UNIVERSITY OF TECHNOLOGY SYDNEY
Faculty of Engineering and Information Technology

Blockchain Meets IoT: What Needs To Be Addressed

by

Guangsheng Yu

A Thesis Submitted
in Partial Fulfillment of the
Requirements for the Degree

Doctor of Philosophy

Sydney, Australia

2021

Certificate of Authorship/Originality

I, Guangsheng Yu declare that this thesis, is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney. This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. I certify that the work in this thesis has not been previously submitted for a degree nor has it been submitted as a part of the requirements for other degree except as fully acknowledged within the text. This research is supported by the Australia Government Research Training Program.

Signatures: Production Note:
Signature removed prior to publication.

Date: May 31, 2021

Dedication

To my parents Jiuhong Yu and Lixian Wang, and my wife, Aiyun Luo, for their endless support and love.

To my supervisors, for the academic guidance.

To my friends, for their encouragement.

Acknowledgements

Foremost, I would like to express my sincere gratitude to my supervisor Prof. J. Andrew Zhang and Prof. Ren Ping Liu for the continuous support of my Ph. D study and research, for their patience, motivation, enthusiasm, and immense knowledge. My deepest thanks also goes to Dr. Wei Ni in CSIRO. Their guidance helped me in all the time of research and writing of this thesis. My research would have been impossible without their support and supervision.

My sincere thanks also goes to Dr. Xu Wang and Dr. Kan Yu, for their encouragement, insightful comments, and hard questions. A very special gratitude goes out to my mates Xuan Zha, Ping Yu, and Lizhang Tianyi, for the stimulating discussions, for the sleepless nights we were working together before deadlines, and for all the awesome time with you guys. I would also like to thank everyone in GBDTC, UTS, and UCOT Australia who supported me along the way.

Last but not least, many thanks goes to my family: my parents Jiuhong Yu and Lixian Wang, and my wife, Aiyun Luo, for supporting me spiritually throughout my life.

Guangsheng Yu

Sydney, Australia, 2021

List of Publications

Published Journal Papers

J-1. **G. Yu**, X. Zha, X. Wang, W. Ni, K. Yu, P. Yu, J. A. Zhang, R. P. Liu and Y. J. Guo, "Enabling Attribute Revocation for Fine-Grained Access Control in Blockchain-IoT Systems," *IEEE Transactions on Engineering Management*, pp. 1-20, Feb, 2020.

J-2. **G. Yu**, X. Wang, K. Yu, W. Ni, J. A. Zhang and R. P. Liu, "Survey: Sharding in Blockchains," *IEEE Access*, vol. 8, pp. 14155-14181, Jan, 2020.

J-3. **G. Yu**, X. Zha, X. Wang, W. Ni, K. Yu, J. A. Zhang and R. P. Liu, "A Unified Analytical Model for Proof-of-X Schemes," *Elsevier Computers & Security*, Jun, 2020.

J-4. **G. Yu**, L. Zhang, X. Wang, K. Yu, W. Ni, J. A. Zhang and R. P. Liu, "A Novel Dual-Blockchained Structure for Contract-Theoretic LoRa-based Information Systems," *Elsevier Information Processing and Management*, Jan, 2021.

J-5. X. Wang, **G. Yu**, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, K. Zheng and X. Niu, "Capacity of Blockchain based Internet-of-Things: Testbed and Analysis," *Elsevier Internet of Things*, vol. 8, Dec, 2019.

Published Conference Papers

C-1. **G. Yu**, X. Wang, X. Zha, J. A. Zhang and R. P. Liu, "An Optimized Round-Robin Scheduling of Speakers for Peers-to-Peers-based Byzantine Faulty Tolerance," *Proc. IEEE Globecom Workshops*, 2018.

C-2. X. Wang, X. Zha, **G. Yu**, W. Ni, R. P. Liu, Y. J. Guo, X. Niu and K. Zheng, "Attack and Defence of Ethereum Remote APIs," *Proc. IEEE Globecom Workshops*, 2018.

C-3. X. Wang, P. Yu, **G. Yu**, X. Zha, W. Ni, R. P. Liu and Y. J. Guo, "A High-Performance Hybrid Blockchain System for Traceable IoT Applications," *Network and System Security, 13th International Conference*, Dec, 2019.

Submitted Papers

C-1. X. Wang, **G. Yu**, R. P. Liu, et al, "Blockchain-Enabled Fish Provenance and Quality Tracking System," *IEEE Internet of Things Journal*.

C-2. P. Yu, W. Ni, **G. Yu**, H, Zhang, R. P. Liu and Q. Wen, "Efficient Anonymous Data Authentication for Vehicular Ad-Hoc Networks," *Hindawi Security and Communication Networks*.

C-3. X. Wang, W. Ni, X. Zha, **G. Yu**, R. P. Liu, N. Georgalas and A. Reeves, "Capacity Analysis of Public Blockchain," *Elsevier Computers & Security*.

ABSTRACT

Blockchain Meets IoT: What Needs To Be Addressed

by

Guangsheng Yu

The connection between Blockchain and Internet of Things (IoT) has no longer been futuristic. However, the research of Blockchain-based IoT is challenging. The traditional Blockchain technologies become gradually incapable of satisfying the growing market of IoT networks, and demand for significant improvements. This research proposes a variety of novel approaches, aiming to point out and address the key challenges from different aspects, i.e., consensus algorithms, Blockchain scalability, privacy/access control, and integration of the system.

The main contributions of this thesis are summarized as follows.

- This thesis proposes a Markov model explicitly capturing the weighted resource distribution of Proof-of-X (PoX) schemes in large-scale networks and unifying the analysis of different PoX schemes. The new model leads to the development of three new unified metrics for the evaluation, namely, *Resource Sensitivity*, *System Convergence*, and *Resource Fairness*, accounting for security, stability, and fairness, respectively. The generality and applicability of our model are validated by simulations in the context of the proposed metrics.

- This thesis proposes detailed comparison and quantitative evaluation of major Blockchain-based sharding mechanisms in a systematic and comprehensive way. Specifically, the contents include our insights analyzing the features and restrictions of the existing solutions. We also provide theoretical upper-bound of the throughput for each considered sharding mechanism. The remaining challenges and future research directions are also reviewed.

- This thesis proposes a new Blockchain-based IoT system which is compatible with attribute-based encryption (ABE) technique, and fine-grained access control is implemented with the attribute update enabled by integrating Chameleon Hash (CH) algorithms into the Blockchains. We design, and implement a new verification scheme over, a multi-layer Blockchain architecture to guarantee the tamper-resistance against malicious and abusive tampering. We also provide analysis and simulations showing that our system outperforms other solutions in terms of overhead, searching complexity, security, and compatibility.

- This thesis proposes a novel Dual-Blockchain-based Long Range (LoRa) system providing global cross-validated security, as a case study of integration between Blockchain and IoT. The rational behaviours of participators, the state-of-the-art contract-theoretic incentive mechanism, and the newly designed flow control protocol, can be secured by the tamper-resistance of Blockchains. Being part of the proposed incentive mechanism, the self-driven flow control scales both the Dual-Chain system and the LoRa network. We provide analysis and simulations showing that the system motivates the self-deployed LoRa Gateways in a more secure way, thus optimize the utilization of coverage while improving the Blockchain scalability and flexibility.

Contents

List of Figures

List of Tables

Abbreviation

ABE: Attribute-based encryption

BFT: Byzantine Fault Tolerance

BGP: Byzantine Generals Problem

BW: Bandwidth

CH: Chameleon Hash

CoSi: Collective signing

CR: Code rate

CP-ABE: Ciphertext-policy ABE

DAG: Directed acyclic graph

DDoS: Distributed Denial of Service

GHOST: Greedy Heaviest Observed Subtree

IC: Incentive Compatibility

IoT: Internet of Things

IR: Individual Rationality

KP-ABE: Key-policy ABE

MPT: Merkle Patricia Tree

LoRa: Long Range

LPWAN: Low-Power Wide-Area Network

NB-IoT: Narrowband IoT

NFV: Network-Function-Virtualization

NGN: Next Generation Network

P2P: Peer-to-peer

PBFT: Practical BFT

PoW: Proof-of-Work

PoS: Proof-of-Stake

PoTO: Proof-of-Task-Overhead

PoX: Proof-of-X

PVSS: Publicly verifiable secret sharing

SDN: Software-Defined-Network

SF: Spreading factor

SPOF: Single point of failure

SPV: Simple Payment Verification

TTN: The Things Network

UTXO: Unspent transaction output

VANETs: Vehicular ad hoc networks

VRF: Verifiable Random Function

VDF: Verifiable Delay Function

WAN: Wide area network