ISEC-700 Fall 2022

Professor Yair Levy

Eric Webb

Assignment #1 Research Problem and Theory Review in Cybersecurity Management Paper November 6th, 2022

## **Research-Worthy Problem Summary**

In today's world economy blockchain technology is typically marketed as a variety of decentralized distributed systems. The problem is modern blockchain technology naturally manifests centralization. To put it “The impossible triangle of blockchain, i.e., efficiency, security, and decentralization, often cannot be satisfied at the same time and has been the limitation and bottleneck of blockchain’s development.” (Liu et al., 2021). From this blockchain triad one can see there is no one size fits all answer to a blockchain solution.

Some arguments have already been made on why these decentralized distributed systems are more centralized than they appear. This has been well established in the world's largest cryptocurrency Bitcoin. This is because of Bitcoins Proof-of-Work (PoW) consensus algorithm having the flaw of the 51% network vulnerability. Meaning that a few large mining pools that support over 51% of the network can get together nefariously and all agree to make a lie the truth. This is supported by the statement “emerging huge mining farms with strong mining resources and fast processing power is another trend toward centralization.” (Beikverdi and Song, 2015) Because the largest few mining pools can get together and create compromised transactions, Bitcoin is not as decentralized as it is marketed to be. This is through application-specific integrated circuit (ASIC) miners pooling together to overpower the network competition.

The same is true with the world's second largest cryptocurrency Ethereum. This blockchain recently, as of September 2022, switched from PoW to the Proof of Stake (PoS) protocol. Unfortunately, since it is such a recent even most if not all prior scholarly research is done on Ethereum's old PoW algorithm with little done since the PoS merge. This is an additional reason why this research is important. Even though the PoS algorithm is more cost efficient the concept of centralization manifestation still holds true. The difference being that validators must stake up front a large amount of Ethereum to participate. This means larger competitors with the capital to set up many validators will inevitably be able to influence the network disproportionately to the smaller pools or single node validators. This “indicates that Ethereum mining is going towards centralization” (Yang, Chen, and Chen, 2020) and is another example of how blockchain is not so decentralized as marketed.

From the previous research we can see that blockchain technology is marketed as decentralized distributed systems. The problem is that as these systems scale, they tend to become less decentralized and seem to manifest centralization. The viability of this problem will continue to grow if effort is not made to defend against centralization. The magnitude of this is that many people are at risk of fraud of epic proportions. The impact can be devastating financial loss on the world stage and everlasting repercussions of the development of decentralized distributed systems. The benefits of addressing this problem is it enables discussions on how to prevent centralization in blockchain technology, brings attention to current risks of modern blockchain technology, and furthers the development of secure decentralized distributed systems.

## **Theory Summary**

As consumers begin to become more knowledgeable on decentralized distributed systems, they will begin to realize that the blockchain technology previously sold to them is more centralized than previously marketed. This will ultimately lead to more distrust for that technology and push the market towards a more truly decentralized network. My theory is the more the blockchain market matures the greater the advancements in decentralization through the application of asynchronous consensus protocols. All this while maintaining efficiency, security, and having a Byzantine Fault Tolerance (BFT). The major focus of this argument will be on the advancement of Asynchronous Byzantine Fault Tolerant (aBFT) consensus protocols and how they will be integrated into blockchain technology to circumvent the manifestation of centralization in the future. Meaning that synchronous consensus protocols that are based off of time such as a time stamp, will integrate with or be replaced by asynchronous consensus protocols that are not based off of time. As the shortcomings of aBFT consensus protocols are improved upon over time the use of these protocols will become more prevalent in the security of blockchain technology and the field of decentralized distributed systems.

Coming to a consensus asynchronously has been a known challenge in the field of distributed systems for a while with one of the well-known arguments tailored for this discussion being notarized by the FLP theorem in 1985 stating that “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) Since decentralized distributed systems have become more researched the FLP theorem is being challenged by new asynchronous protocols.

This was supported by the research of (Liu et al., 2016) where their team was able to arguably implement an aBFT protocol called The Honey Badger Byzantine Fault Tolerant protocol (HoneyBadgerBFT) . In their research they argue their asynchronous consensus satisfies the FLP Theorem. They market their blockchain product as no leader, no timing assumptions, and to be efficient. Their main claim is the HoneyBadgerBFT protocol is more resilient because of their asynchronicity, which is an ode to the honey badger as a species being resilient. The HoneyBadgerBFT was not the first to demonstrate traits of asynchronicity and give credit for their work being based off the SINATRA protocol. (Cachin & Portiz, 2002) This protocol is well summed up by the HoneyBadgerBFT giving homage to SINTRA by saying “Our work is most closely related to SINTRA, a system implementation based on the asynchronous atomic broadcast protocol from. This protocol consists of a reduction from atomic broadcast (ABC) to common subset agreement (ACS), as well as a reduction from ACS to multi-value validated agreement (MVBA)” This is where The Honey Badger adopted the concept of atomic broadcasting first proposed by SINTRA in 2002. This is important because it was one of the first aBFT protocols to be established in secure asynchronous decentralized distributed systems.

Moving forward since the conception of the HoneyBadgerBFT in 2016 as a practical asynchronous byzantine fault tolerant consensus protocol, other blockchain engineering endeavors have begun to explore the field of aBFT. Another protocol of interest that is often referenced in the academia of decentralized distributed systems is the BEAT protocol who claim “BEAT protocols are significantly more efficient than HoneyBadgerBFT, the most efficient asynchronous BFT known. We also develop new distributed system ingredients, including generalized fingerprinted crosschecksum and new asynchronous verifiable information dispersal.”(Duan,Reiter, and Zhang, 2018). This is an example of aBFT protocols developing as the blockchain market matures. The BEAT protocol and the HoneyBadgerBFT protocols are popularly researched and referenced protocols when it comes to the study and theory of aBFT. Because it only started gaining traction in 2016 most research papers reference BEAT and HoneyBadgerBFT as their relative work and bench mark these protocols against theirs for empirical data. This is shown in a more recent study from (Knudsen et al., 2021) where they were able to create a new aBFT protocol that they also coincidentally named Asynchronous Byzantine Fault Tolerance protocol (ABFT) and compared its benchmarks against the benchmarks of BEAT and HoneyBadgerBFT. From the empirical data collected they argue that their new ABFT protocol “improved the Asynchronous Byzantine Fault Tolerance consensus protocol and designed a high performance one. The evaluation results show that our consensus protocol is faster and more reliable than state-of-the-art protocols.” (Knudsen et al., 2021) In this case the state-of-the-art protocols being HoneyBadgerBFT, BEAT, along with others. The ABFT is one of the more recent protocols to argue the advancement of aBFT protocols.

It is important to keep in mind that an aBFT protocol may not work alone and that a blockchain can also be developed to instill principles of both synchronous and asynchronous properties. An example of this is if a blockchain acted synchronously until a threshold is met, then it could implement its asynchronous behavior.

This is important to risk management in the context of cybersecurity because consensus protocols are the underlying architecture for transactions on distributed systems. By implementing aBFT on their own or in tangent with traditional synchronous consensus protocols we strength are positions in the blockchain triad and get a better understanding of solving the Byzantine Generals Problem (BGP). This imperative when assessing the risk of decentralized distributed systems because researchers will be able to identify the risks associated with blockchain and be able to perform a risk assessment accordingly. An example of this is choosing between two networks who are defined by low-latency and high centralization vs high-latency and low decentralization. Understanding the risks associated in this example can help define the risk appetite for that network. As blockchain matures we will see more aBFT protocols become more prevalent whether on their own or part of a semi-asynchronous framework. Understanding the benefits and shortcomings of these aBFT protocols compared to their BFT counterparts will help increase the field of cybersecurity specifically in the area securing decentralized distributed systems.

## **Literature Summary Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Article/Study:** | **Description**  **of the Problem** | **Methodology** | **Sample** | **Instrument** | **Main**  **findings or Contributions** |
| Liu et al. (2021) | There is no single solution for scaling blockchain technology and exists a triad of security, efficiency, and decentralization that needs to be satisfied. | Empirical  Investigation | The sample was 12 nodes, and the experiment ran three times with 1,2, or 3 shards within those nodes. | The instrument was a Hyperledger Fabric environment built locally using  a virtual machine Ubuntu 20.04 with 8GB RAM and 120G hard  disk. | Solidified the blockchain triad theorem while also making advancements in blockchain technology through sharding. |
| Beikverdi and Song, (2015) | Bitcoin has a 51% vulnerability in its decentralization and can be attacked if some of the major mining pools all acted in accordance. | Empirical  Investigation | The sample consists of more than  6 million data points from  the beginning of 2009 starting with genesis block to 22nd of  October 2014 | The instrument was implementing a JavaScript program to call an API provided by BlockTrail to gather data. | This contributed to the argument that Bitcoin is becoming more centralized through large mining pools. |
| Yang, Chen, and Chen. (2020) | Ethereum has a 51% vulnerability in its decentralization and can be attacked if some of the major mining pools all acted in accordance. | Empirical Investigation | The sample was the ﬁrst 6,000,000  Blocks of the Ethereum blockchain. | The instrument was a mathematical analysis on the data set. | This supported that Ethereum is trending towards centralization and provided context for improving the network decentralization through their Historical Weighted Difficult PoW protocol. |
| Liu et al., (2016) | BFT protocols rely critically on network timing assumptions, and only guarantee liveness when the network behaves as expected. | Empirical Investigation | 104 nodes in five continents | Developed a prototype implementation of HoneyBadgerBFT in Python deployed on Tor and AWS. | Was the first efficient and high throughput asynchronous BFT protocol. |
| Duan,Reiter, and Zhang, (2018) | Performance issues of aBFT.  No one-size-fits-all aBFT.  Smart contracts are hard to accomplish.  Flexible readings are hard to accomplish | Empirical Investigation | 92-instances of BEAT nodes. | AWS EC2 deployment written with Jerasure 2.0 a C library. | This argued to be faster and more efficient to HoneyBadgerBFT along with extending capabilities and allowing configuration of protocol to specialize. |

## **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.

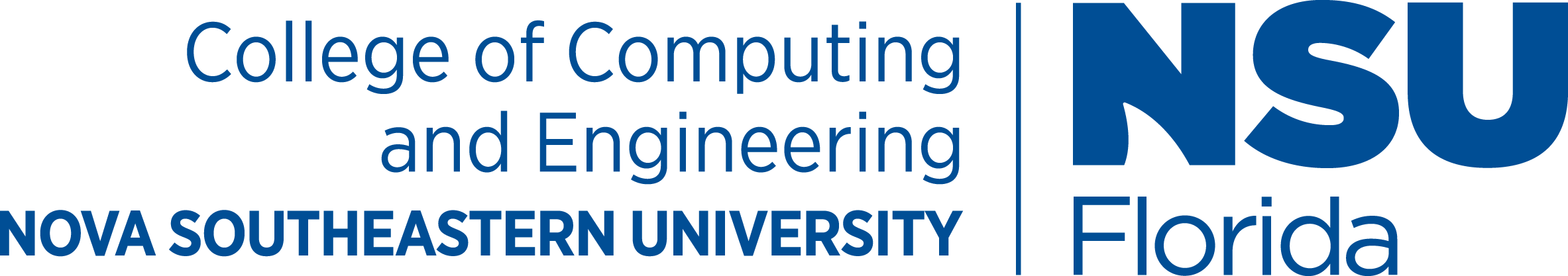
L. Baird and A. Luykx, "The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers," 2020 International Conference on Omni-layer Intelligent Systems (COINS), 2020, pp. 1-7, doi: 10.1109/COINS49042.2020.9191430.

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