Post-Quantum Blockchain

Andrew Tan

Abstract

The advent of blockchain-based cryptocurrencies has garnered significant attention in recent years: reaching market capitalizations of the order of $100 billion USD in 2018; however, the cryptography underlying the security of modern blockchain networks is based on assumptions of intractability for certain tasks for classical adversaries which do not necessarily hold for adversaries equipped with a quantum computer. Given the rapid progress being made in realizing large-scale quantum computers, it is important to investigate these vulnerabilities and potential solutions. An overview of the vulnerabilities of modern blockchain networks to a quantum adversary is provided along with potential post-quantum mitigations. Additionally, a proposal for an unconditionally secure blockchain over a quantum internet and potential enhancements using causality in a Minkowski spacetime are investigated.

1. Introduction

Blockchain technology has gained significant prominence in recent years due to its widespread applicability for applications requiring distributed trustless consensus. The decentralized nature and scale of blockchain networks proves to be an interesting case study for applying quantum cryptography and cryptanalysis. As quantum computation and communication technologies improve, it will become increasingly important to understand the vulnerabilities of current blockchain networks to quantum attack. In addition, it is interesting to consider future blockchain networks based on post-quantum cryptographic protocols as well as blockchains over quantum channels. This report will address these questions with a focus on blockchains for cryptocurrency applications.

2. Overview of Blockchain

2.1. Basic Operation

Blockchain is a term used widely to describe a public, distributed, append-only database. The first functional blockchain was first proposed by Nakamoto in 2008 as the backbone of the Bitcoin cryptocurrency [31]. In addition to its applications for securing cryptocurrencies, blockchain technology has since found many other applications requiring distributed database structures with high Byzantine fault tolerance.

2.2. Blockchain for Cryptocurrencies

The distributed consensus problem is that of achieving consensus among multiple parties without the help of a trusted central authority. The main issue in securing a public ledger for a cryptocurrency is to arrive a a distributed consensus on the time-ordering of transaction. Blockchains solve this problem by combining transactions into blocks and appending them to the existing database. The creation of each block requires investment of resources: preventing adversaries with limited resources from introducing faulty blocks. A typical modern blockchain for cryptocurrency applications consists of two main parts: a proof-of-work protocol for delegating the creation of new blocks and a signature scheme used to authenticate transactions.

2.2.1. Signature Scheme

An asymmetric signature scheme is used to authenticate the spending of coins. Coins are assigned to public key accounts. In a typical blockchain network, a user transfers a coin by signing a hash of the previous transaction along with the public key of the new owner. The balance of the account can be verified by tracing the transaction history through the public ledger. All transactions are broadcast and only the first attempt to spend a coin is accepted [31].

2.2.2. Proof-of-Work for Distributed Consensus

New transactions are not considered finalized until they are placed into a block and attached to the blockchain. Bitcoin and most modern blockchains use a system known as proof-of-work (PoW) to achieve distributed consensus. The basic idea is that being delegated to create the next block requires a certain investment in the form of computational work: typically this is a search problem. The delegated block creator is disincentivized from introducing faulty blocks as a network with an honest majority will reject

such a block with high probability resulting in the forfeit of the invested computational work.

The Bitcoin network uses a variant of the Hashcash PoW system [31]. In order to append a block, a node must find a combination of a nonce and block-specific data that hashes to a value less than T set by the network. That is, given a cryptographically secure hash function $h : \{0,1\}^* \to \{0,1\}^n$; the task is to find a nonce, x, such that $h(B||x) \leq T$, where B is some function of the block. It is assumed that the output of hash cannot be predicted with any significant probability and therefore computing a block requires a brute-force search over nonces.

Let p be the probability that an honest node in the network computes the next block and let q be the probability that an attacker finds the next block. It is assumed that the probabilities of computing the next block p and q are directly proportional to the amount of compute resources owned by the honest nodes and attackers respectively. Using the fact that the Bitcoin network accepts the longest chain of blocks and modeling the block appending processes as a binomial random walk, the probability of a successfully changing a block at depth d is proportional to $(q/p)^d$. Assuming honest parties own a sizable majority of the compute power of the network, blocks at a depth $d = \mathcal{O}(1)$ can be assumed to be safe from modification: securing a distributed consensus on the time-ordering of blocks [31].

3. Basic Assumptions and Definitions

3.1. Model of Quantum Adversary

Early work by Deutsch [14] extended the Church-Turing hypothesis for classical computers through the proposal of a quantum Turing machine, a simplistic model that captures computational power of any computation that can be performed with quantum unitary dynamics. Deutsch showed that a universal quantum computer could not compute non-recursive functions demonstrating that quantum computers solve the same set of problems as classical computers.

Bernstein and Vazirani [8] later constructed an efficient quantum Turing machine and demonstrated a key relationship between problems that could be solved by a universal quantum computer with high probability in polynomial time, the complexity class known as bounded-error quantum polynomial time (**BQP**), and problems solvable by a classical Turing machine, with an oracle for randomness, with high probability in polynomial time, the complexity class known as bounded-error probabilistic polynomial time (**BPP**, a superset of **P**). Formally, they showed that $\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP}$,

with equality if and only if $\mathbf{P} = \mathbf{PSPACE}$; it is commonly believed that this last equality does not hold implying proper containment of **BPP** by **BQP**. Later, Bennett et al. [4] gave evidence that $\mathbf{NP} \not\subseteq \mathbf{BQP}$, however this is also not proven. To summarize, it is commonly believed (but not proven) that $\mathbf{NP} \not\subseteq \mathbf{BQP}$, but $\mathbf{P} \subsetneq \mathbf{BQP}$. This means problems that are provably **NP**-complete are likely safe from super-polynomial quantum speedup, but classically difficult problems (in $\mathbf{NP} \setminus \mathbf{P}$) could potentially be solved efficiently by quantum computers – some of these problems are described below.

For the purposes of this report, the adversary will be assumed to have access to an efficient quantum Turing machine and the above relationships and their consequences on computational tractability will be assumed true.

3.2. Notions of Security

Computational security is a definition of security that assumes adversaries are computationally limited. This is the standard to which most modern cryptography is held. The security of the RSA public-key cryptosystem, for example, is based on the assumed intractability of integer factorization for a classical adversary. It will be seen that this is no longer a valid assumption against a quantum adversary.

Information-theoretic security, which will be used interchangeably with unconditional security, is a stronger notion of security defined initially by Shannon [35, 29]. Unconditionally secure systems cannot be broken regardless of the amount of computational power available to the adversary. These systems derive security from information-theoretic arguments; or, based on laws of physics as in the case with most quantum cryptographic protocols.

3.3. Spacetime Structure

We will investigate some relativistic quantum protocols that make use of the causal structure of spacetime. For our purposes, we will be considering only flat, Minkowski spacetimes.

4. Quantum Vulnerabilities

4.1. Signature Scheme

The digital signature schemes used for authentication in most blockchain networks presents a significant vulnerability to a quantum adversary due to well-known quantum attacks. A quantum computer affords super-polynomial speedup to integer factorization, the discrete logarithm, and an entire related class of problems significant to most modern asymmetric cryptosystems described below.

4.1.1. Hidden Subgroup Problem

Broadly, attacks on many popular digital signature schemes can be cast as an instance of the Abelian Hidden Subgroup Problem (HSP) [20]. A formal statement of the HSP is as follows:

Let $(G, +)$ be a group, with a subgroup $H \leq G$ and a function $f : G \to X$ with the property that $\forall g, g' \in G,\ g + H = g' + H \iff f(g) = f(g')$. In other words, f is an injective mapping of the cosets of H. We say that the function f hides the subgroup H.

The Hidden Subgroup Problem: Given G, and an oracle for f, find a generating set for H.

The case where G is a finite Abelian group is known to admit quantum algorithm with super-polynomial speedup over classical algorithms. Nearly all common public key cryptosystems are based on finite Abelian groups. For example, the RSA cryptosystem is built upon the finite Abelian group $\mathbb{Z}_n^\times$. The Bitcoin protocol, for example, makes uses the Elliptic Curve Digital Signature Algorithm (ECDSA) which uses a finite Abelian group structure based on elliptic curves [1].

It is worth mentioning that finite Abelian HSP is not known to be NP-complete, and therefore the existence of a polynomial-time quantum algorithm does not violate our assumptions stated above.

4.1.2. The Quantum Fourier Transform

It will be seen that integer factorization, the discrete logarithm, and other instances of the Abelian HSP can be reduced to the problem of period finding. The main advantage of using a quantum computer is in its ability to quickly perform the Fourier transform.

Given a set of N orthonormal basis states labeled $|0\rangle, ..., |N-1\rangle$, the quantum Fourier transform is the unitary map acting as follows on the basis states (adapted from [32]):

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle$$

It will be taken for granted that such a transform is unitary and has a quantum implementation requiring $\mathcal{O}(\log(N)^2)$ quantum gates. This provides an exponential speedup over the best known classical algorithms for computing the Fourier transform which require $\mathcal{O}(N \log N)$ classical gates [32].

Shift invariance is an important property of the Fourier transform that will be useful in constructing an algorithm for the HSP. Formally stated, for an Abelian group G, and elements $k, k' \in G$, $\mathcal{F}\,|k + H\rangle = e^{i\phi}\mathcal{F}\,|k' + H\rangle$; where $|k + H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |k + h\rangle$, a uniform superposition over states in the coset $k + H$. The Fourier transform of coset states are related by a phase that does not affect measurement probabilities.

4.1.3. Shor's Algorithm

Shor first demonstrated a quantum algorithm providing an exponential speedup for integer factorization and the discrete logarithm in 1994 [36]. Both algorithms made use of the exponential speedup provided by the quantum Fourier transform by reducing the problems to one of period finding. The reduction of the finite Abelian HSP to a period finding problem is described below:

Algorithm 1: General outline of an algorithm for the Abelian HSP. Adapted from [6].

Input : An instance of the HSP with a quantum oracle for $f : G \to X$

Output: Hidden subgroup $H \leq G$

for $\mathcal{O}(poly(\log |G|))$ **do**
- prepare uniform superposition of states in first register
- $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x, 0\rangle$
- apply quantum oracle for f
- $\frac{1}{\sqrt{|G|}} \sum_{x \in G} |x, f(x)\rangle$
- measure second register
- $\frac{1}{\sqrt{|H|}} \sum_{h \in H} |k + h, f(k)\rangle = |k + H\rangle\,|f(k)\rangle$
- compute the Fourier transform of the first register
- $\mathcal{F}\,|k + H\rangle$
- measure

end

Compute H from measurements made above

First, a random coset state $|\psi\rangle = |k + H\rangle$ is created uniformly in the first register. The quantum Fourier transform is computed $|\tilde{\psi}\rangle = \mathcal{F}\,|\psi\rangle$. Due to the *shift invariance* property of the Fourier transform described above, the preparation of $|\tilde{\psi}\rangle$ for each instance of $|k + H\rangle$ produced uniformly will provide the same measurement probabilities for all cosets. Performing this

operation $\mathcal{O}(poly(\log|G|))$ times provides enough information to construct a generating set for H with probability $\mathcal{O}(1)$ [20, 6].

4.2. Example: Application to RSA Cryptosystem

To gain more insight into the HSP algorithm, its application to the RSA cryptosystem and integer factorization will be described in more detail.

With slight simplification, the RSA protocol consists of an integer $n = pq$ where p and q are large primes, and $e, d \in \mathbb{Z}$ satisfying $ed = 1 \pmod{|\mathbb{Z}_n^\times|}$; where $|\mathbb{Z}_n^\times| = \varphi(n) = (p-1)(q-1)$ is the order of the finite group. For this report, we will take for granted that given the order of the group, $\varphi(n)$, these above quantities are easy to compute [9]. Given this construction, the public key of RSA is defined as (n, e) and the private key to be (n, d). To encrypt a message $M \in \mathbb{Z}_n^\times$ in this scheme we compute the ciphertext as $C = M^e \pmod{n}$. Given the private key (N, d) and the ciphertext $C \in \mathbb{Z}_n^\times$, the plaintext can be recovered as $M = C^d \pmod{n} = M^{ed} \pmod{n}$.

The problem of *breaking* RSA can be defined as follows: given only (N, p, C), find M [9]. This can be cast as a HSP problem over the Abelian group $\mathbb{Z}$ as follows [20]:

Let $G = (\mathbb{Z}, +)$, and H be the subgroup of G containing all multiples of $\varphi(n)$, $H = \varphi(n)\mathbb{Z} \leq G$. The function $f : \mathbb{Z} \to \mathbb{Z}_n^\times$ defined as $x \mapsto a^x \pmod{n}$ for $a \in \mathbb{Z}_n^\times$ *hides* the subgroup $H \leq G$. Note that the construction of f requires only the public key for the RSA scheme. Solving the above instance of the HSP provides $\varphi(n)$. Note that since $\mathbb{Z}$ is not a finite group in this case, we choose a superposition in the first step of Algorithm 1 that is sufficient large (i.e. $\mathcal{O}(n^2)$). From $\varphi(n)$, we can deduce that $p + q = n + 1 - \varphi(n)$. The factorization is provided as the roots of the following quadratic equation $(x-p)(x-q) = x^2-(p+q)x+pq = x^2-(n+1-\varphi(n))x+n$, which is easy to compute.

Shor's algorithm provides an exponential quantum speedup for the HSP problem for $G = \mathbb{Z}$. In fact, $\mathbb{Z}$ is not a finite group, but in this case, some additional structure can be used to solve the problem [36].

4.3. Attacks on Proof-of-Work

PoW systems rely on solving a search problem. Grover's algorithm provides a quadratic speedup for search problems giving advantage to adversaries with a quantum computer.

4.3.1. Grover's Algorithm

Grover's algorithm provides a speedup for all search problems without requirement for additional structure. A search problem is defined as follows:

given a search set, X, of size N indexed by $\{1, ..., N\}$, a solution set $Y \subseteq X$, the search problem is to find any $x \in Y$.

Grover's algorithm requires a quantum oracle $O : |x\rangle |0\rangle \mapsto |x\rangle |f(x)\rangle$, where $f : X \to \{0, 1\}$ has the property that $f(x) = 1 \iff x \in Y$. The function f recognizes solutions to the search problem and is not difficult to realize for most useful search problems. For example, f can be implemented in polynomial time for search problems in **NP** even though the search problem in general cannot. The Grover operator is defined as $G = (2 |\psi\rangle \langle\psi| - I)O$ which can be seen as a rotation in the plane defined by the states of equal superposition of $x \in Y$ and of $x \in X \setminus Y$; where $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N} |x\rangle |0\rangle$ is the equal superposition of all states.

Algorithm 2: Grover's Algorithm. Adapted from [18, 32].

Input : A search problem with a quantum oracle, O
Output: A solution, $y \in Y$, to the search problem

1 prepare uniform superposition of states in first register
2 $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N} |x\rangle |0\rangle$
3 for $k = \mathcal{O}(\sqrt{N})$ compute and measure
4 $|\phi\rangle = G^k |\psi\rangle$

Some subtleties have been overlooked, but given $k = \mathcal{O}(\sqrt{N})$ iterations of the Grover operator, we are guaranteed to obtain $y \in Y$ after measurement with probability $\geq 1/2$.

5. Post-Quantum Mitigation over Classical Channels

While quantum computers are assumed to be able to solve a larger set of problems efficiently, roughly the set **BQP** $\supsetneq$ **P**, they are still believed to be constrained by some computational complexity arguments. New problems based on these revised computational assumptions can be used to secure a blockchain network over existing classical channels.

5.1. Post-Quantum Signature Schemes

Public-key cryptographic protocols that derive security from hard problems not known to permit super-polynomial quantum speedup has been the subject of intensifying research; however, these post-quantum signature schemes are relatively nascent and have not undergone significant analysis for vulnerabilities [7]. These post-quantum cryptographic algorithms can

largely be classified into several groups based on the type of problem upon which they are based: several of the most popular types are described below.

5.1.1. Hash-Based Cryptography

Hash-based signature schemes are based on the difficulty of finding the pre-image of a trapdoor function. The ability to create signature schemes based on hash functions has been investigated as early as 1975 by Lamport [23].

Lamport's signature works as follows: given a trapdoor function, $h : \{0,1\}^* \rightarrow \{0,1\}^n$; a message, $M \in \{0,1\}^m$; and a secret key of $2m$ k-bit strings, $X = (x_0^i, x_1^i)_{i\in\{1,...,m\}}$, where k is the security parameter; the public key is $Y = (h(x_0^i), h(x_1^i))_{i\in\{1,...,m\}}$; and the signature is $S = (x_{M_i}^i)_{i\in\{1,...,m\}}$. To verify a signature, the verifier computes and checks each $h(x^i)$. There are several drawbacks to this scheme: the public key and signatures sizes are large $2mk$-bits and mk-bits respectively, and additionally, each public key can only be used once. Merkle improved on the Lamport's one-use signature scheme by combining several Lamport public keys into one using a hash-tree structure [30]. One of the modern variants of this scheme, the Extended Merkle Signature Scheme (XMSS), extends the Merkle scheme by allowing a single XMSS key to generate multiple one-time-signature keys [10].

Hash-based signature schemes are attractive post-quantum options since they are not affected by Shor's attack and are based on the security of hash functions which have been analyzed for decades [7].

5.1.2. Lattice-Based Cryptography

Given a basis $b_1, ..., b_n \in \mathbb{R}^n$, the lattice L is defined to be the set

$$L = \left\{ \sum a_i \mathbf{b_i} | a_i \in \mathbb{Z} \right\} \subset \mathbb{R}^n$$

Lattice-based cryptography is typically achieved by hiding a point in a high-dimensional lattice by adding noise to a lattice vector. There are lattice problems that are known to be computationally intractable and therefore make good candidates for the basis of quantum-resistant cryptosystems [7].

Among the proposed lattice-based signature schemes, Lyubashevsky's signature scheme (LYU) shows promise [27]. Lyubashevky's signature scheme has been demonstrated to be based on the difficulty of an instance of the Shortest Independent Vectors Problem (SIVP), known to be intractable. Variants of LYU include a protocol known as BLISS [15], which has significantly reduced public key and signature sizes (see Table 1).

5.2. Quantum Resistant Proof-of-Work

All search problems will be vulnerable Grover's algorithm-based attacks that provide polynomial speedup; however, some PoW schemes that impose additional structure on top of a search problem may admit lesser speedups.

The Momentum PoW based on finding birthday collisions [24] was analyzed by Aggarwal et al. [1] and shown to admit a quantum speedup of $\mathcal{O}(n^{2/3})$ less than the $\mathcal{O}(n^{1/2})$ for a pure Grover speedup. Other PoW schemes may permit even lesser quantum speedups; however, many modern blockchain networks are seeking to replace PoW with an alternate block delegation procedure known as proof-of-stake that is agnostic to the computational power of attackers.

5.3. Proof-of-Stake

Proof-of-stake (PoS) is an alternative to PoW for arriving at a distributed consensus. A PoS protocol elects a node to append a new block by randomly selecting a node with probability proportional to an invested stake – a number of Bitcoins, for example – instead of invested compute resources in the case of PoW. The security of PoS is based on economic limitations to deter attackers instead of computational limitations: attackers introducing faulty blocks are at risk of forfeiting their invested stake. Fifty-one percent attacks are disincentivized as attackers with a large enough stake in the network to affect such an attack are unlikely to do so as the attack would significantly devalue their own position [5].

PoS is by design compute power agnostic and therefore quantum adversaries would not have an advantage under such a scheme. Several major blockchain networks, like Etherium, are looking to move over to PoS to reduce the energy cost of appending new blocks; it is likely that there will be many tested examples of PoS-based networks in the coming years.

One of the main technical challenges that needs to be addressed by a PoS protocol is that entropy needs to be introduced to perform the randomized election process in a manner that cannot be unduly influenced by adversaries [21]. Most of the proposed PoS protocols rely on a form of secure multi-party coin flipping based on vulnerable public key cryptography [21]. Unconditionally secure multi-party coin flipping algorithms and secure multi-party computation algorithms for PoS will be investigated in the next section.

6. Blockchain over a Quantum Internet

Although easier to implement as they require only existing classical channels, all classical post-quantum algorithms are based on the unproven computational assumptions. Unconditionally secure quantum protocols provide a higher standard of security derived from fundamental physical laws.

6.1. Quantum Digital Signatures

An unconditionally secure, one-use quantum digital signature scheme was proposed by Gottesman and Chuang in 2001 [17]. The idea behind this signature scheme is similar to that of Lamport's one-use signatures described above: using a quantum one-way function in place of the classical one-way function.

The security of this scheme relies on several important results of quantum information theory. This scheme requires a quantum one-way function, $h : \{0,1\}^k \to H_2^{\otimes n}$, where H_2 is a two-dimensional Hilbert space, that maps $h : x \mapsto |h_x\rangle$. For the function h to be considered one-way, we desire that $k \gg n$. It was shown by Buhrman et al. [11] that the number of states that are mutually nearly orthogonal in $H_2^{\otimes n}$ is exponential in $\mathcal{O}(2^n)$. That is, there are an exponential number of $|h_x\rangle \in H_2^{\otimes n}$, such that $|\langle h_x|h_{x'}\rangle| < \delta$, $\forall x, x'$. We will consider a quantum one-way function that produces nearly orthogonal states. The property of near-orthogonality is required to allow verification that $x = x'$ given $|h_x\rangle$ and $|h'_x\rangle$ (this is described in more detail in [17]). Holevo's theorem states that at most n-bits of classical information can be obtained from a measurement of n-qubits which contains 2^n parameters [19]. Therefore, measurements of an exponential number of instances of $|h_x\rangle$ are needed in general to recover x making h a quantum one-way function.

The scheme works as follows: given a quantum one-way function described above, h, a message, $M \in \{0,1\}^m$, and a secret key of $2m$ k-bit strings, $X = (x_0^i, x_1^i)_{i\in\{1,\ldots,m\}}$, the public key is $(|h_{x_0^i}\rangle, |h_{x_1^i}\rangle)_{i\in\{1,\ldots,m\}}$. Signing works similarly to the Lamport scheme, where the signer will disclose $(x^i_{M_i})_{i\in\{1,\ldots,m\}}$. Since the states, $|h_x\rangle$, are nearly orthogonal, a verifier can reliable verify the legitimacy of the signature.

It is likely that this one-use quantum signature scheme can be extended using a hash tree structure in fashion analogous to the extension of the Lamport scheme by XMSS. Distributing quantum keys provides another challenge, since public keys cannot be broadcast nor can they be cloned: a discussion of this is provided in [17]. An extension of this scheme could be used to secure a quantum blockchain network.

6.2. Quantum Key Distribution

The first quantum key distribution (QKD) protocol was developed by Bennett and Brassard in 1984 and is known as the BB84 protocol [3]. The protocol allows two parties with a quantum channel to generate a shared secret key. The protocol makes use of communication using qubits in conjugate bases [39] and the quantum no-cloning theorem to ensure that any eavesdroppers will be detected. The BB84 protocol is unconditionally secure [37] and can be used to generate key bits for unconditionally secure communication. The existence of unconditionally secure communication channels is used for several of the protocols described below.

6.3. Decentralized Block Creation

A protocol recently proposed and tested by Kiktenko et. al. [22] forgoes a signature scheme entirely. New transactions are broadcast through authenticated secure channels secured with QKD. Block creation in this scheme is done in a decentralized fashion without an elected leader. Unconfirmed transactions are verified and grouped into blocks periodically the protocol for Byzantine agreement by Pease et al. [33] over pairwise QKD secured channels. This is provably secure as long as the number of dishonest parties is less than $n/3$, where n is the number of nodes in the network.

However, the number of QKD authenticated communications for the block creation procedure in this scheme scales as $\mathcal{O}(n^2)$. This is likely not viable for securing a full-scale cryptocurrency, but may be useful for securing smaller distributed databases.

6.4. Secure Multi-Party Coin Flipping

A secure multi-party coin flipping protocol can be used in a blockchain network as a source of entropy to elect a block creator in a PoS scheme. Coin flipping through secure multi-party computation along with secret sharing will be considered below.

A secret sharing protocol allows for a secret value to be shared by a dealer among n participants requiring a subset of size $k \leq n$ shares to be combined in order to retrieve the initial secret, this is known as a (k, n) secret sharing scheme. Additionally, any subset of size less than k will reveal no information about the secret.

A simple scheme based on polynomial interpolation over a finite field was described by Shamir [34]: given a secret, $D \in \mathbb{Z}$, the idea is to use a $(k-1)$-degree polynomial over $\mathbb{Z}_p^\times$ for a prime, p, where $p > D$ and $p > n$. A polynomial $q(x) = D + a_1 x + ... + a_{k-1} x^{k-1} \pmod p$ is chosen with integer

coefficients a_i in uniform distribution between 0 and p. The n shares are computed as $D_i = q(i)$ for $i \in \{1, ..., n\}$. It is easy to see that any k shares will uniquely determine the $(k-1)$-degree polynomial and allow recovery of $D = q(0)$; additionally, the choice of coefficients uniformly at random ensures that any $m < k$ shares will reveal no information about D.

Shamir's secret sharing scheme does not account for a dishonest dealer. Namely, the dealer could construct the shares in such a way that there is no consistent D. Later work by Chor et al. in verifiable secret sharing addressed this problem by adding additional rounds of communication after initial share distribution to verify consistency [13]: this also increases the communication complexity of the protocol.

Verifiable secret sharing is an important component of secure multi-party communication. The problem of secure multi-party computation is as follows: given n parties each with corresponding inputs $x_1, ..., x_n$ that wish to compute an agreed upon multi-variable function, $z = F(x_1, ..., x_n)$, the protocol guarantees the correctness of z and reveals no information about any of the x_i's beyond what is implicit in z. A protocol for unconditionally secure classical multi-party computation was proposed by Chaum et al. in 1988 [12, 16] using a variation of the verifiable secret sharing scheme described above. Chaum et al.'s protocol assumed the existence of pairwise authenticated secure channels between all participants, which can be accomplished using QKD, and guaranteed unconditional security as long as the number of dishonest parties is less than $n/3$.

A secure multi-party computation protocol can be used for coin flipping and used as the basis for a secure a PoS system. For example, each node in the network can contribute a random string that is combined using a bitwise XOR to arrive at a string that is uniform at random. This is true as long as there is one honest node in the computation that independently provides a string that is uniformly distributed at random. A node can then be selected to secure the next block using the entropy generated by the coin flip.

Unfortunately, the unconditionally secure multi-party computation protocols described above do not scale well for a large-scale blockchain network requiring $\mathcal{O}(n^3)$ pairwise authenticated communications at each round, although recent work has improved on this [2]. Of course, the problem of secure multi-party computation is more general than that of coin flipping, and it is possible that more efficient secure multi-party coin flipping protocols exist that are not based on an underlying multi-party computation algorithm.

Type	Name	Security [bits]	PK Size [kbits]	Sig. Size [kbits]
Conventional	ECDSA	128	0.5	0.07
Lattice	LYU [27]	100	65	103
Lattice	BLISS [15]	128	7	5
Hash	XMSS [10]	128	0.5	20

Table 1: Comparison of classical security level, public key (PK) size and signature length of select post-quantum signature schemes with the elliptic curve-based ECDSA signature scheme currently used by the Bitcoin network. Adapted from [1].

7. Can we Take Advantage of Minkowski Causality?

Bit commitment is a protocol whereby one party wishes to verifiably commit to a value at a given time without revealing any information about the committed value until a later time. Bit commitment can also be used to implement coin flipping and therefore used as a source of entropy for a PoS scheme as described above.

General bit commitment protocols along with ideal coin flipping protocols, assuming time-like separated communication events, were proved to be impossible independently by Lo and Chau, and Mayers [25, 28].

Recent work by Lunghi et al. [26] has shown that bit commitment can be achieved if space-like separation of communication events is maintained. The commit time is of the order of time that it takes for light to travel between the parties involved in the protocol. Such relativistic bit commitment protocols have recently been implemented using a multi-round protocol that continues for the duration of the commit time [38].

It is possible that coin flipping through bit commitment can be more scalable than coin flipping based on multi-party computation: for example, a committed value could be broadcast in this scheme requiring $\mathcal{O}(n)$ communications. However, the use of space-like separation imposes considerable geographic constraints on nodes in the network that is unlikely to be scalable for any practical ad hoc blockchain network.

8. Outlook

8.1. Classical Mitigation

Post-quantum cryptographic schemes are the most immediate solution to quantum attacks as they can be accomplished over existing classical channels; however, there is still work to be done in evaluating and standardizing post-quantum algorithms before they can be deployed. In addition, many

currently proposed post-quantum schemes have key and signature sizes several orders of magnitude larger than those used today (see Table 1). This is not attractive to blockchain networks since the public record must contain the signatures and public keys related to all past transactions. Lattice-based signature schemes like BLISS show the most promise in this regard. These new signature algorithms, however, are still based on unproven assumptions on computational complexity and may prove vulnerable to attack in the future.

PoS algorithms will likely be deployed and tested in the next few years to replace existing PoW-based blockchains. The security of these PoS schemes are not based on computational assumptions, but rather economic deterrents and as a result, PoS schemes are not susceptible to direct quantum attacks. However, the security of the underlying entropy source required for a fair PoS scheme is currently based on public key cryptography which is susceptible to quantum attacks.

8.2. Unconditionally Secure Blockchain over Quantum Channels

In the ideal case, blockchain could be secured using unconditionally secure protocols; that is, a blockchain network that would not be vulnerable to adversaries regardless of their computational power. One could conceive of a scheme that used quantum digital signatures for signing transactions together with a PoS-based consensus procedure using unconditionally secure multi-party coin flipping over QKD secured channels. Of course, such a blockchain network would still be vulnerable to a fifty-one percent stake attack, but it is assumed that the proper economic incentives will be in place to deter such events. Additional research into communication-efficient unconditionally secure multi-party coin flipping will be important to address the issue of the scalability of such a system.

9. Conclusion

Based on some estimates, progress in quantum computing will render the modern cryptographic algorithms used to secure blockchain networks vulnerable in the next 10 to 20 years [1]. This report contains an overview of both short term and long term options for securing a scalable post-quantum blockchain. The most pressing challenge for blockchain cryptographers in the short term will be to develop and test new public-key protocols that are not susceptible to Abelian HSP-based attacks and that have small public key and signature sizes important for scalability. Adoption and testing of proof-of-stake based blockchains over proof-of-work systems will make the

block delegation process agnostic to computational power. In the long term, security based on computational assumptions can be dropped in favor of unconditionally secure protocols over a quantum internet.

10. References

[1] Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., and Tomamichel, M. Quantum attacks on bitcoin, and how to protect against them.

[2] Beerliová-Trubíniová, Z., and Hirt, M. Perfectly-secure mpc with linear communication complexity. In *Theory of Cryptography* (Berlin, Heidelberg, 2008), R. Canetti, Ed., Springer Berlin Heidelberg, pp. 213–230.

[3] Bennett, C., and Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (1984), 174–179.

[4] Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. Quantum complexity theory. *SIAM Journal on Computing 26*, 5 (1997), 1510–1523.

[5] Bentov, I., Gabizon, A., and Mizrahi, A. Cryptocurrencies without proof of work. arXiv preprint, 2014.

[6] Bernstein, D. J., Buchmann, J., and Erik, D. *Post-quantum cryptography*. Springer, 2009.

[7] Bernstein, D. J., and Lange, T. Post-quantum cryptography. *Nature 549*, 188 (2017).

[8] Bernstein, E., and Vazirani, U. Quantum complexity theory. *SIAM Journal on Computing 26*, 5 (1997), 1411–1473.

[9] Boneh, D. Twenty years of attacks on the rsa cryptosystem. *NOTICES OF THE AMS 46* (1999), 203–213.

[10] Buchmann, J., and Dahmen, Erikand Hülsing, A. Xmss - a practical forward secure signature scheme based on minimal security assumptions. In *Post-Quantum Cryptography* (Berlin, Heidelberg, 2011), Springer Berlin Heidelberg, pp. 117–129.

[11] Buhrman, H., Cleve, R., Watrous, J., and de Wolf, R. Quantum fingerprinting. *Phys. Rev. Lett. 87* (Sep 2001), 167902.

[12] Chaum, D., Crépeau, C., and Damgard, I. Multiparty unconditionally secure protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1988), STOC '88, ACM, pp. 11–19.

[13] Chor, B., Goldwasser, S., Micali, S., and Awerbuch, B. Verifiable secret sharing and achieving simultaneity in the presence of faults. In *26th Annual Symposium on Foundations of Computer Science (sfcs 1985)* (Oct 1985), pp. 383–395.

[14] Deutsch, D. Quantum theory, the church-turing principle and the universal quantum computer. *Proceedings of the Royal Society of London A* (1985), 97–117.

[15] Ducas, L., Durmus, A., Lepoint, T., and Lyubashevsky, V. Lattice signatures and bimodal gaussians. Cryptology ePrint Archive, Report 2013/383, 2013.

[16] Goldreich, O., Micali, S., and Wigderson, A. How to play any mental game. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1987), STOC '87, ACM, pp. 218–229.

[17] Gottesman, D., and Chuang, I. Quantum digital signatures, 2001.

[18] Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing* (New York, NY, USA, 1996), STOC '96, ACM, pp. 212–219.

[19] Holevo, A. Problems in the mathematical theory of quantum communication channels. *Rep. Math. Phys. 12* (1977), 273–278.

[20] Jozsa, R. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in Science Engineering 3*, 2 (Mar 2001), 34–43.

[21] Kiayias, A., Russell, A., David, B., and Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive, 2016.

[22] Kiktenko, E., Pozhar, N., Anufriev, M., Trushechkin, A., Yunusov, R., Kurochkin, Y., Lvovsky, A., and Fedorov, A. Quantum-secured blockchain.

[23] Lamport, L. Constructing digital signatures from a one way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, 1979.

[24] Larimer, D. Momentum- a memory-hard proof-of-work via finding birthday collisions, 2014.

[25] Lo, H.-K., and Chau, H. F. Is quantum bit commitment really possible? *Phys. Rev. Lett. 78* (Apr 1997), 3410–3413.

[26] Lunghi, T., Kaniewski, J., Bussières, F., Houlmann, R., Tomamichel, M., Wehner, S., and Zbinden, H. Practical relativistic bit commitment. *Phys. Rev. Lett. 115* (Jul 2015), 030502.

[27] Lyubashevsky, V. Lattice signatures without trapdoors. Cryptology ePrint Archive, Report 2011/537, 2011.

[28] Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett. 78* (Apr 1997), 3414–3417.

[29] Mayers, D. Unconditional security in quantum cryptography. *J. ACM 48*, 3 (May 2001), 351–406.

[30] Merkle, R. C. A certified digital signature. In *Advances in Cryptology — CRYPTO' 89 Proceedings* (New York, NY, 1990), G. Brassard, Ed., Springer New York, pp. 218–238.

[31] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system.

[32] Nielsen, M. A., and Chuang, I. L. *Quantum computation and quantum information*. Cambridge University Press, 2016.

[33] Pease, M., Shostak, R., and Lamport, L. Reaching agreement in the presence of faults. *J. ACM 27*, 2 (Apr. 1980), 228–234.

[34] Shamir, A. How to share a secret. *Commun. ACM 22*, 11 (Nov. 1979), 612–613.

[35] Shannon, C. E. Communication theory of secrecy systems. *The Bell System Technical Journal 28*, 4 (Oct 1949), 656–715.

[36] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing 26*, 5 (1997), 14841509.

[37] Shor, P. W., and Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett. 85* (Jul 2000), 441–444.

[38] Verbanis, E., Martin, A., Houlmann, R., Boso, G., Bussières, F., and Zbinden, H. 24-hour relativistic bit commitment. *Phys. Rev. Lett. 117* (Sep 2016), 140506.

[39] Wiesner, S. Conjugate coding. *SIGACT News 15*, 1 (Jan. 1983), 78–88.

Glossary

$\varphi(n)$ Euler's totient function.. 7

BPP The class of decision problems solvable by a classical computer with high probability in polynomial time.. 3, 4

BQP The class of decision problems solvable by a quantum computer with high probability in polynomial time.. 3, 4, 8

NP The class of decision problems solvable in non-deterministic polynomial time.. 4, 8

NP-complete The class of decision problems in NP that can be reduced in polynomial time to all other problems in NP.. 4

$\mathcal{O}$ Big O notation describing the worst-case asymptotic behavior of a function. . 3, 5–8, 10–14

P The class of decision problems solvable in deterministic polynomial time.. 3, 4, 8

PSPACE The class of decision problems solvable with a polynomial amount of memory.. 4

$\mathbb{Z}_n^\times$ The multiplicative group of integers modulo n (i.e. $(\mathbb{Z}/n\mathbb{Z}, \times)$) . 5, 7