RUNCHAO HAN

20 Exhibition Walk, Clayton VIC 3800, Australia
runchao.han@monash.edu ◇ https://runchao.rocks

EMPLOYMENT

BabylonChain Inc. July 2022 - Now
Senior Research Engineer *Melbourne, Australia*

Bytom Blockchain September 2018 - January 2019
Intern Blockchain Engineer *Hangzhou, China*

CNIC, Chinese Academy of Sciences June 2017 - July 2017
Intern Researcher *Beijing, China*

EDUCATION

Monash University and CSIRO's Data61 *February 2019 - September 2022*
Doctor of Philosophy Supervisors: Jiangshan Yu, Joseph Liu and Shiping Chen
Department of Software Systems and Cybersecurity

The University of Manchester *August 2017 - September 2018*
MSc Advanced Computer Science (with Distinction) Supervisor: Christos Kotselidis
School of Computer Science Overall Percentage: 82/100

Beijing University of Posts and Telecommunications *September 2013 - July 2017*
BSc E-Commerce Engineering with Law Overall Percentage: 83/100

RESEARCH AND IMPACT

I'm broadly interested in distributed systems security. My current research focuses on designing secure and scalable Blockchains and decentralised protocols (e.g., Decentralised Randomness Beacon). My research applies techniques from Cryptography and Distributed Computing.

My research has led to real-world impacts and media coverage. For example,

- I invented RandChain [HYL20], a new family of Decentralised Randomness Beacon protocols that are simple, secure and scalable. This research is featured in VDF Research and was presented at Decrypto seminar series.
- My paper analysing *shard allocation* (a key component and a missing abstraction in sharded blockchains) [HYZ22] is selected as "Paper of the Week" (Issue #68) by ZK Capital.
- I studied two overlooked 51% attacks on PoW-based blockchains [HSY+20]. Three large-scale 51% attacks on Ethereum Classic (1,2,3) happened within a month are likely to be our analysed attacks.
- I identified and formalised an overlooked design flaw of the Atomic Swap protocol [HLY19]. The flaw allows the swap initiator to arbitrage, making the protocol unfair. Our proposed fixes are standardised as an Ethereum Improvement Proposal (EIP-2266). This research is covered by CryptoNews and Monash University, and was presented at Peep an EIP series #23.
- I conducted the first performance analysis on memory-hard mining algorithms [HFK19]. This research is nominated for the best paper at ISPASS'19 and is covered by Horizon Globex.

PUBLICATIONS

Full publication list can be found at DBLP and Google Scholar. All of my papers are available online, and most of them are hosted on IACR ePrint.

HYL+20 On the Security and Performance of Blockchain Sharding. Runchao Han, Jiangshan Yu, Haoyu Lin, Shiping Chen, Paulo Esteves-Veríssimo. **In submission**.

HYL20 RandChain: Decentralised Randomness Beacon from Sequential Proof-of-Work. Runchao Han, Jiangshan Yu, Haoyu Lin. **In submission**.

HYZ22 Analysing and Improving Shard Allocation Protocols for Sharded Blockchains. Runchao Han, Jiangshan Yu, Ren Zhang. The 4th ACM Conference on Advances in Financial Technologies (AFT'22).

HHD+22 Reputation-based state machine replication. Muhong Huang, Runchao Han, Zhiqiang Du, Yanfang Fu, and Liangxin Liu. The 21th IEEE International Symposium on Network Computing and Applications (NCA 2022).

NGH+22 Crystal: Enhancing Blockchain Mining Transparency with Quorum Certificate. Jianyu Niu, Fangyu Gai, Runchao Han, Ren Zhang, Yinqian Zhang, Chen Feng. IEEE Transactions on Dependable and Secure Computing (TDSC'22)

LHY20 General Congestion Attack on HTLC-Based Payment Channel Networks. Zhichun Lu, Runchao Han, Jiangshan Yu. The 3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics'21).

HSY+20 Fact and Fiction: Challenging the honest majority assumption of permissionless blockchains. Runchao Han, Zhimei Sui, Jiangshan Yu, Joseph Liu, Shiping Chen. The 16th ACM ASIA Conference on Computer and Communications Security (AsiaCCS'21).

HYL20a VRF-based mining: Simple Non-outsourceable Cryptocurrency Mining. Runchao Han, Haoyu Lin, Jiangshan Yu. The 4th International Workshop on Cryptocurrencies and Blockchain Technology, in conjunction with the 25th European Symposium on Research in Computer Security (CBT@ESORICS'20).

HLY19 On the optionality and fairness of Atomic Swaps. Runchao Han, Haoyu Lin, Jiangshan Yu. The 1st ACM Conference on Advances in Financial Technologies (AFT'19).

HFK19 Demystifying Crypto Mining: Performance Analysis and Optimizations of PoW Algorithms. Runchao Han, Nikolaos Foutris, Christos Kotselidis. IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS'19, best paper nominee).

HSGX19 On the performance of distributed ledgers for internet of things. Runchao Han, Gary Shapiro, Vincent Gramoli, Xiwei Xu. Internet of Things; Engineering Cyber Physical Human Systems (Elsevier IoT'19).

HYLZ18 Evaluating CryptoNote-Style Blockchains. Runchao Han, Jiangshan Yu, Joseph Liu, Peng Zhang. International Conference on Information Security and Cryptology (Inscrypt'18).

HGX18 Evaluating Blockchains for IoT. Runchao Han, Vincent Gramoli, Xiwei Xu. The 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS'18).

TALKS

- Analysing and Improving Shard Allocation Protocols for Sharded Blockchains. AFT conference talk. September, 2022.
- Fact and Fiction: Challenging the honest majority assumption of permissionless blockchains. AsiaCCS conference talk. June, 2021.

- RandChain: Decentralised Randomness Beacon from Sequential Proof-of-Work.
  - Seminar at Nervos Foundation. June, 2022.
  - Seminar at Decrypto. November, 2020.
- VRF-Based Mining: Simple Non-Outsourceable Cryptocurrency Mining. CBT@ESORICS workshop. September, 2020.
- Demystifying Crypto-Mining: Analysis and Optimizations of Memory-Hard PoW Algorithms. Seminar at Huawei Noah's Ark Lab. July, 2020.
- On the optionality and fairness of Atomic Swaps.
  - Peep an EIP #23: EIP-2266. February, 2021.
  - AFT conference at Zurich. October, 2019.

TEACHING

- Teaching associate for FIT 5214 Blockchain, Monash University. 2019 Fall.

PROFESSIONAL SERVICES

(External) reviewer

- 2022: EuroS&P, IEEE Blockchain, Journal of Network and Systems Management, ACM DLT Journal, IEEE Transaction of Service Computing
- 2021: DSN, ICBC, IEEE Blockchain, NSS, MSN, TrustCom, IEEE Trans. of Service Computing
- 2020: AFT, ICDCS, SRDS, ACNS, AsiaCCS, TrustCom, ACISP, ICBC, TDSC, The Computer Journal, IEEE IoT Journal, IEEE Software Journal, IEEE Trans. of Service Computing
- 2019: Indocrypt, TrustCom, Future Generation Computing System

ADDITIONAL INFORMATION

Membership	ACM (student), IEEE (student), USENIX, IACR
LinkedIn	runchao-han
Github	SebastianElvis
Wechat	elvisage
References	Available upon request