**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 distributed ledger, merkle roots, coinbase transactions, and the use of proof of work 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 blockchain to 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 technology industry first started significantly paying attention to blockchain terminology when Bitcoin was launched in 2008 (Phan, Hien, Hien, Pham, 2018. Pg 1). 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. (Bartoletti, Lande, Pompianu, Bracciali. 2017. Pg 1)

**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? Another example is 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. (Wenbing Zhao, Shunkun Yang, and Xiong Luo. 2019.)

**1.2. Distributed Ledgers.**

A big role in blockchain applications is the concept of a distributed ledger being applied in a decentralized environment. The “core” is a global public distributed ledger, called a blockchain. (Thai, Njilla, Duong, Fan, Zhou, 2018. Pg. 1). 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). (Rot, Blaicke, 2019. Pg 1). 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 blockchain technologies 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 because Bitcoin was the first decentralized cryptocurrency for worldwide digital payment systems that transfer values as fast and as efficiently as data and was created in 2009 by pseudonymous developer Satoshi Nakamoto. (Pai, Mondal, 2019. Pg. 2) 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 keys and UTXO.**

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 (Gentilal, Martins, Sousa, 2017. Pg. 1).This is private and not be shared with anyone or else the contents of your wallet can be stolen. When creating a transaction 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.

Bitcoins distributed ledger works on the concept of unspent transaction outputs (UTXO). In high level it works as follows. Traditionally ledgers act as so, 5 deposits of 1 of the same item would equal 5 of the same items in the database. Let’s say 5 deposits of $1 would equal $5 in your bank account. Essentially Bitcoin works in the opposite manner of that. When you get 5 inputs of 1 BTC to your wallet. You wallet and the ledger will see that as 5 different increments of 1BTC to spend. So if you are spending 1.5 Btc on a purchase, your transaction will use up your first 1BTC unspent transaction, then it will use up you’re a second 1 BTC unspent transaction, and then surplus you an unspent transaction total of 0.5 BTC to be added to your UTXO list to be accounted for later on when needed. This is a magnificent feat in that the Bitcoin uses digital forensics to account for unspent transaction outputs rather than just accumulating deposits into a single object. (Zhang, Xue, Liu, 2019. Pg. 7)

**2.2 Bitcoin Transactions, Merkel Root, and Coinbase.**

When a transaction is performed on the network a record of that transactions gets added to the block chain and stored in the next block to be added. A block will have a collection of transactions stored as Sha -256 hash values. These hash values of transactions will be added together and hashed again with Sha-256 to provide a merkel root. This is how Bitcoin implements double Sha-256 encryption. The merkel root is what is used to append to the blockchain as the previous blocks location since it’s a hashed list of transactions and a coinbase transaction. Through a chain of merkel roots, transactions can be followed eventually leading back to the initial coinbase transaction. This is done so that data can be verified without knowing its contents of the data. (Wirachantika, Barmawi, Wahyudi, 2019. Pg 1.) The next block being added is broadcast to the network where miners will start competing to start verifying it. The reason they do this is because if they perform the extremely difficult task of adding a block to the chain they will get rewarded with the privilege of adding the final transaction to that block before the merkel root is conducted. This final transaction is called a coinbase transaction. This coinbase transaction is where new bitcoins will be credited to the miner who added the blocks public address. (Gjermundrød, Chalkias, Dionysiou, 2016.Pg. 2). It is called the coinbase transaction because it can cryptographically traced back to this originating transaction, meaning it is the coin’s base transaction of origin. By being able to trace all transactions of the coin back to its creation in the coinbase transaction via a hashed chain of values for transactions is a good example how Bitcoin has advanced the field of digital forensics. This is done by architecting and implementing a self-governing digital analysis of code embedded within itself to verify authenticity of transactions while also maintaining transparency.

**2.3 Bitcoin Mining Difficulty.**

As discussed earlier, Miners will use time, computing power, and electrical energy in hopes of getting to be able to add a coinbase transaction inside a block for themselves to get rewarded. The interesting thing is how Bitcoin applies new concepts of digital forensics to apply the concepts of decentralization and upholding the BGP when competing for this right.

When more miners are competing on the network a network difficulty goes up. This is measured in the amount of hashing power that is being applied on the network. This has a direct correlation with the target hash of the network. The target hash is a cryptographic number that hashes must be equal to or less than to be able to add a block to the network. The Bitcoin proof of work algorithm will have miners verify transactions and these verified transactions will essentially spit out a number. If that solved transaction number is smaller or equal to the target hash of the network then they will be added to the chain. So as more miners are added to the network the network difficulty will increase, this intern means that the target hash value will decrease making the chance of these new miners to produce such a small number less likely. Therefore, increasing the network difficulty. This algorithm applies a nonce value to these blocks to support the pseudo randomness a miner will get a small enough target hash value (Vilim, Duwe, Kumar, 2016. Pg 1). This is an arguable achievement in digital forensics by applying decentralization through an analysis of target hash and network hashing power to manage the competitive playing field.

**2.4 Bitcoin Halvening.**

Another interesting advancement in the self-governing digital forensics of Bitcoin is how it applies decreasing the supply overtime. Essentially, Bitcoin is designed to decrease its output from miners as time goes by. This decreases the supply as the demand increases, in a secure and digital format.

In an attempt to cap the supply of 21,000,000 Btc’s. The code base will half the output to the rewarding miner every 210,000 blocks. Btc started out with rewarding coinbase transactions 50, 25, and then 12.5 Bitcoins. The next halvening will have miners only producing 6.75 Btc’s. Once these halvening reach there smallest amount of BTC possible they will no longer perform coinbase transactions and miners will only collect verification fees. . (Gjermundrød, Chalkias, Dionysiou, 2016.Pg. 2).

Bitcoin applied digital forensics in its code to secure scarcity of its tokens. This is innovative because a blockchain application had not been public at that point and the concept of digitally verifying scarcity by lowering rewards per every set amount of blocks had not been performed yet.

**3.0 Conclusion.**

In this narrative I have discussed many abstracts concepts that apply to blockchain and its advancement of digital forensics through its conception. This is shown in the topics of how blockchain uses digital forensics to create trust between distributed systems and helps aim to solve theByzantine General Problem like never before. In a more specific example, this narrative discussed on how Bitcoins application advanced the field of digital forensics. This is argued by Bitcoins capabilities within its code to use digital forensics to create trust, verification, and transparency between entities. This is shown through the Public Key Infrastructure of the wallets, ability to verify transactions and creations of coins using merkel roots and coinbase transactions, and modify mining competition by comparing the target hash value with the network hash rate to establish a network difficutly. These are arguably all new concepts that use digital forensics in a way never used before to establish a peer-to-peer payment network.

**2.2 Future Work.**

In my previous work I have written more in depth longer narratives about the inner workings of blockchain, specifically Bitcoin and Etherium. In my future work I would like to find more peer reviewed material on other lesser known applications and see how they attempt to solve the problems of decentralization and their rational behind solving the Byzantine General Problem.

**Work Cited:**

Matthew Vilim, Henry Duwe, and Rakesh Kumar. 2016. Approximate bitcoin mining. In Proceedings of the 53rd Annual Design Automation Conference (DAC ’16). Association for Computing Machinery, New York, NY, USA, Article 97, 1–6. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/2897937.2897988

A. Rot and B. Blaicke, "Blockchain’s Future Role in Cybersecurity. Analysis of Defensive and Offensive Potential Leveraging Blockchain-Based Platforms," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 447-451.

N. D. Pai and S. Mondal, "A study on Blockchain enabled Applications and its Security Issues," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-5.

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

Phan The Duy, Do Thi Thu Hien, Do Hoang Hien, and Van-Hau Pham. 2018. A survey on opportunities and challenges of Blockchain technology adoption for revolutionary innovation. In Proceedings of the Ninth International Symposium on Information and Communication Technology (SoICT 2018). Association for Computing Machinery, New York, NY, USA, 200–207. DOI:https://doi- org.ezproxylocal.library.nova.edu/10.1145/3287921.3287978

Phuc Thai, Laurent Njilla, Tuyet Duong, Lei Fan, and Hong-Sheng Zhou. 2018. *A Generic Paradigm for*

*Blockchain Design*. Association for Computing Machinery, New York, NY, USA, 460–469. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3286978.3286982

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

Massimo Bartoletti, Stefano Lande, Livio Pompianu, and Andrea Bracciali. 2017. A general framework for blockchain analytics. In Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers (SERIAL ’17). Association for Computing Machinery, New York, NY, USA, Article 7, 1–6. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3152824.3152831

Harald Gjermundrød, Konstantinos Chalkias, and Ioanna Dionysiou. 2016. Going Beyond the Coinbase Transaction Fee: Alternative Reward Schemes for Miners in Blockchain Systems. In Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI ’16). Association for Computing Machinery, New York, NY, USA, Article 35, 1–4. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3003733.3003773

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

Widya Wirachantika, Ari Moesriami Barmawi, and Bambang Ari Wahyudi. 2019. Strengthening fawkescoin against double spending attack using merkle tree. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (ICCSP ’19). Association for Computing Machinery, New York, NY, USA, 49–54. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3309074.3309105

Wenbing Zhao, Shunkun Yang, and Xiong Luo. 2019. On Consensus in Public Blockchains. In Proceedings of the 2019 International Conference on Blockchain Technology (ICBCT 2019). Association for Computing Machinery, New York, NY, USA, 1–5. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3320154.3320162

Miraje Gentilal, Paulo Martins, and Leonel Sousa. 2017. TrustZone-backed bitcoin wallet. In Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems (CS2 ’17). Association for Computing Machinery, New York, NY, USA, 25–28. DOI:https://doi-org.ezproxylocal.library.nova.edu/10.1145/3031836.3031841