RUNCHAO HAN

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

EDUCATION

Monash University and CSIRO-Data61 *February 2019 - Present*
Doctor of Philosophy Supervisors: Jiangshan Yu, Joseph Liu and Shiping Chen
Faculty of Information Technology and Distributed Systems Security group

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 system security. I'm currently focusing 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.
- My paper analysing *shard allocation* (a key component and a missing abstraction in sharded blockchains) [HYZ20] is selected as "Paper of the Week" (Issue #68) by ZK Capital.
- I study 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 identify and formalise 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 included in the Ethereum Improvement Proposals (EIP-2266). This research is covered by CryptoNews.
- I conduct the first performance analysis on memory-hard cryptocurrency mining algorithms [HFK19]. This research is covered by Horizon Globex.

SELECTED PUBLICATIONS

Full publication list can be found at https://dblp.org/pers/hd/h/Han:Runchao. All of my papers are available online, and most of them are hosted on IACR ePrint.

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

HYZ20 Analysing and Improving Shard Allocation Protocols for Sharded Blockchains. Runchao Han, Jiangshan Yu, Ren Zhang. **In submission**.

HSY+20 Challenging the honest majority assumption of permissionless blockchains. Runchao Han, Zhimei Sui, Jiangshan Yu, Joseph Liu, Shiping Chen. **In submission**.

HLY19 On the optionality and fairness of Atomic Swaps. Runchao Han, Haoyu Lin, Jiangshan Yu. 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**.

TALKS

- VRF-Based Mining: Simple Non-Outsourceable Cryptocurrency Mining. CBT workshop, virtual. September, 2020.
- Demystifying Crypto-Mining: Analysis and Optimizations of Memory-Hard PoW Algorithms. Virtual seminar at Huawei Noah's Ark Lab. July, 2020.
- Scaling blockchains via sharding. Confirmation seminar at Monash University. March, 2020.
- On the optionality and fairness of Atomic Swaps. AFT conference presentation at Zurich. October, 2019.

TEACHING

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

PROFESSIONAL SERVICES

External reviewer

- 2020: AFT, ICDCS, SRDS, ACNS, AsiaCCS, TrustCom, ACISP, ICBC, TDSC, The Computer Journal, IEEE IoT Journal, IEEE Software Journal, IEEE Transaction of Service Computing
- 2019: Indocrypt, TrustCom, Future Generation Computing System

WORK EXPERIENCE

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

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

ADDITIONAL INFORMATION

Github	SebastianElvis
Wechat	elvisage
References	Available upon request