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 this study will address is… (Support the problem with solid reference that indeed indicates it as a problem.

- Lack of decentralization

BTC, ETH , ETC…

Explain who in literature claim that it is a problem? And explain, from literature, why is this still a problem?

BTC, ETH , ETC…

- lack of understanding from public.

- lack of TRIAD decentralization.

What is the current known impact of the problem?

-Gaining speed and security losses decentralization.

What are the key theories that have studied about that problem?

- FLP theorem

-Block chain triad.

What is/are the current gap in knowledge or contradicting research findings reported in the research literature)

-They all argue decentralization but come up short.

## **Research Goals**

- The main goal of this research study is to…

- Better understand the future of aBFT

- The need for this work is demonstrated by the work of ...(explain precisely but short each research and based on what conclusions were made)

- HoneyBadgerBFT, BEAT, ALGO, ABFT

- This dissertation builds on previous research by…

- HoneyBadgerBFT, BEAT, ALGO, ABFT

- The X\* specific goals of this research study are…

-Understand how asyncronicity can help defend against centralization.

- The main research question that this study will address is…

- how does asynchronicity defend again centrlaization.

- The X\* hypotheses that this study will address are... (Each hypothesis should directly be tied to a specific research goal and be a “measurable outcome” – see dissertation guide on what constitute goals!)

-aBFT will become more prevalent in blockchain in the future.

-aBFT will provide advancements in blockchain.

-

## **References**

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.

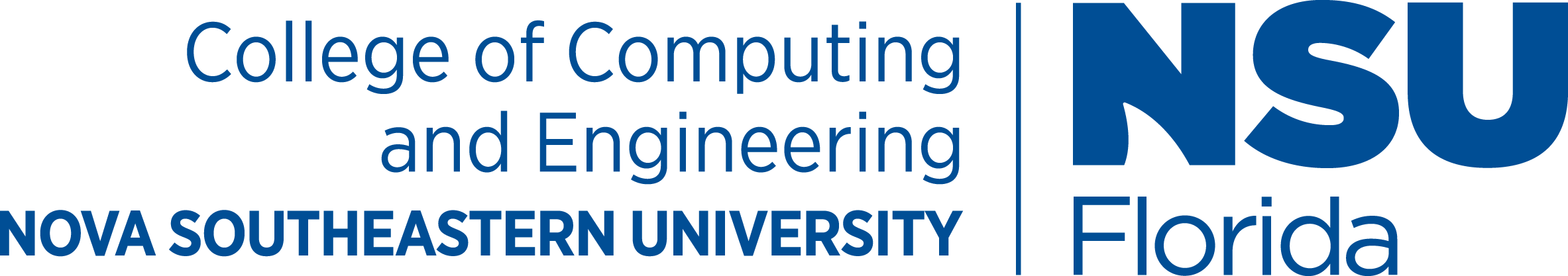
L. Baird and A. Luykx, "The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers," 2020 International Conference on Omni-layer Intelligent Systems (COINS), 2020, pp. 1-7, doi: 10.1109/COINS49042.2020.9191430.

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