**The Advancement of Digital Forensics Through Blockchain Technologies.**

Nova Southeastern University

ISEC-650 Winter, 2020

College of Computing and Engineering

Dr. J. Richard Kiper

April, 7th, 2020

Eric Webb

**Abstract.**

In this narrative we will discuss how blockchain has advanced the field of digital forensics through concepts such as a digital ledger, merkle roots, coinbase transactions, proof of work, and proof of stake algorithms. The knowledge gap being that blockchain has mainly been a speculation of theories about financial collapse rather than giving due credit to its advancements in the field of digital forensics and the underlying architecture that is revolutionizing the field. This is resolved by a better understanding of decentralization, the Byzantine General Problem, and educating the general knowledge of the public.

**Introduction.**

Since blockchains conception it has been a controversial yet invigorating topic. Many of these being its theoretical use in transactions without a centralized entity. The term blockchain is currently most synonymous with the product Bitcoin, and although this was the first public implication of this technology it would not be the last. Many companies, applications, and entities, have emerged from the trials and tribulations of development to find success and get their foothold in such a new and niche market. When new technology is being innovated, there are the initial innovators followed by early majority adopters. As times goes by and communication across platforms becomes accessible and more standards are introduced into the industry not only to benefit production but to also enhance the quality of the technology as a whole. Since blockchain is such new technology a lot of what it is comprised of has been deemed innovative since a lot has not technically been done before, or at least what has been known to be done in the public eye.

Since Blockchain is centered on encryption and comparing hash values, digital forensics is constantly being applied and fine-tuned to enhance these features. This paper will define how digital forensics are being applied to blockchain technology and argue how they are inherently advancing concepts in the field of digital forensics.

Coinbase transaction – merkel root

Etherium shards

NEO ?

IOTA

Blockchain-based cryptocurrencies system like Bitcoin are increasingly

popular and successful. The łcore” is a global public distributed

ledger, called blockchain, that records all transactions between users (stakeholders). 🡨-- BC\_Design

T he data

is stored in multiple locations (in contrast to centrally stored

databases) therefore being by definition public and widely

verifiable thus more difficult to manipulate given that the

same copy exists simultaneously in many places. 🡨-- BC IN cybersecurity

**Work Cited:**

Bagaria, V., Fanti, G., Viswanath, P., Tse, D., & Kannan, S. (2019, November 15). *Deconstructing the Blockchain to Approach Physical Limits.* doi: 10.1145/3319535.3363213

Duy, P. T., Hien, D. T. T., Hien, D. H., & Pham, V.-H. (2018). *Proceedings of the Ninth International Symposium on Information and Communication Technology*. New York NY: ACM. doi: 10.1145/3287921.3287978

Gjermundred, H., Chalkias, K., & Dionysiou, L. (2016, November 12). *Going Beyond the Coinbase Transaction Fee: Alternative Reward Schemes for Miners in Blockchain Systems*. doi: 10.1145/3003733.3003773

Lee, D., Jang, Y., & Kim, H. (2019, November 15).*A Proof-of-Stake (PoS) Blockchain Protocol using Fair and Dynamic Sharding Management.* doi:10.1145/3319535.3363254

Tong, C., & Yan, M. (2019, November 13). Neo Documentation UTXO. Retrieved November 24, 2019, from <https://docs.neo.org/docs/en-us/tooldev/concept/blockchain/utxo.html>.

Vilim, M., Duwe, H., & Kumar, R. (2016, June 9).*Approximate Bitcoin Mining* doi:10.1145/2897937.2897988

Zamanov, A., Erokhin, V., & Fedotov, P. (2018, February 1). *ASIC-resistant hash functions* doi: 10.1109/EIConRus.2018.8317115

Zhang, R., Xue, R., & Liu, L. (2019). *Security and Privacy on Blockchain*. New York, NY: ACM New York. doi: 10.1145/3316481

Zohar, A. (2019). *Recent trends in decentralized cryptocurrencies.* (49th ed.). New York, NY: ACM New York. doi: 10.1145/3055399.3079074



