Kaihua Qin

E-mail: kaihua@qin.ac Homepage: https://qin.ac

CURRENT POSITIONS

Assistant Professor September 2025 – present
Department of Computer Science
University of Warwick

Co-founder December 2022 – present
Decentralized Intelligence AG
https://d23e.ch

EDUCATION

PhD in Computer Science 2019 – 2024
Imperial College London London, United Kingdom
Advisor: Prof. Arthur Gervais
Thesis: Blockchain and Decentralized Finance Security: Incentives, Attacks, and Mitigations

MSc in Communications and Signal Processing 2014 – 2015
Imperial College London London, United Kingdom

BE in Information Engineering 2010 – 2014
Southeast University Nanjing, China

RESEARCH

I work at the intersection of information security, distributed computing, and AI, developing methods to make decentralized systems, such as blockchains, secure, trustworthy, and incentive-compatible. My research spans distributed systems, confidential computing, applied cryptography, and game theory, and applies AI to analyze, protect, and optimize these systems.

I am also interested in the security of AI, focusing on how to keep machine learning models and AI-driven systems robust against adversarial manipulation, privacy breaches, and other emerging threats.

At the heart of my work is a clear goal: to transform rigorous academic research into practical tools and insights that strengthen the digital infrastructure on which society increasingly depends.

GRANTS

- Grants Innosuisse Start-Up Innovation Project (703K CHF) 2024 - 2026
  AI-Enhanced Smart Contract Auditing
- Ethereum Foundation Academic Grant (55K USD) 2024
  Training an EVM-native Generative Pre-trained Transformer
- The Latest in DeFi Research (30K USD) 2024
  Fellowship on stablecoin research

- Ethereum Foundation Academic Grant (50K USD) 2023
  Dynamic Analysis Framework for EVM
- Ethereum Foundation Academic Grant (72K USD) 2023
  Denial-of-Service Implications of Blockchain Censorship
- Ethereum Foundation Academic Grant (25K USD) 2023
  Blockchain Censorship — Quantitative Analysis of Censorship on Public Blockchains

PUBLICATIONS AND PREPRINTS

Bibliometrics from Google Scholar: citations = 2,496, h-index = 20, i10-index = 23 (as of September 2025).

28. **Qin, Kaihua**, Zhe Ye, Zhun Wang, Weilin Li, Liyi Zhou, Chao Zhang, Dawn Song, and Arthur Gervais. "Enhancing Smart Contract Security Analysis with Execution Property Graphs". *Proceedings of the ACM on Software Engineering* 2, no. ISSTA (2025): 1101–1122.

27. Guan, Maggie Yongqi, Yaman Yu, Tanusree Sharma, Molly Zhuangtong Huang, **Kaihua Qin**, Yang Wang, and Kanye Ye Wang. "Security Perceptions of Users in Stablecoins: Advantages and Risks within the Cryptocurrency Ecosystem". In *2025 IEEE Symposium on Security and Privacy (SP)*, 2753–2771. IEEE, 2025.

26. Yang, Sen, **Kaihua Qin**, Aviv Yaish, and Fan Zhang. "Insecurity Through Obscurity: Veiled Vulnerabilities in Closed-Source Contracts". *arXiv preprint arXiv:2504.13398* (2025).

25. Tsuchiya, Taro, Liyi Zhou, **Kaihua Qin**, Arthur Gervais, and Nicolas Christin. "Blockchain Amplification Attack". *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 9, no. 1 (2025): 1–30.

24. Potter, Yujin, Kornrapat Pongmala, **Kaihua Qin**, Ariah Klages-Mundt, Philipp Jovanovic, Christine Parlour, Arthur Gervais, and Dawn Song. "What Drives the (In) stability of a Stablecoin?" In *2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 316–324. IEEE, 2024.

23. Wahrstätter, Anton, Jens Ernstberger, Aviv Yaish, Liyi Zhou, **Kaihua Qin**, Taro Tsuchiya, Sebastian Steinhorst, Davor Svetinovic, Nicolas Christin, and Mikolaj Barczentewicz. "Blockchain censorship". In *Proceedings of the ACM Web Conference 2024*, 1632–1643. 2024.

22. Gan, Rundong, Liyi Zhou, Le Wang, **Kaihua Qin**, and Xiaodong Lin. "Defialigner: Leveraging symbolic analysis and large language models for inconsistency detection in decentralized finance". In *6th Conference on Advances in Financial Technologies (AFT 2024)*, 7–1. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2024.

21. Yaish, Aviv, **Kaihua Qin**, Liyi Zhou, Aviv Zohar, and Arthur Gervais. "Speculative {Denial-of-Service} Attacks In Ethereum". In *33rd USENIX security symposium (USENIX Security 24)*, 3531–3548. 2024.

20. David, Isaac, Liyi Zhou, **Kaihua Qin**, Dawn Song, Lorenzo Cavallaro, and Arthur Gervais. "Do you still need a manual smart contract audit?" *arXiv preprint arXiv:2306.12338* (2023).

19. Wahrstätter, Anton, Liyi Zhou, **Kaihua Qin**, Davor Svetinovic, and Arthur Gervais. "Time to bribe: Measuring block construction market". *arXiv preprint arXiv:2305.16468* (2023).

18. Zhou, Liyi, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, **Kaihua Qin**, Roger Wattenhofer, Dawn Song, and Arthur Gervais. "Sok: Decentralized finance (defi) attacks". In *2023 IEEE Symposium on Security and Privacy (SP)*, 2444–2461. IEEE, 2023.

17. Feng, Ding, Rupert Hitsch, **Kaihua Qin**, Arthur Gervais, Roger Wattenhofer, Yaxing Yao, and Ye Wang. "Defi auditing: Mechanisms, effectiveness, and user perceptions". In *International Conference on Financial Cryptography and Data Security*, 320–336. Springer, 2023.

16. Wang, Zhipeng, Stefanos Chaliasos, **Kaihua Qin**, Liyi Zhou, Lifeng Gao, Pascal Berrang, Benjamin Livshits, and Arthur Gervais. "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy". In *Proceedings of the ACM Web Conference 2023*, 2022–2032. 2023.

15. Gai, Yu, Liyi Zhou, **Kaihua Qin**, Dawn Song, and Arthur Gervais. "Blockchain large language models". *arXiv preprint arXiv:2304.12749* (2023).

14. Raun, Christoffer, Benjamin Estermann, Liyi Zhou, **Kaihua Qin**, Roger Wattenhofer, Arthur Gervais, and Ye Wang. "Leveraging machine learning for bidding strategies in miner extractable value (mev) auctions". *Cryptology ePrint Archive* (2023).

13. Yaish, Aviv, Maya Dotan, **Kaihua Qin**, Aviv Zohar, and Arthur Gervais. "Suboptimality in defi". *Cryptology ePrint Archive* (2023).

12. **Qin, Kaihua**, Stefanos Chaliasos, Liyi Zhou, Benjamin Livshits, Dawn Song, and Arthur Gervais. "The blockchain imitation game". In *32nd USENIX Security Symposium (USENIX Security 23)*, 3961–3978. 2023.

11. **Qin, Kaihua**, Jens Ernstberger, Liyi Zhou, Philipp Jovanovic, and Arthur Gervais. "Mitigating decentralized finance liquidations with reversible call options". In *International Conference on Financial Cryptography and Data Security*, 344–362. Springer, 2023.

10. Wang, Zhipeng, **Kaihua Qin**, Duc Vu Minh, and Arthur Gervais. "Speculative multipliers on defi: Quantifying on-chain leverage risks". In *International Conference on Financial Cryptography and Data Security*, 38–56. Springer, 2022.

9. **Qin, Kaihua**, Liyi Zhou, and Arthur Gervais. "Quantifying blockchain extractable value: How dark is the forest?" In *2022 IEEE Symposium on Security and Privacy (SP)*, 198–214. IEEE, 2022.

8. **Qin, Kaihua**, Liyi Zhou, Pablo Gamito, Philipp Jovanovic, and Arthur Gervais. "An empirical study of defi liquidations: Incentives, risks, and instabilities". In *Proceedings of the 21st ACM internet measurement conference*, 336–350. 2021.

7. Zhou, Liyi, **Kaihua Qin**, Antoine Cully, Benjamin Livshits, and Arthur Gervais. "On the just-in-time discovery of profit-generating transactions in defi protocols". In *2021 IEEE Symposium on Security and Privacy (SP)*, 919–936. IEEE, 2021.

6. Zhou, Liyi, **Kaihua Qin**, Christof Ferreira Torres, Duc V Le, and Arthur Gervais. "High-frequency trading on decentralized on-chain exchanges". In *2021 IEEE Symposium on Security and Privacy (SP)*, 428–445. IEEE, 2021.

5. **Qin, Kaihua**, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti, and Arthur Gervais. "CeFi vs. DeFi–Comparing Centralized to Decentralized Finance". *arXiv preprint arXiv:2106.08157* (2021).

4. Zhou, Liyi, **Kaihua Qin**, and Arthur Gervais. "A2mm: Mitigating frontrunning, transaction reordering and consensus instability in decentralized exchanges". *arXiv preprint arXiv:2106.07371* (2021).

3. **Qin, Kaihua**, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. "Attacking the defi ecosystem with flash loans for fun and profit". In *International conference on financial cryptography and data security*, 3–32. Springer, 2021.

2. Janin, Simon, **Kaihua Qin**, Akaki Mamageishvili, and Arthur Gervais. "Filebounty: Fair data exchange". In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 357–366. IEEE, 2020.

1. **Qin, Kaihua**, Henryk Hadass, Arthur Gervais, and Joel Reardon. "Applying private information retrieval to lightweight bitcoin clients". In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 60–72. IEEE, 2019.

PROFESSIONAL SERVICES

Program Committee Chairs

- ACM CCS Workshop on Decentralized Finance and Security 2024 (co-chair with Liyi Zhou)
- ACM CCS Workshop on Decentralized Finance and Security 2023 (co-chair with Fan Zhang)

Program Committee Members

- ACM Conference on Computer and Communications Security (CCS '24, '25, '26)
- IEEE Symposium on Security and Privacy (S&P '25)
- USENIX Security Symposium (Security '25)
- The Network and Distributed System Security Symposium (NDSS '25, '26)
- IEEE European Symposium on Security and Privacy (EuroS&P '25)
- International Conference on Financial Cryptography and Data Security (FC '24, '25, '26)
- The international conference on Advances in Financial Technologies (AFT '24, '25)
- IEEE International Conference on Blockchain and Cryptocurrency (ICBC '25)
- ACM Workshop on Decentralized Finance and Security (DeFi '22, '21)
- Crypto Economics Security Conference (CESC '22)

Reviewer

- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- ACM Transactions on Software Engineering and Methodology (TOSEM)
- ACM Transactions on the Web (TWEB)
- Distributed Ledger Technologies: Research and Practice (DLT)
- Future Generation Computer Systems
- Financial Innovation
- Electronic Commerce Research

- 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)

EXPERIENCE

Affiliated Researcher February 2024 – August 2025
Yale University
Host: Prof. Fan Zhang and Prof. Zhong Shao

Visiting Researcher May 2022 – August 2022
University of California, Berkeley
Host: Prof. Dawn Song

Research Intern February 2022 – April 2022
Chainlink Labs

Software Engineer March 2016 – August 2018
Cisco

Updated September 2025