**How Blockchain has Advanced the Field of Applied Cryptography,**

**And Why the Public Should Trust it.**

**Eric Webb**

**Nova Southeastern University.**

**NSU ID: 01927543**

**NSU Email:** [**ew774@mynsu.nova.edu**](mailto:ew774@mynsu.nova.edu)

**Contact Number: (386) 490 - 6637**

Table of Contents

Abstract1

Keywords2

[Introduction](#_Toc50574532) 2

[Risk Management Analysis (RMA) Outline 3](#_Toc50574533)

[Project Scope and Goals](#_Toc50574534) 4

[Recommended Solution and Action Plan](#_Toc50574535) 4

[Anticipated Results 5](#_Toc50574536)

[Proposed Costs 6](#_Toc50574537)

[Conclusion 7](#_Toc50574538)

[Technical Appendix 8](#_Toc50574539)

[Reference 11](#_Toc50574539)

Abstract:

In this academic narrative, topics will be researched on why the general public does not trust blockchain applications. This will include a brief introduction to blockchain including: the difference between a decentralized system and a distributed ledger, its history through the conception of Bitcoin and thus the birth of Alternate Coins (Altcoins), and the known public distrust from previous thefts such as the infamous Mt.Gox incident and others. Through a technical perspective, an analysis will be performed on why the general public should have more faith in blockchain applications. Popular cryptocurrencies and their respective consensus algorithms will be discussed such as: Bitcoin and its Proof of Work (Pow) , Ethereum and its Proof of Stake (PoS), and Neo with its Delegate Proof of Stake (dPos). These will be expected to answer and show their work on how they solve the Byzantine General Problem (BGP). This will expose their shortcomings while also simultaneously arguing their validity. Following that, some methodologies based off this research will provide examples of how blockchain applications could be used for the general public’s greater good. To protect the validity of this informational, all research was conducted via academic and professional literature. This all was gained from the Institute of Electrical and Electronics Engineers (IEEE) and Association for Computing Machinery (ACM) databases, along with the proprietary documented white papers of the blockchain themselves.

Keywords:

Decentralization , Distributed Ledger, Consensus Algorithm, Proof of Stake, Proof of Work, Byzantine Generals Problem, Unspent Transaction Output, Public Key Infrastructure,

Introduction:

Since the conception of blockchain it has created numerous amounts of topics for discussion. When it comes to understanding what blockchain is, often times we find over simplified answers that abstract away the technical details of the underlying architecture. This maybe be fine when first dipping ones toes into this new technology, but doesn’t really serve as a long term benefit when the worlds needs to be so vested.

Generally speaking, when blockchain first appeared the public wasn’t sure what it was, where it came from, where it was heading, and what it still holds. In this section we will begin to define those answers to those questions. This has been a confusing topic for most because when the general public hears the word blockchain it is often most synonymous with the cryptocurrency Bitcoin and be it true that Bitcoin does use blockchain in its underlying architecture. It is not the only blockchain application.

The truth is that the term blockchain is not a one stop shop term but but more of a blanket term that can be interpreted many ways. There are many blockchain applications out there with different underlying architectures built for many different reasons.

Distributed Ledger vs Decentralization:

When discussing blockchain architecture, often times you will hear the terms distributed ledger and decentralization thrown around loosely. Although they can have a direct relation to each other, they are not one in the same. In this excerpt of what blockchain is, you can see characteristics at work: “From a data management perspective, a blockchain is a distributed database that logs an evolving list of transaction records by organizing them into a hierarchical chain of blocks. From a security perspective, the block chain is created and maintained using a peer to peer overlay network and secured through intelligent and decentralized utilization of cryptography with crowd computing.”(Viewable on Chain, Security and Privacy on Blockchain). This essentially means that blockchain applications are typically distributed ledgers on a decentralized network. A distributed ledger is essentially a list or a database that is stored in multiple locations or on multiple machines. A decentralized network means that no one single entity or small cliques can take advantage of nodes on the network. So although an application is a distributed ledger with multiples copies stored in multiple locations, does not mean it is decentralized if all those copies are owned by the same entity! If every entity had a copy and have a fair chance to make changes then it would be decentralized.

These ledgers are typically made of blocks that are chained together creating long chains of stored information. Hence the name “Blockchain”. These databases are stored within the blockchain community and are not centrally located under one entity. Each one of these databases keep a copy of the ledger and agree to make changes to it (Zhang, Xue, & Liu, 2019, Pg. 2). The beauty of this being that if one entity makes a change the others can pinpoint who is trying to make or made the change. This bring the concept of transparency into light. Because transactions are stored transparently on a distributed ledger, they are able to establish trust between multiples parties who once did not trust each other. More formally one could think of blockchains as digital escrow accounts in a loose sense. Except that the escrow account is not managed by a central entity but by a large community of members. If one member were to lie about their copy of the ledger, then the others could cross check their copies and flag the faulty actor as irrelevant and untrustworthy effectively disconnecting them from the network. Sometimes in blockchain technology there will be instances were there can be consequences for acting maliciously as well which can result in a large financial loss.

The CIA triad:

Since everyone has access to the main copy of the database and can cross reference with each other, blockchain covers the concept of Availability in the Confidentiality , Integrity, and Availability (CIA) triad. To cover Integrity, most blockchains implement a consensus algorithm. This is a voting algorithm on who gets to decide what is added to master chain. This is similar to how in an Agile software engineering environment when a team lead and other reviewers will be the deciders of what gets added to the master branch. This time instead of one or a few deciders from entity, it is a multitude of entities agreeing on a change. This bring integrity because no single entity can manipulate the network and you can be insured that your information is true by checking the latest data, pin pointing where the changed occurred, who changed it, and then discussing and comparing with other nodes. Since Blockchain applications are high in the Availability and Integrity factors of the CIA triad, they sometimes struggle to overcome the Confidential aspect. Again, your accounts and transactions are typically displayed for all the world to see. So how does one over come the burden of remaining confidential? Many blockchains will overcome this by establishing a Public Key Infrastructure (PKI) of public and private keys. The Public key is your Pseudonym or alias for all your transactions. If no one knows who that public key belongs to then your assets are still confidential. Keeping in mind that the CIA triad of each blockchain application will vary for each’s specific purpose. How each applications purpose fills out the CIA triad should directly influence the general public trust about that blockchain application.

The Byzantine Generals Problem:

After an application is developed it will be analyzed using the CIA triad to give its characteristics. This is more of a score card although should always be kept in mind when developing projects. The true problem that blockchain aims to solve is the Byzantine Generals Problem (BGP). Although this problem is referenced though the lens of a medieval general, it shows, and questions the trust between different parties still today. The BGP is a huge topic of discussion and many narratives have been written on how to solve it.

In essence the problem goes as so, In the days of the Byzantine Empire. Many general are camped outside an enemy city that needs to be besieged. The generals all need to make a decision on a plan, and verify it is executed at the correct time, with out falling prey to malicious actors. In the case of the Byzantine General, bad actors would be traitors or impersonators to their cause. Communications between generals are only by message so trust has to be established so that the message is authenticated and shows integrity. In those days a seal or stamp would be a sign of authenticity and integrity but in a digital word this is now resolved through digital certificates and digital signatures.

Another concept of establishing trust is by staking, If a general wanted to vote on plan of action to take the city they could put up something as collateral. If armies did not win the battle the general would loose their collateral. This gives them incentive not act maliciously. This hold especially true when in the middle ages your collateral could be your loves ones.

Blockchain Conception:

Since its conception, blockchain has showed properties that would make even the most bullish or novice investors weary. We do not really even know where this technology came from!

Publics Negative Trust: Silk road.

Ut ohhhh Mt.Gox:

Why the Public Should Adopt More Blockchain Applications:

Bitcoin and Proof of Work:

UTXO:

Ethereum and Proof of Stake:

Neo and Delegate Proof of Stake:

Quantum Proof Blockchain:

Introduction



Certification of Authorship of Assignment

Submitted to (Professor’s Name): Junping Sun.

Class/Semester: ISEC620 Applied Cryptography, Winter 2020.

Students’ Names: Eric Webb

Date of Assignment: 11-14-2020

Title of Assignment: How Blockchain has Advanced the Field of Applied Cryptography,

And Why the Public Should Trust it.

Certification of Authorship: By submitting this document we certify that we are the authors of this paper and that any assistance we received in its preparation is fully acknowledged and disclosed in the paper. We have also cited any sources from which we used data, ideas or words, either quoted directly or paraphrased. We also certify that this paper was prepared by us specifically for this course.

Students’ Signatures: Babatunde Somade Eric Webb