Fangyu Gai

Résumé

✉ fangyu.gai@ubc.ca
https://fangyugai.me/
gitferry

Educational Background

2018

Ph.D., *University of British Columbia*, Vancouver and Kelowna, Canada, research on the general area of blockchain technology, mainly focusing on BFT consensus protocols and layer-2 scaling of blockchain systems.

2015 2017

Master of Science, *National University of Defense Technology*, Changsha, China, major in Computer Science and Technology.
Thesis: Research on Trust Management for Internet of Things

2011 2015

Bachelor of Science, *Beijing Institute of Technology*, Beijing, China, major in Information Security.
Thesis: Enhance Adaboost Algorithm by Integrating LDA Topic Model

Research Interests

- Distributed Systems
- Consensus Protocols
- Blockchain

Research Experience

2020

Dissecting the Performance of BFT SMR in the Era of Blockchain, *June 2020 - present*.

Description A framework that provides an apple-to-apple comparison for state-of-the-art chained BFT SMR. HotStuff introduced chained framework into BFT SMR and classified into two categories, two-chain protocols (PBFT, Tendermint, Casper), three-chain protocols (HotStuff, LibraBFT), according to their commit rule. These protocols have different safety rules (voting, commit) and liveness rules and therefore, should have varying performance under different conditions, especially under performance-failure attacks. This gives us a chance to build a general framework to easily implement these protocols using the same primitives, only leaving safety rules and liveness rules for developers.

Funding Agency Natural Sciences and Engineering Research Council of Canada (NSERC).

Project website `https://github.com/gitferry/bamboo`

2019 2020

Rethinking Byzantine Fault Tolerant (BFT) Protocols in the Age of Blockchains, *June 2019 - December 2019*.

Description This is a joint research project with our industrial partner Dapper Labs. In this proposed research, we aim to develop such a framework together with Dapper Labs. As a starting point, we made use of HotStuff, which provides an algorithmic foundation for describing several new-generation BFT protocols such as Tendermint and Casper. In particular, we combined HotStuff with a realistic network model based on our previous work. This combination enabled us to analyze the throughput and delay performance of various BFT protocols. Finally, lessons learned from this research contributed to the consensus component of Dapper Labs's Flow Blockchain.

Funding Agency Natural Sciences and Engineering Research Council of Canada (NSERC).

Project website `https://www.onflow.org/`

2019 – 2020 **Research and implementation on Layer 2 scaling of blockchain systems**.

Role Group leader.

Description Sidechains enable off-chain scaling by sending transactions in a private network rather than broadcasting them in the public blockchain (i.e., the mainchain) network. To this end, classic Byzantine fault-tolerant (BFT) consensus protocols such as PBFT seem a good fit to fuel sidechains for their permissioned settings and inherent robustness. This project is to propose Cumulus, a novel BFT-based sidechain framework for blockchains to achieve off-chain scaling without compromising any security and efficiency properties of the consensus protocols of both sides. Cumulus encompasses a novel cryptographic sortition algorithm called Proof-of-Wait to fairly select sidechain nodes to communicate with the mainchain in an efficient and decentralized manner. To further reduce the operational cost, Cumulus provides an optimistic checkpointing approach in which checkpoints will not be verified by the mainchain unless disputes happen. Meanwhile, end users enjoy a two-step withdrawal protocol, which ensures that they can safely collect assets back to the mainchain without relying on the BFT committee.

Project website `https://github.com/cumulus-sidechain/cumulus`

2017 – 2018 **Research and implementation on reputation-based consensus protocol**.

Role Group leader.

Description Beyond cryptocurrencies, it is believed that blockchain can also be used to protect other properties such as reputation. This project presents a reputation-based consensus protocol called Proof of Reputation (PoR), which guarantees reliability and integrity of transaction outcomes.

Funding Agency National Science Foundation of China (NSFC).

Project website `https://github.com/gitferry/PoR`

2016 – 2017 **Research on Blockchain based Identity Authentication and data protection for Internet of Things**.

Role Group leader.

Description IoT suffers from potential systemic failures as it scales with disastrous consequences. This project proposes an integrated blockchain and IoT hardware solution to solve IoT's issues with identity, security, and interoperability.

Funding Agency State Scientific and Technological Commission.

Working Experience

Internship

2021 **Research Intern**, *Alibaba DaMo Academy*, Hangzhou, China, Research on building blockchain-based database systems..
Apr. 2021 - Present.

2020 **Research Intern**, *Hyperchain*, Hangzhou, China, Research on enhancing BFT-based consensus algorithms for blockchain systems.
Sep. 2020 - Mar. 2021

2019 **Back-end Engineer (part-time)**, *Dapper Labs Inc.*, Vancouver, Canada, Consensus nodes for Flow blockchain..
Jan. 2020 - Mar. 2020.

2019 **NSERC Research Project**, *Dapper Labs Inc.*, Vancouver, Canada, Rethinking Byzantine Fault Tolerant (BFT) protocols in the age of Blockchains..
Jun. 2019 - Dec. 2019

2014 **Front-end Developer**, *JoyShare Inc.*, Beijing, China, Developed an iOS App named JoyShare, which helps users share their goods online..
Oct. 2013 - Feb. 2014

Teaching Assistant

2019 **ENGR 453 Internet of Things**, *University of British Columbia*, Kelowna, Canada.
SUPERVISOR Prof. Chen Feng

2016 **Cryptography**, *National University of Defense Technology*, Changsha, China.
SUPERVISOR Prof. Xinwen Jiang

Open Source Contributor

2020 **CCF Conference Countdown**, Vancouver, Canada.
Building a website to show countdown of deadlines of CCF recommended conferences.

2018 **Solidity Document Translation**, *HiBlock Inc.*, Beijing, China.
Working as a member of Chinese Solidity document translation team, which is authorized by Solidity team.

Languages

Chinese Native

English Non-Native *Professional Fluency*

Skills

Programming Golang, Python, Solidity, Objective-C, Javascript, C++, Shell LaTeX

Tools Git, Vim, Docker *Program Version Control and Program Repositories.*

Consensus Protocols	Paxos, Raft, PoW, PoS, PBFT, HotStuff, Tendermint, Casper.
Other Skills	Communication, Organization, Writing, Translation

References

1. Gai, F., Niu, J. & Feng, C. Dissecting the Performance of BFT SMR in Blockchain Era. *Accepted to ICDCS, CCF-B conference in the field of distributed systems.* (2021).
2. Jalalzai, M. M., Niu, J., Feng, C. & Gai, F. *Fast-HotStuff: A Fast and Resilient HotStuff Protocol* 2021. arXiv: 2010.11454 [cs.DC].
3. Niu, J., Gai, F., Feng, C. & Jalalzai, M. M. On the Performance of Pipelined HotStuff. *Accepted to INFOCOM 2021, CCF-A conference in the field of networking.* (2021).
4. Niu, J., Gai, F. & Feng, C. Crystal: Enhance Blockchain Mining Transparency with Quorum Certificatef. *Major revision from USENIX SECURITY, CCF-A conference in the field of information security.* (2020).
5. Niu, J., Wang, Z., Gai, F. & Feng, C. Incentive Analysis of Bitcoin-NG, Revisited. *Accepted to IFIP WG 7.3 Performance 2020, CCF-B conference in the field of networking.* (2020).
6. Gai, F., Grajales, C., Niu, J. & Feng, C. A Secure Consensus Protocol for Sidechains. *CoRR.* arXiv: 1906.06490. http://arxiv.org/abs/1906.06490 (2019).
7. Gai, F., Wang, B., Deng, W. & Peng, W. *Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network* in *Database Systems for Advanced Applications - 23rd International Conference, DASFAA 2018, Gold Coast, QLD, Australia, May 21-24, 2018, Proceedings, Part II* (Springer, 2018), 666–681.
8. Li, D., Peng, W., Deng, W. & Gai, F. *A Blockchain-Based Authentication and Security Mechanism for IoT* in *27th International Conference on Computer Communication and Networks, ICCCN 2018, Hangzhou, China, July 30 - August 2, 2018* (IEEE, 2018), 1–6.
9. Liu, D. *et al. Pangr: A Behavior-Based Automatic Vulnerability Detection and Exploitation Framework* in *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering, TrustCom/BigDataSE 2018, New York, NY, USA, August 1-3, 2018* (IEEE, 2018), 705–712.
10. Gai, F., Zhang, J., Zhu, P. & Jiang, X. *Ratee-Based Trust Management System for Internet of Vehicles* in *International Conference on Wireless Algorithms, Systems, and Applications* (2017), 344–355.
11. Gai, F., Zhang, J., Zhu, P. & Jiang, X. *Multidimensional Trust-Based Anomaly Detection System in Internet of Things* in *International Conference on Wireless Algorithms, Systems, and Applications* (2017), 302–313.
12. Gai, F., Zhang, J., Zhu, P. & Jiang, X. Trust on the Ratee: A Trust Management System for Social Internet of Vehicles. *Wirel. Commun. Mob. Comput.* (2017).