

**The Case for Post Quantum Cryptography on Blockchain
Technology -Survey Paper**

by

Elsa Velázquez

B.S., Texas AM University, 1998


A.A.S., Seattle Central Community College, 2002

M.Ed., University of Texas, El Paso, 2009

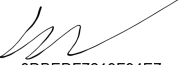
A thesis submitted to the
Faculty of the Undergraduate School of the
University of Colorado, Boulder, in partial fulfillment
of the requirements for the degree of
Bachelor's of Science
Department of Computer Science

2019

This thesis entitled:
The Case for Post Quantum Cryptography on Blockchain Technology -Survey Paper
written by Elsa Velázquez
has been approved for the Department of Computer Science

DocuSigned by:

12A7040F8964464...

Dr. Dan Massey


DocuSigned by:

8DBEDF7219F94E7...

Dr. Eric Rozner

DocuSigned by:

717B8DA8E0C145E...

Dr. Hunter Albright

DocuSigned by:

96626B5346474D0...

Dr. Jim Curry

12/13/2019
Date _____

The final copy of this thesis has been examined by the signatories, and we find that both the content and the form meet acceptable presentation standards of scholarly work in the above mentioned discipline.

Velázquez, Elsa (B.S., Computer Science)

The Case for Post Quantum Cryptography on Blockchain Technology -Survey Paper

Thesis directed by Prof. Dr. Dan Massey

The largest global corporations in the financial, medical, and governmental sectors that have invested in blockchain innovations are soon to face a significant cybersecurity threat posed by the emergence of quantum computers. By openly publishing scientific research on quantum-resistant cryptographic schemes, security agencies [turn these into footnotes, these were formerly leaders but now it's open space (e.g. NSA and NIST)], respected academic institutions [Takagi], and major tech companies [Conover]are moving forward in securing their data and assets. In this survey paper I aim to inform the broader blockchain community involved with governance, application, and security on the technical specifics as to why they, too, should pre-emptively protect their blockchain innovations systems with quantum-resistant cryptography. I also propose the development of dedicated quantum-resistant hardware as an added layer of protection. In alignment with quantum-resistant cryptography proponents, I ask: Is it possible to proactively protect data and assets from acknowledged, impending, quantum computing cybersecurity threats by using quantum-resistant cryptography in combination with dedicated quantum-resistant hardware? While these technologies do not yet exist, I have scouted, shortlisted, and helped execute Proof of Concept as a Firmware Security Engineer Intern at Seagate in 2019.

This survey paper serves as a technically accurate, detailed guide to empower the broader Blockchain community about emerging quantum-resistant cryptography in software, the possibility of applying it to dedicated hardware, and why it is important to keep up with advances in quantum computing. The specific technical usefulness of this paper is to make clear to a general audience how and why to protect themselves during the subtle step before generating hashed keys, from erroneously assuming a SHA-256 meets future post-quantum security recommendations, or from claims that a platform is legitimately using a SHA-3, 512 bit encryption scheme in their

blockchain application. This highly relevant, cutting-edge technical information has traditionally been written by, and therefore mostly only accessible only to, mathematicians, cryptographers, and scientists. Other sectors and the public in general are typically the last to know, making them the best targets for black-hat hackers. However, in this paper, it will be clear to anybody involved with Blockchain innovations, that the entire Blockchain technology is based completely upon the same quantum-vulnerable cryptography that the most prominent security, academic and technical institutions are already preparing to be safe against. Readers will easily see beyond the illusion of trust in decentralized, immutable ledger technology, so will therefore be able to proactively prepare and protect themselves and their Blockchain innovations effectively, so as to thrive during the next wave of new technology.

Dedication

To my dogs and my dawgs.

Acknowledgements

Many thanks to Dr. Dan Massey, Dr. Hunter Albright, Dr. Eric Rozner, Dr. Jim Curry, Lisa Christain, my managers at Seagate Technology Wajahat Ali, Aung Than, and Meherzad Aga, my Veteran's Administration counselors, the CU Disabilities Services Department, the McNeil Academic Program, and the creators of the movies Goodwill Hunting and The Pursuit of Happyness, all which played a role in making this dream become my reality.

Contents

Chapter

- 1 Overview
 - 1.1 Preface.....
 - 1.2 Introduction
- 2 What is a Blockchain?
 - 2.1 High Level Overview of a Blockchain
 - 2.2 Low Level Deep Dive - The Blockchain (Main-Chain) Algorithm
 - 2.3 Transactions- Bitcoin's Payment System
- 3 Current Blockchain Security Features
- 3.1 Existing Security Encryption Methods On the Bitcoin Blockchain.....
- 4 Threats and Assumptions
- 5 What is quantum computing?
- 5.1 Quantum Computing- Definition
- 6 Post-quantum Threats On the Bitcoin Blockchain
- 6.1.A. Schnorr’s Algorithm
- 6.1.B. Attacker Entry points
- 6.1.C Blockchain- Cryptographic Vulnerabilities
- 7 Proposed Quantum-Resistant Solutions
 - 7.1. Lattice-Based Cryptography,
 - 7.2. One Time Use Hashed Keys

7.3 Dedicated Hardware
8 Future Research for BB Cybersecurity
9 Conclusion

Bibliography

Tables

Table

1.1: Common Bitcoin Blockchain Terminology..... 4

Figures

Figure

1 Bitcoin Blockchain's Basic Process3

2 Basic UTXO's as Purchase Transactions on BB10

3 Blocks Chained Using Previous Hashes 11

4 Payment Channels Explanation 12

5 The ledger data structure in linked timestamping 14

6 Inputting a Public Key Necessitated to Perform a Bitcoin Blockchain UTXO 18

7 Blocks Chained Using Previous Hashes 18

8 Lightning Network Sidechain Vulnerabilities 19

9 Elementary Depiction of Quantum-Resistant, Lattice-Based Cryptography 20

Chapter 1

Overview

1.1 Preface

The United States has the good fortune of a stable fiat currency and banking system [5], so it's easy to be in the dark about the cryptocurrency, often referred to as "nerd money," that is taking hold throughout the rest of the world [20]. This "nerd money" has mysterious origins in that nobody knows who wrote the brilliant 30,000 lines of code that were subtly introduced in a 2008 cryptography mailing list as a technical white-paper under the name Satoshi Nakamoto [15]. All within those 30,000 lines of code, Nakamoto coded the new underlying technology (Blockchain) to then create the first successful cryptocurrency (Bitcoin) [16]. Bitcoin's first major PR was association to the dark web's money laundering, drugs and hitman-for-hire activity. This was possible because Bitcoin is a form of currency that is not backed by anything such as gold or government, is pseudonymous, and is worth billions of dollars in global currency exchanges [20]. Much like the California Gold Rush of 1848, Bitcoin and its underlying technology, Blockchain, has drawn major investors and hopeful individuals alike. It is changing the world.

1.2 Introduction

The blockchain audience now includes the fintech sector, insurance companies, government agencies, private individuals, artists, non-profits, and a slew of other industries [12]. Therefore, the need for diverse parties to understand blockchain security has become increasingly significant. Among the brightest software engineers to the most talented hackers, the blockchain code, which allows for the mining of Bitcoin cryptocurrency, is sometimes described as "a perfect system." Nakamoto's vision, to create a trustless system that only allows transactions that are solvent, is achieved by the code. Bitcoin blockchain code has never allowed an insolvent transaction. However, this is exactly what creates the illusion of complete safety within a known, reliable system.

At the same time that Blockchain technology and Bitcoin is gaining traction as a viable, global currency, investments in quantum computing advancements are also quickly increasing [6]. The capabilities of quantum computing are already known to be detrimental to current software-based cryptographic security

schemes [14]. These security schemes are known as Symmetric Key Cryptography schemes, and here we will focus on RSA [24]. RSA is used in combination with the SHA-256 (/SHô/ two fifty-six) hashing algorithm, which has been the gold standard data encryption method for providing safety and privacy by "scrambling" data and communications for the past nine years [19]. Everything related to online security as we know it, relies upon this RSA and SHA-256 combination or something similar.

To assume that security is irrelevant or otherwise already integrated into the blockchain ecosystem is naïve. The blockchain's architecture ensures that the blockchain itself is safe from overdrawn transactions [15], however this is not to say that the blockchain is safe from cybercrime. There will be more entry points for hacker theft and windows of opportunity for cryptocurrencies embezzlement schemes within exchanges [8] as other technologies such as quantum computing, evolve.

There exists significant research that shows the SHA-256 is quantum-safe, so the ultimate purpose of this paper is to protect Blockchain users for the subtle vulnerability that happens before generating the 256-bit hashed key. Regardless, during the latest PQC conference, NIST mentioned its intention to change the quantum-safe recommendations to SHA-3-512, which uses 512 bits. As is described in this paper, a hash of that size does not fit within the Bitcoin Blockchain architecture. Therefore, it is imperative to consider the impact of quantum computing on Blockchain security.

The goal of this survey paper is to provide technically accurate information that propels investigation into Blockchain cybersecurity beyond the currently used RSA and SHA-256 encryption method. The focus is on dissecting the specific cryptography-reliant Bitcoin Blockchain elements that will be vulnerable to cyber security threats when more people have access to quantum computers, and as more such computers become available. This paper makes evident that the SHA-256 is the only security feature of the Bitcoin Blockchain, describes the impending susceptibility to attacks, aligns with other research on securing the Blockchain with lattice-based cryptography, and proposes adding dedicated hardware for an added layer of security features.

While the attempt is made to make specific Bitcoin Blockchain cybersecurity and quantum computing topics more easily digestible by a broader cybersecurity and blockchain audience, the reader is encouraged to seek outside resources for low-level explanations of the vast technical details of Blockchain technology that are outside the scope of this survey paper. The scope of this paper is strictly regarding the Bitcoin Blockchain technology, although some concepts are applicable to other blockchains and cryptocurrencies that mimic the Bitcoin Blockchain.

Chapter 2

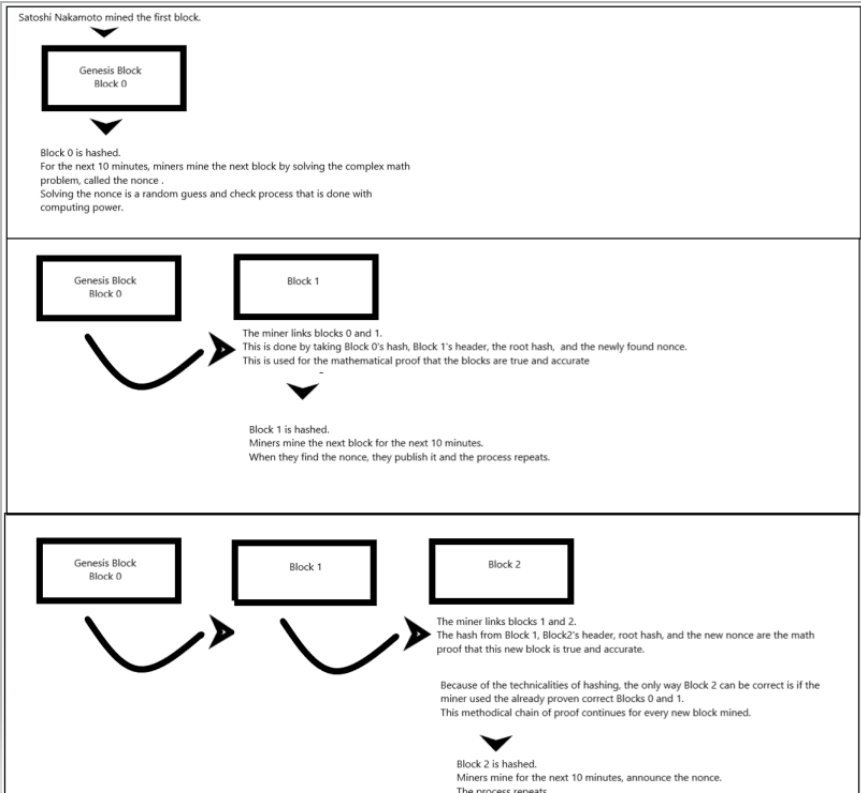
What is a Blockchain?

2.1 High Level Overview of a Blockchain

A blockchain was intended to be a peer-to-peer electronic cash system [15]. As an analogy, it can be thought of as a permanent, digital transactions ledger of inputs and outputs [22] that allows for solvent transactions between parties without the need of a bank or other third party [15]. In place of the trust granted to banks, the blockchain architecture relies on peer to peer networks, complex math problems that chain together, and cleverly coded processes to verify all transactions are solvent [15]. The following diagram illustrates the fundamental process of the Bitcoin Blockchain.

Figure 1.1: Bitcoin Blockchain's Basic Process

It is not possible to 'bounce a check' on the Bitcoin Blockchain because as the blocks chain together, the code utilizes a built-in checks and balances system to ensure there is never double spending from any account.



The following is a brief summary of common terms used in the subsequent section that are not described elsewhere. Though they are not meant as detailed, complete, technical explanations, they are useful and accurate for building an intuitive understanding of the Blockchain algorithms in general.

Table 1.1: Common Bitcoin Blockchain Terminology

broadcast	to announce some change in the blockchain to the rest of the network by posting the change in their version of the blockchain ; spreading an update about previously known information; analogy: conveying new business hours by updating them on the company website
-----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

cryptocurrency	<p>a homogenous bartering tool; exchanged for goods and services; analogy: people used to use rocks and shells instead of paper money to pay for things, cryptocurrency is like the modern, digitized version of rocks and shells</p>
main-chain	<p>the actual blockchain where transactions are permanently recorded, forever, and no changes can be made, ever analogy: like having a child, once it has happened, the truth behind it can't be changed or altered, and can be proven by tracing back to the origin using the DNA as proof (in Blockchains, the address is the proof)</p>
mine	<p>to attempt to solve the cryptographic math puzzle in an effort to win the Bitcoin reward analogy: similar to the act of searching for gold</p>
miner	<p>the person, group of people, or entity who takes it upon themselves to gather the resources and tools necessary to mine in order to look for cryptocurrency rewards and in the process are the ones who post the solvent transactions (UTXO's) permanently onto the blockchain; miners can choose to mine or not at will, and their presence or absence doesn't affect the rest of the network beyond providing competition; miners also serve as nodes analogy: similar to those who work in the industry of searching for gold</p>
node	<p>a person, group or entity that doesn't post UTXO's onto the blockchain, but can download, provide, broadcast, and verify solvency of transactions; contribute to consensus analogy: a person on Facebook or Twitter who posts something so everyone can see it, and if the person goes offline or erases their account, it doesn't bring down the entire network, it's just one less person who's online using that platform</p>
peer to peer	<p>neighboring nodes and miners who broadcast and receive updates from each other</p>
reward	<p>the cryptocurrency earned for mining a block analogy: winning tickets at a carnival that can be exchanged for rides or food within the carnival, or even sold to others who want to participate in such events at the same carnival</p>

side-chain	<p>a next-layer, more sophisticated protocol that is layered on top of the main Blockchain technology that allows for different forms of agreements to happen between parties;</p> <p>the agreements happen on "channels" and are not recorded onto the main-chain until certain steps are carried out;</p> <p>The Lightning Network is an example of a side-chain</p> <p>analogy: Alice pays Bob and Bob gives her some change, and then Bob makes the deposit at his bank</p>
------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.2 Low Level Deep Dive - The Blockchain (Main-Chain) Algorithm

1. ACreating a Block

- a. Start with Block 0, the Genesis Block
- b. Find the Proof of Work

1. Proof of Work- Definition

1. The Nonce:

a. Nonce- the solution to the crypto puzzle

b. The nonce is a number that:

- i. is some random, arbitrary number
- ii. is found using guess and check
- iii. is not a structured math problem, it's just a guessed number
 1. the guessed number is hashed using the SHA-256 hashing algorithm
 2. the hashed result is also a number
 3. the resulting, hashed number has some amount of leading zeros
- iv. it is the correct answer if its hash yields a number with an amount of leading 0's that matches the amount of leading 0's being sought
- v. drives the difficulty level of the crypto puzzle
 1. The difficulty level:
 - a. is determined by the number of leading 0's
 - b. the more zeros, the more difficult the crypto puzzle
 - c. ensures blocks are mined at a rate of 1 block/10 minutes
 - d. requires correlated computing power
 - e. is auto-adjusted with every block by the blockchain's code

2. The Nonce's Purpose:

a. The Nonce's traits

- i. is hard to find but easy to verify

- ii. the harder to find, the more cryptocurrency reward it yields
- iii. changes with each iteration of this algorithm

3. The Process:

a. If the current nonce is the right answer

- i. the right answer has the requested amount of leading 0's
- ii. using this correct answer, the miner creates the next block
- iii. the next block is the hash of
 - *the valid hash of the previous block (0 for the genesis block)
 - *the new block's header
 - *the root hash (Merkle root)
 - *the newly found nonce
- iv. the block includes the following important information:
 - 1. the transactions
 - a. miners choose which transactions to include
 - i. a party can attach a fee with their transaction
 - ii. the fee is like a 'tip' for the miner
 - iii. miners tend to pick transactions based on tips
 - iv. only solvent transactions can be included
 - 2. a timestamp assigned by a timestamp server
 - a. this is the determining factor in case of a tie
 - 3. the number of the current block
 - 4. the blockchain address of the miner who found the correct answer
- v. go to 2. Broadcasting the Correct Answer

b. If the current nonce is not the right answer

- i. find a new, different, arbitrary number to try
 - 1. some miners use the previously tried number + 1
 - 2. some miners use equations to create new arbitrary numbers
 - 3. the new arbitrary number is referred to as the new nonce
 - a. the new nonce will get tested to see if it is the correct answer
- ii. restart the process from the beginning using the new nonce

2. Broadcasting the Correct Answer

a. The winner with the correct answer rushes to propagate their answer

- i. miners propagate their answers to other nodes and miners
 - 1. it is imperative to let the greatest amount of others know, the fastest
 - 2. propagation is what wins the race
 - 3. the winner is the miner that gets more nodes and miners to validate and include their block as the latest, longest blockchain

4. to let others know, the winner broadcasts the old blockchain, plus this new block attached to the end of it
 - a. adding their block is what makes the chain the new longest chain
 - b. other miners know to check this block because it belongs to a chain that is now longer than the chain they were previously working on
 - i. the blockchain protocol states that the correct chain is the longest validated chain by the majority of nodes and miners
 - ii. miners are not likely to publish the wrong answers because it would be an incredible waste of their own resources
 - c. nodes also receive the broadcasted new chain
5. propagation speed is mostly only affected by the size of the mined block
 - a. having more transactions in the block means a slower propagation time due to the bigger block size [Eyal]
 - b. some independent analysts suggest neither geographic proximity to peers nor network speeds affect propagation [Eyal]

3. Validation Using the Proof of Work

a. The other nodes and miners verify the broadcasted block

- i. the proof of work is what is validated
- ii. the miners utilize the newly broadcasted block from 2aiii, and the previous published block's hash for the verification
 1. (the last block on the current chain, and the newly broadcasted block)
 - a. they each compare the submitted hash to the hash stored in their own local drives/hardware/cloud storage
 - b. all miners and nodes eventually have the exact same blockchain to refer back to, so there will be consensus throughout the network regarding the match
 - c. this strategy is a math-based proof that there is no cheating and ensures there is never any double spending by any account
 2. the miners and nodes combine the last block on the current chain with the newly broadcasted block as 1 long string
 3. they hash this 1 long string

4. if the hashed string from the above step results in a number that has the required leading 0's set by the Blockchain code at the beginning, the block has been validated

2. Linking the New Block

a. Consensus determines the latest mainchain

- i. each miner that is aware and in consensus with the new block, mines this new iteration of the blockchain (the old chain + the newly found block)
 1. a miner is de-incentivized from mining the wrong block because there is no payout for a block that has no potential of being validated
 - a. mining a block that has no potential for validation is also a huge waste of resources
 - b. every node and miner independently adds and propagates the latest chain with the latest block included
 2. After the new block is included in the next n iterations of the main-chain, the winner is considered official

b. The reward for winning

1. mining a block produces a substantial cryptocurrency payout
 - a. the payout is pre-programmed
 - b. the payout is programmed to diminish over time
 - c. The block reward started at 50 BTC in mined block #1 and halves every 210,000 blocks, so at block #210,000 the miner will be rewarded 25 Bitcoin per block
2. the reward is disseminated by the Blockchain code to the address that sent in the correct solution to the greatest amount of nodes first
 - a. the method to process the reward is encoded in 'the generation transaction' [cpsola]
3. the reward is programmed to be sent to the miner after n more blocks are mined

3. The Last Block

a. Bitcoin cryptocurrency is finite in amount

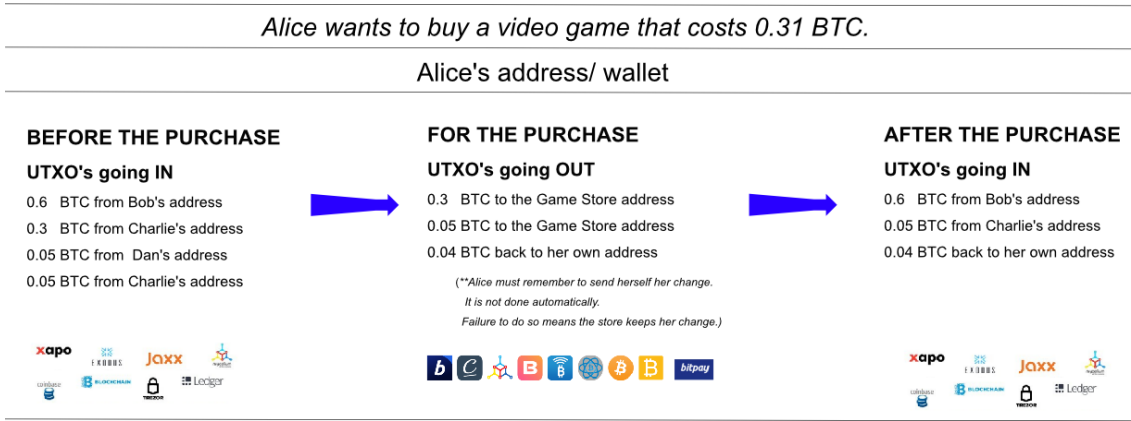
- b. Blocks will only be mined until the total cryptocurrency ever created sums to 21 million Bitcoins
 - i. it is hoped that miners will be incentivized to mine transactions by being paid fees ("tips")
- c. Until the last block is reached, repeat 1 and 2
 - i. it is not known exactly how many blocks will be mined, only the finite amount of cryptocurrency

2.3 Transactions- Bitcoin's Payment System

a. Main-Chain Payments

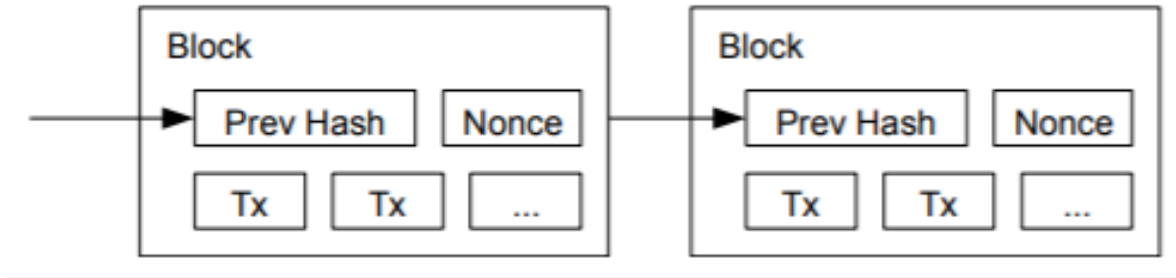
Figure 2, Basic UTXO's as Purchase Transactions on BB, shows the most basic form of funds transfer on the Bitcoin Blockchain. These transactions are called Unspent Transaction Outputs (UTXO's). The cryptocurrency at the address is what must be solvent to be included as a valid transaction on the Blockchain Main-Chain. The example shows what happens in Alice's address when she purchases a video game using Bitcoin. Every UTXO in this example would eventually be posted on the Bitcoin Main-Chain immutable ledger. This means that when the miners accept these transactions on their block, every time the word "address" is used under the "FOR THE PURCHASE" column, the SHA-256 is utilized and the itemized information, the UTXO, is recorded forever (Figure 3 - Blocks Chained Using Previous Hashes).

Figure 2: Basic UTXO's as Purchase Transactions on BB



UTXO's on a Blockchain are simply transfers in the ledger's balance “go in” from one "address" and “go out” to another. An "address" is referred to as a "wallet." Note that while it is similar to a wallet, it is not the same as a physical wallet or traditional bank account . The "wallet," in the blockchain context, is any software or hardware that stores the secure private key used to unlock the "address." Unlocking the address with the private key is what allows access the cryptocurrency [Investopedia]. Every time an address is used, as is shown in the "FOR THE PURCHASE" column, her private key is necessary to access her cryptocurrency. And then, when being posted onto the main-chain Blockchain, hashing is again used as the primary means of security.

Figure 3: Blocks Chained Using Previous Hashes [15]
 (**Tx refers to "UTXO's going OUT" in the Figure 2 example)



There are two significant nuances regarding security worth noting. First, while the blockchain keeps track of where and when its currency is transacted, it does not have access to any of the funds or a way to retrieve them. This is analogous to a delivery service that only cares to keep track of the details "to, from and when." The delivery company is neither authorized nor interested in (hopefully) breaking into the "to and from" addresses or breaking into the package being delivered, nor do they keep keys to the addresses. Only the entities with keys to the "to and from" locations can get into that location (address) or access what it is inside the package (the cryptocurrency funds) using their keys. Similarly, the Blockchain's only job and concern is to take currency from address X to address Y. The second important nuance is that while there are no rubber checks on a blockchain, i.e. double spending is not possible, this is not the same thing as an entity's assets being safe just because the assets originate from or reside on a blockchain.

It is valuable to differentiate what is meant by a secure blockchain system, and the safety of assets on a blockchain. In the Bitcoin whitepaper, Nakamoto's proposed solution to the double-spend problem (i.e. no bounced checks) hinges on "transactions that are computationally impractical to reverse" and "cryptographic proof instead of trust" [in third parties]. The assumptions of trust in a system that may be threatened are discussed later in this paper.

b. Side-Chain Transactions, An Application of Off-Chain Technology

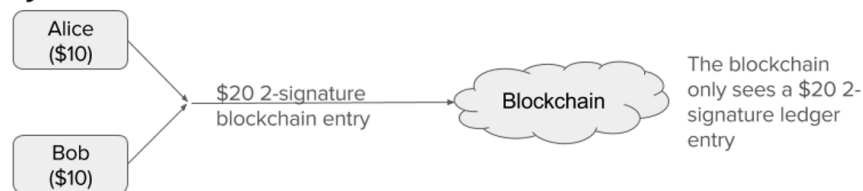
A version of Nakamoto's Simplified Payment Verification method, The Lightning Network, is one of the emerging technologies to solve the Bitcoin Blockchain scalability problem [17]. The technology has been coined "Off-Chain" because the smaller, Satoshi-sized transactions between n participants are not put on the BB's main-chain, but rather happen off to the side (Poon), unless an uncooperative party forces the need to access the main-chain [17]. Using encrypted asymmetric digital signatures via an off-chain channel, the participants create an address, also known as channel, side-channel, or Smart Contract [17].

Regardless of which participant(s) donate the funds, there must be \geq \$total transaction available in the address.

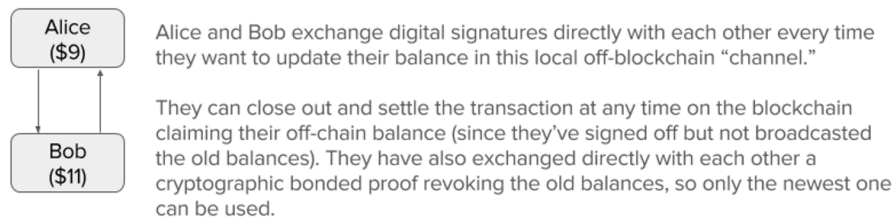
The concept is similar to the Main-Chain UTXO method described prior, in that it uses the same mechanism between n parties by repackaging anything that happened between addresses into 1 UTXO to the Main-Chain.

Figure 4: Payment Channels Explanation [15]

How Payment Channels Work



Two participants assign funds on the blockchain into an entry which requires both parties to sign off to spend from the blockchain entry.



Chapter 3

Current Blockchain Security Features

3.1. Existing Security Encryption Methods On the Bitcoin Blockchain

Bitcoin Blockchain uses the same security features available to the majority of applications available today. The same vulnerabilities that exist for other applications, also exist for the Bitcoin Blockchain.

a. Asymmetric Keys Using Elliptic Curve Cryptography (ECC)

In 2006, The Internet Society published new key exchange algorithms based on ECC for the Transport Layer Security (TLS) protocol [Blake-Wilson]. The Elliptic Curve Diffie-Hellman (ECDH) key agreement in a TLS handshake and the use of Elliptic Curve Digital Signature Algorithm (ECDSA) as new authentication mechanisms have remained an attractive alternative to RSA because it offers as much security for smaller key sizes [Blake-Wilson]. ECC is the security system used to give access to spending Bitcoin to only the person with the key pair. Note that Bitcoin uses a timestamping scheme that releases the private key of a transaction to prevent replay attacks [21].

Asymmetric Key Encryption is a signing algorithm that cycles through four steps: key generation, key distribution, encryption, and decryption. The security scheme is built upon the underlying math, which is the factorization of the product of 2 very large prime numbers. Thus, it is an NP-Hard Problem, meaning it is difficult to solve, but easy to verify, i.e., it is easy to multiply, and difficult to factor.

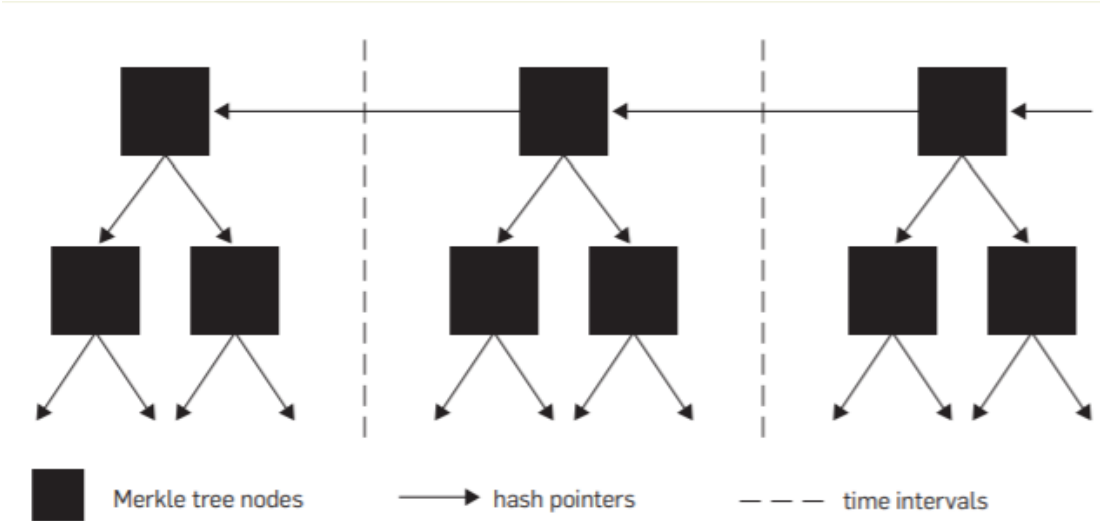
b. SHA-256

Besides RSA, Bitcoin uses the SHA-256 hashing algorithm for transaction validation via consensus [15]. Both are necessary because SHA-256 is used in https security, even though RSA alone is what generates the public and private key pair. There exists extensive research that shows the SHA-256 is quantum-safe, so as stated previously, the specific technical usefulness of this paper is to make clear to a general audience how and why to protect themselves during the subtle step before generating the hashed key, as it is typical that hashed keys are automatically generated online behind the scenes, from users erroneously assuming a SHA-256 meets post-quantum security recommendations, or from claims that a platform is legitimately using a SHA-3, 512 bit hashing algorithm in their blockchain application.

c. Root Hashes and Merkle Roots

Bitcoin leverages the Merkle Root data structure and timestamp feature to effectively and efficiently prove the authenticity of transactions [16]. Nodes and leaf pointers, which are common solutions in typical computer science problems, allow a Blockchain participant to verify that claimed transactions are true, without concern for the source of the claim [16]. Narayan’s paper, Bitcoin’s Academic Pedigree, illustrates the data structure as it is applied to Bitcoin Blockchain. Figure 5 shows a simplified version of the underlying data structure used to secure against replay attacks in the Bitcoin Blockchain.

Figure 5: The ledger data structure in linked timestamping [16]



Chapter 4

Threats and Assumptions

Only a decade ago, Dr. Bernstein made the relatively convincing case that qubits were too slow for quantum computers to pose a threat to computer security [7]. However, a slew of more recent publications, as well as NIST (National Institute of Standards and Technology) and the NSA (National Security Agency), have acknowledged the high likelihood of quantum computers breaking all encryption schemes used today [11] within ten years. This means that all forms of online security as we know it will be compromised, as will the new blockchain technology because they all rely on these same, vulnerable encryption schemes.

Dr. Massey of CU Boulder stated that the cyber-security vulnerability [to encryption schemes] stems from the assumption that we can't easily reverse engineer things, but quantum breaks some of these assumptions . With asymmetric encryption, we [were safe from attack because we] didn't know how to factor prime numbers, but with quantum computers, it's trivial to factor the private key [2]. He went on to say, "We don't have large scale quantum now, but if we did some of these assumptions [would be] wrong." In an unrelated communication, Professor Christian pointed out Canada, the US, Australia and the UK have quantum computer start-up companies, each with over \$50 million worth of private funding , which shows that we are on our way to large scale quantum computing. Because quantum computing is closer to becoming publicly accessible, there is an increased risk of black-hat hackers using it for cyber crimes.

Chapter 5

What is quantum computing?

5.1 Quantum Computing- Definition

In order to understand the concept of large scale quantum, it is useful to first establish the requirements for categorizing a computer as such. In 1996, the Watson Research Center published the following list of minimal requirements that distinguish a quantum computer [10].

1. The Hilbert space, i.e. the Euclidean definition of distance as applied to n number of dimensions by way of linear algebra vectors and dot products [1], must grow exponentially fast because each particle has up to 4 states and the system can contain infinite particles per molecule [10]. Thus, we need a multi-particle system that describes a space of $(n \text{ dimensions})^\infty$ [10]. This introduces the need for Calculus-based limits, which is outside the scope of our topic. It is important to note that a qubit, the term we use in quantum computing, is a molecule that decomposes into $(n \text{ parts } 2(1/2 + 1))$, which is a 2-dimensional particle and, therefore, analogous to our classical computer's usual bit of 0 or 1 [10]. This property is formally known as "superposition."
2. All spins must start off face down, which is achieved by keeping the system in an extremely cold state [10].
3. The system must be isolated to the point of eliminating entanglement [10]. Schrödinger's cat is the usual analogy for this phenomenon [23], and was observed and then dismissed by Einstein as "spooky action at a distance" [18]. It is formally known as "decoherence" [23].
4. The system must be able to do step by step computation that causes entanglement between the computer and the qubits [23].
5. The coupling of the entanglement must be sufficient enough to be measurable, preferably as a strong measurement, with sensitive enough equipment [10].

The usefulness of quantum computers is that once the hardware for fault-tolerant algorithms is developed, it will be possible to process many, many possible solutions simultaneously to narrow down the pool of correct solutions [3]. In November of 2019, Google made the public claim that they had developed the first quantum computer.

Chapter 6

Post-quantum Threats On the Bitcoin Blockchain

6.1.A. Schnorr's Algorithm

The development of Schnorr's Algorithm changed the security of encryption for good. It is based on the hardness to compute discrete logs and prime numbers [4]. The advent of quantum computers once the hardware for fault-tolerant algorithms is developed, is that it will be possible to process many, many possible solutions simultaneously to narrow down the pool of correct solutions [3]. In our present encryption methods, which as mentioned are the core of Blockchain technology, we can apply cryptography methods and further narrow down our solution set [2], making a brute force attack on any Blockchain UTXO key easily successful.

Blockchain posts the hashed public key, which is hashed online, behind the scenes, by third party software. Though I am not able to decrypt keys using the hash directly, I can monitor a transaction hash, and can then use a quantum computer to narrow down the subset of likely used numbers that originate that public key and run that subset of numbers to create a set of hashes, then launch a brute force attack using that subset of hashes. This is known as a pre-image attack on the SHA-256, and allows me to extract a public key from a publicly posted hash.

I can then use that public key to get the private key, because I again use quantum reverse engineering to deduce the very large prime numbers that were used for creating the public key. This is how quantum computers pose a significant threat to the Bitcoin Blockchain-- QC's are able to very quickly calculate the factorization numbers using Schnorr's Algorithm. Having both the public and private keys, I can commandeer a targeted victim's wallet address (the hashed public key) and post Bitcoin transactions on their behalf.

6.1.B Attacker Entry points

In our present encryption methods, which as mentioned are the core of Blockchain technology, we can apply cryptography methods and further narrow down our solution set [2], making a brute force attack on any SHA-256 key easily successful.

In the following diagrams, the same UTXO and side-chain transactions from before are

decomposed. Under closer scrutiny, all SHA-256 instances are circled in red to highlight hash-based attacker entry points. Note that these entry points are not the only vulnerability, there are far more cybersecurity issues to consider, however these are the focus of this paper as susceptible to quantum computing attacks.

Potential attacks on blockchains' encryption methods can be seen in Figures 6, 7, and 8 below. The specific points of vulnerability are circled in red. Shown in this way, it might seem overly obvious. However, one of the goals of this paper is to extract from the available collection of information on Bitcoin Blockchain, important vulnerabilities and depict them in a way that is easier to identify quickly and easily by broader audiences.

Figure 6: Inputting a Public Key Necessitated to Perform a Bitcoin Blockchain UTXO [13]

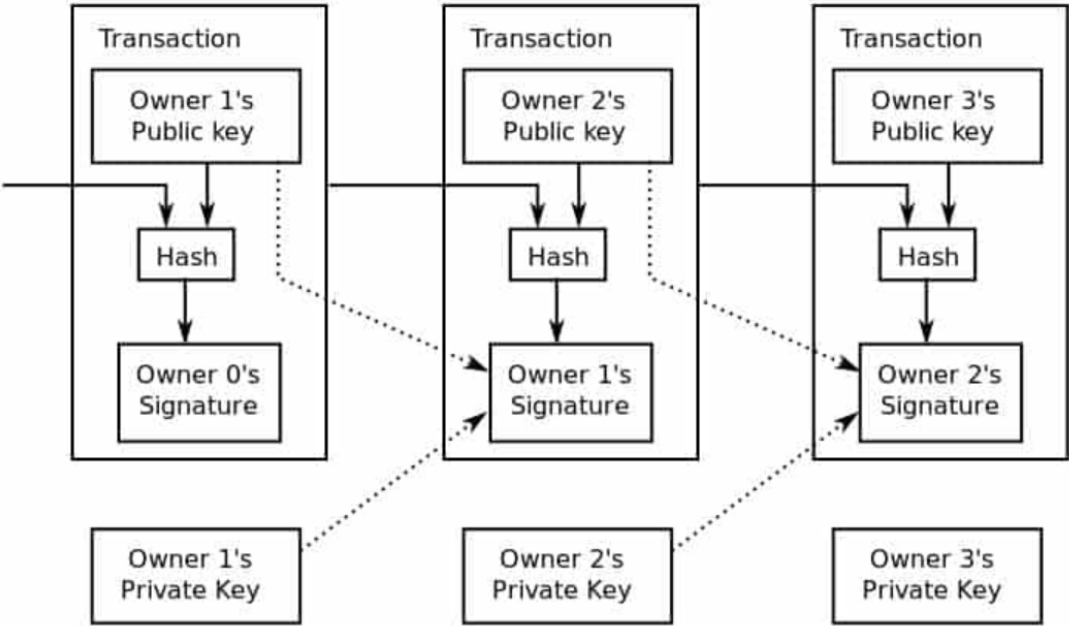
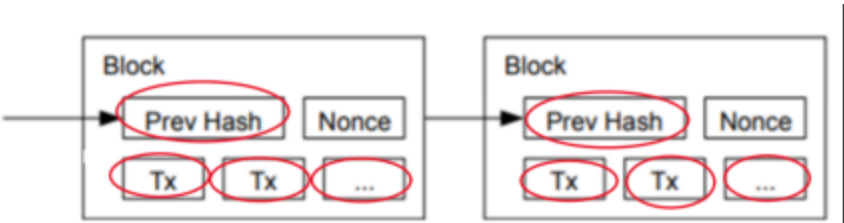
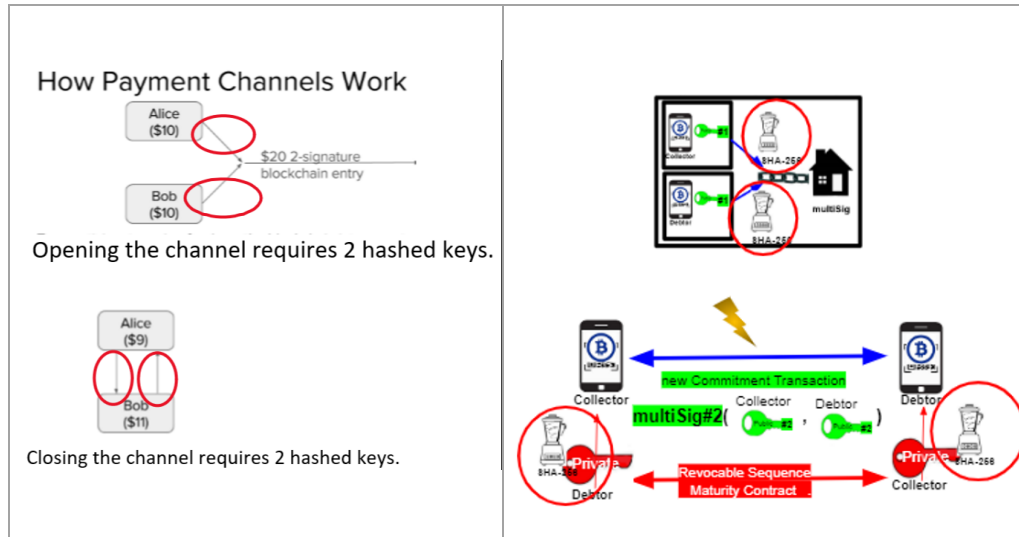


Figure 7: Blocks Chained Using Previous Hashes [15]
(** Tx refers to "UTXO's going OUT" in the Figure 2 example)



In Figure 8, Side-Chain UTXO's are shown in more detail. The side-by-side comparison of the simple explanation as compared to the underlying mechanism and technology easily highlights cybersecurity vulnerabilities that might otherwise be unknown, discounted, or overlooked.

Figure 8: Lightning Network Sidechain Vulnerabilities



6.1.C. Blockchain- Cryptographic Vulnerabilities

It is not the Blockchain that is vulnerable, it's the technology behind the encrypted keys used to access the addresses, or wallets, that cause the most obvious vulnerabilities. In Figure 1 - Blockchain mainchain vulnerabilities, it is evident that the initial UTXOs to the Bitcoin Blockchain are susceptible to the attack described in the quantum computing description. In this case, a UTXO via a unidirectional multiSig channel being opened by the Lightning Network on the mainchain relies solely on the SHA-256, so is ridiculously easy to exploit once hashes are decrypted with quantum computers. Even more vulnerable is the currently more secure method depicted in Figure 8 as Lightning Network bidirectional multiSig sidechain vulnerabilities. Ironically, the attack entry points are precisely the extra layers added for security, because all of those, too, are created by the same, susceptible SHA-256 cryptography. It is therefore critical that the entities currently researching safer cryptographic methods continue testing solutions, particularly as they apply to the misleadingly secure space of blockchain cryptocurrencies.

Chapter 7

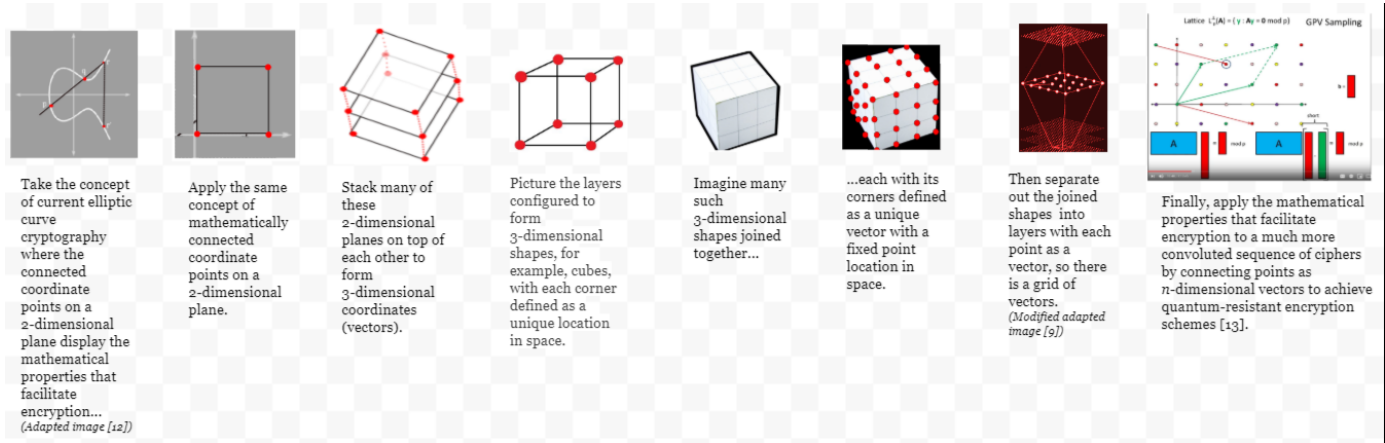
Proposed Quantum-Resistant Solutions

7.1. Lattice-Based Cryptography

Gao and Chi list the following lattice-based cryptography models as their basis for choosing this type of security over others [11][10][2]. This list includes: stochastic and short lattice construction algorithm, trapdoor functions with preimage sampling, the Lattice-based Blind Signature Scheme, which uses the trapped trapdoor one-way function, the Lattice-based Identity-based Signature Scheme (LIBSS), the bonsai tree based on hard lattice, several proxy blind signature schemes from lattice basis delegation, identity-based signcryption from lattices, and PQB [11]. All these variations of lattice based cryptography have specific nuances, therefore here we will provide only a high-level overview of lattice-based cryptography.

Figure 9, Elementary Depiction of Quantum-Resistant, Lattice-Based Cryptography, gives a simplified explanation lattice-based cryptography by using traditional traditional elliptic curve encryption as a familiar starting point and then explaining the added processes in lattice-based schemes. Going from left to right, the important points to note are that cryptography maintains the element of interesting mathematical connections dealing with symmetry, reflection, rotation, and other, more sophisticated attributes and well-known math formulas. Quantum-resistant cryptography also relies on trap doors, meaning solutions are difficult to find but easy to verify. The difference is that in lattice-based cryptography, these connections and trapdoors operate in multi-dimensional space, vs. traditional cryptography that uses only 2-dimensional points on a curve.

Figure 9: Elementary Depiction of Quantum-Resistant, Lattice-Based Cryptography



7.2. One Time Use Hashed Keys

Among the candidates submitted to NIST for the Post Quantum Non-Competition, Competition, was the use of one-time hashed keys. These have not been vetted, nor formally approved by NIST, so will not be discussed in their entirety here, but are of interest as possible future solutions.

7.3. Dedicated Hardware

Hardware with Post Quantum Cryptography features is not currently on the market, but there are companies dedicating resources to this effort. As of December, 2019, my work at Seagate included scouting for possible PQC algorithms, short listing candidates, and completing a Proof of Concept for Applications at the Firmware level with PQC. It is important to note that any product, as of this time, claiming to have PQC, would not be using algorithms enforced by NIST and the other world security organizations, as the submitted algorithms are still under review and will not be formally recommended for another year to three years.

Chapter 8

Future Research for BB Cybersecurity

Future research on the impact of QC on the BB will likely largely revolve around the development of layers to the internet protocol that are able to handle larger key sizes. Presently, there is some research showing promise in some encryption schemes, which is publicly available but is limited and falls under nondisclosure agreements in most cases. Overall there have been a few reliable PQC schemes that have been successful in being able to function with current internet protocols, but future research would be necessary to prove long-term reliability, especially as more PQC schemes begin to exist in the web.

Chapter 9

Conclusion

It is imperative to maintain public trust in blockchain technology by keeping secrets and secret keys, secret. It is equally important to support the efforts such as IBM's, who has made quantum computer access publicly available for a long time [3], so as to speed the evolution into our next phase of computing. This paper has shown that the present security schemes on the Bitcoin Blockchain is not sufficient, and that it is possible that creating quantum-resistant hardware that can provide an added layer of encryption and thus security, is the next phase in keeping public trust in Blockchain technology.

Bibliography

- [1] Hilbert space.
- [2] Lattice based cryptography for beginners.
- [3] What is quantum computing?
- [4] E Antoniadis, D Serpanos, A Traganitis, and A Voyiatzis. Software simulation of active attacks on cryptographic systems. Technical Report TR-CSD-2001-01, 2001.
- [5] Luis Araujo and Braz Camargo. Information, learning, and the stability of fiat money. Journal of Monetary Economics, 53(7):1571–1591, 2006.
- [6] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. Nature, 574(7779):505–510, 2019.
- [7] Daniel J Bernstein. Cost analysis of hash collisions: Will quantum computers make sharxs obsolete?, 2009.
- [8] S. Blake-Wilson and Y. Wang. Ecdsa with xml-signature syntax.
- [9] Chohan and Usman W. The problems of cryptocurrency thefts and exchange shutdowns, Mar 2018.
- [10] Emily Conover. Newsquantum physics- google officially lays claim to quantum supremacy a quantum computer reportedly beat the most powerful supercomputers at one type of calculation.
- [11] D.P Divincenzo. Topics in quantum computers.
- [12] Chen Xiu-Bo Chen Yu-Ling Gao, Yu-Long. A secure cryptocurrency scheme based on post-quantum blockchain, 2009.
- [13] Garrick Hileman and Michael Rauchs. Global blockchain benchmarking study, 2017.
- [14] Josh Lake. Understanding cryptography’s role in blockchains.
- [15] Michele Mosca. Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy, 16(5):38–41, 2018.
- [16] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

- [17] Arvind Narayanan and Jeremy Clark. Bitcoin’s academic pedigree. Communications of the ACM, 60(12):36–45, 2017.
- [18] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, Jan 2016.
- [19] Gabriel Popkin. Einstein’s ‘spooky action at a distance’ spotted in objects almost big enough to see.
- [20] NIST FIPS Pub. 180-2. Secure Hash Standard, National Institute of Standards and Technology, US Department of Commerce, DRAFT, 2004.
- [21] Ludwig Christian Schaupp and Mackenzie Festa. Cryptocurrency adoption and the road to regulation. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, page 78. ACM, 2018.
- [22] Yeonji Seo. Practical implementations of ecc in the blockchain. ANALYSIS OF APPLIED MATHEMATICS, page 43, 2017.
- [23] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt. Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack. Royal Society Open Science, 5(6):180410, Jun 2018.
- [24] Tsuyoshi Takagi. Post-quantum cryptography. Proc. PQCrypto, 16:1–320, 2016.
- [25] Frank Wilczek. Entanglement made simple.
- [26] Xin Zhou and Xiaofei Tang. Research and implementation of rsa algorithm for encryption and decryption. In Proceedings of 2011 6th International Forum on Strategic Technology, volume 2, pages 1118–1121. IEEE, 2011.