**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 I 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 digital forensics embedded within these applications 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.

**1.0 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 more standards are introduced into the industry. This is 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 is developed 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 for this industry. This is the basic construct that argues digital forensics has advanced by being deployed with in these new blockchain applications to verify trust in ways never previously done before.

**1.1 Byzantine General Problem.**

When discussing Blockchain technology the concept of the Byzantine General Problem (BGP) is often mentioned. It is widely accepted that Blockchain should aim to solve the BGP. The problem dates back to a concept of multiple Byzantine Generals commanding their armies and need to work together at the same time to successfully besiege a city. If any orders are executed not in unison and without complete trust then there operations will fail. Basic examples of how to solve this would be that generals send letters to each other agreeing on when to attack the city. The questions then arise, how can Generals be sure the other general wrote the letter and it was not forged? And how can the generals be sure the other Generals are genuine in their intentions? Possibly by holding the other general’s family as hostage until the operations is a success? That way all parties have a stake in the situation. These are examples on how answers to this problem can be layered and not so clear. Ultimately, the BGP aims to verify trust between parties and execute operations in a synchronous manner. Conversely, in Blockchain applications this needs to also be applied. Multiple entities should be able to verify, trust, and be synchronized all in a digital format. That is where digital forensics comes into play because Blockchains will have their own forensic analysis imbedded within their applications codes to verify transactions, validate trust between parties, while also mandating synchronicities. That is how and why you will often see the BGP being referenced when it comes to Blockchain theory and architecture.

**1.2. Distributed Ledgers.**

A big role in blockchain applications is the concept of the distributed ledger being applied in a decentralized environment. In a high level abstract view, a distributed ledger is essentially a database (ledger) that has copies stored in multiple locations (Distributed) so that multiple entities can agree on its contents and history without a single governing power. (Decentralized). When transactions happen in a distributed system multiple parties agree that some data (Blocks) needs to be added to all parties ledgers (Chain). This how blockchain gets its name from multiple blocks being added to chains of previous ones with multiple entities having agreed copies of these chains for verification and accounting.

In a perfect scenario for decentralization, no single governing body would hold the majority influence of the application, and having a copy and fair share of the decisions making should be obtainable to smaller organizations. This aims to reduce the advantage of large competitors over small ones, hopefully evening the playing field. Blockchain applications aim to do this securely through the use of digital forensics. Since all blockchain applications are different it is impossible to group their architectures into one lump sum, but again at a high level design an example of this could be as follows. Since all ledgers need to be the same across entities, one way digital forensics aims to solve this is by producing a hash algorithm of the database to compare with others, if the hashes do not match then you know the databases are not the same. Blockchain applications will repeatedly compare hash values at many steps throughout their processes. Examples of this are when verifying ledgers, making transactions, locations of next and previous transactions, and so on. Using hashing algorithms to compare values to see if they are the same is not new by any means, but what is arguably innovative is when, how, and why they are hashing these values to help solve the Byzantine General Problem. Blockchain applications must prove out via digital forensics that without a doubt that ledgers on the network are synchronized, trusted, and immutable. If any change has occurred, the blockchain should be able to detect and verify these errors through a digital analysis and then act accordingly.

**2.0 Bitcoin**

Infamously enough blockchain seems to always be synonymous with the application “Bitcoin”. This is due to this technology first appearing in a whitepaper under the guise of a mysterious pseudonym “Satoshi Nakomto”. The creator of this blockchain application is unknown but is credited with using a “Proof of Work” algorithm and the digital forensics embedded within itself to verify transactions. In this section, I will entail how Satoshi’s embodiment of digital forensics are found within Bitcoins POW algorithm.

**2.1 Bitcoins Wallet.**

Bitcoins distributed ledger is governed by a system of checks and balances within the application. The database is public so that anyone can download it, but is also immutable in that no one can change it. Embedded within Bitcoins code is a self-checking digital forensic analysis of a decentralized database system.

When creating a digital wallet, you are given a private and public key. Your public key is a hashed value that represents your public address. This is where your Bitcoin will be sent for owner ship of transactions and what you give out to the public on where they should send you payments. Your private address is also known as a seed and is often relayed as a pneumonic seed. This ensures you are the owner of the account and validates your authenticity. This is private and not be shared with anyone or else the contents of your wallet can be stolen. When creating a transactions wallets will sign the transaction with their private keys to ensure they are the creator and that the data has not changed. This is an example of how digital forensics is applied within Bitcoins wallets through the use of Private Key Infrastructure to help solve the Byzantine General Problem.

**2.2 Bitcoin Mining.**

Coinbase transaction – merkel root

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