

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.

Production Note:

Signatures: Signature removed prior to publication.

Date: May 31, 2021

© Copyright 2021 Guangsheng Yu

Dedication

To my parents Jihong 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 Jihong 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

Certificate	ii
Dedication	iii
Acknowledgments	iv
List of Publications	v
Abstract	vii
List of Figures	xv
List of Tables	xx
Abbreviation	xxi
1 Introduction	1
1.1 Background	2
1.1.1 Overview of IoT	2
1.1.2 Overview of Blockchains	6
1.1.2.1 Decentralization and the Byzantine Generals Problem	6
1.1.2.2 Blockchain as a solution	7
1.1.3 Blockchain-based IoT: benefits and challenges	8
1.1.3.1 Benefits	8
1.1.3.2 Challenges	8
1.2 Research Objectives	10
1.3 Thesis Organization	13

2 Literature Survey	16
2.1 Analytical Models for PoX Consensus Algorithms	16
2.2 Scale-out Solutions	17
2.3 Fine-grained Access Control	20
2.4 Blockchain-based LoRa networks: A case study	22
2.5 Chapter Conclusion	23
3 A Unified analytical model for Proof-of-X schemes	24
3.1 Introduction	24
3.2 Preliminary	27
3.2.1 Bitcoin's Security Model	27
3.2.2 PoX-based Consensus Algorithms	27
3.3 New Infinite-Dimensional Markov Chain Model for PoX Schemes	30
3.3.1 Overview	30
3.3.2 System Model - Small-slotted mechanism	31
3.3.3 The Proposed Analytical Model	33
3.3.3.1 The infinite-dimensional Markov chain	34
3.3.3.2 The per-miner-per-slot mining probability $f_{i,h}$	37
3.3.3.3 Steady-state probability	38
3.3.3.4 Relation between the total per-slot mining probability R and the per-slot mining probability of an individual node $f_{i,h}$	40
3.3.3.5 Generalization of $\mathcal{P}_{i,\gamma}^{win}$	41
3.3.4 Proposed Evaluation Metrics	42
3.3.4.1 Resource sensitivity	43

3.3.4.2	System convergence	44
3.3.4.3	Resource fairness	45
3.4	Consideration on Network Setting	46
3.4.1	Sparse Blockchain Networks	46
3.4.2	Large-scale Blockchain Networks	47
3.5	Simulation and Evaluation	48
3.5.1	Framework	48
3.5.2	Simulation Result	50
3.5.2.1	Accuracy of the proposed model - margin of error	50
3.5.2.2	Resource sensitivity	54
3.5.2.3	System convergence	55
3.5.2.4	Resource fairness	58
3.5.2.5	Summary	59
3.6	Conclusions	59
4	Scaling-out Blockchains with Sharding	61
4.1	Introduction	61
4.2	Intra-Consensus Protocol	64
4.2.1	Nakamoto-based - Monoxide - Chu-ko-nu mining	67
4.2.2	BFT-based - Elastico	68
4.2.3	BFT-based - Chainspace	69
4.2.4	BFT-based - OmniLedger	70
4.2.5	BFT-based - RapidChain	72
4.2.6	BFT-based PoS - Ethereum 2.0	73
4.3	Atomicity of Cross-Shard	75

4.3.1	Monoxide - Relay Transactions	76
4.3.2	Elastico - No cross-shard Transactions	78
4.3.3	OmniLedger - Atomix Protocol	78
4.3.4	RapidChain - Three-way Confirmation	79
4.3.5	Ethereum 2.0 - Using Receipts	81
4.3.6	Chainspace - The inter-part of S-BAC	82
4.4	General Improvements	82
4.4.1	Reducing Transaction Latency	84
4.4.2	Inter-Communication Protocol	85
4.4.3	Shards Ledger Pruning	86
4.4.4	Decentralized Bootstrapping	87
4.4.5	Securing the Epoch Reconfiguration	87
4.4.6	Sharded Smart Contract	89
4.4.7	Replay Attacks and Defenses against Cross-shard Protocols	89
4.5	Challenges and Future Trend	91
4.5.0.1	Future Trend for Reducing the Overhead	94
4.5.0.2	Future Trend for Strengthening the Security and	
	Atomicity	95
4.6	Conclusions	97
5 Enabling Attribute Revocation for Fine-grained Access		
Control in Blockchain-IoT Systems		99
5.1	Introduction	99
5.2	Preliminary	102
5.2.1	Attribute-based Encryption	102

5.2.2	Chameleon Hash (CH) Algorithm	103
5.3	Multi-layer Blockchain-IoT System with Redactable Key Chain	104
5.3.1	System Overview	104
5.3.2	The Proposed Multi-layer Blockchain System	107
5.3.3	New Design of Redactable Key Chain	110
5.3.3.1	Block Structure	111
5.3.3.2	Block Generation and Verification	115
5.3.4	New Design of Inter-Chain Protocol	117
5.3.4.1	Protocol of Message Encryption and Publication	118
5.3.4.2	Protocol of Message Decryption and Retrieval	120
5.3.4.3	Protocol of Attribute Updates on a Key Chain	123
5.4	Analysis and Evaluation	126
5.4.1	System Analysis	126
5.4.1.1	Energy Overhead	126
5.4.1.2	Scalability and Compatibility	130
5.4.2	Security Analysis	137
5.5	Conclusions	139
6	A Novel Dual-Blockchained Structure for Contract-Theoretic	
	LoRa Networks	141
6.1	Introduction	141
6.2	System Model	143
6.2.1	Dual-Chain Structure and Cross-Validation	148
6.2.2	Flow Control Protocol in a self-driven way	155
6.2.2.1	Congested LoRa Gateways	156

6.2.2.2	Incentive allocation	158
6.2.2.3	Cross-validation of Flow Control	159
6.2.3	Practical Implementation of the Incentive Mechanism	159
6.2.3.1	Uploading data size in LoRa Gateways	161
6.2.3.2	Utility of LoRa Controllers	162
6.2.3.3	Utility of LoRa Gateways	163
6.2.3.4	Interaction between Dual-Chain to secure incentive	164
6.3	Simulation and Discussion	165
6.3.1	Security Analysis	169
6.3.1.1	Dual-Chain Structure: Why Splitting Functions?	169
6.3.1.2	Dual-Chain Structure: The Performance Gap	170
6.3.1.3	PoTO Protocol: The Improved Spam Protection	171
6.4	Conclusions	173
7	Contributions and Future Work	174
7.1	Contributions	174
7.2	Future Work	177
	Bibliography	179

List of Figures

1.1 The system architecture shows that Blockchain-based networks can	
be built on top of cloud-based platforms.	9
1.2 Research targets, key research point, and chapters.	11
3.1 The small-slotted mechanism divides a round into multiple slots.	
The number of slots contained in a round is subject to the expected	
value of the block period T .	33
3.2 The state transition of the proposed infinite-dimensional Markov	
chain at Node- i . $f_{i,h}$ is denoted as f_h for simplicity.	34
3.3 $\pi(h)$ of the outlier with a Pareto distributed system resource for	
coinage-based PoS and Non-Fairness-oriented PoS-Velocity	
respectively, where $N = 10$, $H = 5$, $\alpha = \frac{1}{2H \sum \omega_i}$. An invalid $\pi(H)$	
that is negative appears when $h = H$.	51
3.4 The line plots are with respect to the blue axis on the left-hand side,	
while the bar plots are with respect to the upside-down red axis on	
the right-hand side. The margin of error with the growth of the	
resource ratio owned by an arbitrary miner that is the outlier, where	
$N = 10$, $H = 5$, $\alpha = \frac{1}{2H \sum \omega_i}$, in terms of both S and $ARSQ$. Here,	
the system resource is Pareto distributed. Note that the ratio is the	
system resource ratio that a specific outlier miner owns.	52

3.5	The line plots are with respect to the blue axis on the left-hand side, while the bar plots are with respect to the upside-down red axis on the right-hand side. The margin of error with the growth of $\frac{t}{T}$, where $N = 10, H = 5, \alpha = \frac{1}{2H \sum \omega_i}$, in terms of both S and $ARSQ$. Here, the system resource is Pareto distributed with the ratio of the amount of system resource owned by a specific outlier miner is 33%.	53
3.6	The correlation between the resource ratio and the average block probability \mathcal{P} , where $N = 20, H = 10, \alpha = \frac{1}{2H \sum \omega_i}$.	56
3.7	The comparison among the four different PoX schemes in terms of <i>System Convergence</i> , where $N = 10, H = 5, \alpha = \frac{1}{2H \sum \omega_i}$.	57
4.1	The sharding technology partitions the network into different groups, while each of the groups maintains its own ledger and processes and stores a disjoint set of transactions. By implementing a secure cross-shard communication protocol, such disjoint transaction sets that could not have been interacted become securely verifiable and interactively executable in parallel. Note that, nodes in some sharding mechanisms (e.g., Monoxide) can choose to participate in the processing of multiple shards and maintain their ledgers, as illustrated by the multicolored circles, while the unicolored circles denote the nodes only participating in a single shard to which they are assigned in terms of the color.	62
4.2	(Left) ByzCoin implements a tree with a fixed branching factor and an increasing depth. (Right) ByzCoinX implements a shadow tree with a fixed depth and an increasing branching factor.	70

4.3	(Top) Each committee (shard) maintains a routing table containing $\log_2 n$ other committees. The routing table improves the efficient communication among multiple shards, as described in Section 4.4.2. Committee C_0 can locate C_3 (via C_2) responsible for transactions with prefix $0x11$. (Bottom) To cross-validate a UTXO-based cross-shard transaction requires this transaction to be spilt in three-way confirmation.	79
4.4	The pain points that each of the proposed improvements are expected to solve	83
5.1	This figure illustrates an overview of the proposed system. The bottom-half-side shows the architecture of the network-layer where the hierarchical topology of facilities is specifically described, upon which Blockchains being run among these facilities charged with different roles are described in the top-half-side. The table regarding the allocation of roles describes the relationship between the considered facilities and roles.	105
5.2	The process of encrypting and publishing a new message is shown on the left-hand side. The right-hand side shows the process of decrypting and retrieving a new published message. A Data Publisher (DP) and Data Users (DUs) implement the Inter-chain Protocol to deal with the data encryption/decryption between the <i>Data Chain</i> and <i>Key Chain</i>	107
5.3	The block structure of a block in a <i>Key Chain</i> that stores redactable messages	112
5.4	The scheme of $MPT(h)$ delivers reliable verification for every editing conducted at block height- h , by maintaining an additional MPT dedicated for the logs.	116

5.5 The process of an attribute update is shown. Only the non-revoked DU and new DUs obtain the updated ABE private key, so that they can access to all related data across the *Data Chain*. In contrast, the revoked DU can only access to the history with the outdated ABE private key and updated ciphertext edited by the miners. 123

5.6 The comparison among our three proposed structures and the structure proposed in [154] regarding the storage overhead with respect to H , where $R = K = 1000$. Note that the y-axis denotes the storage complexity. 132

5.7 The comparison among our three proposed structures and that of [154] regarding the overhead with respect to a constant $H = 10000$ and an upper bound of K in two different values of R . Note that the y-axis denotes the storage complexity. 134

5.8 The comparison among our three proposed structures and that of [154] regarding the overhead with respect to a constant $H = 10000$ and an upper bound of R in two different values of K . Note that the y-axis denotes the storage complexity. 135

5.9 The comparison among our proposed structures and that of [154] regarding the searching complexity with respect to H , where $R = K = 1000, C = 1000000$. Note that the y-axis denotes the searching complexity. 136

6.1	The system architecture of the proposed Blockchain-based LoRa system with contract-theoretic incentive mechanism. A star-of-stars network is established between end-devices and a LoRa Gateway, and LoRa Gateways and a LoRa Controller. A group of controllers constitute a committee and maintain a Dual-Chain structure, i.e., the ID Chain providing registration and monitoring service, and Data DAG providing data storage service. Each controller as a task publisher collects data from its corresponding gateways and pays incentives. Such behaviors are included in a DAG block to be injected to the Data DAG, and cross-validated by other controllers.	. 144
6.2	The flow chart of practical implementation of the contract-theoretic incentive mechanism to relieve the information asymmetry 165
6.3	(Left) The trajectory of the overall scoring along with the increasing number of LoRa Gateways changed by a LoRa Controller. (Right) The trajectory of the overall scoring along with the increasing percentage of the overlapping coverage area among gateways. 167

List of Tables

3.1	Expressions of (non-)Fairness-oriented PoX schemes	29
3.2	Parameters of the analytical model	32
4.1	A comparison regarding the protocols (ranged from the settings of intra-consensus to the design of cross-shard atomicity, as well as the corresponding overhead) among the discussed sharding mechanisms in this chapter is elaborated.	92
4.2	A comparison among the discussed sharding mechanisms in this chapter is elaborated. The results of throughput and cost are shown in [205]. The latency is also obtained and shown (N/A: Not Available).	93
5.1	Notation Definition	102
5.2	It shows the computation overhead and performance comparison between different types of Raspberry Pi with a security level of 80 bits under 30 attributes (the last column shows the performance of 4B with a 128-bit security level under 30 attributes); $C = 10,000\text{mAh}$, $V = 3.3\text{V}$ and 5V . We focus on the cryptographic operations. The typical AES scheme proposed in [51] with pipelining is used to encrypt (and protect the confidentiality of) conversation keys. We consider the widely accepted CP-ABE scheme [27] which is part of AndrABEn, an open source ABE library particularly optimized for Android/smartphone/IoT operating systems. The ABE library has been adopted in many existing studies, e.g., [11, 12].	129

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