**Fall 2023 ISEC 885 : Project Overview Report: Research on Asynchronous Consensus Protocols**

Introduction:

The exploratory research for the Fall 2023 ISEC 885 course aims to develop a problem direction for a doctoral research idea concept paper leading to an idea paper. The research will lead to the identification of a problem direction and work toward a problem identification leading to a potential goal of improving some aspect in the field of the asynchronous consensus through the protocol Asynchronous Byzantine Fault Tolerance (ABFT), yet to be determined. ABFT was chosen because it claims to have recent advancements in the fields of asynchronous consensus when comparing its throughput and latency to that of the HoneyBadgerBFT and two DUMBO protocol variations (Knudsen et al., 2021).

Objectives:

*Problem Identification:* Identify and define specific problems within the field of asynchronous consensus through ABFT based on the existing literature.

*Concrete Problem Direction:* Establish a concrete problem direction and established a need that will serve as the foundation for a doctoral research idea concept paper.

*Goal Establishment:* Establish a clear and concise goal for further research, with a focus on improving some aspect of asynchronous consensus through ABFT.

*Literature Review:* Conduct a review of literature, including Knudsen et al. (2021), and the work cited to understand the current state of ABFT and its existing challenges and limitations.

*Experimental Validation:* Explore different experimental setups and network environments to validate the protocol's performance under various conditions and deployments, addressing concerns about external validity.

*Performance Analysis:* Investigate performance-related issues within ABFT, including the Threshold ECDSA Scheme, experimental setup, scalability, and handling network degradation.

*Quantitative Assessment:* Quantify the performance benefits of potential solutions, such as threshold ECDSA signatures, in comparison to previous threshold BLS signatures for efficiency.

*Resource Optimization:* Research methods to reduce computational overhead and explore efficient methods for delegating precomputing to other machines in the ABFT protocol.

*Scalability Improvement:* Develop strategies to make ABFT more scalable, particularly for very large networks or those with a high churn rate.

*Network Degradation Mitigation:* Investigate adaptive strategies to mitigate performance degradation when the number of affected nodes exceeds the fault tolerance threshold.

Current Level of Completion: At this stage, the project is in its early exploratory phase. Literature review and problem identification have been initiated, but specific goals, milestones, and deliverable are yet to be fully defined.

Milestones and Deliverables: The project will progress through the following milestones and deliverables:

* Problem identification and definition
* Concrete problem direction, need, and goal
* Literature review completion
* Experimental setup exploration and validation
* Quantitative assessment and performance analysis
* Threshold ECDSA versus BLS Signatures trade off strategies
* Scalability improvement strategies
* Network degradation mitigation strategies

Current Accomplishments:

* Initiated literature review and identified key problems within ABFT.
* Began the process of defining performance-related challenges and researching potential solutions.

Scheduled Completions:

* Literature review completion by [Q4 2023]
* Finalization of concrete problem direction, need, and goal by [Q4 2023]
* Experimental setup exploration and validation by [Q2 2024]
* Quantitative assessment and performance analysis by [Q4 2024]
* Threshold ECDSA versus BLS Signatures trade off strategies by [Q2 2025]
* Scalability improvement strategies by [Q4 2025]
* Network degradation mitigation strategies by [Q4 2025]

Missed Targets: There are currently no missed targets as the project is still in its early stages.

Issues and Changes: No major issues or changes have arisen thus far. However, adjustments may be made as the project progresses and more insights are gained.

Open Issues:There are no open issues at this time.

Open Change Requests: There are no open change requests at this time.

Next Phase Schedule (Start and Completion Targets): The next phase the “Literature review completion” will involve the detailed investigation into the literature of ABFT and related work. The schedule for this phase is as follows:

* Start Date: [September 2023]
* Completion Target: [November 2023]

Summary: The exploratory research project for the Fall 2023 ISEC 885 course is focused on identifying and addressing critical challenges within the field of asynchronous byzantine fault tolerance specifically through the ABFT protocol. The primary goal is to establish a concrete problem direction, need, and goal that will pave the way for a comprehensive doctoral research idea concept paper. The project is currently in its early stages, with a literature review initiated, and it is poised to delve deeper into performance analysis, scalability, and network degradation mitigation in subsequent phases.