Preparation for Post-Quantum era: a survey about blockchain schemes from a post-quantum perspective

Andrada-Teodora Ciulei[*] Marian-Codrin Crețu[†] Emil Simion [‡]

January 9, 2022

Abstract

Blockchain is a type of *Distributed Ledger Technology* (DLT) that has been included in various types of fields due to its numerous benefits: transparency, efficiency, reduced costs, decentralization, and distributivity realized through public-key cryptography and hash functions. At the same time, the increased progress of quantum computers and quantum-based algorithms threatens the security of the classical cryptographic algorithms, in consequence, it represents a risk for the Blockchain technology itself. This paper briefly presents the most relevant algorithms and procedures that have contributed to the progress of quantum computing and the categories of post-quantum cryptosystems. We also included a description of the current quantum capabilities because their evolution directly influences the necessity of increasing post-quantum research. Further, the paper continues as a guide to understanding the fundamentals of blockchain technology, and the primitives that are currently used to ensure security. We provide an analysis of the most important cryptocurrencies according to their ranking by market capitalization (MC) in the context of quantum threats, and we end up with a review of post-quantum blockchain (PQB) schemes proposals.

Keywords: Quantum Computing, Blockchain, Post-Quantum Cryptography, Post-Quantum Blockchain, Quantum Algorithms

1 Introduction

Blockchain is a promising technology that originated as the underlying mechanism of the bitcoin digital currency and continues to gain much interest from a variety of sectors, including banking, healthcare, cybersecurity, government, insurance, transportation, cloud storage, and real estate, due to their ability to offer ownership to verification, transparency and improved security and privacy. In the current data structure of blockchain, all these benefits are obtained using hash functions and public-key cryptography.

Quantum technologies represent one of many classes of emerging technologies, with a huge impact on actual cryptosystems, and open huge perspectives about many of nowadays open problems, especially computationally hard ones. The main cryptographic problems which are being exploited

[*] Faculty of Computer Science, Alexandru Ioan Cuza University of Iași, Email: andradatciulei@gmail.com

[†] Faculty of Computer Science, Alexandru Ioan Cuza University of Iași, Email: cretu.marian.5000@gmail.com

[‡] Politehnica University of Bucharest, Email: emil.simion@upb.ro

by quantum procedures are factoring, discrete logarithmic problem, finding the hidden subgroup in abelian finite groups, due to the order finding Shor's algorithm. [179]. Also, another canonical quantum procedure is represented by Grover's Algorithm [103], which brings quadratic speed in searching in unordered collections.

The potential of quantum technologies is continuously growing; in 2019, Google claimed Quantum Supremacy - which states that a quantum device can outperform a problem that is not solvable by a classical machine in a reasonable amount of time. Many companies are engaged in Quantum Research (for example IBM, Google, Amazon(AWS), D-Wave, Rigetti, IonQ, Xanadu, etc.), which makes this domain very competitive and with huge perspectives of evolution. Taking into account the expansion of quantum technologies, we must have a different vision about blockchain from a post-quantum perspective: we must take a look at how safe are current blockchain schemes against quantum threats. As a consequence, we might figure out the possible approaches to mitigate the distress of quantum computing, and what solutions are proposed for blockchain from this point of view.

Our review presents in the first chapter (Section 2 *Background*) a survey, which is structured as follows:

- In Section 2.1 *Quantum Computing*, there are presented the main representative quantum algorithms in the context of cryptanalysis;
- In Section 2.2 *Post-Quantum Cryptography*, we show the perspectives of quantum-resistant cryptographic schemes;
- In Section 2.3 *Quantum hardware capabilities*, the status of quantum machines is exposed (at the date of writing, from the knowledge of the authors;
- In Section 2.4 *Blockchain*, we described the concept of blockchain, the fundamentals of blockchain, and the main elements of blockchain security.

In the next chapter (*Section 3*), our work provides an exploration of the main cryptographic primitives from current blockchain schemes which are vulnerable to quantum attacks. Finally (*Section 4*), we present a short review of some proposed post-quantum blockchain solutions and a few cryptographic solutions to enhance the quantum security of blockchain.

2 Background

2.1 Quantum Computing

The concept of quantum computation was early shaped in 80s by Paul Benioff [39], Yuri Manin ([141] - according to [181]) and Richard Feynman ([151], [108], [97]). Feynman noted that it is difficult for a classical computer to simulate a quantum system that evolves in time, and stated that there is needed a machine that works under quantum physics laws to simulate that system efficiently. One of the first quantum mechanical computation models was proposed by Benioff in [40]. David Deutsch introduced and rigorously described in 1985 the *universal quantum computer* framework in [79], and after that, it was improved in 1997 by Bernstein and Vazirani in [50]. ([108])

Some of the incipient algorithms in Quantum Computing are the Deutsch-Jozsa algorithm [80] (checks if a decisional function is constant or balanced in $O(1)$) and Bernstein-Vazirani algorithm [50] (given a byte-string x of length n and a function $f(x) = s \cdot x = s_1x_1 + s_2x_2 + .. + s_nx_n$, finds the byte-string s in $O(1)$ - [162]). The first algorithm which expresses exponential speedup is the Simon's algorithm [182] : given a function f such that for two bit strings x_1 and x_2 of length n, $f(x_1) = f(x_2) \Leftrightarrow s = x_1 \oplus x_2$, for bit string s constant, the algorithm finds s in $O(n)$. [164]

A breakthrough in Quantum Computing is represented by Shor's procedures for factoring and discrete logarithm problem (DLP) ([179], [180]). These problems are based on the quantum procedure of order finding in an abelian group over $\mathbb{Z}_N$, which is based on Quantum Fourier Transform, a FFT variant implemented with quantum circuits. An important note is that we can extend the order finding procedure to period finding [151]. To summarize, the complexity of factoring and the discrete logarithmic problem is induced by the complexity of QFT, modular exponentiation, euclidean GCD, and Continuous Fraction algorithms. Therefore, the Shor's factoring and DLP procedures have the complexity $O((log\ N)^2 log(log(N)) log(log(log(N))))$ ([180],[151],[122]). In comparison, the best known classical factoring algorithm is General Number Field Sieve from [133], which complexity is $O(exp(c(log(N)^{1/3}(log(log(N)))^{2/3}))$. According to [144], some of the most popular procedures for DLP are Ro-Pollard and Silver-Pohling-Hellman algorithms, which require also the factorization of N. In conclusion, we can observe that Shor's procedures benefit of exponential advantage to the detriment of classical ones, hence cryptosystems like RSA, DSA, Diffie-Hellman, El Gamal, and elliptic curve schemes are not suitable for a post-quantum world.

Another breakthrough is highlighted by Grover's method for enhancing the search in unordered collections of size N [103]. This algorithm uses two subroutines: the first one negates the probability amplitude corresponding to the element with given property and the second one, called *inversion about mean*, amplifies that amplitude. These are repeated $O(\sqrt{N})$ times to extract with high probability the desired element. Having this result, a quantum adversary can benefit from quadratic speedup for finding a private/secret key from the whole key space. To mitigate this attack, we can simply double the size of the key. Two applications inspired from Grover's algorithm are *Quantum Counting* (see [151], [122] and [163]), and *Quantum Collision Search*, for which there is a procedure proposed by Brassard et. al. in [59] with complexity of $O(N^{1/3})$ for a function f with cardinality of domain N (see also the section *Collision Finding and Element Distinctness* from [117]). Other interesting results derived from Grover's algorithm are [57] and [85]. A quantum factoring procedure that uses Grover's algorithm to accelerate EECM (Elliptic Curve Method using Edwards Curves) was proposed in [49] by Bernstein, Heninger, Lou, and Valenta. The authors claim in the abstract that this algorithm is often much faster than Shor's algorithm.

The *Hidden Subgroup Problem* (HSP) over finite abelian groups can be solved efficiently in polynomial time (in terms of size of group) using a quantum procedure, generalized from Shor's and Simon's algorithms ([60], [92], [91], [197], [151], [122]). However, there is no polynomial quantum/classical solution for HSP over generic nonabelian groups, although there exist some special cases of noncommutative groups over which the HSP is efficiently solvable (see the references on [117] on *Non-Abelian Hidden Subgroup* subsection). A special case of groups is dihedral groups. Regev proves in [167] and [166] that the HSP over dihedral groups is polynomial reducible to

$\Theta(n^{2.5})$*-unique-SVP*, which belongs to *Shortest Vector Problem*(SVP) class, a hard relying problem of lattice-based cryptography. The current approaches for solving dihedral HSP are subexponential (Ettinger and Høyer [89], Kuperberg [128], Regev [168]). Another notable quantum-hard case is represented by the symmetric groups, over which HSP is polynomially reducible to *Graph Isomorphism Problem* (see [90], [34], [151]), which is crucial for the quantum security of the Goldreich-Micali-Wigderson Zero-Knowledge Protocol [102]. Regarding infinite abelian groups, [105] remarks that there is a direct reduction from solving HSP over $\mathbb{R}$ to solving Pell's equation (compute a pair of integers (x, y) such that $x^2 - dy^2 = 1$, for d a given nonsquare positive integer), which is the core for *Buchmann-Williams key exchange protocol* [62]. Hallgren proposed in [104] a polynomial quantum algorithm for solving Pell's equation.

In [193] and [192], there are proposed some efficient quantum solutions for problems which are instances of *Hidden Shift Problem* class. A representative example is, according to [193] and [105], the *shifted Legendre symbol problem*. Hallgren, van Dam, and Ip provided a framework in [193] which shows that the solving of the *shifted Legendre symbol problem* can conduct to breaking algebraically homomorphic encryption systems.

2.2 Post-Quantum Cryptography

Post-Quantum Cryptography reunites all research efforts to propose efficient, confident, and usable quantum-resistant cryptographic primitives to replace those current primitives whose security might be compromised by quantum algorithms [44]. Post-Quantum Cryptography permanently assumes a quantum adversary with enough hardware capacity to perform the attacks, even if the current quantum hardware capabilities do not correspond with the attack requirements.

There are deployed several efforts to decide between proposed post-quantum schemes. *National Institute of Standards and Technologies*(NIST) initiated a program called *Post-Quantum Cryptography Standardization Process* [12]. This program was calling for post-quantum cryptosystems submissions. At the time of writing this paper, there were already consumed 3 rounds of this program ([13] - 2016, [14] - 2019, [15] - 2020). Fernández-Caramès and Fraga-Lamas deployed a valuable effort in [96] to expose and to compare the performance between the cryptosystems which passed the second round of NIST call, in the context of blockchain post-quantum primitives replacement. In this section, we are using the reference [96], and the work of Bernstein, Buchmann, and Dahmen (editors) [45]. Two tables representing the cryptosystems and key exchange schemes, and signature schemes proposed and accepted in NIST second call, along with the status on NIST third call, are exposed below:

Scheme proposed	Type	Reference	Round 2	Round 3
BIKE	Code-based	[30]	✓	Alternative
Classic McEliece	Code-based	[46]	✓	✓ (merged with NTS-KEM)
CRYSTALS-KYBER	Lattice-based	[176]	✓	✓
FrodoKEM	Lattice-based	[148]	✓	Alternative
HQC	Code-based	[142]	✓	Alternative
LAC	Lattice-based	[138]	✓	
LEDAcrypt (merger of LEDAkem and LEDApkc)	Code-based	[35]	✓	
NewHope	Lattice-based	[159]	✓	
NTRU (merger of NTRUEncrypt and NTRU-HRSS-KEM)	Lattice-based	[67]	✓	✓
NTRU Prime	Lattice-based	[47]	✓	Alternative
NTS-KEM	Code-based	[27]	✓	✓ (merged with Classic McEliece)
ROLLO (merger of LAKE, LOCKER and Ouroboros-R)	Code-based	[31]	✓	
Round5 (merger of HILA5 and Round2)	Lattice-based	[100]	✓	
RQC	Code-based	[143]	✓	
SABER	Lattice-based	[78]	✓	✓
SIKE	Supersingular EC Isogenic-Based	[116]	✓	Alternative
Three Bears	Lattice-based	[106]	✓	

Table 1: Cryptosystems and key exchange protocol proposals which qualified to the second round of NIST Post-Quantum Cryptography standardization (References: [14], [15], [96]) (The references of the cryptosystem proposals are from [14] and [96])

According to [45], [44], [96] and [87], the main classes of post-quantum cryptography are the following ones:

Lattice-based cryptography: The hard cryptographic problem which relays on the security of the Lattice-based cryptosystems is *Shortest Vector Problem*(SVP), which can be reduced to another hard problems: *Closest Vector Problem* and *Shortest Basis Problem.* A particular case of the SVP is the $f(n)$*-unique-*SVP, with the extra hint that the shortest vector in an n-dimensional lattice

Scheme proposed	Type	Reference	Round 2	Round 3
CRYSTALS-DILITHIUM	Lattice-based	[139]	✓	✓
FALCON	Lattice-based	[161]	✓	✓
GeMSS	Multivariate	[64]	✓	Alternative
LUOV	Multivariate	[51]	✓	
MQDSS	Multivariate	[171]	✓	
PICNIC	Hash-based	[206]	✓	Alternative
qTESLA	Lattice-based	[52]	✓	
Rainbow	Multivariate	[82]	✓	✓
SPHINCS+	Hash-based	[111]	✓	Alternative

Table 2: Digital signature schemes which qualified to the second round of NIST call (References: [14], [15], [96]) (The references of the cryptosystem proposals are from [14] and [96])

is at least $f(n)$ times shorter that the all nonparallel vectors with it [167]. We have presented in the previous chapter that there is no quantum polynomial solution for *unique-SVP* class of problems, and by generalization, for *SVP* class (see the Stephens-Davidowitz's work [183]). The classical solutions for *SVP* have exponential time complexity (Ajitai, Kumar, Sivakumar - [26], Kannan - [120]). A less restrictive version of the *SVP* is *approx-SVP*. The solution of *f(n)-approx-SVP* is at most $f(n)$ times greater than the solution of *SVP*. Analogously, we can define the *approx-CVP*. Due to the contributions from Lenstra, Lenstra and Lovasz in [134], the *LLL* algorithm can provide a LLL-reduced basis for a lattice which can be used for solving $2^{n/2}$*-approxCVP*, and later the *BKZ-LLL* algorithm for solving $\beta^{n/\beta}$*-approxCVP*, which have polynomial complexity in lattice dimension n (see [109]). A special class of hard problem related to lattice-based cryptography is *Learning With Errors* (*LWE*), proposed by Regev in [169]. All lattice-based cryptosystems which passed the second call of the NIST PQC standardization challenge are based on *LWE* and its variants ([96]). Another solutions for lattice-based cryptography are based on the polynomial algebra, according to [96]. There are other several approaches spotted in [96] for designing the lattice-based signing schemes (for example: based on *Short Integer Solution problem* (SIS), Bonsai Trees).

Hash-based digital signature schemes: Buchmann, Dahmen and Szydlo remark in [61] that the post-quantum security of the hash-based signatures schemes relies on the collision-resistance of the underlying hash functions. We noted in the previous section that a hash collision can be found in $O(N^{1/3})$, where N is the hash space dimension. The canonical hash-based signature schemes are split in [61] in two categories: Hash-based One-Time signature schemes (Lamport-Diffie [129], Winternitz [145]) and Merkle Signature Scheme (*MSS* [145]) based. There are several extensions of MSS mentioned in [96] such as *XMSS*, *XMSS-T*, *PICNIC*, *SPHINCS* and *XNYSS* (mentioned in this order).

Code-based cryptography: In [155], Overbeck and Sendrier remark that there is no connection between the HSP problem and the coding theory, so we can conclude that code-based cryptography is quantum-resistant at this time. The code-based cryptography is based on the hardness of the Syndrome Decoding problem [155]. The canonical code-based schemes are, according to [155], the McEliece cryptosystem, Niederreiter cryptosystem, CFS signature scheme, and Stern's identification scheme, from which there are derived the majority of the code-based cryptosystems. [155] and

[96] mention that there are several error-correcting code types which are suitable for cryptographic applications (for example: Goppa, GRS, Gabidulin, Red-Muller, BCH, quasi-cyclic [155], low-rank parity-check, low-density parity-check [96], graph-based, algebraic-geometric [155]). In addition to the already mentioned types, there are proposed according to [96] code-based signature schemes based on Fiat-Shamir (which might be generally quantum-unsafe [96] - see [28], [190]) and Unruh transformations.

Multivariate-quadratric-equations cryptography: According to Ding and Yang [83], the cryptosystems based on multivariate quadratic equations are quantum-resistant, due to the NP-hardness of solving quadratic polynomials over a finite field. The main classes of multivariate public key cryptosystems are Matsumoto-Imai and *Hidden Field Equations* HFE-based cryptosystems. For digital signing, some extra classes of schemes are *Unbalanced Oil and Vinegar* (UOV)-based and Rainbow-like schemes (TTS, TRMS, Rainbow - mentioned in this order in [96]) ([83], [96]).

Supersingular elliptic curve isogeny cryptosystems: This class of cryptosystems is based on isogeny between elliptic curves on a finite space. A relevant protocol is *Supersingular Isogeny Diffie-Hellman key exchange protocol* (SIDH) proposed in [95]. SIKE [116] is the only protocol from this class that passed the second round of the NIST call, relying on ”pseudo-random walks in supersingular isogeny graphs” ([116], [96]). An important result belongs to Childs, Dao, and Soukharev in [71] and cited in [96], which states that there exist subexponential-time quantum procedures for constructing elliptic curve isogenies.

Secret-key cryptography: A relevant result belongs to Bennett, Bernstein, Brassard, and Vazirani in [41], which states that quantum computing cannot bring an exponential advantage of searching problems. This implies that all symmetric encryption and hash algorithms are quantum-safe because the brute force searching of the key and the collisions are, in these conditions, intractable ([158], [44]). However, [75] notes that there exist some symmetric cryptosystems which might be broken. The referenced cited by [75] are [172] and [121], which expose quantum solutions based on Simon’s algorithm for breaking cryptosystems based on Feistel network ([172], [121]) and for forgery on CBC-MAC ([172]) and also for another block cipher modes for MAC ([121]).

Bibliographic remark: In [96], there is exposed a separate category of protocols: **hybrid public-key cryptography**, which is represented by some post-quantum enhancements of the actual key exchange protocols to be replaced in TLS. Two major works in this direction are CECPQ1 and CECPQ2 (*Combined Elliptic-Curve and Post-Quantum* [58], [130]), developed and conducted by Google. These schemes use ECDH protocol combined with NewHope, in CECPQ1, and with variants of NTRU in CECPQ2 ([96], [130]).

2.3 Quantum hardware capabilities

The evolution of quantum hardware is an important factor for the urgency of Post-Quantum research. Therefore it is very important to spot the current quantum capabilities and the perspective of evolution. Nowadays, there are several important players in the quantum computing industry. In the following section, there are presented some of the most important current quantum capabilities.

Nielsen and Chuang enumerate in [152] the main physical candidates of quantum computers:

- **Optical Photon Quantum Computers**
- **Optical Cavity Quantum Electrodynamics**
- **Ion Traps**
- **Nuclear Magnetic Resonance Quantum Computers**
- **Spin-Based Quantum Computers**
- **Quantum Dots**
- **Superconducting Quantum Computing (Josephson junctions)**

The most promising in implementing *discrete(universal) quantum computers* are the technologies based on superconducting qubits and ion traps, according to the observations made in [70]. But we must also note that there is made staggering progress in linear optics quantum computation (also called as *photonic quantum computers*) ([125], [127], [56]).

One major obstacle in implementing quantum machines suitable for cryptographic quantum attacks is the decoherence of the qubits. First, we have to distinguish between the *physical qubit* and *logical qubit*. The logical qubit is a "theoretical" quantum bit (a superposition of two base states) that is used in describing all quantum algorithms in quantum computing formalism. However, the physical implementation of the logical qubits is extremely hard because of the decoherence. Every external interaction with the qubit can collapse its state and reduce it to a base state. This is the reason the cores of quantum computers (excepting the photonic ones) operate at very low temperatures ($-273.135°C$ [187]), as an effort to keep quantum states alive as long as possible. For example, [96] notes that the 1024-bit RSA needs approx. 2000 qubits, but the decoherence is not considered here. A challenge for the quantum computing community is constructing Noisy-Intermediate-Scale-Quantum (NISQ) devices, which proposal is to construct the logical information from physical qubits even if some of them suffer from decoherence (*fault tolerance* – see also Preskill's paperwork [160]). Google Research shows in [124] that the number of qubits to perform *Quantum Error Correction* is huge (starting from $10^5 - 10^8$ qubits).

We are going to note the following quantum devices:

- **IBM**: On 16th November 2021, IBM announced the launch of the *Eagle* superconducting 127-qubit quantum processor ([112], [36]). IBM claimed that they are the first to achieve the 100-qubit threshold. Also, Nature noted in [36] that this is an important step to accomplish the 433-qubit and 1121-qubit goals by 2023. Until then, the 65-qubit *Hummingbird* machine (2020 [98]) and 53-qubit machine (2019 ([22], [21])) from IBM were available for research, and also many other machines of smaller dimensions.
- **Google:** Google developed three superconducting quantum processors: *Foxtail*, *Bristlecone*, and *Sycamore* [17]. According to [23] and [32], Sycamore 53-qubit processor has been built using *transmon* technology, which is more resistant to external noise than classical superconducting processors (see also Transmon paper - [126]). In 2019, Google claimed the Quantum Supremacy on sampling the output distribution of random quantum circuits task using

Sycamore [32]. In 2018, Google claimed also that their processor *Bristlecone* can go up to 72 qubits [124].

- **Zuchongzhi chips:** In 2021, Zhu et.al. claimed also quantum supremacy using a superconducting transmon 66-qubit processor called *Zuchongzhi 2.1.* The chip was used on random quantum circuit sampling task on 60 qubits. The authors spotted also that their task is harder by 6 orders of magnitudes than the sampling task of *Sycamore* ([210]; see also *Zuchongzhi 2.0* - [204]).

- **Intel:** Intel revealed their 49-qubit superconducting quantum chip called *Tangle Lake* in 2018, at Consumer Electronics Show (CES) 2018 ([113], [72]).

- **Rigetti:** Rigetti is another important player in the superconducting quantum industry. At the time of the writing, the actual Rigetti *Aspen-10* machine has 32 qubits [18]. Amazon Braket (AWS) uses Rigetti Aspen as universal superconducting quantum provider [3].

- **IonQ:** IonQ is a representative example for ion-trapped quantum computing. They constructed a device with 160 qubit storage, executing properly unary qubit operations on 79 qubits and binary qubit operations on 11 qubits [10]. IonQ is the ion-trapped quantum provider for Amazon Braket service [3].

- **Jiuzhang (USTC):** In 2020, a group of researchers, mainly from the University of Science and Technology of China (USTC), projected a photonic quantum computer composed of 76 output qubits (equivalent), called *Jiuzhang*, reaching the quantum supremacy on the gaussian boson sampling task ([209],[76]). A new version of Jiuzhang, *Jiuzhang 2.0* was proposed by the same research group from USTC in [208], which is capable to produce output on 113 qubits (equivalent) on the same task.

- **Xanadu:** Xanadu provides also photonic quantum computers, based on X8 architecture (chips of 8 qubits each [73]). In 2021, Bourassa et.al. from Xanadu published an article called *Blueprint for a Scalable Photonic Fault-Tolerant Quantum Computer* [56], which might be a promising framework for future universal quantum machines. Also, they provide APIs for photonic simulation and quantum machine learning applications ([20], [19], [16]).

Also, there are other promising classes of quantum computers, which are *analog quantum computers*, which are based on quantum harmonic oscillators (boson sampling devices) and quantum annealers (or *adiabatic quantum computing*) ([70], [19], [8], [81]). There is remarked in [70] that these classes of quantum devices are not bringing significant impact in cryptanalysis.

- **D-Wave:** D-Wave provides quantum annealing systems, with applications in discrete optimization and constraint satisfaction problems ([81], [3]). This class of devices enhances the simulated annealing process by using the quantum tunneling effect, to spot the optimal or near-optimal solutions. D-Wave is the adiabatic quantum provider for Amazon Braket, which enables cloud access to two types of quantum processors: *2000Q* and *Advantage* [3].

2.4 Blockchain

Blockchain is a digital decentralized and distributed global ledger [86]. Informally, it is a database that instead of storing all the database entries on a single computer, divides data into blocks across multiple computers, called peers or nodes, connected to one network that is ruled following a precise policy.

The underlying support of blockchain is cryptography. The ideas of securing data chains using cryptography and the creation of digital currencies, at a theoretical level, have emerged since the 1980s.

David Chaum is considered to be the inventor of digital cash and blind signatures after publishing the paper [66] in 1982. In 1990 he founded *DigiCash*, an electronic cash company that created an untraceable digital currency using cryptography and private and public digital signatures [101] but declared bankruptcy 8 years later.

In May 1997 Adam Back added another brick to the foundation of today's blockchain when creating a Proof-of-Work algorithm, called *Hashcash.* It was initially proposed as a mechanism to reduce systematic abuse of illimitable internet resources such as email, and anonymous remailers [33]. In 2005, the same author gathers details about the diverse applications, improvements, and the initial experience from experiments with the algorithm in [33].

Integrating the Proof-of-Work algorithm into a computer network, in 1998, Nicholas Szabo proposed the design for the decentralized, digital currency called *Bit gold*, where a member devotes computer power to solve a cryptographic puzzle. It uses a Byzantine agreement protocol that relies on a quorum of addresses rather than a quorum of computing power [189]. Although never implemented, it is considered a forerunner of the Bitcoin architecture.

In the same year, Wei Dai introduced b-money, another precursor of today's digital currencies. He described a scheme for a group of untraceable digital pseudonyms to pay each other with money and to enforce contracts amongst themselves without outside help [4].

In 2008, the paper [149] was published under the pseudonym, Satoshi Nakamoto, which described a solution to the double-spending problem using a peer-to-peer network [115], then followed by the creation of the Bitcoin network as the first application based on blockchain technology, in 2009. Ever since Bitcoin, blockchain history has abounded in many applications using the principles and capabilities of digital ledger technology [149].

Blockchain 1.0 focused on the creation of cryptocurrencies and the development of applications with an innovative method of approaching the finance system, where the transactions are stored in decentralized, immutable, and distributed records.

Starting with 2013, we can talk about Blockchain 2.0. Ethereum was born in 2013 and officially launched in 2015, with the extended ability to support smart contracts and decentralized applications – Dapps [1] and DAOs [2]. As stated in [186], Blockchain 2.0 involves the use of blockchains in more complex processes than simple cash transactions: smart property, smart contracts, stocks, bonds, futures, mortgages, titles, and loans.

The next chapter in a world of innovation proposes the use of blockchain-based technology to a wider range of areas to record and transfer almost anything of value, and facilitate various types of business transactions when combined with other areas of development as big data, artificial intelligence, Internet of Things, and cloud/edge computing [24] [195]. Such relevant implications in other domains are presented in [24]:

1. **Contractual agreements execution and settlement**
   Instead of maintaining a bank account and shares with the institutions which assist with the agreement, share tokens can take the place of share certificates in digital format while smart contracts can be used to automate the execution of agreements and assign rights to classes of shares to these tokens [24].

2. **Reconciling and auditing information**
   Contemporary techniques of auditing entail adding accounting information in multiple databases, and preparing cyclical reports and audits for regulators [24].

   Using blockchain technologies, the registration of transactions takes place when the transaction is initiated, allowing to obtain consistent data in real-time, in a recurring format, reducing human errors, processing time, and removing the necessity for auditors to reconcile distinct ledgers[173]. In addition, adopting blockchain technologies more automation, analytics, and machine-learning capabilities could be added to the actions of the auditors to obtain features like automatically alerting parties about suspicious transactions [7].

3. **Signing on behalf of a counter-part**
   As presented in [24], an example of this would be the action of undertaking a proof of funds, in which case the process of importing or exporting financing is facilitated by the possibility for clients to demonstrate the availability of funds by signing a message on the Blockchain, instead of requesting a letter from their bank.

4. **Connecting systems to IoT devices**
   IoT devices capture data to be analyzed by systems that are Blockchain oracles or forward the results to other Blockchain oracles. These data are useful in fraud prevention, production facility status [24], and insurance where smart contracts can be used in monitoring temperature-sensitive products during transportation to reduce the costs for insurance companies, shippers, and exporters [195].

5. **Transfer of assets**
   Assets can be registered and transferred more easily by linking them to smart objects. The participants will access the same copy of one ledger instead of multiple ledgers from different owners. Timestamping helps with avoiding conflicts between counterparty proposals [24], the double-spending problem on an asset is prevented, and it ensures non-repudiation taking into consideration that only authenticated and authorized users can update or transfer the asset.

6. **Regulatory compliance automation**
   Blockchain can be used to improve the efficiency, reliability, and transparency of compliance and regulation, and bring evolution to the service industry through innovating its structure

and producing new business models [6]. It can provide access to auditable, time-stamped, and immutable data, creating in this way a transparent environment, with instruments to monitor and quantify the reliability and reputation of users, where the community approves the changes via consensus, thus reducing the counterparty and settlement risks [6]. As stated in [6], the balance between market stability and regulations leads to the convergence of industry and government interests. More accurately, blockchain can help in providing access to tamper-proof public records such as passports, licenses, vehicle registrations, building permits, and official records such as patents, certificates, degrees.

7. **Providing portable identity**
   Through cryptography, participants in a Blockchain can generate their own identity and use it across multiple services.

8. **Automating companies and investment vehicles**
   The use of smart contracts facilitates corporate governance management, offering near-free, and zero transaction/agency cost coordination of agency relationships[119]. They automate processes like listing the investors, storing board decisions, and allocating assets. Another aspect to mention is that smart contracts bring transparency in managing the holdings of a business, taking into consideration that their execution depends only on the code, without any intervention from a biased agent.

Based on hash functions and public-key cryptography, immutability, decentralization and distributivity, security, efficiency, and reduced costs are the key principles that highlight blockchain technology to the researchers.

- **Immutability**: Transactions cannot be altered or deleted after adding them. All the nodes have a copy of the digital ledger, and a new transaction can be added only after it is considered valid by the majority of nodes.

- **Decentralization and distributivity**: The network does not have a governing authority, the intermediaries are removed promoting transparency and trust between the participants. Each node of the blockchain has access to the entire distributed network which is controlled through the consensus algorithm.

- **Efficiency and reduced costs**: Removal of intermediaries leads to faster settlements compared to the traditional banking systems, and reduced costs by replacing individual ledgers with a single shared ledger, providing real-time settlement and auditing from all parties connected to the network each time a transaction occurs [101].

2.5 Blockchain fundamentals

On a broad level, a blockchain is a list of records of transactions, named blocks, connected using cryptography. As mentioned before, the computers are grouped to each other in a network (peer-to-peer), without having a central server.

There are several types of blockchains leading to the need of having nodes with different roles in the system.

- **Public blockchains** are permissionless and completely decentralized. They allow anyone to join and participate in the core activities of the network with equal rights to access, create and validate blocks of data. They have challenges in privacy and scalability, but anonymity is high in these types of systems.

  Bitcoin, **Ethereum**, **Litecoin**, **Monero**, **Zerocash** are popular examples of permissionless public blockchains.

- **Permissioned public blockchains** are partially decentralized. Anyone can read, but the rights of writing and taking part in the consensus protocol are controlled by the network administrator.

  In permissioned public blockchains, the anonymity is high, scalability is moderate and their main challenges are privacy and centralization.

  Examples of permissioned public blockchains are **Ripple**, a business-to-business virtual currency exchange network, **EOS**, and **Libra**.

- **Permissionless private blockchains** are governed by a group of organizations that collaborate with each other while maintaining their data private to the exterior. Anonymity and scalability are both moderate for this type of blockchain, while the consensus protocol is challenging.

  An example is **LTO** which is a permissionless private blockchain that creates a ”live contract” on the network [165].

- **Permissioned private blockchains** are used in organizations and access to the blockchain is controlled by some members of the organization. The network administrator has the role of granting membership in the network, and read and write rights.

  In this type of blockchain, anonymity is low, scalability is high and challenges may occur in the consensus protocol or centralization.

  Examples of permissioned private blockchains are **Monax** and **Multichain**.

- **Consortium blockchains/federated blockchains** are obtained by combining the permissioned public blockchain type with the permissionless private blockchain type.

  Examples: **Corda**, **Hyperledger**, **Quorum**.

- A **hybrid blockchain** is a type of blockchain that integrates a private permissioned system along with a public permissionless system, allowing the establishment of the entities that access the recorded data and which data will be publicly available.

2.5.1 Blockchain nodes

Nodes are the electronic devices connected to the network which possess an IP address. They are the communication endpoints through users or applications interact and at the same time, they can be viewed as a point of communication redistribution [115]. Not all the devices interacting with the network are nodes, and the functionality for a node depends on the role inside the blockchain ecosystem.

To offer a seamless experience, the roles are defined by the requirements of the network. Among these roles, we mention the following:

- **Managing and validating transactions:** the node takes part in the consensus algorithm for validating transactions, records the data, and sends the data back to the peers to maintain the synchronization. Storing the cryptographically linked blocks: when a new block is added to the chain, the nodes must synchronize to maintain a single copy of the ledger.

- **Acting as a point of communication:** the node gives access to the data stored on the Blockchain. For example, **Corda Blockchain** has two types of nodes, one for the client and one for the digital notary that validates the transactions. Another prominent example is the **Hyperledger Fabric Blockchain Network** that requires multiple roles to provide a modular architecture. This includes a node for a Membership Service Provider, Users, Endorsers, Anchors, and more such entities [115].

Blockchain node classification:

1. **Full nodes:** considered the servers of blockchains, they maintain all the transaction records and are a part of the governing model, voting if upgrades or improvements should be accepted in the blockchain. If most of the full nodes agree with a certain modification, there is the option to create a hard cryptocurrency fork, splitting the blockchain in two. The full nodes can also be classified into:

   (a) **Pruned Full Nodes:** the nodes have a limit of how many blocks can be stored on them. When the limit is reached, they delete the old blocks maintaining only the essential metadata and sequence, and then add the new blocks.

   (b) **Archival Full Nodes:**

      i. **Authority nodes:** authorize other nodes to join the network or define other nodes' access to a particular data channel

      ii. **Miner nodes:** they carry out the mining process (through some consensus algorithms as Proof-of-Work) as validation tasks require significant computational power and energy consumption

      iii. **Staking nodes:** do not require high computation power, they are selected according to some pre-defined rules such as time spent on the network in some algorithms as Proof-of-Stake to stake the money, validate the transaction, and get rewarded for the process

      iv. **Masternodes:** do not have enough power to add new blocks but they maintain the ledger and validate the transactions

2. **Light Nodes** or **Simplified Payment Verification nodes:** store and provide only the necessary data to accommodate daily activities or faster transactions

3. **Super Nodes:** created to resolve special tasks like maintaining the Blockchain rules

4. **Lightning Nodes:** used to avoid the congestion that leads to delayed transactions by creating a separate network with a user and pushing transactions to the main network

Blockchain node structure:

To initiate a transaction, a user will obtain a digital signature by signing it with the private key. Then, the transaction will be broadcasted to the verifying nodes which will validate the transaction following one of the consensus algorithms.

As presented in *Figure 1*, on a large level, each block holds a block header and a body with the list of transactions recently added.

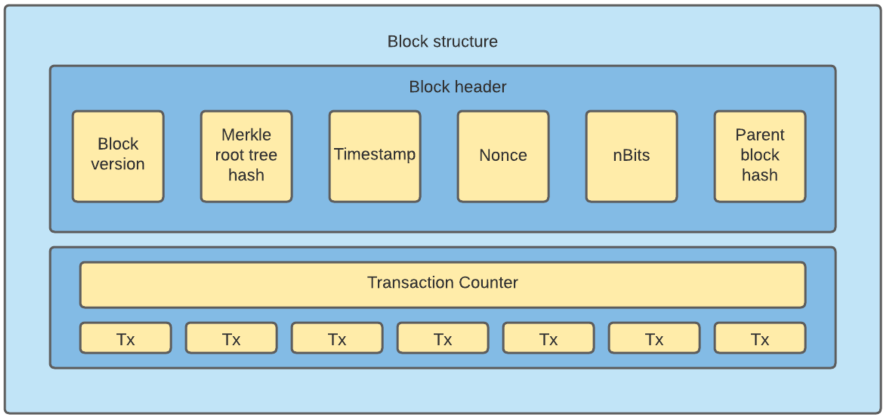

Figure 1: Block structure

The block header contains:

- **The block version:** indicating the set of rules to follow when validating the block.
- **The Merkle tree root hash:** the hash of the Merkle tree stored in the block body. The root is used to simplify the efforts of verifying the transactions in a block.

  The Merkle tree is a binary tree with leaf nodes tagged with the hash of one transaction saved in the block body, and the non-leaf nodes labeled with the concatenation of the hash of its children [136].
- **A timestamp:** representing the current time in seconds in the universal time since January 1, 1970. It proves that the content has not changed since the time of the transaction.
- **A nonce:** used in the creation and verification of a block.
- **nBits:** a target threshold of a valid block hash.
- **The parent block hash:** a hash of the previous block header.

Further, we will briefly explain what consensus algorithm entails and 2 of the most popular consensus algorithms.

The idea of reaching a consensus is a necessity between the blockchain nodes because it is a way to create fairness and equality among the participants and to establish an agreement even though there are minorities who disagree with the resolution. For this objective, there exists a wide variety of consensus algorithms, with various advantages and disadvantages.

1. **Proof of Work (PoW):** The miner nodes deploy hardware to guess the answer to a mathematical problem. Every time a miner guesses, it constructs a block that will be accepted as legitimate if the chain is the one with the most accumulated Proof of Work. If an entity controls enough hashing power to surpass the honest chain, it can re-write the blockchain by mining on an existing block instead of the latest block. If there are changes in the network's consensus rules, they must be approved by the majority of the miners. There are soft forks where enough miners must agree with a new rule set, while hard forks will split the network into 2 components where the chain with the most PoW will decide which one is accepted as legitimate.

2. **Proof of Stake (PoS):** It was firstly introduced by Sunny King as an alternative method of deciding which node can add new blocks and verify the current state of the blockchain. In contrast to PoW, in PoS the new block is added based on a process influenced by the number of coins staked in the network. It reduces 51% attack because, for an attack to work, it would be necessary for the attacker to buy half of the cryptocurrency and then destroy it.

Other consensus algorithms are: *Practical Byzantine Fault Tolerance (PBFT)*, *Proof of Burn (PoB)*, *Proof of Capacity*, *Proof of Elapsed Time*, *Proof of Activity*, *Proof of Weight*, *Proof of Importance*, *Leased Proof of Stake*, etc.

2.6 Blockchain security

According to [198], at the moment, blockchain security primitives can be categorized as **primary** and **optional**.

- Hash functions and standard digital signatures belong to the first category, being fundamental for ensuring the blockchain as a globe ledger with tamper-proof, public verifiability, and achievable consensus [198].

- In the second category, we mention special signatures, accumulators, zero-knowledge proof, and commitments which are primarily used for improving the privacy, anonymity, and traceability of the transactions, to which we add secret sharing and oblivious transfer which participate indirectly in commitments construction and zero-knowledge proof [198], [184], [205], [156].

2.6.1 Hash functions

Hash functions are used for solving cryptographic puzzles, in the process known as mining (PoW), address generation for public/private keys, block generation (in Merkle-tree paradigm, MKT), message digest in signatures (MDS), pseudorandom number generation (PNG), and bridge components (in mechanisms like Fiat-Shamir mechanism abbreviated FSM) [165] [198].

Bitcoin uses the *SHA256d* construction defined as:

$SHA256d(message) = SHA256(SHA256(message))$

To add a new block to the blockchain, during the mining process, it is necessary for the miner to find the Nonce that solves the following puzzle:
$SHA256d(X||Nonce) \leq T$, where T is the 256-bit target value.

The first l blocks from the hashed value must be all zero, and l is adjusted, after each generation of 2016 blocks, to maintain the average time for the generation process to about 10 minutes.

Inspired by the Back's idea from 1997, the main role of PoW is to enable a decentralized group without pre-established trust to agree on consistent transaction history and prevent double-spending attacks [149].

Given that the code for **Bitcoin** is open-source [5], **Bitcoin** forks appeared in the following years introducing various ASIC-resistant and memory-hard hash functions to resist the development of the mining techniques [198].

Litecoin replaced *SHA256d* with *SCrypt* [157], a memory-intensive compilation of use of the HMAC construction instantiated with *SHA256*, and use of the stream cipher *Salsa20/8* [43] [165]. Other cryptocurrencies that use *SCrypt* are **Tenebrix** and **Fairbrix**. **Ethereum**-based cryptocurrencies use *Ethash* [9] as ASIC-resistant hash function, original from *Keccak256* and *Keccak512* [198].

Darkcoin uses *X11*, a memory-hard hash function proposed by Duffield by combining sequentially 11 hash functions like *Blake*, *Grostl*, *JH*, *Keccak*, *Skein*, *ECHO*, *Luffa*, *BMW*, *CubeHash*, *SHAvite*, and *SMID*.

2.6.2 Digital signatures

The main purpose of signing the transactions with standard digital signatures in the blockchain is to prove the authenticity of the source of a transaction [137] [198], and to ensure integrity, and non-repudiation of the sender. In the signing process, the private key is used to sign the transaction, while the public key is used to verify the validity of the signature.

The most used digital signatures in blockchains are based on the hardness of the elliptic curve version of discrete logarithm problem [198]: *ECDSA - Elliptic Curve Digital Signature Standard* (used in **Bitcoin**, **Ethereum**) and *EdDSA-Edwards-curve Digital Signature Algorithm* [118] [48] (used in **Naivecoin**, **Monero**).

Most often, special signatures schemes are used to provide extra features such as privacy, unlinkability, and anonymity or to generate constant size signatures through signature aggregation [165].

For instance, in **Bitcoin**, *Schnorr Signatures* have replaced *Pay to script hash*(P2SH), being considered a form of signature aggregation [165], and whose scope is to provide scalability[77].

2.6.3 Special signatures

- **Ring Signature:**

  First introduced by Rivest, Shamir, and Tauman [170], they enable a user to sign a message so that a ring of possible signers (of which the user is a member) is identified, without revealing exactly which member of that ring generated the signature.

  Even though other signatures can be applied to provide anonymity, only ring signatures are used to provide the anonymity [165] of the signer in blockchains.

  Another use is to create untraceable payments (**CryptoNote**) [194] [198] [38].

- **Threshold Signature:**

  Used to provide anonymity, a (t, n) threshold signature is a signature where n parties receive a part of the private key and any t or more participating parties can produce signatures on behalf of the group.

  Used in: **CoinParty** [211], **ShareLock** - practical privacy-enhancing tool for cryptocurrencies which uses *ECDSA* [178], *EdDSA* [118] [48] that uses the *Edwards25519* curve. *EdDSA* is also used in **Libra** in the process of generating new account addresses.

- **Multi-Signature:**

  A group of signers realizes a common signature, to obtain a more compact signature than an assembly of signatures on the same message from all the signers [132].

  It is worth mentioning that aggregate signature is a non-trivial generalization of multi-signature, used for saving storage and bandwidth [198].

  An example of such a signature is EC-Schnorr multi-signature scheme extended from the EC-Schnorr signature scheme for only one user [146].

- **Blind Signature:**

  Blind signatures are used to provide unlinkability and anonymity of the transaction in the case when the signer and the message authors (transaction in case of blockchain) are different parties.

  Used in: **BlindCoin** [191] and **Bitcoin** to provide the anonymity for the **Bitcoin** on-chain and off-chain transactions [107] [165].

2.6.4 Encryption schemes

They are mainly used to achieve the confidentiality of data in blockchain systems.

Some examples of use are: in **Hyperledger fabric** to offer confidentiality of smart contracts [29] [165] and Blockchain for Smart Home [84] [165].

Authenticated encryption can be used to provide confidentiality and authenticity of data[165].

Broadcast encryption is used to provide the anonymity of blockchain receiver nodes [165]. [55] presents mechanisms to provide devices updates availability and innocuousness.

3 Analysis of cryptographic primitives of most important blockchain schemes in the context of quantum threat

In this section, we are considering the most important cryptocurrencies according to their ranking by market capitalization (MC) from [74]. There are done several cryptographic classification research in [94], [198] and [185], which we are going to use in this section.

3.1 Signature schemes

According to Ethan Fast's work [94] and to the previous subsection *Blockchain Security: Digital Signatures*, the main algorithms used in digital signing in the first 100 cryptocurrencies from February 2021 are *ECDSA*, *EdDSA*, *Schnorr*, *EC-Schnorr*, *RSA*, *Bulletproofs*, *Winternitz OTS* and *ZK-SNARK*.

3.1.1 ECDSA

Mainly, the elliptic curves used in ECDSA in cryptocurrencies are *secp256k1* (see [65]) and rarely *NIST P-384*, *NIST P-256* (see [153]) [94].

Cryptocurrency	Symbol	Signing algorithms	Curves
Bitcoin	BTC	ECDSA	*secp256k1*
Ethereum	ETH	ECDSA	*secp256k1*
Binance Coin	BNB	ECDSA	*secp256k1*
XRP	XRP	ECDSA, EdDSA	*secp256k1*, *curve25519*
Terra	LUNA	ECDSA	*secp256k1*
Polkadot	DOT	ECDSA, Schnorr, EdDSA	*secp256k1*, *curve25519*
Avalanche	AVAX	ECDSA	*secp256k1*
Dogecoin	DOGE	ECDSA	*secp256k1*
Crypto.com Coin	CRO	ECDSA	*secp256k1*
Litecoin	LTC	ECDSA	*secp256k1*
TerraUSD	UST	ECDSA	*secp256k1*
NEAR Protocol	NEAR	ECDSA, EdDSA	*secp256k1*, *curve25519*
Bitcoin Cash	BCH	ECDSA	*secp256k1*
Tron	TRX	ECDSA	*secp256k1*
Cosmos	ATOM	ECDSA	*secp256k1*
VeChain	VET	ECDSA	*secp256k1*
Hedera	HBAR	ECDSA, EdDSA, RSA	*NIST P-384*, *curve25519*
Filecoin	FIL	ECDSA	*secp256k1*
Theta Network	THETA	ECDSA	*secp256k1*
Ethereum Classic	ETC	ECDSA	*secp256k1*
Tezos	XTZ	ECDSA, EdDSA	*secp256k1*, *curve25519*, *NIST P-256*
EOS	EOS	ECDSA	*secp256k1*

Table 3: The top 22 cryptocurrencies which use ECDSA and are present in [94], ordered by MC by 1st January 2022; Adapted from Ethan Fast's research [94]; References: [94], [198], [185], [74]

There exist a class of cryptocurrencies that run on the Ethereum network, instead of their ones. These cryptocurrencies implement the ERC-20 (*Ethereum Request for Comments*) standard ([196],[93], [94]). Peter Waterland mentioned in [199] that there were 45 ERC-20 cryptocurrencies in the top of 100 blockchain schemes in May 2020. Hence, these schemes implement the same digital signature scheme as Ethereum, respectively ECDSA. (example: *OpenZeppelin* - a library for creating smart contracts for Ethereum, which implements ERC-20 standard using ECDSA - see [154]).

Examples of ERC-20 tokens (excepting the already mentioned in tables): **Tether**(USDT), **ChainLink**(LINK), **Shiba Inu**(SHIB), **USD Coin**(USDC) ([88], [93], [94])

3.1.2 EdDSA

The elliptic curve used in Edwards-curve Digital Sign Algorithm (EdDSA) in cryptocurrencies is mainly *curve25519* (see [42]) [94].

Cryptocurrency	Symbol	Signing algorithms	Curves
Solana	SOL	EdDSA	*curve25519*
Cardano	ADA	EdDSA	*curve25519*
XRP	XRP	ECDSA, EdDSA	*secp256k1*, *curve25519*
Polkadot	DOT	ECDSA, Schnorr, EdDSA	*secp256k1*, *curve25519*
Algorand	ALGO	EdDSA	*curve25519*
NEAR Protocol	NEAR	ECDSA, EdDSA	*secp256k1*, *curve25519*
Stellar	XLM	EdDSA	*curve25519*
Hedera	HBAR	ECDSA, EdDSA, RSA	*NIST P-384*, *curve25519*
Elrond	EGLD	EdDSA	*curve25519*
Monero	XMR	EdDSA, Bulletproofs	*curve25519*
Tezos	XTZ	ECDSA, EdDSA	*secp256k1*, *curve25519*, *NIST P-256*

Table 4: The top 11 cryptocurrencies which use EdDSA and are present in [94], ordered by MC by 1st January 2022; Adapted from Ethan Fast's research [94]; References: [94], [198], [185], [74]

3.1.3 Other cryptographic signing algorithms examples

According to the examples captured in [94] and [185], other signature algorithms used in blockchain are:

- **RSA:** RSA is used in **Hedera**(3072 bits) and **Arweave**(4096 bits) [94]
- **Schnorr** and **EC-Schnorr:** Schnorr's signature scheme was proposed in [174] (see also [175] and [177]), and is used on **Polkadot** and **Kusama**. According to [177], the hardness of this scheme relies on the hardness of the discrete logarithm problem. The Schnorr's scheme variant on elliptic curves (EC-Schnorr) is used on **Zilliqa** and **Decred** [94].
- **Winternitz one-time signature scheme:** Winternitz one-time signature (Winternitz OTS) is a hash-based signature algorithm, as presented in Section 2.2 *Post-Quantum Cryptography.* The intractability of quantum forgery of Winternitz OTS is detailed in the paperwork of Majenz et.al. in [140]. Winternitz OTS is used in **IOTA** [94] and in **Mochimo** [147].

- **ZK-SNARK:** *Zero-knowledge Succinct Non-Interactive Argument of Knowledge* (ZK-SNARK) is a mechanism of proof of possession of a secret without interaction nor revealing the secret ([207],[54]). **Zcash** creators claimed that **Zcash** is the first extensive application that uses ZK-SNARK [207]. Also, [94] notes that ZK-SNARK is used in **Zcash** only in anonymous transaction. Kearney et.al. remark in [123] that the ZK-SNARK hardness relies on the discrete logarithm problem. For other types of transactions, there are used ECDSA with *secp256k1* and EdSA among *curve25519* ([123], [110], [94]).

- **Bulletproofs:** The *Bulletproofs* non-interactive zero-knowledge proof scheme was proposed by Bünz et.al. in [63]. According to the authors, the scheme is based on the hardness of the discrete logarithm problem, but they also suggested some extensions to satisfy quantum security. *Bulletproofs* is used in **Monero** [94].

3.1.4 Preliminary conclusions

A significant number of cryptocurrencies implement quantum vulnerable signing algorithms. The hardness of ECDSA, EdDSA, RSA, Schnorr's schemes, and also specific zero-knowledge proof protocols, relies on the hardness of factoring and discrete logarithm problem. We spot in Section 2.1 *Quantum Computing* that these problems could be solved efficiently [179] if we possess a quantum machine of sufficient capacity and computational power. This implies that the authenticity of the signatures might be compromised, which will be a major issue in blockchain security, and hence, a drop of trust in blockchain technologies.

3.2 Hash functions

In the Section 2.6.1 *Hash functions*, there are exposed the main hash functions used in blockchain. According to the observations from Sections 2.1 *Quantum Computing* and 2.2 *Post-Quantum Cryptography*, quantum computing cannot bring a signifiant (exponential) advantage in brute-force searching and collision-finding problems ([41], [158], [44]). The most defining results are the Grover's search algorithm [103] ($O(\sqrt{N})$ complexity) and the method for collision finding [59] ($O(N^{1/3})$ complexity) of Brassard et.al. The classical algorithms have the complexity $O(N)$ for searching and $O(\sqrt{N})$ for collision searching (based on the birthday paradox - see [59]).

Therefore the hash functions are considered to be quantum secure to exponential speedup. Nevertheless, to keep the initial security level of the brute-force search on hash functions, it is necessary to double up the size of the digests used (for example: to consider switching to SHA-256 from SHA-128). And in the context of collision search, we might have digests with lengths 1.5 times greater than the initial ones, to keep the same security confidence.

Nota bene: All the assumptions regarding Grover's algorithm complexity assume that the property function (the "criteria" of selection of the element we are looking for) that we would like to emulate could be efficiently implemented in quantum gates.

4 Post-quantum blockchain schemes

Taking into account the actual vulnerabilities of the current blockchain schemes discussed in Section 3, we must think about blockchain from a post-quantum view. This implies the replacement of the vulnerable cryptographic primitives with ones resistant to the quantum attacks discussed earlier. In this section, we will provide a very frugal review of existing literature about post-quantum blockchain (PQB) schemes proposals.

- ***A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain*** [99]: In the article of Gao et.al. [99], the authors propose a lattice-based signature scheme with respect to their declared goal of developing a quantum-resilient scheme. The hardness of the signature algorithm relies on the hardness of the *Short Integer Solution*(SIS), with the observation from the authors that the SIS problem and the *Shortest Independent Vector Problem*(SIVP) are equivalent [99]. The work of Stephens-Davidowitz [183] is an excellent review about the reduction between lattice hard problem classes, where is shown that there exists a reduction from $\gamma - unique - SIVP$ to $\gamma - SIVP$. The $\gamma - unique - SIVP$ problem can be reduced from *Dihedral Hidden Subgroup Problem* (Regev [167] - see Section *Quantum Computing*).

- Regarding the ***Proof of Work***(PoW) mechanism, Cojocaru et.al. made an analysis [75] of the hardness of finding chains of PoWs in a post-quantum context. Also, Behnia et.al. proposed in [37] a lattice-based PoW scheme based on the hardness of a variant of SVP called *Hermite-SVP*. A PoW proposal based on solving multivariate quadratic equations was proposed by Chen et.al. in [68]. More PoW proposals are cited in the work of Aggarwal et.al [25]: [131], [188], [53].

- ***On the Construction of a Post-Quantum Blockchain for Smart City*** [68] : Also, in this paperwork from Chen et.al. cited previously, at the section *"A Lightweight Post-quantum Blockchain Transaction"*, the authors incorporate in the new-proposed mechanism of transaction an identity-based multivariate-quadratic signature scheme called *ID-Rainbow* (proposed by Chen et.al. in [69]).

- ***A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network*** [135]: In the context of post-quantum blockchain, Li et.al. suggested in [135] a lattice-based signature scheme, whose keys are generated using *Bonsai Trees.*

- ***QRL: The Quantum Resistant Ledger*** [201]: There is mentioned in the work of Fernández-Caramès and Fraga-Lamas [96] and in the list provided by *WebPlaces.org* [202] a quantum-resistant blockchain scheme called *QRL* [201]. The authors of QRL declare that there is used *XMSS* hash-based signature scheme, and claim that the extension to other signature schemes (examples provided by them: *SPHINCS*, *FALCON*) would be versatile [201]. Another product developed by the same team is *enQlave* [200], a quantum-resistant wallet for Ethereum-based coins [199].

- ***Nexus*** [150]: Nexus is a proposed post-quantum blockchain technology mentioned in [202]. According to the Nexus site [150], Nexus uses the digital signature lattice-based scheme *FALCON*, the hash algorithm *Keccak* and the key derivation function *Argon2* (see [203]).

- ***IOTA*** [114] and ***Mochimo*** [147] : We have discussed in the previous section that IOTA and Mochimo schemes use quantum-resistant Winternitz one-time signature scheme ([94], [147]).

As mentioned also in [202], [96] and [147], IOTA and Mochimo are suitable candidates for post-quantum blockchain proposals.

Another post-quantum blockchain related work examples are mentioned in [202] and presented in [96].

5 Concluding Remarks

Blockchain is considered one of the most promising technologies that have emerged in recent years. In order to make the most of its potential, we must maintain its security against possible future attacks. On the other hand, quantum computing is an emerging technology that is still situated in an incipient stage. Nevertheless, we must consider the rapid expansion of the quantum technologies (see for example IBM's roadmap [112] and the paper of Bourassa et.al. from Xanadu [56]) and its huge potential to compromise the security of the large-scale used cryptographic primitives at this time.

In this paper, we succinctly presented how blockchain technology is influenced by the appearance of quantum computers. Analyzing the most relevant blockchains we concluded that the majority of them implement quantum vulnerable signing algorithms, thus raising issues in trusting the blockchain technology itself. In the idea of avoiding the threats imposed by an attacker with quantum capabilities, we outlined the existing post-quantum schemes proposed to be used in blockchain.

References

[1] Decentralized Applications (DApps) . Last accessed: 29th December 2021; Available at: https://coinmarketcap.com/alexandria/glossary/decentralized-applications-dapps.

[2] Decentralized Autonomous Organizations (DAO) . Last accessed: 29th December 2021; Available at: https://coinmarketcap.com/alexandria/glossary/decentralized-autonomous-organizations-dao.

[3] Amazon Braket Quantum Computers - from Amazon Braket site . Last accessed: 1st December 2021; Available at: https://aws.amazon.com/braket/quantum-computers/.

[4] B-money . Last accessed: 29th December 2021; Available at: http://www.weidai.com/bmoney.txt.

[5] Bitcoin GitHub . Last accessed: 1st December 2021; Available at: https://github.com/bitcoin/.

[6] Blockchain technologies for automatic regulation and compliance . Last accessed: 29th December 2021; Available at: https://www.openaccessgovernment.org/blockchain-technologies-automatic-regulation-compliance/41885/.

[7] Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession . Last accessed at: 30th December 2021 ; Available at: https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/

downloadabledocuments/blockchain-technology-and-its-potential-impact-on-the-audit-and-assurance-profession.pdf.

[8] D-Wave site. Last accessed: 1th December 2021; Available at: https://www.dwavesys.com/solutions-and-products/systems/.

[9] Ethereum . Last accessed: 1st December 2021; Available at: https://ethereum.org/en/.

[10] IonQ Announcement - IonQ breaks records for quantum computing performance. Last accessed: 1th December 2021; Available at: https://ionq.com/news/december-11-2018.

[11] List of quantum processors - Wikipedia Page . Last accessed: 1st December 2021; Available at: https://en.wikipedia.org/wiki/List_of_quantum_processors.

[12] NIST's Post-Quantum Cryptography Standardization . Last accessed: 28th November 2021; Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

[13] NIST's Post-Quantum Cryptography Standardization Round 1 Call for Post-Quantum public key cryptosystems submissions . Last accessed: 28th November 2021; Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/Round-1-Submissionsn.

[14] NIST's Post-Quantum Cryptography Standardization Round 2 Call for Post-Quantum public key cryptosystems submissions . Last accessed: 28th November 2021; Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.

[15] NIST's Post-Quantum Cryptography Standardization Round 3 Call for Post-Quantum public key cryptosystems submissions . Last accessed: 28th November 2021; Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.

[16] Pennylane site. Available at: https://pennylane.ai/.

[17] Quantum computing hardware - Quantum AI Lab Site from Google . Last accessed: 1st December 2021; Available at: https://quantumai.google/hardware.

[18] Rigetti site . Last accessed: 1st December 2021; Available at: https://www.rigetti.com/.

[19] Strawberry site - Integrated quantum nanophotonics. Available at: https://strawberryfields.ai/photonics/hardware/details.html.

[20] Xanadu site - The Photonic Advantage Fastest path to scalable, robust, and practical quantum computers. Available at: https://www.xanadu.ai/hardware.

[21] IBM Blogs - On "Quantum Supremacy" , 2019. Last accessed: 1st December 2021; Available at: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/.

[22] MIT Technology review - IBM's new 53-qubit quantum computer is the most powerful machine you can use , 2019. Last accessed: 1st December 2021; Available at: https://www.technologyreview.com/2019/09/18/132956/ibms-new-53-qubit-quantum-computer-is-the-most-powerful-machine-you-can-use/.

[23] Quantum Computer Datasheet - a presentation of Sycamore and Weber Quantum Computer , 2021. Last accessed: 1st December 2021; Available at: https://quantumai.google/hardware/datasheet/weber.pdf.

[24] Distributed ledger technology cybersecurity - improving information security in the financial sector. January 18, 2017. Last accessed: 29th December 2021; Available at: https://www.enisa.europa.eu/publications/blockchain-security.

[25] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel. Quantum attacks on bitcoin, and how to protect against them. *Ledger*, 3, Oct 2018.

[26] Ajtai, Miklós and Kumar, Ravi and Sivakumar, D. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*, STOC '01, page 601–610, New York, NY, USA, 2001. Association for Computing Machinery.

[27] M. Albrecht, C. Cid, K. G. Paterson, C. J. Tjhai, and M. Tomlinson. NTS-KEM . Last checked : 30 November 2021 ; Available at: https://nts-kem.io/.

[28] A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems - the hardness of quantum rewinding, 2014.

[29] Androulaki Elli et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. 2018. Last accessed: 1st December 2021; Available at: https://arxiv.org/pdf/1801.10228.pdf.

[30] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. A. Melchor, R. Misoczki, E. Persichetti, N. Sendrier, J.-P. Tillich, G. Zemor, and V. Vasseur. BIKE: Bit Flipping Key Encapsulation. Last accessed : 30 November 2021 ; Available at: https://bikesuite.org/files/BIKE.pdf.

[31] N. Aragon, O. Blazy, J.-C. Deneuville, P. Gaborit, A. Hauteville, O. Ruatta, J.-P. Tillich, G. Zemor, C. A. Melchor, S. Bettaieb, L. Bidoux, M. Bardet, and A. Otmani. ROLLO (Rank-Ouroboros, LAKE and LOCKER) . Last checked : 30 November 2021 ; Available at: https://pqc-rollo.org/.

[32] Arute, F. and Arya, K. and Babbush, R. et al. Quantum supremacy using a programmable superconducting processor , 2019. Last accessed: 1st December 2021; https://www.nature.com/articles/s41586-019-1666-5citeas.

[33] A. Back. Hashcash - A denial of Service Counter measure. 2002. Last checked : 30 November 2021 ; Available at: https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure.

[34] D. Bacon. Reading List: Graph Isomorphism . A good descriptive web article about graph isomorphism. Available at: https://dabacon.org/pontiff/2010/08/04/reading-list-graph-isomorphism/.

[35] M. Baldi, A. Barenghi, F. Chiaraluce, G. Pelosi, and P. Santini. LAC's NIST Submission Package. . Last checked : 30 November 2021 (deprecated site) ; Available at: https://www.ledacrypt.org/.

[36] P. Ball. Nature article - First quantum computer to pack 100 qubits enters crowded race , 2021. Last accessed: 1st December 2021; Available at: https://www.nature.com/articles/d41586-021-03476-5.

[37] R. Behnia, E. W. Postlethwaite, M. O. Ozmen, and A. A. Yavuz. Lattice-based proof-of-work for post-quantum blockchains. Cryptology ePrint Archive, Report 2020/1362, 2020. `https://ia.cr/2020/1362`.

[38] A. Bender, J. Katz, and R. Morselli. Ring Signatures: Stronger Definitions, and Constructions without Random Oracles . 2005. Last accessed: 1st December 2021; Available at: https://eprint.iacr.org/2005/304.pdf.

[39] P. Benioff. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, 22:563–591, 05 1980.

[40] P. A. Benioff. Quantum Mechanical Hamiltonian Models of Discrete Processes That Erase Their Own Histories: Application to Turing Machines. *International Journal of Theoretical Physics*, 21(3/4):177–201, 1982.

[41] Bennett, Charles H. and Bernstein, Ethan and Brassard, Gilles and Vazirani, Umesh. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, Oct 1997.

[42] D. J. Bernstein. Curve25519: New diffie-hellman speed records. In M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, editors, *Public Key Cryptography - PKC 2006*, pages 207–228, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[43] D. J. Bernstein. The Salsa20 family of stream ciphers . 2008.

[44] D. J. Bernstein. Introduction to post-quantum cryptography . *Chapter from Post-Quantum Cryptography, Daniel Bernstein, Johannes Buchmann, Erik Dahmen, 2009, Springer*, 2009.

[45] D. J. Bernstein, J. Buchmann, and E. D. (Editors). *Post-Quantum Cryptography.* Springer, 2009.

[46] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang. Classic McEliece . Last accessed : 30 November 2021 ; Available at: https://classic.mceliece.org/.

[47] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal. NTRU Prime . Last checked : 30 November 2021 ; Available at: https://ntruprime.cr.yp.to/.

[48] D. J. Bernstein, N. Duif, T. Lange, P. Schwabe, and B.-Y. Yang. High-speed high-security signatures . 2017. Last accessed: 1st December 2021; Available at: https://ed25519.cr.yp.to/ed25519-20110926.pdf.

[49] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta. Post-quantum rsa. Cryptology ePrint Archive, Report 2017/351, 2017. `https://ia.cr/2017/351`.

[50] E. Bernstein and U. Vazirani. QUANTUM COMPLEXITY THEORY . *SIAM Journal of Computing*, 26(5):1411–1473, 1997.

[51] W. Beullens, B. Preneel, A. Szepieniec, and F. Vercauteren. LUOV An MQ signature scheme . Last checked : 30 November 2021 ; Available at: https://www.esat.kuleuven.be/cosic/pqcrypto/luov/.

[52] N. Bindel, S. Akleylek, E. Alkim, P. S. L. M. Barreto, J. Buchmann, E. Eaton, G. Gutoski, J. Kramer, P. Longa, H. Polat, J. E. Ricardini, and G. Zanon. qTESLA EFFICIENT AND POST-QUANTUM SECURE LATTICE-BASED SIGNATURE SCHEME . Last checked : 30 November 2021 ; Available at: https://qtesla.org/.

[53] A. Biryukov and D. Khovratovich. Equihash: Asymmetric proof-of-work based on the generalized birthday problem. *Ledger*, 2:1–30, Apr. 2017. Available at: https://www.ndss-symposium.org/wp-content/uploads/2017/09/equihash-asymmetric-proof-of-work-based-generalized-birthday-problem.pdf.

[54] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. Cryptology ePrint Archive, Report 2011/443, 2011. `https://ia.cr/2011/443`.

[55] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey. Towards better availability and accountability for iot updates by means of a blockchain. 2017. Last accessed: 1st December 2021; Available at: https://hal.archives-ouvertes.fr/hal-01516350/document.

[56] J. E. Bourassa, R. N. Alexander, M. Vasmer, A. Patil, I. Tzitrin, T. Matsuura, D. Su, B. Q. Baragiola, S. Guha, G. Dauphinais, and et al. Blueprint for a scalable photonic fault-tolerant quantum computer. *Quantum*, 5:392, Feb 2021.

[57] M. Boyer, G. Brassard, P. Høyer, and A. Tapp. Tight bounds on quantum searching . *https://arxiv.org/pdf/quant-ph/9605034.pdf*, 1996.

[58] M. Braithwaite. Experimenting with Post-Quantum Cryptography. 2016. Last accessed: 12th December 2021 ; Available at: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[59] G. Brassard, P. Høyer, , and A. Tapp. Quantum algorithm for the collision problem. . *ACM SIGACT News*, 28:14–19, 1997. Available at: https://arxiv.org/pdf/quant-ph/9705002.pdf.

[60] G. Brassard and P. Høyer. An Exact Quantum Polynomial-Time Algorithm for Simon's Problem . *https://arxiv.org/pdf/quant-ph/9704027.pdf*, 1997.

[61] J. Buchmann, E. Dahmen, and M. Szydlo. Hash-based Digital Signature Schemes . *Chapter from Post-Quantum Cryptography, Daniel Bernstein, Johannes Buchmann, Erik Dahmen, 2009, Springer*, 2009.

[62] J. A. Buchmann and H. C. Williams. A key exchange system based on real quadratic fields (extended abstract) . *In G. Brassard, editor, Advances in Cryptology—CRYPTO '89, volume 435 of Lecture Notes in Computer Science, pages 335–343. Springer-Verlag, 1990*, 1989.

[63] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell. Bulletproofs: Short proofs for confidential transactions and more. Cryptology ePrint Archive, Report 2017/1066, 2017. `https://ia.cr/2017/1066`.

[64] A. Casanova, J.-C. Faugere, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. GeMSS: A Great Multivariate Short Signature . Last checked : 30 November 2021 ; Available at: https://www-polsys.lip6.fr/Links/NIST/GeMSS.html.

[65] Certicom Research ; Contact: Daniel R. L. Brown (dbrown@certicom.com). Standards for Efficient Cryptography 2 (SEC 2): Recommended Elliptic Curve Domain Parameters . 2010. Last checked : 1st January 2022 ; Available at: https://www.secg.org/sec2-v2.pdf.

[66] D. Chaum. Blind Signatures for untraceable payments . Last checked : 30 November 2021 ; Available at:
https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.

[67] C. Chen, O. Danba, J. Hoffstein, A. Hulsing, J. Rijneveld, J. M. Schanck, P. Schwabe, W. Whyte, and Z. Zhang. NTRU A submission to the NIST post-quantum standardization effort . Last checked : 30 November 2021 ; Available at: https://ntru.org/.

[68] J. Chen, W. Gan, M. Hu, and C.-M. Chen. On the construction of a post-quantum blockchain for smart city. *Journal of Information Security and Applications*, 58:102780, May 2021.

[69] J. Chen, J. Ling, J. Ning, and J. Ding. Identity-based signature schemes for multivariate public key cryptosystems. *The Computer Journal*, 62:1132–1147, 08 2019.

[70] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone. Report on post-quantum cryptography, 2016. Available at:
https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[71] Childs, Andrew and Jao, David and Soukharev, Vladimir. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, Jan 2014.

[72] C. Q. Choi. CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy> Intel's new superconducting quantum chip, called Tangle Lake, has enough qubits to make things very interesting from a scientific standpoint , 2018. IEEE Spectrum article; Last accessed: 1st December 2021; Available at: https://spectrum.ieee.org/intels-49qubit-chip-aims-for-quantum-supremacy.

[73] C. Q. Choi. In the Race to Hundreds of Qubits, Photons May Have "Quantum Advantage"> Canadian startup Xanadu says their quantum computer is cloud-accessible, Python programmable, and ready to scale. *IEEE Spectrum*, Mar 2021. Article from IEEE Spectrum; Last accessed: 30 December 2021; Available at: https://spectrum.ieee.org/race-to-hundreds-of-photonic-qubits-xanadu-scalable-photon.

[74] CoinMarketCap. All Cryptocurrencies - ranking of all available cryptocurrencies . Last checked : 31 December 2021 ; Available at: https://coinmarketcap.com/all/views/all/.

[75] A. Cojocaru, J. Garay, A. Kiayias, F. Song, and P. Wallden. Post-quantum blockchain proofs of work, 2021. Available at: https://arxiv.org/pdf/2012.15254.pdf.

[76] E. Conover. The new light-based quantum computer Jiuzhang has achieved quantum supremacy - article from ScienceNews . Last accessed: 1st December 2021; Available at: https://www.sciencenews.org/article/new-light-based-quantum-computer-jiuzhang-supremacy.

[77] C. Coverdale. Scaling Bitcoin: Schnorr Signatures , 2018. Last accessed: 1st December 2021; Available at: https://bitcointechtalk.com/scaling-bitcoin-schnorrsignatures-abe3b5c275d1.

[78] J.-P. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren. SABER . Last checked : 30 November 2021 ; Available at: https://www.esat.kuleuven.be/cosic/pqcrypto/saber/.

[79] D. Deutsch. Quantum Theory, the Church-Turing principle and the universal quantum computer . *Proceedings of the Royal Society of London*, A(400):97–117, 1985.

[80] D. Deutsch and R. Jozsa. Rapid solutions of problems by quantum computation. *Proceedings of the Royal Society of London*, A(439):553–558, 1992.

[81] C. Dilmegani. Quantum Annealing in 2021: Practical Quantum Computing. Last accessed: 1th December 2021; Available at: https://research.aimultiple.com/quantum-annealing/.

[82] J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, and B.-Y. Yang. ThreeBears Three Bears post-quantum encryption algorithms - SourceForge repository . Last checked : 30 November 2021 ; Available at: https://sourceforge.net/projects/threebears/.

[83] J. Ding and B.-Y. Yang. Multivariate Public Key Cryptography . *Chapter from Post-Quantum Cryptography, Daniel Bernstein, Johannes Buchmann, Erik Dahmen, 2009, Springer*, 2009.

[84] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 618–623, United States, May 2017. Institute of Electrical and Electronics Engineers (IEEE). 2nd IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things 2017 ; Conference date: 13-03-2017 Through 17-03-2017.

[85] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum . *https://arxiv.org/pdf/quant-ph/9607014.pdf*, pages 212–219, 1996.

[86] E. Elrom. *The blockchain developer*. Apress, 2019.

[87] ENISA. Post-quantum cryptography: Current state and quantum mitigation. Last accessed: 12 December 2021; Available at: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[88] Etherscan. Token Tracker ERC-20. Last accessed: 1st January 2021; Available at: https://etherscan.io/tokens.

[89] M. Ettinger and P. Høyer. On Quantum Algorithms for Noncommutative Hidden Subgroups . *http://arxiv.org/abs/quant-ph/9807029*, 1998.

[90] M. Ettinger and P. Høyer. A Quantum Observable for the Graph Isomorphism Problem . *Available at https://arxiv.org/pdf/quant-ph/9901029.pdf*, 1999.

[91] M. Ettinger and P. Høyer. The quantum query complexity of the hidden subgroup problem is polynomial . *https://arxiv.org/pdf/quant-ph/0401083.pdf*, 2004.

[92] M. Ettinger, P. Høyer, and E. Knill. Hidden Subgroup States are Almost Orthogonal. . *http://arxiv.org/abs/quant-ph/9901034*, 1999.

[93] T. Falk. What is an ERC20 token?, 2021. Finder article; Last accessed: 1st January 2021; Available at: https://www.finder.com/erc20-tokens.

[94] E. Fast. Cryptography behind the top 100 cryptocurrencies . Last checked : 1st January 2022 ; Available at: http://ethanfast.com/top-crypto.html?fbclid=IwAR0_81BN9s7-gTc6zjuub7-2ofSYstRP1G3PoZBUaSHmXpCcRHNjwrqOfn4.

[95] L. D. Feo, D. Jao, and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. Cryptology ePrint Archive, Report 2011/506, 2011. `https://ia.cr/2011/506`.

[96] Fernández-Caramès, Tiago M. and Fraga-Lamas, Paula. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, 8:21091–21116, 2020.

[97] R. Feynman. Simulating Physics with Computers . *International Journal of Theoretical Physics*, 21(6/7):467–488, 1982.

[98] J. Gambetta. IBM's roadmap for scaling quantum technology , 2020. Last accessed: 1st December 2021; Available at: https://research.ibm.com/blog/ibm-quantum-roadmap.

[99] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, 6:27205–27213, 2018.

[100] O. Garcia-Morchon, Z. Zhang, S. Bhattacharya, R. Rietman, L. Tolhuizen, J.-L. Torre-Arce, H. Baan, M.-J. O. Saarinen, S. Fluhrer, T. Laarhoven, R. Player, J. H. Cheon, and Y. Son. Round5: compact and fast post-quantum public-key encryption . Last checked : 30 November 2021 ; Available at: https://round5.org/.

[101] M. Gates. *Blockchain ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and future of money.* CreateSpace Independent Publishing Platform, 2017.

[102] O. Goldreich, S. Micali, and A. Widgerson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. . *Journal of the ACM*, 38(1):691–729, 1991.

[103] L. K. Grover. A fast quantum mechanical algorithm for database search . *Proceedings, STOC 1996, Philadelphia PA USA*, pages 212–219, 1996.

[104] S. Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem . *Journal of the ACM*, 54(1):1–19, 2007.

[105] S. Hallgren and U. Vollmer. Quantum computing . *Chapter from Post-Quantum Cryptography, Daniel Bernstein, Johannes Buchmann, Erik Dahmen, 2009, Springer*, 2009.

[106] M. Hamburg. ThreeBears Three Bears post-quantum encryption algorithms - SourceForge repository . Last checked : 30 November 2021 ; Available at:
https://sourceforge.net/projects/threebears/.

[107] E. Heilman, F. Baldimtsi, and S. Goldberg. *Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions.* Springer, 2016. Last accessed: 1st December 2021; Available at: https://eprint.iacr.org/2016/056.pdf.

[108] M. Hirvensalo. *Quantum Computing - Natural Computing Series.* Springer, 2001.

[109] J. Hoffstein, J. Pipher, and J. H. Silverman(Editors). *An Introduction to Mathematical Cryptography.* Springer-Verlag New York, 2014.

[110] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox. Zcash protocol specication version 2022.2.18 [nu5 proposal], 2022. `https://zips.z.cash/protocol/protocol.pdf`.

[111] A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, and J.-P. Aumasson. SPHINCS+ Stateless hash-based signatures . Last checked : 30 November 2021 ; Available at: https://sphincs.org/.

[112] IBM. IBM Announcement - IBM Quantum breaks the 100-qubit processor barrier . Last accessed: 1st December 2021; Available at: https://research.ibm.com/blog/127-qubit-quantum-processor-eagle.

[113] Intel. The Future of Quantum Computing is Counted in Qubits , 2018. Last accessed: 31th December 2021; Available at: https://newsroom.intel.com/news/future-quantum-computing-counted-qubits/gs.kwhh9a.

[114] IOTA. Iota site. Last accessed: 4th January 2022; Available at: https://www.iota.org/.

[115] G. Iredale. History of Blockchain Technology: A Detailed Guide , 2020. Last accessed: 1st December 2021; Available at: https://101blockchains.com/history-of-blockchain-timeline/.

[116] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, and G. Pereira. SIKE – Supersingular Isogeny Key Encapsulation . Last checked : 30 November 2021 ; Available at: https://sike.org/.

[117] Jordan Stephen (Microsoft Quantum). Quantum Algorithm Zoo . A comprehensive catalog of quantum algorithms. Available at: https://quantumalgorithmzoo.org/.

[118] S. Josefsson and I. Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA) . 2017. Last accessed: 1st December 2021; Available at:
https://datatracker.ietf.org/doc/html/rfc8032.

[119] W. A. Kaal. Blockchain-based corporate governance. *Stanford Journal of Blockchain Law Policy*, 1 2021. https://stanford-jblp.pubpub.org/pub/blockchain-corporate-governance.

[120] Kannan, Ravi. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC '83, page 193–206, New York, NY, USA, 1983. Association for Computing Machinery.

[121] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding, 2016.

[122] P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing.* Oxford University Press, USA, 2007.

[123] J. J. Kearney and C. A. Perez-Delgado. Vulnerability of blockchain technologies to quantum attacks. *Array*, 10:100065, 2021.

[124] J. Kelly. A Preview of Bristlecone, Google's New Quantum Processor , 2018. Last accessed: 1st December 2021; Available at: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

[125] L.-R. Knill, E. and G. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001. Available at: https://arxiv.org/pdf/quant-ph/0006088.pdf.

[126] J. Koch, T. M. Yu, J. Gambetta, A. A. Houck, D. I. Schuster, J. Majer, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf. Charge-insensitive qubit design derived from the cooper pair box. *Physical Review A*, 76(4), Oct 2007.

[127] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135–174, Jan 2007. Available at: https://arxiv.org/pdf/quant-ph/0512071.pdf.

[128] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. . *http://arxiv.org/abs/quant-ph/0302112*, 2003.

[129] L. Lamport. Constructing digital signatures from a one way function . 1979. Available at: https://www.microsoft.com/en-us/research/uploads/prod/2016/12/Constructing-Digital-Signatures-from-a-One-Way-Function.pdf.

[130] A. Langley. CECPQ2. 2018. Adam Langley's blog. Last accessed: 12th December 2021; Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901595.

[131] D. LARIMER. Momentum - a memory-hard proof-of-work via finding birthday collisions. `http://www.hashcash.org/papers/momentum.pdf`.

[132] D.-P. Le, G. Yang, and A. Ghorbani. A new multisignature scheme with public key aggregation for blockchain. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–7, 2019.

[133] A. Lenstra and H. Lenstra(Jr.)(eds.). The development of the number field sieve . *Lecture Notes in Mathematics*, 1554, Berlin, Springer-Verlag, 1993.

[134] Lenstra, A.K., Lenstra, H.W. Lovász, L. Factoring polynomials with rational coefficients. . *Math. Ann.*, 261(6/7):515–534, 1982.

[135] C.-Y. Li, X.-B. Chen, Y.-L. Chen, Y.-Y. Hou, and J. Li. A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access*, 7:2026–2033, 2019.

[136] Y.-C. Liang. *Blockchain for Dynamic Spectrum Management*, pages 121–146. 01 2020.

[137] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang. An ID-Based Linearly Homomorphic Signature Scheme and Its Application in Blockchain . 2008. Last accessed: 1st December 2021; Available at:
$https : //ieeexplore.ieee.org/stamp/stamp.jsp?tp = arnumber = 8302552$.

[138] X. Lu, Y. Liu, D. Jia, H. Xue, J. He, Z. Zhang, Z. Liu, H. Yang, B. Li, and K. Wang. LAC's NIST Submission Package. . Last checked : 30 November 2021 (deprecated site) ; Available at: https://csrc.nist.gov/CSRC/media/Projects/Post-QuantumCryptography/documents/round-1/submissions/LAC.zip.

[139] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, and D. Stehle. CRYSTALS Cryptographic Suite for Algebraic Lattices - Dilithium . Last accessed : 30 November 2021 ; Available at: https://pq-crystals.org/dilithium/index.shtml.

[140] C. Majenz, C. M. Manfouo, and M. Ozols. Quantum-access security of the winternitz one-time signature scheme. Cryptology ePrint Archive, Report 2021/387, 2021. https://ia.cr/2021/387.

[141] Y. Manin. Computable and Uncomputable (in Russian). *Sovetskoye Radio, Moscow*, 1980.

[142] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and J. Bos. HQC . Last accessed : 30 November 2021 ; Available at: http://pqc-hqc.org/.

[143] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zemor, A. Couvreur, and A. Hauteville. RQC . Last checked : 30 November 2021 ; Available at: http://pqc-rqc.org/.

[144] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography.* CRC Press, 2001.

[145] R. C. Merkle. A CERTIFIED DIGITAL SIGNATURE . *Advances in Cryptology - CRYPTO '89 Proceedings, LNCS 435.*, page 218–238, 1989. Available at: https://link.springer.com/content/pdf/10.1007/0-387-34805-0_21.pdf.

[146] S. Micali, K. Ohta, and L. Reyzin. Accountable-subgroup multisignatures: Extended abstract. CCS '01, page 245–254, New York, NY, USA, 2001. Association for Computing Machinery.

[147] Mochimo. Mochimo - currency for the post-quantum era. Mochimo site; Last accessed: 4th January 2022; Available at: https://mochimo.org/.

[148] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM Practical quantum-secure key encapsulation from generic lattices . Last accessed : 30 November 2021 ; Available at: https://frodokem.org/.

[149] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System . 2009. Last checked : 30 November 2021 ; Available at: https://bitcoin.org/bitcoin.pdf.

[150] Nexus. Nexus site. Last accessed: 4th January 2022; Available at:
https://www.webplaces.org/quantum.htm.

[151] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2004.

[152] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information - 10th Anniversary Edition.* Cambridge University Press, 2010.

[153] NIST; National Institute of Standards and Technology - Information Technology Laboratory. Digital Signature Standard (DSS) . *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION*, 2013. FIPS PUB 186-4; Last checked : 1st January 2022 ; Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[154] OpenZeppelin. OpenZeppelin GitHub repository - A library for secure smart contract development. Last accessed: 1st January 2021; Available at:
https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC20/extensions/draft-ERC20Permit.sol.

[155] R. Overbeck and N. Sendrier. Code-based cryptography . *Chapter from Post-Quantum Cryptography, Daniel Bernstein, Johannes Buchmann, Erik Dahmen, 2009, Springer*, 2009.

[156] I. Ozcelik, S. Medury, J. Broaddus, and A. Skjellum. An overview of cryptographic accumulators. pages 661–669, 01 2021.

[157] C. Percival. STRONGER KEY DERIVATION VIA SEQUENTIAL MEMORY-HARD FUNCTIONS . 2009. Last accessed: 1st December 2021; Available at:
http://www.tarsnap.com/scrypt/scrypt.pdf.

[158] R. A. Perlner and D. A. Cooper. Quantum Resistant Public Key Cryptography: A Survey. *ACM*, 2009. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901595.

[159] T. Poppelmann, E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. de la Piedra, P. Schwabe, D. Stebila, M. R. Albrecht, E. Orsini, V. Osheter, K. G. Paterson, G. Peer, and N. P. Smart. NewHope Post-quantum key encapsulation . Last checked : 30 November 2021 ; Available at: https://newhopecrypto.org/.

[160] Preskill, John. Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79, Aug. 2018. Available at:
https://arxiv.org/pdf/1801.00862.pdf.

[161] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. FALCON - Fast-Fourier Lattice-based Compact Signatures over NTRU . Last checked : 30 November 2021 ; Available at: https://falcon-sign.info/.

[162] Qiskit. Bernstein-Vazirani algorithm presentation in Qiskit Tutorial notebook. Available at: https://qiskit.org/textbook/ch-algorithms/bernstein-vazirani.html.

[163] Qiskit. Quantum Counting presentation in Qiskit Tutorial notebook. Available at: https://qiskit.org/textbook/ch-algorithms/quantum-counting.html.

[164] Qiskit. Simon algorithm presentation in Qiskit Tutorial notebook. Available at: https://qiskit.org/textbook/ch-algorithms/simon.html.

[165] M. Raikwar, D. Gligoroski, and K. Kralevska. Sok of used cryptography in blockchain. *IEEE Access*, 7:148550–148575, 2019.

[166] O. Regev. New Lattice Based Cryptographic Constructions . 2003. Available at: http://arxiv.org/abs/cs/0309051v1.

[167] O. Regev. Quantum Computation and Lattice Problems . *http://arxiv.org/abs/cs/0304005*, 2003.

[168] O. Regev. A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space . *http://arxiv.org/abs/quant-ph/0406151*, 2004.

[169] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery.

[170] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*. Springer Berlin Heidelberg, 2001.

[171] S. Samardjiska, M.-S. Chen, A. Hulsing, J. Rijneveld, and P. Schwabe. MQDSS Post-quantum signature . Last checked : 30 November 2021 ; Available at: http://mqdss.org/.

[172] T. Santoli and C. Schaffner. Using simon's algorithm to attack symmetric-key cryptographic primitives, 2017.

[173] J. Schmitz. The Future of Blockchain-based Auditing is Called "Multi-chain Reconciliation through Blockchain Interoperability" . Last accessed at: 29th December 2021 ; Available at: https://cryptoeconomics-aus.medium.com/the-future-of-blockchain-based-auditing-is-called-multi-chain-reconciliation-through-blockchain-d909ee41f89d.

[174] C. P. Schnorr. Efficient identification and signatures for smart cards. In G. Brassard, editor, *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 239–252, New York, NY, 1990. Springer New York.

[175] C. P. Schnorr. Efficient signature generation by smart cards. In *Journal of Cryptology 4(3)*, page 161–174, 1991. Available at: https://d-nb.info/1156214580/34.

[176] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, and D. Stehle. CRYSTALS - Cryptographic Suite for Algebraic Lattices - Kyber . Last accessed : 30 November 2021 ; Available at: https://pq-crystals.org/kyber/index.shtml.

[177] Y. Seurin. On the exact security of schnorr-type signatures in the random oracle model. Cryptology ePrint Archive, Report 2012/029, 2012. `https://ia.cr/2012/029`.

[178] O. Shlomovits and I. A. Seres. Sharelock: Mixing for cryptocurrencies from multiparty ecdsa. *IACR Cryptol. ePrint Arch.*, 2019:563, 2019. Last accessed: 1st December 2021; Available at: https://eprint.iacr.org/2019/563.pdf.

[179] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring . *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, FOCS:124–134, 1994.

[180] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer . *https://arxiv.org/pdf/quant-ph/9508027.pdf*, 1996.

[181] P. W. Shor. Introduction to Quantum Algorithms. 07 2001. Available at:
https://arxiv.org/abs/quant-ph/0005003.

[182] D. R. Simon. On the Power of Quantum Computation . *SIAM Journal on Computing*, 26(5):1474–1483, 1997.

[183] N. Stephens-Davidowitz. Dimension-preserving reductions between lattice problems. Available at:
https://www.noahsd.com/latticeproblems.pdf, 2015.

[184] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie, and X. Peng. A survey on zero-knowledge proof in blockchain. *IEEE Network*, 35(4):198–205, 2021.

[185] T. Susanka. Cryptography behind top 20 cryptocurrencies . Last checked : 1st January 2022; Available at: https://www.susanka.eu/coins-crypto/.

[186] M. Swan. *Blockchain Blueprint for a New Economy.* O'Reilly Media, 2015.

[187] The Daily Dug. The world's first room-temperature quantum computer brings the future a step closer. Last accessed: 18 December 2021; Available at: https://dug.com/the-worlds-first-room-temperature-quantum-computer-brings-the-future-a-step-closer/.

[188] J. Tromp. Cuckoo cycle: a memory bound graph-theoretic proof-of-work. Cryptology ePrint Archive, Report 2014/059, 2014. `https://ia.cr/2014/059`.

[189] F. Tschorsch and B. Scheuermann. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies . 2015. Last checked : 30 November 2021 ; Available at: https://eprint.iacr.org/2015/464.pdf.

[190] D. Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. Cryptology ePrint Archive, Report 2014/587, 2014. `https://ia.cr/2014/587`.

[191] L. Valenta and B. Rowan. *Blindcoin: Blinded, accountable mixes for bitcoin.* Springer, 2015. Last accessed: 1st December 2021; Available at:
https://link.springer.com/content/pdf/10.1007%2F978-3-662-64322-8.pdf.

[192] W. van Dam and S. Hallgren. Efficient Quantum Algorithms for Shifted Quadratic Character Problems . *Available at https://arxiv.org/pdf/quant-ph/0011067.pdf*, 2018.

[193] W. van Dam, S. Hallgren, and L. Ip. Quantum algorithms for some hidden shift problems. . *SIAM Journal on Computing*, 36(3):763–778, 2006.

[194] N. van Saberhagen. CryptoNote v 2.0 , 2013. Last accessed: 1st December 2021; Available at: https://bytecoin.org/old/whitepaper.pdf.

[195] Virginia Cram Martos, Vice Chair Tahseen Khan. Lance Thompson, Tomas Malik and Helen Ross. White Paper Blockchain in Trade Facilitation Version 2 . Last accessed: 29th December 2021; Available at:
https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain.pdf.

[196] Wackerow Paul et.al. . ERC-20 TOKEN STANDARD, 2021. Last accessed: 1st January 2021; Available at: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/.

[197] F. Wang. The Hidden Subgroup Problem - master's project . *Datalogisk Institut, Det Naturvidenskabelige Fakultet, Aarhus Universitet, Danmark,; École Nationale Supérieure, d'Informatique pour l'Industrie et l'Entreprise, Evry, France*, 2010. Available at: https://arxiv.org/ftp/arxiv/papers/1008/1008.0010.pdf.

[198] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang. Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*, 127:43–58, 2019.

[199] P. Waterland. Enqlave — the quantum safe for your crypto assets, 2020. Medium article; Last accessed: 4th January 2022; Available at: https://medium.com/the-quantum-resistant-ledger/enqlave-the-quantum-safe-for-your-crypto-assets-beaf9e933725.

[200] P. Waterland and collaborators. Enqlave — the quantum safe for your crypto assets. EnQlave article; Last accessed: 4th January 2022; Available at: https://www.enqlave.io/.

[201] P. Waterland(Founder), K. K. Singh, J. Lomas, C. Thompson, J. Gordon, A. Bilican, and et.al. Qrl - the quantum resistant ledger. Last accessed: 4th January; Available at: `https://www.theqrl.org/`.

[202] WebPlaces.org. Quantum secure cryptocurrencies - cryptocurrencies striving to be quantum secure. Last accessed: 4th January 2022; Available at:
`https://www.webplaces.org/quantum.htm`.

[203] J. Wetzels. Open sesame: The password hashing competition and argon2, 2016. Available at: https://arxiv.org/abs/1602.03097.

[204] Wu, Yulin and Bao, Wan-Su and Cao, Sirui and Chen, Fusheng and Chen, Ming-Cheng and Chen, Xiawei and Chung, Tung-Hsun and Deng, Hui and Du, Yajie and Fan, Daojin and et al. Strong quantum computational advantage using a superconducting quantum processor. *Physical Review Letters*, 127(18), Oct 2021.

[205] H. Yang, J. Shen, J. Lu, T. Zhou, X. Xia, and S. Ji. A privacy-preserving data transmission scheme based on oblivious transfer and blockchain technology in the smart healthcare. *Security and Communication Networks*, 2021:1–12, 09 2021.

[206] G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, J. Katz, X. Wang, V. Kolesnikov, and D. Kales. Picnic - A Family of Post-Quantum Secure Digital Signature Algorithms . Last checked : 30 November 2021 ; Available at: https://microsoft.github.io/Picnic/.

[207] Zcash. What are zk-SNARKs? Last accessed: 1st January 2021; Available at: https://z.cash/technology/zksnarks/.

[208] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su, and et al. Phase-programmable gaussian boson sampling using stimulated squeezed light. *Physical Review Letters*, 127(18), Oct 2021. Available at: https://arxiv.org/abs/2106.15534.

[209] Zhong, Han-Sen and Wang, Hui and Deng, Yu-Hao and Chen, Ming-Cheng and Peng, Li-Chao and Luo, Yi-Han and Qin, Jian and Wu, Dian and Ding, Xing and Hu, Yi and et al. Quantum computational advantage using photons. *Science*, 370(6523):1460–1463, Dec 2020. Available at: https://arxiv.org/ftp/arxiv/papers/2012/2012.01625.pdf.

[210] Q. Zhu, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, C.-Y. Lu, C.-Z. Peng, X. Zhu, and J.-W. Pan. Quantum computational advantage via 60-qubit 24-cycle random circuit sampling, 2021. Available at https://arxiv.org/abs/2109.03494.

[211] J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle. Coinparty: Secure multi-party mixing of bitcoins. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 2015. Last accessed: 1st December 2021; Available at: https://www.comsys.rwth-aachen.de/fileadmin/papers/2015/2015-ziegeldorf-codaspy-coinparty.pdf.