Defending Against Centralization via Asynchronicity  
by  
Eric Brandon Webb  
An assignment submitted in partial fulfillment of the requirements   
for ISEC-700 course as part of the degree of Doctor of Philosophy  
in  
Cybersecurity Management   
College of Computing and Engineering   
Nova Southeastern University   
 ISEC-700 – Research Seminar in Information Security  
Fall 2022  
Professor: Dr. Yair Levy  
Due: Nov 27, 2022  
2022

## **Chapter 1**

**Research Problem**

**Researching the Problem of Centralization**

The research problem that the proposed study will address is how to defend against centralization in blockchain technology with a focus in Asynchronous Byzantine Fault Tolerance (aBFT) protocols. To properly address how to defend against centralization in blockchain, a few key theories need to be discussed. Beginning with a fault tolerance problem proposed by the works of Lamport et al. (1982) called the Byzantine General Problem (BGP). The BGP is argued to be the underlying philosophy behind blockchain theory and is supported by the proposed statement from Kuo et al. (2019) that “The Byzantine general problem is the core problem that consensus algorithms are trying to solve, which is at the heart of the design of blockchains” (p. 1). The research articles on the BGP mentioned above solidify the importance of defending against centralization in blockchain technology because the contents proposed the underlying issues related to consensus algorithms in decentralized distributed systems.

The next theory that needs to be addressed is the Blockchain Trilemma. A reference to the Blockchain Trilemma was stated in the proposed research of Aiyar et al. (2021) that “three important properties of a blockchain system, involving decentralization, security, and scalability, cannot perfectly co-exist” (p. 1).The establishment of the Blockchain Trilemma proposed in the research above is important example of defending against centralization because the research quoted claims that there is no one size fits all answer to blockchain solutions, and that gaining a better position on one side of the Blockchain Trilemma means losing positions on the other side (Aiyar et al., 2021).

The next theory to be discussed is the Fischer Lynch Patterson (FLP) Theorem that states “No completely asynchronous consensus protocol can tolerate even a single unannounced process death”(Fischer et al., 1985, p. 375).The FLP theorem is an important theorem in asynchronous consensus and can be seen referenced in other research articles such as in the proposed works of Kaushal et al. (2017)that states **“**The consensus in a decentralized environment raises serious issues. In literature, there are some impossibility results in distributed consensus like Byzantine’s Generals’ Problem, and Fischer Lynch Paterson impossibility of distributed consensus with one faulty process” (p. 173). The FLP theorem is specifically important to asynchronous consensus protocols because FLP influenced The Honey Badger (HoneyBadgerBFT) protocol’s implementation of atomic broadcasting(Miller et al., 2016, p. 33). The HoneyBadgerBFT protocol is argued in academic research as a breakthrough in practical asynchronous BFT algorithms (Knudsen et al., 2021, p. 476).The FLP theorem from 1985 influencing the conception of the HoneyBadgerBFT in 2016 is important to defending against centralization in blockchain because HoneyBadgerBFT showed that aBFT consensus is starting to be developed in a practical manner (Duan et al., 2018).

The problem of centralization in blockchain is that centralization can create vulnerabilities in the distributed system with the impacts potentially being Denial of Service (DoS) attacks and falsified records(Lin et al., 2021, p. 80). Because of the potential impacts to security mentioned above decentralization is important to defend against vulnerabilities in blockchain systems. The current gap in knowledge being that blockchain systems have high costs and low throughput or can gain advantages in the two categories by giving up decentralization (Jia et al, 2021).The gap is particularly true in aBFT protocols such as the HoneyBadgerBFT that are considered to have a high run time overhead and low scalability (Knudsen et al., 2018).

## **Chapter 2**

**Research Goals**

**Goals of Defending Against Centralization Research**

The main goal of the proposed research paper is to better understand how to defend against the manifestation of centralization in blockchain technology with a focus in asynchronous implementations. The need for the dissertation work is expressed in the following research studies. The first need is the ability to create solutions to the BGP and Blockchain Trilemma. The BGP and Blockchain Trilemma are the underlying architecture arguments to blockchain (Kuo et al., 2019; Aiyar et al., 2021). By addressing the two issues, blockchain can better defend against centralization(Beikverdi and Song, 2015). The dissertation builds upon the BGP and Blockchain Trilemma problems by getting a better understanding of how to solve the two problems with a focus in asynchronicity. The second need for the dissertation work is to build upon and create implementations that argue the FLP theorem. The FLP theorem proposed the issues of consensus with asynchronicity (Fischer et al., 1985). By understanding and addressing the FLP theorem, aBFT consensus algorithms can become more concrete. An example of the FLP problem and the Blockchain Trilemma providing context to aBFT development was supported by the proposed HoneyBadgerBFT protocol (Miller et al., 2016).The next need for the dissertation work is to challenge previous research findings empirical data. HoneyBadgerBFT has been used as a baseline to compare to in aBFT consensus research, such as in the works of the BEAT protocol (Duan et al., 2018)and the ABFT protocol (Knudsen et al., 2021). By validating the findings of previous aBFT empirical research the field of aBFT gets more peer review on the subject matters.

There are a few specific goals outlined in the research dissertation being proposed. The first specific goal is how to address centralization in blockchain with a focus in asynchronous protocols. The second specific goal is to validate previous research data on aBFT. Another specific goal is to expose the short comings of aBFT. The last specific goal is to propose future trends in aBFT relating to decentralization.

The main research question that the study will address is how can asynchronicity defend against centralization? Is the currently researched data validated by other peer reviewed sources? Are the outcomes the same or similar? What are the future trends of aBFT regarding blockchain decentralization in the future? There are a few hypotheses that the proposed study will address. The first being the hypothesis that aBFT is just now being practicalized and that there is nothing implemented well enough to compete with the security of traditional blockchain technologies. Metrics can be measured to argue decentralization such as the Gini coefficient (Kwon et al., 2019), Shannon entropy (Wu et al., 2019), and the Nakamoto coefficient (Lin et al., 2021). The three metrics are popular in the measurement of decentralization as seen in the proposed research of Lin et al. (2021). The next hypothesis that the study will address is that the peer reviewed research on aBFT has conflicting data. The research will validate that other research dealing with aBFT has similar outcomes when comparing baseline data of consensus protocols. The consensus protocols will be judged on the empirical data metrics mentioned above and other metrics such as throughput and latency. Lastly the study will address the hypothesis that future trends in aBFT will become more prevalent in blockchain technology. The prevalence will be quantifiable by researching and validating studies that are continuing to research the problems in aBFT and address the proposed research potential contributions using the metrics listed above to define a one through ten scoring in the three categories of the blockchain Trilemma and the three categories of the Confidentiality, Integrity, and Availability (CIA) triad.

## **References**

Aiyar, K., Halgamuge, M., & Mohammad, A. (2021). Probability Distribution Model to Analyze the Trade-off between Scalability and Security of Sharding-Based Blockchain Networks. *IEEE 18th Annual Consumer Communications & Networking Conference*, pp. 1-6. <https://doi.org/10.1109/CCNC49032.2021.9369563>

Baird, L., & Luykx, A. (2020). The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers. *International Conference on Omni-layer Intelligent Systems*, pp. 1-7. <https://doi.org/10.1109/COINS49042.2020.9191430>

Beikverdi, A., & Song, J. (2015). Trend of centralization in Bitcoin's distributed network. *Proceedings of the 2015* *IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp. 1-6. <https://doi.org/10.1109/SNPD.2015.7176229>

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>

Fischer, M., Lynch, N., & Paterson, M. (1985). Impossibility of Distributed Consensus with One   
Faulty Process. *Journal of the ACM*, pp. 374–382.

Hood, K., Oglio, J., Nesterenko, M., & Sharma, G. (2021). Partitionable Asynchronous Cryptocurrency Blockchain. *IEEE International Conference on Blockchain and Cryptocurrency,* pp. 1-9. https://doi.org/10.1109/ICBC51069.2021.9461080

Jia, Y., Xu, C., Wu, Z., Feng, Z., Chen, Y., & Yang, S. (2022) Measuring Decentralization in Emerging Public Blockchains. *International Wireless Communications and Mobile Computing*, pp. 137-141. <https://doi.org/10.1109/IWCMC55113.2022.9825341>

Kaushal, P., Bagga, A., & Sobti, R. (2017). Evolution of Bitcoin and Security Risk in Bitcoin Wallets. *International Conference on Computer, Communications and Electronics*, pp. 172-177. <https://doi.org/10.1109/COMPTELIX.2017.8003959>

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>

Kuo, P., Chung, H., Chao, T., & Cheng, C. (2020). Fair Byzantine Agreements for Blockchains. *IEEE Access*, pp. 70746-70761. <https://doi.org/10.1109/ACCESS.2020.2986824>

Kwon, Y., Liu, J., Kim, M., Song, D., & Kim, Y. (2019). Impossibility of Full Decentralization in Permissionless Blockchains. *Proceedings of ACM Conference on Advances in Financial Technologies*, pp. 110–123. <https://doi.org/10.1145/3318041.3355463>

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, pp. 382-401.

Lin, Q., Li, C., Zhao, X., & Chen, X. (2021). Measuring Decentralization in Bitcoin and Ethereum using Multiple Metrics and Granularities. *IEEE 37th International Conference on Data Engineering Workshops*, pp. 80-87. <https://doi.org/10.1109/ICDEW53142.2021.00022>

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>

Wu, K., Peng, B., Xie, H., & Huang, Z. (2019). An Information Entropy Method to Quantify the Degrees of Decentralization for Blockchain Systems. *International Conference on Electronics Information and Emergency Communication*, pp. 1–6. <https://doi.org/10.1109/ICEIEC.2019.8784631>

**Certification of Authorship of Doctoral Course Assignment**

A picture containing text, outdoor, sign

Description automatically generated

Submitted to: Dr. Yair Levy

Student’s Name: Eric Webb

Date of Submission: November 27th, 2022

Purpose and Title of Submission: Assignment #2 Pre-Idea Paper “Defending Against Centralization via Asynchronicity.”

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: ERIC WEBB