（修士課程）
Master’s Program

令和　7　年　1　月　26　日
Date(yymmdd)

教務課　御中
To the Student Division

審査員主査：　Xavier Défago
Chief Examiner

修士論文要旨の提出について

SUBMISSION OF MASTER’S THESIS SUMMARY

このことについて、修士の学位授与が可とされた下記の学生の修士論文要旨１通を、別紙のとおり提出します。
I hereby submit a copy of the Master’s Thesis Summary of the student below who has been approved for conferment of a Master’s Degree.

記

系・コース： Department of,Graduate major in	情報工学 情報工学	系 コース
学籍番号： Student ID Number	23M30508	
学生氏名： Student’s Name	市来優典	

備考　上記の論文には、大学院学則第４３条第２項に規定する特定の課題についての研究の成果を含む。
note　The above thesis includes the result of research on a specific theme noted in clause 2, article 43 of the Institute Regulations.

（修士課程）
Master’s Program

令和　7　年　1　月　26　日

Date(yymmdd)

系・コース： Department of/Graduate major in	情報工学　系 情報工学　コース	審査員主査： Chief Examiner	Xavier Défago
学籍番号： Student ID Number	23M30508	審査員： Examiner	Xavier Défago
学生氏名： Student’s Name	市来優典	審査員： Examiner	渡部卓雄
指導教員（主）： Academic Supervisor(main)	Xavier Défago	審査員： Examiner	鄭顕志
指導教員（副）： Academic Supervisor(sub)		審査員： Examiner	

論文要旨

THESIS SUMMARY

論文題目 Thesis Title	Blockchain Algorithms with Random Committee Selection （ランダムな委員会選出によるブロックチェーンアルゴリズム）

要旨（和文 1000 字程度又は英文 400 語程度）
Thesis Summary(approx.1000 Japanese Characters or approx.400 English Words)

The master’s thesis titled Blockchain Algorithms with Random Committee Selection focuses on addressing the scalability and efficiency challenges of blockchain consensus mechanisms, particularly in distributed systems such as energy trading in microgrids. The work applies enhancements to Byzantine Fault Tolerance (BFT) algorithms using unanimous, random, and unpredictable committee selection mechanisms.

Traditional consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT) face significant scalability and energy efficiency issues as blockchain networks grow in size. Committee-based consensus mechanisms, which involve randomly selecting subsets of nodes to validate transactions, offer an efficient alternative. However, challenges such as ensuring randomness, security against adversarial influence, and maintaining scalability persist.

The proposed solution focuses on the integration of a random beacon mechanism and distributed verifiable random functions (DVRFs) to create a secure, efficient, and unpredictable random committee selection process. The random beacon generates

備考　上記の論文には、大学院学則第４３条第２項に規定する特定の課題についての研究の成果を含む。
note　The above thesis includes the result of research on a specific theme noted in clause 2, article 43 of the Institute Regulations.

cryptographically secure random numbers agreed upon by all nodes, ensuring that committee formation is tamper-resistant and uniformly random. This process dynamically selects two types of committees: proposing committees responsible for block creation and verifying committees tasked with transaction validation and block confirmation. To further enhance efficiency, the system allows for multiple proposers in each round, reducing redundant rounds and improving throughput.

The results of the study shows that the proposed solution significantly improves the performance of BFT-based blockchain systems: PBFT and HotStuff-2, particularly in low-latency environments. Simulations conducted in a decentralized microgrid setting reveal that incorporating random committee selection enhances throughput and reduces latency compared to traditional consensus mechanisms without committee selection. Particularly, the introduction of multiple proposers improves transaction processing rates while maintaining security and fault tolerance. However, the results also highlight limitations in high-latency conditions, where the additional overhead of multiple proposers leads to performance degradation. In addition, we emphasize that it is possible the high-latency network invokes more degression of performance when the algorithm has a large message complexity. These findings underscore the importance of tailoring the solution to network conditions and optimizing parameters like committee size and round timeouts to maximize efficiency and scalability.

This work contributes a foundational framework for scalable, secure, and decentralized blockchain systems, with applications in areas like decentralized finance and energy trading. By addressing the limitations of existing BFT algorithms and application of random committee selection, the thesis sets the stage for future advancements in blockchain scalability and security. The research shows the room for further research into optimizing view-change processes within the committee selection framework.