**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 even though its development has led to advancements in the field of Applied Cryptography.. 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 (BTC) 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 BTC and its Proof of Work (Pow) , ETH and its Proof of Stake (PoS). These will be expected to answer and show their work on how they solve the Byzantine General Problem (BGP). 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 we find over simplified answers that abstract away the technical details of the underlying architecture. This maybe be fine when first dipping one’s toes into this new technology but doesn’t really serve as a long term benefit when the worlds needs to be so vested.

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 BTC 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 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 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 these characteristics exemplified: “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 had 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 can 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 separate entities. 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 or loss of voting rights.

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 like 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 agreeing with other nodes on resulting disciplinary actions. 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 overcome 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. Keep in mind not all blockchains have public distributed ledgers so in those cases their ratio of confidentiality will be higher than their availability. 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 can be thought of as 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 theoretic papers have been written on how to solve it.

The problem goes as so, In the days of the Byzantine Empire. Many generals 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, without 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 must 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 lose their collateral. This gives them incentive to not act maliciously. This could hold especially true when in the middle ages your collateral could be your loves ones.

Publics Negative Trust:

When it comes to conversations about blockchain, it is all too common to hear the general public’s negative review. More often or not associated with words like scam or pyramid scheme without knowing what the underlying functionality of it is.In this section we will discuss and analyze a few notorious facts and incidents that would bestow the public’s trust.

Blockchains Informal Conception.

Since its conception, blockchain has showed properties that would make even the most bullish or novice investors weary. We do not even know where this technology came from! It is no secret that the concept of blockchain technology was first general introduced through the publication of the Bitcoin white paper. What makes the story that more intriguing is that the author of this white paper went under the pseudonym pen name of Satoshi Nakomoto. There has been much speculation as to who Satoshi is and whether they are a singular person or multiple entities. None the less not knowing who the creator of this technology is sure to have misguided the public’s trust.

Silk road:

One of the most infamous reasons why BTC came to light was its was for a short time perfect for black market trading. One of the most notorious was the Silk Road where users could purchase all kinds of devious products and services using BTC. That eventually got shut down and even raided by the FBI. The inherently confiscated a lot of servers that held cryptocurrency wallets ultimately making uncle Sam one of the largest holders of Bitcoin. Since cryptocurrency’s are synonymous with black markets the inherently have lost the public’s trust.

Mt.Gox.

One of the largest online thefts in history happened on the Mt.Gox cryptocurrency exchange. Interestingly enough. Mt.Gox stands for Magic the Gathering Online Exchange and was originally used to trade Magic the Gathering Cards until it transferred its business into a crypto currency exchange. In short, the exchange got hacked and over a million Bitcoin were stolen, this was due to the agile software development process of Mt. Gox or rather lack thereof, and how digital wallets were designed. Essential anyone with access to the private wallets could see the wallets private keys in clear text to be used nefariously later at another point. There is nothing inherently wrong with this if you are the only one with access to that repository (It should obviously be stored in an encrypted format) but the issue was at Mt.Gox team members were able to access those repositories that should not have been able to. This large of a cryptocurrency heist was a huge set back for bridging trust between blockchain and the general public. Although most would argue this heist was from a faulty agile pipeline rather than an architectural flaw. The flaw of storing private keys in plaintext within wallets has now been secured further by encrypting them within the wallets themselves for another added layer of security.

Why the Public Should Trust:

Now that we have discussed reasons on why the general public has developed a negative view towards blockchain, we will now begin to discuss why they should change there point of views to further adopt and trust blockchain applications. These will be more technical in nature and argue why blockchain is safe but how its deployed can lead to vulnerabilities. Similarly, to how you can’t hack a dollar bill but you can leave your wallet open to be stolen.

Bitcoin:

When you meet people in the general public who get past the stigmatisms of Bitcoin being a scam, a lot of times they will still ask you questions pertaining on how BTC will replace your credit card. The short answer be it won’t, and it’s not designed too. Although other cryptocurrencies are looking into that. A lot of times BTC will be compared to a digital piece of gold rather than a digital dollar. That’s because gold acts as a store of value rather than a currency. In this narrative we will begin to discuss how BTC’s Proof of Work (PoW) consensus algorithm is designed to solve the BGP specifically through Mining and Unspent Transaction Outputs (UTXO). This will solidify how its conception added led to the advancements of applied cryptography through its revolutionary consensus algorithm.

Why the Public Should Trust: Proof of Work

The BTC network is decentralized in the fact that any participant can join and support the network while having a somewhat competitive advantage. This is done through what is called mining. Mining is when you use a Computer Processing Unit (CPU) or a Graphics Processing Unit (GPU) to solve and verify hashing algorithms. Many miners solve and verify they get the same answers before adding transactions to the public blockchain. One of those lucky miners will produce a hash that is below the targets hash rate, and if so, they will be the ones who add the new Coinbase transaction to the blockchain. Each miner is verifying the same transactions and will hopefully get the same answer, ones who do not will be kicked from the network because their trust will be broken at that point. Each miner solves the algorithm and then applies a random nonce value to their output. If that nonce value and their output is less than the target hash value, they will be the one to add the block and get rewarded, if not it’s on to the next transaction and more work. This produces coins to be added to their wallets since they are being rewarded for solving the hashing algorithm. This initial Coinbase transaction contains proof of their work for solving the algorithm along with everyone else also agreeing as well. This will be stored and will be able to be referenced from the Coinbase transactions block header and transactions as the block is added to the chain. This is where BTC’s Proof of Work comes from, because miners are proving their work of the Coinbase transaction that was added. What protects the decentralization is the target hash rate gets lower and harder to solve as more miners are added to the network. In return this raises network difficulty. Network difficulty and target hash are directly inverse related. As one goes up the other goes down. The higher the network Difficulty the lower the hash value. This means that no one single entity could come in with a bunch of computing power and mine all the BTC’s. This is because added power to the network would make the difficulty raise intern making it harder to mine. This is the key behind BTC’s decentralization and adds to solve the BGP by establishing that no one single entity can make decisions for or influence the network.

This has added to the field of applied cryptography because BTCs blockchain architecture essential took current technology of SHA-256 encryption and used it in a new light to chain blocks of information together in a decentralized fashion through distributed ledgers.

Unspent Transaction Output

The wallet of BTC does not work in a traditional account model architecture, but rather added up as unspent transactions. This is referred to the unspent transaction output model (UTXO). When a miner is lucky enough to create a Coinbase transaction their wallet and the public blockchain sees an input of what ever that award is at the time. The awards originally started at 50BTC and halves ever “X” number of blocks and currently only produces 6.25 BTC as a reward as of November,2020. This is true until it halves again to only reward 3.125 BTC. These are unused outputs until they are used and sent out. This can be beneficial because amounts can be sent in varying denominations with out and relying on the receiver to give back change. In the typical account model, you would have to take out denominations of pennies to dollar amounts whiles in the UTXO model you can get a more finite or larger exact number with out relying on the counterparty to provide change. Since these spent and unspent transactions are reviewable on the block chain that is distributed among many decentralized public nodes, they help aim to solve the BGP by establishing trust between accounting of transactions through a chaining of unspent transactions as the account balance.

Ethereum

After the birth of Blockchain through the conception of BTC and its Proof of Work algorithm came the introduction of Altcoins. This led to development and advancements in the field of blockchain technology. One of the most notable is Ethereum and its ability to deploy smart contracts. In a high level view a smart contract is essentially a programmable application deployed on blockchain. Because the network is decentralized and an app is running on it, the nomenclature is it is called a Decentralized Application (dApp). This advancement turned blockchain from just a wallet to being able to host financial services, web blogs, games and many more!

Proof of Stake:

Ethereum and its smart contracts are built off the Proof of Stake (PoS) consensus algorithm. This aims to solve the BGP in a different manner the BTC’s PoW algorithm. To begin, the whole point of staking is to speed up transaction times without giving up trust. This is done through staking assets up front to be a node on the network. This acts as sort of an escrow account that will be forfeited if a node is caught acting nefariously on the network. This incentivizes nodes to act accordingly so they don’t loose their stake. Previously with BTC’s PoW, nodes spend excess time and energy to be rewarded proof they can add the next block to the network. In PoS, instead of spending excess time and energy to establish trust, it is abstracted away in the form of putting something up front. In the time of the Byzantine Generals Problem this could be represented as Generals keeping other generals jewelery, food, or families as collateral until the siege is carried out successfully. This is how Ethereum’s PoS consensus algorithm aims to solve the BGP by establishing trust through staking. This also validates how blockchain advanced the field of applied cryptography, because its PoS consensus algorithm created a new way of deploying applications and assets.

Theoretical Example Voting System.

In this informational we have discussed how the field of blockchain has advanced digital forensics through the conception of new consensus algorithms. Anytime financials are involved it makes anyone weary. So, lets take a practical and theoretical use case example of how blockchain could benefit humanity through non-financial means. This can be displayed as a voting system for American politics based on blockchain.

Now more then ever the American people need a voting system that is transparent and trustable. Currently the system is centralized with the main curator of collecting ballots being the Federal Election Commission (FEC). The problem is being that malicious actors can perpetrate that single entity and influence counts. Failing the BGP. A distributed blockchain ledger would distribute trust between many entities allowing for a more secure record that is not mutable. The public could even look up all the votes and verify that their vote was not changed or counted maliciously from the final count. This is because all nodes would agree to store that value on the public ledger and the one who got caught lying about the false vote could be traced back to origin. Creating a voting system of off blockchain could potentially facilitate the transfer of power since passing laws into action could only accept voting tokens distributed among parties. If a new president elect is selected the previous presidents theoretical voting tokens could be instantly transferred via smart contract without any type of resistance or coup.

Conclusion

This narrative has covered a wide array of topics. Including: Why the general public has mistrust about blockchain, how blockchain has advanced digital forensics via new consensus algorithms, and a theoretical use case example of how blockchain could benefit American politics. In In my future work I hope to dwell deeper into the understanding of other consensus algorithms such as Proof of Elapsed Time (PoEY), Proof of Authority (PoA), and Delegate Proof of Stake(dPoS). Along with a more in-depth practical example of how American politics can be protected through blockchain applications.

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: 11-15-2020

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: Eric Webb