ISEC-700 Fall 2022

Professor Yair Levy

Eric Webb

Assignment #2 Guidelines for Research Pre-Idea Paper in Cybersecurity

November 27th, 2022

## **Problem Statement**

The research problem that the 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 that fuel the decentralization discussions. 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 (**P. Kuo, 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.” The research articles on the BGP mentioned above are important to defending against centralization in blockchain technology because the contents question underlying issues related to decentralized distributed systems through the BGP.

The next theory that needs to be addressed is the Blockchain Trilemma. A reference to the Blockchain Trilemma is proposed in the works of **(Aiyar, Halgamuge and Mohammad,2021)**  and states that “three important properties of a blockchain system, involving decentralization, security, and scalability, cannot perfectly co-exist.” The establishment of the Blockchain Trilemma asserted in the research above is important to 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, Halgamuge and Mohammad,2021)**

The next theory to be discussed is the Fischer Linch Patterson (FLP) Theorem that states “an asynchronous network where messages may be delayed but not lost, there is no consensus algorithm that is guaranteed to terminate in every execution for all starting conditions, if at least one node may experience failure.” **(Fischer, Lynch, and Paterson, 1985)** The FLP theorem is is an important theorem in decentralization and can be seen referenced in other research articles such as such as in the works **(Kaushal, Bagga, and R. Sobti. 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.” The FLP theorem is specifically important to decentralization of asynchronous blockchain protocols because FLP was the base problem for The Honey Badger (HoneyBadgerBFT) protocol innovating its atomic broadcasting.**(Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. 2016. )** The HoneyBadgerBFT protocol is accepted in academic research as major breakthrough in practical asynchronous BFT algorithms **(Knudsen et al., 2021)** The FLP theorem from 1985 influencing the conception of the HoneyBadgerBFT in 2016 is important to defending against centralization in blockchain because it shows that aBFT is just now starting to be developed and researched in regards to blockchain technology.**(Duan,Reiter, and Zhang, 2018)**

The problem of centralization is blockchain is that it can create vulnerabilities in the distributed system whit the impact potentially being Denial of Service (DoS) attacks and falsified records.**(Q. Lin, C. Li, X. Zhao and X. Chen, 2021)** Because of the potential impact to security mentioned above it is important to defend against centralization in blockchain systems. The current gap in knowledge being that blockchain systems have high costs and low throughput or they gain advantages in those categories by giving up decentralization.**( Y. Jia, C. Xu, Z. Wu, Z. Feng, Y. Chen and S. Yang, )** This is particularly true with aBFT protocols such as the HoneyBadgerBFT that are considered to have a high run time overhead and low scalability **(H. Knudsen, J. Li, J. S. Notland, P. H. Haro and T. B. Ræder)**

**Research Goals**

The main goal of this research paper is to better understand how to defend against the manifestation of centralization in blockchain technology with a focus in asynchronousl 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. These problems are the underlying architecture arguments to blockchain **(BGP ref, and Blockchain Trilemma ref)** By addressing these issues blockchain can better defend against centralization.  **(BTC centralized ref.)** 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 argues the issues of consensus with asynchronicity (**FLP ref) .** By understanding and addressing the FLP theorem issue aBFT blockchain technology becomes stronger and an example of this is supported by the implementation of the HoneyBadgerBFT protocol.**( HoneyBadgerREF)** The next need for this dissertation work is to build on the back of giants in the field of aBFT and to challenge there findings. HoneyBadgerBFT is used as a baseline to compare to in aBFT such as in the works of BEAT(Beat ref) and ABFT (ABFT reference.) By challenging the findings of aBFT proposed research the field of aBFT gets more clarification on the subject matter.

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 newly peer reviewed articles on aBFT to verify contents when comparing to other aBFT protocols. The next specific goal is to expose the short comings of aBFT. The last specific goal is to propose future trends in aBFT as it relates to decentralization..

The main research question that this study will address is how does asynchronicity defend against centralization? Are the current researched empirical data validated by other peer reviewed sources? And what are the future trends of aBFT in regards to blockchain decentralization in the future? There are a few hypotheses that this 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 tradition blockchain technologies. This can be measured using three degrees of decentralization metrics:Gini coefcient **(Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae Kim,2019)**, Shannon entropy **(Keke Wu, Bo Peng, Hua Xie, and Zhen Huang.,2019)**, and Nakamoto coefficient (Balaji S Srinivasan et al. 2019) These metrics are popular in the measurement of decentralization as seen in the research of (**Q. Lin, C. Li, X. Zhao and X. Chen,2019) .** The next hypotheses that this study will address is that the peer reviewed research on aBFT probably has conflicting data. The research will validate that other research dealing with aBFT has similar outcomes when comparing baselines of consensus protocols such as BTC PoW, ETH PoS, HoneyBadgerBFT aBFT, along with others. The consensus protocols will be judged on there empirical data metrics mentioned above and other metrics such as throughput and latency. Lastly the study will address the hypotheses that future trends in aBFT will become more prevalent in blockchain technology. This will be quantifiable by researching and validating studies that are continuing to research the problems in aBFT.

## **References**

**Balaji S Srinivasan et al. Quantifying decentralization. https:**

**//news.earn.com/quantifying-decentalization-e39db233c28e,**

**[Accessed Nov. 2020], 2017.**

Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae

Kim. Impossibility of full decentralization in permissionless

blockchains. In Proceedings of the 1st ACM Conference on

Advances in Financial Technologies, pages 110–123, 2019.

Keke Wu, Bo Peng, Hua Xie, and Zhen Huang. An information

entropy method to quantify the degrees of decentralization for

blockchain systems. In 2019 IEEE 9th International Conference

on Electronics Information and Emergency Communication

(ICEIEC), pages 1–6. IEEE, 2019.

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

P. K. Kaushal, A. Bagga and R. Sobti, "Evolution of bitcoin and security risk in bitcoin wallets," 2017 International Conference on Computer, Communications and Electronics (Comptelix), 2017, pp. 172-177, doi: 10.1109/COMPTELIX.2017.8003959.

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

**Q. Zhou, H. Huang, Z. Zheng and J. Bian, "Solutions to Scalability of Blockchain: A Survey," in IEEE Access, vol. 8, pp. 16440-16455, 2020, doi: 10.1109/ACCESS.2020.2967218.**

**P. Kuo, H. Chung, T. -W. Chao and C. -M. Cheng, "Fair Byzantine Agreements for Blockchains," in IEEE Access, vol. 8, pp. 70746-70761, 2020, doi: 10.1109/ACCESS.2020.2986824.**

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

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

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

L. Lamport, R. Shostak, and M. Pease, ‘‘The Byzantine generals problem,’’  
ACM Trans. Program. Lang. Syst. (TOPLAS), vol. 4, no. 3, pp. 382–401,  
Jul. 1982.

L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM, vol. 4, no. 3, pp. 382-401, 1982.

Yufei Liu, Jiqiang Liu, Jian Wang, Tianhao Liu, and Xudong He. 2021. “BSS-ITS: Blockchain Scaling Scheme with Sharding for Intelligent Transportation System: Scale Blockchain for Better Data Exchange and Storage with Full Sharding for Intelligent Transportation System”. In 2021 4th International Conference on Blockchain Technology and Applications (ICBTA 2021). Association for Computing Machinery, New York, NY, USA, 128–134. <https://doi.org/10.1145/3510487.3510506>

Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

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

X. Yang, Y. Chen and X. Chen, *2019* "Effective Scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information" *IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 261-265, doi: 10.1109/Blockchain.2019.00041.

Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. 2016. “The Honey Badger of BFT Protocols”. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 31–42. <https://doi.org/10.1145/2976749.2978399>

M. J. Fischer, N. A. Lynch, and M. S. Paterson. 1985 “Impossibility of distributed consensus with one faulty process”. Journal of the ACM (JACM), 32(2):374–382, 1985.

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

S. Duan, M. K. Reiter, and H. Zhang. BEAT: asynchronous BFT made  
 practical. In D. Lie, M. Mannan, M. Backes, and X. Wang, editors,  
 Proceedings of the 2018 ACM SIGSAC Conference on Computer and  
 Communications Security, CCS 2018, Toronto, ON, Canada, October  
 15-19, 2018, pages 2028–2041. ACM, 2018.

C. Cachin and J. A. Poritz, "Secure INtrusion-Tolerant Replication on the Internet," *Proceedings International Conference on Dependable Systems and Networks*, 2002, pp. 167-176, doi: 10.1109/DSN.2002.1028897.

S. Müller, A. Penzkofer, N. Polyanskii, J. Theis, W. Sanders and H. Moog, "Tangle 2.0 Leaderless Nakamoto Consensus on the Heaviest DAG," in IEEE Access, vol. 10, pp. 105807-105842, 2022, doi: 10.1109/ACCESS.2022.3211422.

H. Liu, H. Zhang, B. Chen and A. W. Roscoe, "Committable: A Decentralised and Trustless Open-Source Protocol," 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022, pp. 1-2, doi: 10.1109/ICBC54727.2022.9805541.

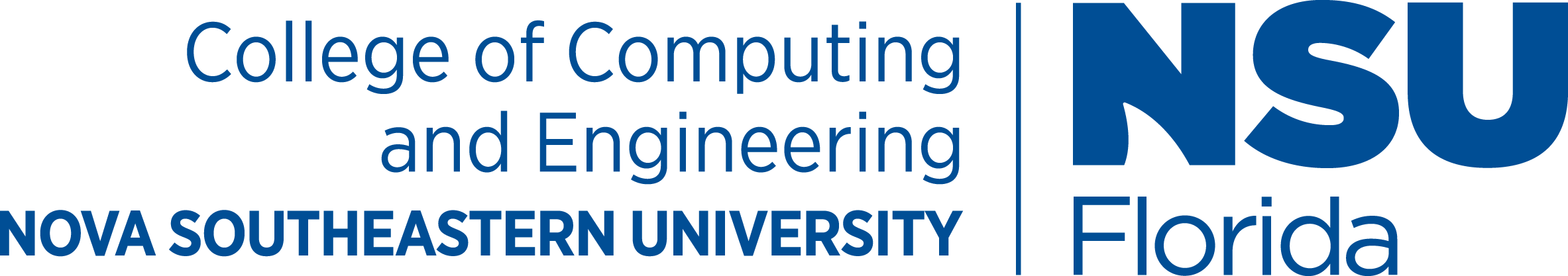
L. Baird and A. Luykx, "The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers," 2020 International Conference on Omni-layer Intelligent Systems (COINS), 2020, pp. 1-7, doi: 10.1109/COINS49042.2020.9191430.

L. Ambrosini, M. Piškorec and C. J. Tessone, "Visualization of Blockchain Consensus Degradation," 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022, pp. 1-2, doi: 10.1109/ICBC54727.2022.9805498.

H. Wang, Z. Wu, Y. Li, Z. Yan and J. Ma, "Architecture Design and Application of distributed power trading System based on blockchain Asynchronous Consensus," 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), 2021, pp. 35-41, doi: 10.1109/AEMCSE51986.2021.00015.

S. Ai, D. Hu, T. Zhang, Y. Jiang, C. Rong and J. Cao, "Blockchain based Power Transaction Asynchronous Settlement System," 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), 2020, pp. 1-6, doi: 10.1109/VTC2020-Spring48590.2020.9129593.

**Certification of Authorship of Doctoral Course Assignment**



Submitted to: Dr. Yair Levy

Student’s Name: Eric Webb

Date of Submission: November 6th, 2022

Purpose and Title of Submission: Assignment #1 Research Problem and Theory Review in Cybersecurity Management Paper

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