**Fall 2023 ISEC 885: Idea Concept First Draft.**

**Introduction:**

The exploratory research for the Fall 2023 ISEC 885 course aims to 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 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 field of asynchronous consensus when comparing its throughput and latency to that of the HoneyBadgerBFT and two DUMBO protocol variations (Knudsen et al., 2021). While ABFT offers strong guarantees of consensus and fault tolerance, the problem is that it performs poorly in the categories of simplicity, scalability, and performance compared to traditional synchronous consensus protocols. Previous literature has addressed the need for further exploration in the field of asynchronous consensus as being arguably the most appropriate solutions for building high-assurance and intrusion tolerant permissioned blockchain environments, as asynchronous protocols inherently perform more robustly against timing and denial-of-service (DoS) attacks. Especially over unprotected networks such as the internet (Duan et al., 2018).

**Problem:**

The following are problems defined in the ABFT literature.

*Threshold ECDSA Scheme Problem*: In (Knudsen et al., 2021, "Limitation of ABFT," p. 7) it is stated that ABFT does not fully implement the threshold ECDSA scheme and relies on a trusted dealer for precomputing signing material. A problem to address is the need to develop a more secure and efficient method of implementing the full threshold ECDSA scheme within ABFT with out a trusted dealer. There is a need to investigate the performance trade-offs between using threshold ECDSA signatures and the cost of running the precomputing protocol. Further research is needed to quantify the performance benefits of threshold ECDSA signatures versus previous threshold BLS signatures in comparison for efficiency. ABFT mentions the need for additional computational resources to maintain precomputed signing material for each round. Research is needed to focus on reducing the computational overhead of this process and exploring methods to delegate precomputing to other machines efficiently.

*Experimental Setup Problem*: In (Knudsen et al., 2021, "Threats to Validity," p. 7) it is stated that the experimental setup is based on previous related work, which might have limitations in terms of external validity. Research is needed to explore different experimental setups and network environments to validate the protocol's performance under various conditions and deployments.

*Scalability Problem*: In (Knudsen et al., 2021, "Results of RQ1," p. 6) it is highlighted that as the number of nodes in the network increases, the communication overhead grows, which can lead to network congestion with less throughput and increased latency. The scalability problem with ABFT make it less practical for very large networks or networks with a high churn rate. There is a need to develop asynchronous consensus in such a way that ABFT can scale practically.

*Handling Network Degradation Problem*: In (Knudsen et al., 2021, "Results of RQ2," p. 7) it states that ABFT performs well when the number of affected nodes is less than the fault tolerance but has a problem of degrading as the number of affected nodes becomes greater than the fault tolerance, there is need for improving the handling of network degradation growing larger than the fault tolerance. There is a need to explore adaptive strategies to mitigate the harsh performance degradation observed under such conditions.

**Goal:**

The goal of the exploratory research, conducted as part of the Fall 2023 ISEC 885 course, is to establish a problem direction for a doctoral research idea concept paper, which will lead to research idea paper. The goal is centered around the improvement of the field of asynchronous byzantine fault tolerance through the ABFT protocol. The final outcome will be a concrete problem, need, and goal.

## **References**

Duan, S., Reiter, M., & Zhang, H. (2018). BEAT: Asynchronous BFT Made Practical. *In ACM SIGSAC Conference on Computer and Communications Security,* pp. 2028–2041. <https://doi.org/10.1145/3243734.3243812>

Knudsen, H., Li, J., Notland, J., Haro, P., & Ræder, T. (2021). High-Performance Asynchronous Byzantine Fault Tolerance Consensus Protocol. *IEEE International Conference on Blockchain*, pp. 476-483. <https://doi.org/10.1109/Blockchain53845.2021.00073>

Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The Honey Badger of BFT Protocols. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 31–42. <https://doi.org/10.1145/2976749.2978399>