant</i>	Imperial College London <i>Spring'20, Spring'21, Spring'22</i>

PUBLICATIONS

Peer-Reviewed

- Security'24** [Speculative Denial-of-Service Attacks in Ethereum](#). Aviv Yaish, **Kaihua Qin**, Liyi Zhou, Aviv Zohar, Arthur Gervais. *USENIX Security Symposium*. 2024.
- WWW'24** [Blockchain Censorship](#). Anton Wahrstätter, Jens Ernstberger, Aviv Yaish, Liyi Zhou, **Kaihua Qin**, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, Mikolaj Barczentewicz, Arthur Gervais. *The Web Conference (WWW)*. 2024.
- Security'23** [The Blockchain Imitation Game](#). **Kaihua Qin**, Stefanos Chaliasos, Liyi Zhou, Benjamin Livshits, Dawn Song, and Arthur Gervais. *USENIX Security Symposium*. 2023.
 Also presented at the Science of Blockchain Conference 2023 (SBC'23)
- 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.
 Also presented at the Science of Blockchain Conference 2022 (SBC'22)
- 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.
 Also presented at the Science of Blockchain Conference 2022 (SBC'22) and the Crypto Economics Security Conference 2022 (CESC'22)
 [Normalized Top-100 Security Papers](#)
 [Cybersecurity Award 2023 – Best Practical Paper](#)

- 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.
- 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.
 Also presented at the Science of Blockchain Conference 2022 (SBC'22)
- 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

- [Do you still need a manual smart contract audit?](#). Isaac David, Liyi Zhou, **Kaihua Qin**, Dawn Song, Lorenzo Cavallaro, Arthur Gervais. 2023.
- [What Drives the \(In\)stability of a Stablecoin?](#). Yujin Kwon, Kornrapat Pongmala, **Kaihua Qin**, Arian Klages-Mundt, Philipp Jovanovic, Christine Parlour, Arthur Gervais, Dawn Song. 2023.
- [Suboptimality in DeFi](#). Aviv Yaish, Maya Dotan, **Kaihua Qin**, Aviv Zohar, Arthur Gervais. 2023.
- [Time to Bribe: Measuring Block Construction Market](#). Anton Wahrstätter, Liyi Zhou, **Kaihua Qin**, Davor Svetinovic, Arthur Gervais. 2023.
- [Towards Automated Security Analysis of Smart Contracts based on Execution Property Graph](#). **Kaihua Qin***, Zhe Ye*, Zhun Wang, Weilin Li, Liyi Zhou, Chao Zhang, Dawn Song, Arthur Gervais (*equal contributions). 2023.
- [Blockchain Large Language Models](#). Yu Gai*, Liyi Zhou*, **Kaihua Qin**, Dawn Song, Arthur Gervais (*equal contributions). 2023.
- [A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges](#). Liyi Zhou, **Kaihua Qin**, and Arthur Gervais. 2021.

Report

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

GRANTS

- [The Latest in DeFi Research](#) — 30K USD
Fellowship on stablecoin research
- [Ethereum Foundation Academic Grant 2023](#) — 50K USD
Dynamic Analysis Framework for EVM (Project leader)
- [Ethereum Foundation Academic Grant 2023](#) — 72K USD
Denial-of-Service Implications of Blockchain Censorship (Contributor)
- [Ethereum Foundation Academic Grant 2023](#) — 25K USD
Blockchain Censorship — Quantitative Analysis of Censorship on Public Blockchains (Contributor)

AWARDS AND SCHOLARSHIPS

Financial Cryptography and Data Security 2023	Student Grant	2023
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

The Blockchain Imitation Game

- [Blockchain@X-OMI Workshop on Blockchain and Decentralized Finance](#) 2023/09/21
- [The Science of Blockchain Conference](#) 2023/08/28
- [USENIX Security Symposium](#) 2023/08/10
- Hong Kong University of Science and Technology (Guangzhou) 2023/04/20

SoK: Decentralized Finance (DeFi) Attacks

- [IEEE Symposium on Security and Privacy](#) 2023/05/24

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 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

ACADEMIC SERVICES

Co-Chair

ACM Workshop on Decentralized Finance and Security (DeFi '23)

Program Committee

The international conference on Advances in Financial Technologies (AFT '24)

ACM Conference on Computer and Communications Security (CCS '24)

International Conference on Financial Cryptography and Data Security (FC '24)

ACM Workshop on Decentralized Finance and Security (DeFi '22, '21)

Crypto Economics Security Conference (CESC '22)

Reviewer

ACM CHI conference on Human Factors in Computing Systems (CHI '24)

IEEE International Conference on Distributed Computing Systems (ICDCS '23)

The Conference on Web and Internet Economics (WINE '22)

International Conference on Information Systems (ICIS '22)

The Web Conference (WWW '21)

[IEEE Transactions on Information Forensics and Security](#)

[IEEE Transactions on Dependable and Secure Computing](#)

[Future Generation Computer Systems](#)

[Financial Innovation](#)

[Electronic Commerce Research](#)

External Reviewer

IEEE Symposium on Security and Privacy (S&P '23, '22, '21),

ACM Conference on Computer and Communications Security (CCS '23, '22, '21)

USENIX Security Symposium (Security '22, '21)

The Network and Distributed System Security Symposium (NDSS '23, '22, '21)

International Conference on Financial Cryptography and Data Security (FC '23, '22, '21, '20)

The international conference on Advances in Financial Technologies (AFT '23, '22, '21)