Navigating the Quantum Computing Threat Landscape for Blockchains: A Comprehensive Survey

Hassan Khodaiemehr, Khadijeh Bagheri and Chen Feng

***Abstract*—Quantum computers pose a significant threat to blockchain technology's security, which heavily relies on public-key cryptography and hash functions. The cryptographic algorithms used in blockchains, based on large odd prime numbers and discrete logarithms, can be easily compromised by quantum computing algorithms like Shor's algorithm and its future qubit variations. This survey paper comprehensively examines the impact of quantum computers on blockchain security and explores potential mitigation strategies. We begin by surveying the existing literature on blockchains and quantum computing, providing insights into the current state of research. We then present an overview of blockchain, highlighting its key components and functionalities. We delve into the preliminaries and key definitions of quantum computing, establishing a foundation for understanding the implications on blockchain security. The application of blockchains in cybersecurity is explored, considering their strengths and vulnerabilities in light of evolving quantum computing capabilities. The survey focuses on the quantum security of blockchain's fundamental building blocks, including digital signatures, hash functions, consensus algorithms, and smart contracts. We analyze the vulnerabilities introduced by quantum computers and discuss potential countermeasures and enhancements to ensure the integrity and confidentiality of blockchain systems. Furthermore, we investigate the quantum attack surface of blockchains, identifying potential avenues for exploiting quantum computing to strengthen existing attacks. We emphasize the need for developing quantum-resistant defenses and explore solutions for mitigating the threat of quantum computers to blockchains, including the adoption of quantum and post-quantum blockchain architectures. By examining vulnerabilities and discussing mitigation strategies, we aim to guide researchers, practitioners, and policymakers in developing robust and secure blockchain systems capable of withstanding advancements in quantum computing technology.**

***Index Terms*—Blockchain technology, quantum computing, hyper ledger, postquantum cryptography, consensus algorithm, zero-knowledge proof.**

I. Introduction

THE advent of quantum computing is poised to revolutionize a multitude of industries, including the world of blockchain technology. At the heart of blockchains lies a complex web of cryptographic algorithms guaranteeing the security and unchangeability of transactional data. However, the power of quantum computing threatens to upend this delicate balance by rendering many of these algorithms vulnerable to attack. The two fundamental cryptographic features employed by blockchains, namely public-key cryptography and hash functions, rely on mathematical operations that can be impacted by quantum computers. Part of these algorithms rely on large prime numbers and discrete logarithms, which can be solved exponentially faster by a quantum computer using Shor's algorithm. Once the private-keys used to secure blockchain transactions are compromised, the entire integrity of the system is thrown into question. However, researchers are not taking this threat lightly, and are working tirelessly to find ways to mitigate this risk. By exploring the use of post-quantum cryptographic algorithms in blockchain technology, these researchers aim to create a system that is resistant to quantum attacks. Such algorithms are designed to withstand the computational power of quantum computers, and could provide a new level of security and resilience to blockchains in the face of this technological revolution. As quantum computing technology continues to advance, the security of blockchain technology will need to evolve accordingly. With the right approach, however, the future of blockchains could be brighter than ever, ushering in a new era of secure and decentralized data management. Blockchain and quantum computing are two technologies that hold great promise in various fields and have the potential to influence one another. Therefore, the focus of this study is to explore the possible impact of quantum computing on blockchain technology.

The architecture of blockchain technology is transparent and entirely distributed among peers which renders it suitable for applications in cryptocurrencies [1], [2], smart contracts [3], [4], the Internet of Things (IoT) [5]–[7], communication systems [8], [9], healthcare [10], [11], financial systems [12], [13], electronic voting [14], [15], censorship resistance [16], and distributed provenance [17], amongst the rest. The blockchain's append-only model ensures that accepted transactions cannot be modified [18], [19], offering significant advantages to these applications. For example, the blockchain's transparency allows for the storage of records that are publicly verifiable and unchangeable [20]. Additionally, the blockchain's peer-to-peer framework offers a way to uphold a verifiable ledger without requiring a central entity. This approach effectively addresses concerns related

H. Khodaiemehr is with Department of Computer Science and Statistics, Faculty of Mathematics, K. N. Toosi University of Technology, Tehran, Iran and also with the Faculty of Applied Science, School of Engineering, The University of British Columbia (UBC), Okanagan Campus, Kelowna, BC, Canada (e-mail: ha.khodaiemehr@kntu.ac.ir).

K. Bagheri is with Electronics Research Institute, Sharif University of Technology, Tehran, Iran (e-mail: kh.bagheri@sharif.edu).

C. Feng is with the Faculty of Applied Science, School of Engineering, The University of British Columbia (UBC), Okanagan Campus, Kelowna, BC, Canada (e-mail: chen.feng@ubc.ca).

This work was supported in part by Public Safety Canada under Grant with Contract No. 4248090-1-NS-5001-22170

to single points of failure and reliance on a single point of trust [21]. These properties have facilitated the development of various blockchain applications, such as cryptocurrencies like Bitcoin, Tether, Dogecoin, smart contract platforms like Ethereum, Cardano, Solana, and Decentralized Autonomous Organizations (DAOs) like BitDAO, Dash and Bitshares [22].

Blockchain technology has introduced functional features to various applications. However, recent findings have brought attention to the security vulnerabilities linked with this technology. Incidents such as the $50 million USD theft from "The DAO" and the $72 million USD theft from Bitfinex demonstrate vulnerabilities in decentralized autonomous organizations and cryptocurrency exchanges. Bitcoin and Ethereum exchanges have also been subjected to distributed denial-of-service (DDoS) attacks and DNS attacks, resulting in interruptions to their services. Fraudulent activities, such as the attack on Mt. Gox, where bitcoins valued at a total of 460 million USD were unlawfully taken, demonstrate the vulnerability of publicly verifiable blockchain-based cryptocurrencies. Additionally, a 51% attack on several cryptocurrencies like Litecoin Cash, Monacoin, Zencash, Verge, and Bitcoin Gold led to a loss of $5 million USD, as malicious actors seized control of the blockchain and executed double-spending transactions [23]. The addition of quantum computing power to these incidents further emphasizes the necessity for strengthened security measures, as well as the potential consequences it may have on cryptocurrency values and transaction processing times. In [23], the authors have discussed the potential applications of blockchain technology and provided an overview of various attacks that can compromise these applications. The attacks are categorized into three main groups: 1) attacks related to the mathematical techniques employed in ledger creation, 2) attacks linked to the decentralized peer-to-peer structure of the blockchain system, and 3) attacks connected to the application context utilizing blockchain. The authors in [23] primarily directed their focus towards the attack surface of public blockchains, which are distinguished by their accessibility to system resources and the anonymity of users. These attributes make public blockchains suitable for systems with a weak trust model and elevated provenance assurance demands. Public blockchains, exemplified by Bitcoin and Ethereum, allow anyone to join the network and transparently audit data. Nonetheless, the frail trust model inherent in public blockchains also renders them susceptible to an array of attacks, creating openings for malicious actors to undermine the system's integrity. Although public blockchains are a good fit for open-access scenarios, their compatibility with closed environments is limited due to the vulnerabilities introduced by their inherent weak trust model. The authors of [23] highlighted the necessity for improved security mechanisms in blockchain applications, particularly in public blockchains, to alleviate the risks of these attacks.

This paper aims to examine the influence of quantum computers on the security of blockchain systems and explore potential mitigation strategies. We begin by surveying the existing literature on the intersection of blockchains and quantum computing to understand the present research landscape in this area. This facilitates the comprehension of the current state of knowledge and aids in identifying areas where gaps exist. To provide a solid foundation, we provide a summary of blockchain technology, highlighting its key components and functionalities. This includes an examination of digital signatures, hash functions, consensus algorithms, and smart contractsessential building blocks of blockchain systems. Subsequently, we delve into the preliminaries and key definitions of quantum computing, establishing the necessary understanding to assess the implications for blockchain security. The application of blockchains in the realm of cybersecurity is explored, considering both their strengths and vulnerabilities in light of evolving quantum computing capabilities. We analyze the specific vulnerabilities introduced by quantum computers to blockchain security and discuss potential countermeasures and enhancements that can be employed to ensure the integrity and confidentiality of blockchains during the quantum age. Furthermore, we investigate the quantum attack surface of blockchains, identifying potential avenues for exploiting quantum computing to strengthen existing attacks. By understanding these threats, we can develop effective defense mechanisms to mitigate the risks posed by quantum computers.

The fields of quantum computing and blockchain technology are extensive areas of research with numerous published articles. In the recent years, many surveys have been published, some of which are compiled in the TABLE I. This article aims to explore the influence of quantum technology on blockchain as a cybersecurity infrastructure that has received limited attention in the previous surveys. Previous surveys have primarily focused on specific blockchain components, or on a specific blockchain platform, lacking a comprehensive review of key components from quantum security point of view. Additionally, there is a significant overlap among published surveys, limiting accessibility to certain areas of research. The field of post-quantum cryptography (PQC), which is essential for quantum-resistant blockchains, has matured in recent years, leading to the publication of final PQC candidates by NIST in July 2022. However, many published surveys predate this announcement and need updating due to the evolving nature of post-quantum cryptography. This survey aims to reduce redundancy by referencing relevant comprehensive surveys and addressing unresolved discussions, thereby filling the existing gaps in knowledge. By doing so, it aims to provide a clearer connection between the scattered research in this field.

The subsequent sections of this paper are structured as follows. In Section II, we provide an overview of blockchain. Section III presents the preliminaries and key definitions of quantum computing. Section IV examines the application of blockchains in cybersecurity. Section V discusses the effect of recent advances in quantum computing on cybersecurity. In Section VI, the quantum security of blockchain's building blocks, including digital signatures, hash functions, consensus algorithms, and smart contracts, is provided. Section VII explores the quantum attack surface of blockchains, indicating the possible exploitation of quantum computing to strengthen available attacks. Section VIII delves into possible solutions for mitigating the threat of quantum computers for blockchains, including quantum and post-quantum blockchains. Finally, Section IX contains the conclusions.

TABLE I: Available related surveys in the literature.

Subject	Ref.	Contributions
Blockchain	[24]	Analyzing blockchain technology, including its features, history, algorithms, cryptography, and applications. Assessing security risks, analyzing attacks, and summarizing security measures. Presenting challenges and research trends for scalable, secure blockchain systems.
	[25]	Surveying existing works on blockchain and (machine learning) ML technologies, presenting overview, advantages, and uses. Discussing unresolved matters, difficulties, and broader outlooks regarding the integration of blockchain and ML in communications and networking systems.
	[23]	Exploring the attack-surface of public-blockchains and highlighting defense measures against attacks and vulnerabilities.
	[5]	Exploring Blockchain's structure and operation, analyzing its role in securing IoT and ensuring privacy. Introducing "stalker," a selfish miner variant aimed at blocking block publication on the main chain.
	[26]	Surveying security service methods based on blockchain including: confidentiality, privacy, integrity, authentication, data/resource provenance and access control.
	[27]	Cataloging notable efforts in analyzing 75 security schemes for vehicular networks employing blockchain technology. Examining applications, security requirements, attacks, blockchain platforms, types, and consensus mechanisms. Compiling widely used simulation softwares for blockchain-based vehicular network simulations.
	[28]	Comparing tradeoffs and explaining taxonomy, architecture, and consensus mechanisms of blockchain. Discussing challenges including: energy consumption, privacy, scalability, interoperability, and regulatory concerns.
	[29]	Surveying literature on the integration of blockchain technology within smart cities. Introducing related works and reviewing blockchain's application in supply-chain management, healthcare, transportation, smart citizen, grid and more.
	[30]	Reviewing and analyzing cutting-edge blockchain consensus mechanisms by considering performance metrics and identifying five fundamental components, namely: block generation, information propagation, validation, incentives and finalization. Gaining insights into differences in fault tolerance, usage scenarios, scalability, assumptions, drawbacks and compromises.
	[31]	Surveying anonymity and privacy in digital cash systems resembling Bitcoin. Listing alternatives enhancing privacy, anonymity and comparing method performances and their relationships.
	[32]	Presenting advantages of integrating Cloud and blockchain technology, focusing on Blockchain-as-a-Service applications. Conducting a detailed survey of recent works combining both technologies.
	[33]	Providing a service-oriented review of blockchain-cloud integration. Exploring various service models integrating blockchain, conducting a comparative analysis for each category to offer a clear and concise view.
	[34]	Categorizing and evaluating healthcare solutions utilizing programmable Blockchain. Applying a software engineering approach to organize existing 23 related papers into categories based on challenges addressed and promoted quality attributes. Exploring the cases where Blockchain is not recommended.
	[35]	Examining vulnerabilities in Bitcoin, blockchain, and PoW-based consensus protocol. Analyzing security threats and assessing state-of-the-art security solutions. Discussing anonymity considerations and privacy threats to Bitcoin users, along with existing privacy-preserving solutions.
	[36]	Providing a vademecum for blockchain adoption, understanding advantages, requirements, consensus mechanisms, and platforms. Highlighting essential prerequisites and their development in permissioned and permission-less blockchains.
	[37]	Surveying anomaly detection integration in blockchain. Discussing security enhancement and evaluation metrics. Presenting a comprehensive examination of models for detecting anomalies across blockchain layers.
	[7]	Surveying blockchain's role in constructing a secure, decentralized, and trustless IoT environment. Addressing challenges in centralized IoT models and discussing recent advances to utilize blockchains for decentralized and secure IoT.
	[2]	Introducing Bitcoin protocol and its building blocks. Exploring design space, and extracting foundational structures and insights. Highlighting the applicability of key ideas beyond Bitcoin in various fields.
	[38]	Investigating the integration of blockchain into cloud solutions and datacenters. Focus on Blockchain-as-a-Service (BaaS), security (access control, searchable encryption), and performance analysis.
	[39]	Exploring the adoption of game theory, ML, stochastic process and the theory of optimization in blockchain systems. Summarizing the advantages and limitations of these methods. Providing blockchain fundamentals and its application in various domains and designing network services.
	[40]	Investigating the integration of edge computing systems and blockchain and discussing research challenges and critical facets of the integration, including motivations, frameworks and enabling functionalities.
	[41]	Reviewing the combination of blockchain and cloud of things (BCoT) for industrial applications. Discussing the benefits of combining blockchain's decentralization and security with scalability and elasticity inherited form cloud of things. Providing an overview of BCoT and its applications in industry, smart city, healthcare and transportation.
	[42]	Surveying the integration of auction models and blockchain technology. Blockchain offers secure and cost-effective auction management, while auctions contribute to consensus and incentive mechanisms of blockchain. Reviewing the existing solutions, achievements, and application-oriented taxonomies.
	[43]	Sorting, comparing, and analyzing blockchain consensus algorithms, highlighting their pros and cons, and suggesting future directions for development.
	[44]	Reviewing consensus algorithms in blockchain and proposing a new algorithm for enhancing consortium blockchain performance.
	[45]	Addressing the challenge of platform selection in blockchain, aligning blockchain with green ecosystem goals, analyzing blockchain architecture evolution, and proposing a classification for platform selection and future research directions.
	[46]	Exploring blockchain architecture, applications, practices, and potential benefits, while identifying future directions and challenges for research.
	[47]	Examining blockchain interoperability through a literature review, analyzing and categorizing existing solutions, and discussing enabling technologies, standards, application instances, obstacles, and forthcoming directions. Classifying investigations grouped into three classifications: public connectors, hybrid connectors and blockchain of blockchains.
	[48]	Capturing blockchain concepts, applications, issues, and suggested improvements based on subsequent publications of Bitcoin whitepaper.
	[49]	Surveying about 30 available consensus algorithms in blockchain (as of Jan. 2023), analyzing their security vulnerabilities and attacks, incorporating advanced cryptographic protocols, and gaining clarity from published articles to provide informative insights.
	[50]	Exploring blockchain's impact, addressing security and privacy challenges, and surveying its applications, structure, consensus algorithms, and future trends.
	[51]	Reviewing literature on blockchain applications across domains, highlighting its disruptive potential and classifying applications in sectors such as supply chain, healthcare, IoT, business, privacy, and data management.
	[52]	Analyzing 2451 papers (between 2013 and 2019) through bibliometric analysis, investigating trends in research development and evolution. Examining publication and citation patterns, author distribution, popular themes, collaboration, top papers, journals, funding agencies, and emerging trends. Results show increasing blockchain literature, shifting research priorities to the distributed ledger, and the inefficiency of blockchain.
	[53]	Surveying 28 consensus algorithms and proposing a framework divided into four categories to analyze and classify them: design, origin, performance, and security. Highlighting the differences between protocols and emphasizing the importance of considering all dimensions for future protocol proposals.
	[54]	Conducting a comparative study of popular blockchain technologies using a bottom-up approach. Breaking down blockchains into foundational components, hierarchically classifying them into main and subcomponents. Identifying and comparing different varieties of subcomponents. Utilizing a taxonomy tree to summarize the study.
	[55]	This study provides a comprehensive survey of applications of blockchain in Industry 4.0, analyzing application design, security, and privacy challenges. It explores security threats and countermeasures, classifies security and privacy techniques, and addresses open issues for future development.
	[56]	Evaluation of blockchain technology using the emerging technology analysis canvas (ETAC): indicating readiness for specific use cases (e.g., digital currency, financial systems), faces gaps in other areas, needs time to mature, sustaining effort challenging. Cautiously optimistic approach recommended, focusing on concrete use cases.

Blockchain	[57]	Presenting a framework aiding adoption of blockchain technology, capturing knowledge from literature, products, forums, experts. Empirical analysis of Bitcoin and top cryptocurrencies, tradeoff analysis of real-world case studies.
	[58]	Reviewing blockchain use in information systems, finance, wireless networks, healthcare, IoT, smart grids, military/defense and government services. Identifying challenges for improved utilization.
	[59]	Due to rapidly evolving nature of the blockchain landscape, this paper contributes : (i) conceptualizing architecture, (ii) designing taxonomy, (iii) classifying DLT systems rigorously using real-world data and crowd wisdom, (iv) deriving DLT design guideline through machine learning.
	[60]	Considering blockchain scalability challenges, the paper outlines: (i) modifying blockchain structure (e.g., block size) as first layer, (ii) implementing external mechanisms as second layer. Focus on sharding: dividing network into committees processing separate transactions. Contributions: (i) proposing committee-based taxonomy, (ii) comparing sharding-based protocols. Performance-based analysis of scalability solutions: throughput, latency, advantages, and disadvantages.
	[61]	Analyzing permissionless blockchain characteristics, summarizing privacy threats, investigating privacy requirements. Surveying and evaluating existing privacy technologies. Identifying open research issues and future directions in privacy.
	[62]	Classifying improvements of Proof of Stake (PoS): (1) PoS-based consensus mechanisms, (2) PoS-based and PoW-based consensus mechanisms, (3) PoS-based and BFT-based consensus mechanisms. Introducing variants and summarizing fundamental concepts, impacts, benefits, and drawbacks. Comparing performance of improved algorithms and discussing network security attacks.
	[63]	Considering blockchain usage in financial sectors. Systematic review of 76 articles, resulting in a 3-dimensional classification framework: blockchain development, challenges and financial sector applications.
	[64]	Collecting relevant blockchain researches for understanding current topics, challenges, future directions. Extracted 41 primary papers. Results: 80% focus on Bitcoin, $< 20\%$ on other applications. Majority address privacy, security limitations with lacking evaluation. Scalability challenges unexplored.
	[65]	Surveying blockchain consensus protocols, this study examines their theoretical basis, models, challenges, and performance, classifying them into proof-based, committee-based, and miscellaneous categories, and discussing future research directions.
	[66]	Exploring applications of blockchain in healthcare, covering medical information management, record sharing, image sharing, log management, IoT integration, drug supply chain tracking, security, and privacy. It analyzes existing surveys and evaluates the benefits and drawbacks of blockchain in healthcare.
	[67]	Conducting systematic survey: IoT blockchain components, popular applications, architecture overview, network structures, protocols, consensus protocols comparison, traffic model analysis, metrics, suitable traffic model for IoT-blockchain systems.
	[68]	Addressing demand for verification of smart contracts in various sectors, this survey examines formal models, specifications in literature, common trends, and current verification approaches.
	[69]	Drawing a roadmap of blockchain surveys (2016-2021), studying applications (IoT, business, security) and recognizing gaps. Identifying and classifying recent research on blockchain systems and networks and guiding researchers in theories, modelings, and tools.
	[70]	Reviewing blockchain security research in process, data, and infrastructure levels (PDI model). Evaluating the status of blockchain security in the existing literature. Suggesting future research directions in blockchain security, addressing business and industrial concerns.
	[71]	Investigating blockchain's progress in terms of performance and security. Discussing architectural choices, metrics, enhancements, and hybrid blockchains for balancing performance and security. Experimenting on Ethereum and surveying scalability in blockchain platforms.
	[72]	Examining security issues of blockchain technologies and applications.
	[73]	Analyzing attacks and countermeasures at each layer of the blockchain architecture. The study highlights the often overlooked security concerns within blockchain itself.
	[74]	This survey examines the security considerations related to Ethereum, categorizing vulnerabilities, attacks, and protective measures to provide insights into underlying reasons, outcomes, and protective capabilities, informing future research directions in Ethereum system security.
	[75]	It reviews existing DLT solutions for the difficulties encountered by IoT-based applications and identifies areas for upcoming research areas, encompassing distributed ledger technology (DLT) security, scalability, and multi-DLT use cases, and the impact of post-quantum scenarios. The article highlights the potential of DLTs to revolutionize various aspects of daily life.
	[76]	This article delves into the research of Byzantine fault-tolerant (BFT) protocols in the context of blockchains. It categorizes BFT protocols based on system models and workflows, aiming to understand the evolution of BFT research over the past four decades, particularly with the emergence of blockchains.
	[77]	This paper examines implementing blockchain technology for enhancing cloud storage security, highlighting the growing demand for blockchain innovation and its potential to address technology concerns related to decentralization, trust, data ownership, and information-driven decisions.
	[78]	This study investigates the incorporation of blockchain technology and digital twins (DTs) in industrial applications. By combining blockchain and DTs, intelligent conclusions can be drawn, faults can be identified, and predictive maintenance can be performed, addressing challenges related to data repositories, data dissemination, and predictive maintenance.
	[79]	This study explores the combination of federated learning methods and blockchain to improve the security and privacy of IoT systems. It highlights the challenges posed by centralized storage and computing in current IoT paradigms and the capability of smart contracts and blockchain to address these issues.
	[80]	Blockchain technology is recognized as a compelling remedy for future data-driven networks (DDNs), offering secure data-storage, analytics, sharing, privacy protection, and decentralized network management. However, challenges and open issues remain in the widespread deployment of blockchain in DDNs. The survey explores the utilization of blockchain in computer networks, identifies challenges, and proposes potential mitigation to enhance the efficiency, security, and effectiveness of network services in future blockchain-empowered DDNs.
	[81]	This study focuses on the incorporation of blockchain technology in federated learning (FL), known as BlockFed. FL faces challenges in coordination, arbitration, and model aggregation, often relying on centralized approaches. Blockchain offers a potential solution by addressing these issues, and the survey categorizes existing system models into decoupled, coupled, and overlapped classes. The advantages, disadvantages, and corresponding solutions for these models are examined
	[82]	This survey comprehensively reviews existing variants of blockchain-enabled FL, identifies challenges, and proposes potential research directions in this evolving field.
	[83]	This article provides a systematic (i.e., replicable and protocol-driven) and multivocal literature review (i.e., encompassing both grey and white literatures similarly). The objectives include defining blockchain technology, exploring its architecture options and tradeoffs, and understanding its current applications and challenges.
	[84]	This article focuses on the concept of blockchain oracles, which enable the connection between smart contracts and off-chain data. The article surveys blockchain oracle technologies and mechanisms, categorizing them into voting-based strategies and reputation-based approaches, and discusses their structure, principles, data integrity, and correctness.
	[85]	It covers the concepts of availability, consistency, and data integrity, while acknowledging the inherent limitations of blockchains. Using Ethereum as an illustrative example, the tutorial explores the internal mechanisms of blockchains and offers a comparison to traditional distributed systems.
	[86]	It characterizes Blockchain-based Software (BBS) engineering based on theoretical foundations, processes, models, and roles. The survey provides insights into development tasks, design principles, models, roles, challenges, and resolution techniques, offering a consolidated body of knowledge for software engineering practitioners and researchers in BBS development.
	[87]	This study offers a thorough examination of the current progress in blockchain interoperability for the next-generation blockchain ecosystem. It explores the principles and procedures for achieving interoperability, surveys practical instances, and compares state-of-the-art systems.
Blockchain	[88]	This paper addresses the need for incentive mechanisms in blockchain-based systems to regulate entity behaviors and improve system performance. It proposes evaluation requirements for assessing incentive mechanisms and presents a taxonomy of blockchain-based incentive mechanisms based on versions, forms, and goals. The review highlights the advantages and disadvantages of existing incentive mechanisms and explores their relationship with blockchain.
	[89]	This survey explores comprehensively the application of blockchain technological advancements in providing security services for cloud computing models. It examines the combination of cloud computing architectures and blockchain, analyzes recent studies on security services based on blockchain, and investigates the potential performance improvements cloud computing can offer to the blockchain.

Blockchain	[90]	This study focuses on the review of available smart contract languages (SCL) and their features in order to enable legally binding contracts in decentralized autonomous organizations (DAO). An organized and methodical review of the literature is conducted, covering both white literature and grey literature which were published from 2015 to 2019. The review identifies 10 critical SCL properties for developing legally compliant DAOs and explores specifications for SCL development.
	[91]	This survey focuses on privacy-preserving reputation systems, which enable users to provide feedback privately without fear of retaliation. The analysis highlights the unique properties of blockchain-based privacy-preserving reputation systems, such as trustlessness, transparency, and immutability, and provides insights and future research directions for leveraging blockchain to develop more secure and robust systems.
	[92]	The survey provides a summary of research efforts made between 2008 and 2019, categorizing privacy and security risks in the IoT realm, and classifying literature on machine learning algorithms and blockchain techniques.
	[93]	This article discusses the utility of blockchains in various applications and introduces the essential security properties required for cryptocurrency systems. The article then explores supplementary security and privacy characteristics sought after in blockchain applications and reviews techniques such as consensus mechanisms, mixing protocols, hash-chained-storage, and anonymous-signatures to achieve these properties.
	[94]	This study provides a thorough overview of the current advancements in smart contract languages for blockchain platforms. It identifies and categorizes 101 different smart contract languages based on various criteria. The study follows rigorous guidelines for conducting a multivocal mapping review, ensuring a replicable and comprehensive examination of smart contract languages.
	[95]	This study offers a detailed examination of blockchain systems based on directed acyclic graph (DAG), which aim to address the limitations of high latency and low scalability in classical blockchain systems. The authors present a general model and identify six design patterns for DAG-based systems. They evaluate these systems in terms of structure, consensus, property, security, and performance, discussing trade-offs, open challenges, and future research directions.
	[96]	This article addresses the unique networking requirements of blockchains and cryptocurrencies, emphasizing the need for a deeper understanding of the design aspects of these networks. It provides a systematic overview of various aspects, including block propagation, neighbor discovery, topology, transaction propagation, sharding, and off-chain networks. The authors also highlight the differences and commonalities with traditional network.
	[97]	This article explores the use of blockchain for decentralized voting. It provides a thorough review of voting systems based on blockchain, categorizing them according to various properties such as blockchain types, consensus approaches, and participant scale.
	[98]	This paper addresses the consensus problem, which involves achieving agreement on the system status despite potential faults or malicious behavior. It provides a survey of research on the consensus problem, comparing different approaches and discussing their applications.
	[99]	This article reviews blockchain interoperability from various perspectives, including blockchain architecture fundamentals, platforms, taxonomy, and consensus mechanisms. The article proposes a hierarchical structure for designing protocols and techniques for interoperable blockchains and discusses potential opportunities, application areas and challenges.
	[100]	The paper surveys relevant literature on building decentralized trust mechanisms using blockchain technology. The paper discusses the architecture of a decentralized trust mechanism, including the layers of data, network, consensus, contract, and application, and provides an overview of blockchain principles, consensus mechanisms, and smart contracts.
	[101]	This study offers an in-depth exploration of blockchain technology, its applications, and challenges beyond cryptocurrencies. It covers recent developments, adoptions, and the cryptography underlying blockchain. The paper also surveys both public and enterprise blockchains.
	[102]	This paper provides a thorough examination of the progression, structure, developmental frameworks, and security concerns related to blockchain technology. It covers various aspects such as consensus algorithms, security risks, and cryptographic primitives. The paper also discusses upcoming pathways, innovative applications, and unresolved research hurdles in the realm of blockchain.
	[103]	This work presents a summary of existing methods and ideas for abnormal behavior awareness in public blockchain and consortium blockchain systems. It highlights the differences between these two types of blockchains and discusses the available datasets for blockchain security analysis.
	[104]	This paper discusses the application of secure multi-party-computation technology in the blockchain to address privacy protection issues. It explores three main technologies -Zero-knowledge proof, secret sharing, and homomorphic encryption- and analyzes their security aspects. The paper concludes by highlighting the potential of secure multi-party computing in solving scalability, key distribution, and quantum attack challenges, emphasizing that the combination of cryptography and blockchain will be a significant trend in the future.
	[105]	This article investigates the security of blockchain and highlights a cyber-attack on a Bitcoin exchange center and clarifies that the attack targeted the exchange, not the blockchain itself. The study concludes that blockchain is effective in defending against injection attacks and DDoS attacks due to its immutable and distributed nature. However, it raises concerns about the future risk of quantum computing and proposes a technique combining Geoencryption and SHA256 to enhance blockchain encryption complexity.
Quantum	[106]	This paper explores the incorporation of quantum key distribution (QKD) into current optical networks and discusses key establishment methods. The paper addresses various challenges in QKD secured optical networks, including routing, resiliency, trusted repeater node placement, and quantum key recycling. It also provides an overview of QKD, describes QKD protocols, and discusses quantum hacking attacks and prevention methods.
	[107]	This report presents a review and mapping of possible military applications of quantum technology. It highlights the dual-use nature of quantum technologies and their relevance to the defense and security industry. The report provides an overview of quantum technologies, estimates their expected delivery or impact, and describes their applications in various warfare domains.
	[108]	This paper highlights the recent cracking of post-quantum cryptography algorithms (Rainbow and SIKE) selected as finalists by NIST and the challenges in building a quantum-safe encryption standard. It proposes an encryption-agnostic approach called zero-vulnerability computing (ZVC) as a potential solution to render computers quantum-resistant. ZVC aims to secure computers by eliminating third-party permissions and simplifying the architecture to create a robust and energy-efficient system resistant to both malware and quantum threats.
	[109]	The study reviews existing efforts to safeguard against quantum attacks and highlights the need for additional measures to mitigate the potential damage to information security caused by quantum computers.
	[110]	Synthesizing studies on quantum cybersecurity, this research explores its dual role: threat and solution. It provides a comprehensive overview, highlights benefits and threats, and supports further research.
	[111]	This article examines the historical impact of quantum computing on encryption codes and the potential risks posed by advanced quantum computing capabilities. The paper further evaluates and compares traditional cryptographic techniques using a SWOT framework and explores security enhancements for data transmission to mitigate the risks introduced by quantum computing.
	[112]	This survey summarizes quantum's state-of-the-art in financial applications, emphasizing modeling, optimization, and learning. It enhances pricing, modeling, optimization, processing, and detection. Feasibility and use cases on near-term quantum computers are explored.
	[113]	This paper reviews quantum software components and platforms, emphasizing the need for quality requirements and assessment.
	[114]	Reviewing the latest progress in quantum computing technology and addressing ongoing challenges.
	[115]	Categorizing papers, tools, frameworks, platforms facilitating quantum computing. Presenting the layers of quantum computing, the features of quantum computing platforms and circuit-simulators, open-source tools including TensorFlow Quantum (TFQ), ProjectQ and Cirq, enabling quantum program implementation in Python.
	[116]	Providing overview of challenges, open problems in distributed quantum computing. Offering easy access, guide to relevant literature, prominent results from computer/communications engineering perspective.
	[117]	highlighting suggestions for utilizing QC techniques in smart grid applications. Identifying potential smart grid applications. Demonstrating real-world QC case studies in various research fields. Providing brief overview of quantum hardware specifications, software tools, algorithms with comparative analysis.
	[118]	Reviewing and comparing properties of key establishment techniques, including QKD. Analyzing scenarios for integrating QKD into cryptographic infrastructures: 1) QKD as key renewal for symmetric cipher over point-to-point link, 2) QKD in network for any-to-any key establishment service. Discussing constraints and potential benefits of using QKD in these contexts.
	[119]	Elucidating implications of quantum computing in present cryptography, introducing basic post-quantum algorithms. Highlighting disparities between classical and quantum computing, addressing quantum computing challenges, exploring Shor and Grover quantum algorithms, examining impacted encryption methods, discussing hash function vulnerabilities, and delving into post-quantum cryptography. Discussing QKD techniques and mathematical approaches within the context of post-quantum cryptography.

	[120]	Providing unified and end-to-end review of 18 years of research (2004-2021) in Quantum Computing and routing problems. Analyzing 53 papers to summarize current state of the art, including study types (practical or theoretical), solving approaches (dedicated or hybrid), open challenges, and frequently used Quantum Computing devices.
	[121]	Discussing security risks in quantum computing stack due to untrusted third parties. Addressing hardware vulnerabilities. Highlighting risks from mis-calibrated qubits and denial-of-service attacks and risks from untrusted compilation services, including Trojans and tampering.
	[122]	Systematic analysis of quantum computing's potential in healthcare. Examining drug discovery, personalized medicine, DNA sequencing, medical imaging, and operational optimization. Developing taxonomies across various dimensions.
	[123]	Analyzing promises/limitations, defining research directions, bridging knowledge gap, surveying applications/advancements/challenges in quantum computing.
	[124]	Surveying literature on quantum computers' impact on information security, this paper explores positives and negatives. It assesses NIST SP 800-53 Rev. 5 controls and outlines progress on quantum-resistant standards.
	[125]	This article reviews QC literature, introduces a taxonomy, and identifies research gaps. It covers quantum software tools, post-quantum cryptography, and quantum hardware development, providing a detailed overview of the present cutting-edge developments.
	[126]	Providing a brief introduction of key concepts in quantum computing. Based on lectures at George Washington University, they aim to engage non-experts seeking a quick overview. Touching on the role of quantum topology in the field.
	[127]	Surveying quantum computing concepts, algorithms, and progress towards scalable quantum computers. Efficient quantum solutions for algebraic problems are explored. Analysis of current quantum computer implementations anticipates the creation of a fully functional quantum computer within the next 10-15 years.
	[128]	This paper reviews quantum machine learning, discussing its potential to enhance classical algorithms and address challenging problems. It explores the limitations and advantages of quantum algorithms and addresses practical considerations for implementing quantum ML.
	[129]	This paper explores the exponential growth of high-performance computing, including cloud and fog computing. It describes the basic concept and history of quantum computing, as well as its applications in networking, cryptography, and game design.
	[130]	This study performs review on quantum software architecture, exploring processes, notations, patterns, tools, and challenges. Findings reveal adaptability of existing processes and notations, using Qubits and Qugates as architectural components.
	[131]	Exploring the potential of quantum computing in the financial industry and its impact on areas such as portfolio management, risk management, and derivative pricing. It reviews platforms, algorithms, methodologies, and real-world use cases, providing a structured overview for finance professionals.
	[132]	This paper reviews quantum-based methodologies in the literature for improving recommendation systems. It highlights challenges and advancements in this emerging approach.
	[133]	This article surveys quantum computing fundamentals and analyzes its impact on IoT security. It aims to provide insights into quantum-enabled IoT communication and examines the challenges of implementing such communication.
	[134]	This paper presents a survey of quantum cryptography. It then reviews fundamental protocols such as quantum key distribution using the BB84 protocol and its security proof. Additionally, the paper discusses the quantum bit commitment protocol and its proof of insecurity.
	[135]	This paper provides an introduction to quantum computations and discusses the gate model and adiabatic quantum computing paradigms. The paper then explores the existing state-of-the-art in quantum-perceptrons and quantum neural-networks implementations, comparing and analyzing different approaches in these areas.
	[136]	This paper focuses on QKD networks, which enable secure key negotiation protocols for information-theoretic security. It provides an overview of QKD basics and reviews the development and implementation of QKD networks. The paper describes the architecture, elements, interfaces, and protocols of QKD networks, and discusses network-layer and physical-layer solutions. It also highlights initiatives for standardization, application scenarios, and prospective avenues for research, providing recommendations for designing QKD networks..
	[137]	The deployment of the Micius satellite has marked a significant advancement in long-range quantum communication. This development demonstrates that quantum protocols, previously limited to terrestrial experiments, can now be extended globally using low-orbit satellites and single-photon discrete-variable quantum states. In this paper, the authors review the upcoming expansion of space based quantum communication into the continuous variable regime, which offers the potential for enhanced communication performance and represents a crucial step towards the development of a worldwide quantum-Internet.
	[138]	This survey explores quantum computing in addressing the performance challenges of wireless communication systems. Quantum algorithms offer the possibility of approaching optimal performance with fewer evaluations. The survey discusses the basics of quantum computing, presents major quantum algorithms for improving wireless communications, and investigates optimization methods in both the physical-layer and network-layer. Furthermore, this paper identifies unresolved issues in wireless communications that could potentially gain from the application of quantum computing.
	[139]	Quantum-Internet (QI) relies on quantum communication between distant nodes via quantum channels protected by cryptographic mechanisms. This study provides a thorough review of QI functionalities, technologies, use cases, and open challenges, aiming to familiarize readers with the infrastructure required for the advancement of a global QI.
	[140]	Quantum communications have revealed fundamental structures, including phenomena like super-activation, super-additivity and causal activation, that lack classical equivalents. Understanding these phenomena is vital for the community of communication engineering. This treatise provides readers with an accessible guide to the pertinent literature and significant findings from the standpoint of communication engineering.
	[141]	This paper explores the duality between quantum and classic coding theory and aims to bridge the gap between the two. It provides a comprehensive survey of the history of classical and quantum codes, focusing on stabilizer-based quantum error correction codes (QECCs). The paper includes a tutorial on constructing QECCs from binary and quaternary codes, specifically discussing Calderbank-Shor-Steane (CSS) codes, non-CSS type codes, and entanglement assisted codes. Design examples are provided for classical and quantum versions of widespread families of codes, such as Bose-Chaudhuri-Hocquenghem (BCH) and convolutional codes.
	[142]	This article reviews significant achievements and recent progress in the field of quantum computing, categorizes the essential components of quantum-Internet into four critical concerns, and investigates them specifically: quantum cryptography, quantum networks, quantum computers and quantum ML. The paper also examines the primary obstacles and trends in the field.
Quantum	[143]	This review discusses the features of channels used for quantum communication and explores diverse measures of capacity specific to quantum channels. The article also emphasizes the fundamental distinctions between quantum and classical channels, providing insights into the unique characteristics and capabilities of quantum communication.
	[144]	This paper focuses on the key exchange primitive in public-key cryptography, with a specific emphasis on the Diffie-Hellman protocol. It reviews and compares three different implementations of this protocol including: core Diffie-Hellman (DH) protocol, elliptic curve Diffie-Hellman (ECDH) protocol, and super-singular isogeny Diffie-Hellman (SIDH) protocol. The paper discusses the steps involved in establishing shared keys, provides security analysis for each implementation in both pre- and post-quantum settings, and concludes with a brief comparison of the three instantiations.
	[145]	This study comprehensively reviews the various branches of quantum cryptography including: QKD, quantum signatures, quantum secure direct communication, quantum secret sharing and quantum private query. The paper also briefly covers other branches in the theoretical research stage, such as quantum anonymous voting, quantum private comparison, quantum secure multi-party summation, and more.
	[146]	This article discusses the potential risk to blockchain security presented by advances in quantum computing and explores the concept of quantum-resistant blockchains as a solution. It highlights the application of asymmetric cryptography and hash-functions in blockchain technology and how they can be vulnerable to quantum attacks. The article proposes a conceptual design for a quantum blockchain identity framework and evaluates its feasibility, effectiveness, and limitations. Despite current limitations and challenges, the authors emphasize the importance of exploring decentralized quantum applications.
	[147]	This paper presents a new post-quantum-PoW consensus algorithm for blockchain systems, providing protection against quantum computing attacks. It also introduces identity-based post-quantum signatures for lightweight transactions. The proposed approach enhances security and expands transaction capacity in future post-quantum blockchains.
	[148]	The article examines the present status of post-quantum cryptography and its applicability in blockchain systems. The article also evaluates post-quantum blockchain solutions and provides comparisons of encryption and signature schemes, offering guidance for ensuring blockchain security in the face of quantum advancements.

Quantum and Blockchain	[149]	This paper discusses the convergence of blockchains and quantum computing, emphasizing the need for post-quantum signatures in blockchain systems. It provides an overview of post-quantum cryptography, including an assessment of NIST's third-round candidates. The paper addresses the challenges and provides guidelines for integrating post-quantum algorithms into blockchain applications.
	[150]	This paper reviews the influence of quantum computing on the security of blockchain and explores the current state of research on countermeasures, emphasizing the need for proactive measures to ensure the long-term security of blockchain applications.
	[151]	This book provides an exploration of the intersection between quantum computing and blockchain technology. It covers topics such as quantum cryptographic techniques, the development of quantum blockchain, the development of quantum Bitcoin, and a theoretical framework for quantum blockchain. The book also delves into challenges and research perspectives of blockchain in the post-quantum era, post-quantum cryptographic systems for blockchains and post-quantum confidential transaction protocols. Additionally, it discusses the influence of quantum computing on the security of blockchain, explores quantum blockchain techniques for sustainable cybersecurity, and examines the prediction of Bitcoin price patterns using supervised learning methods.
	[152]	This paper addresses the risks posed by quantum computers to classical cryptographic algorithms and explores the concept of post-quantum cryptosystems. Additionally, the paper provides an overview of blockchain fundamentals and analyzes the vulnerability of popular cryptocurrencies to quantum threats, concluding with a review of proposed post-quantum blockchain schemes.
	[153]	This study examines the migration process from ECDSA to post-quantum algorithms in blockchain implementations, considering the potential threat of quantum computers. It highlights the challenges and financial implications associated with replacing the cryptographic implementation. The study emphasizes the role of the BIP39 Seed in achieving backward compatibility and proposes strategies to minimize the impact of the migration.
	[154]	This study examines the weakness of blockchain systems to quantum computer attacks and explores the potential of post-quantum cryptography as a solution. It evaluates the performance of different post-quantum digital signature schemes in the blockchain context, considering factors such as execution time and memory consumption. The goal is to assess the feasibility and effectiveness of implementing post-quantum cryptography to enhance the security of blockchain systems against quantum threats.
	[155]	This research evaluates the efficiency and performance of two Hash-based Signature Schemes (MSS and W-OTS) in comparison to classical algorithms (RSA and ECDSA) used in bitcoin transaction security. The study focuses on key generation, signature generation, and verification time as metrics for comparison. The results indicate that W-OTS demonstrates superior efficiency and resistance to quantum computer attacks, making it a recommended choice for enhancing the security of bitcoin transactions.
	[156]	This article provides the analysis of the intersection between blockchain security and law, particularly focusing on post-quantum considerations. It examines the complex relationships among congress, the federal reserve, and blockchain technology in the context of money creation.
	[157]	This systematic literature review explores the vulnerabilities of blockchain technology to quantum attacks. The analysis reveals that a majority of research solutions concentrate on the data, application, and network layers of blockchain, with minimal attention given to hardware and infrastructure. Additionally, alternative distributed ledger technologies are considered as potential solutions.
	[158]	This article explores the use of post-quantum cryptosystems in consensus algorithms to protect blockchain systems from quantum attacks. A comparative study is conducted to analyze different consensus algorithms and their effectiveness in ensuring quantum resistance for blockchain.
	[159]	This paper addresses the impact of quantum computing on the classical blockchain mechanism. It highlights the need for quantum-safe blockchain designs as traditional cryptography algorithms become vulnerable to quantum attacks. The study includes a comprehensive literature review, addressing research questions and identifying research gaps in the field of quantum blockchain.
	[160]	In this survey, the origins and historical progression of quantum-Bitcoin are presented. The correlation between blockchain technology and cryptocurrencies is discussed, with a focus on the benefits of quantum-Bitcoin compared to classical-Bitcoin. The potential benefits and challenges of the future development of quantum-Bitcoin are also examined.
	[161]	This comprehensive survey examines multivariate asymmetric encryption and signature schemes, which offer promising security in the presence of quantum adversaries. It discusses the security challenges, such as MinRank attack and differential attack, and provides insights into the necessary algorithms for implementation. The survey compares different multivariate schemes, addresses open challenges, and serves as a valuable resource for researchers in the field of public-key cryptography.
	[162]	This survey examines the potential of lattice based cryptography as a post-quantum cryptographic solution in the face of quantum computing threats. It discusses the foundational features of lattice based cryptography and its applications in various security domains. The survey also highlights the challenges and considerations involved in implementing lattice-based schemes on different computing platforms.
	[163]	Introducing quantum information theory and computation, this chapter enables understanding of quantum technology in the blockchain industry. It presents a peer-to-peer information system for quantum states, enhancing privacy and security through the laws of physics, surpassing non-quantum approaches.
	[164]	This paper provides the summary of blockchain technology, its structure, and characteristics. It also discusses quantum vulnerabilities, cryptographic concepts, and the point of convergence between blockchain and quantum computing. Finally, it explores the migration from pre-quantum to post-quantum blockchain.
	[165]	This article provides a survey of post-quantum secure digital signatures in the context of blockchain technology. It explores exotic signatures, such as multi-signatures, aggregate-signatures, threshold-signatures, adaptor-signatures, blind-signatures and ring signatures, which offer advanced functionalities beyond traditional signatures. The survey discusses challenges and future research directions, aiming to enhance post-quantum cryptography for secure blockchain systems in the face of quantum threats.
	This Paper	The survey examines the quantum security of key components in blockchain technology, such as digital signatures, hash functions, consensus algorithms, and smart contracts. It analyzes the vulnerabilities introduced by quantum computers and explores countermeasures to protect the integrity and confidentiality of blockchain systems. The survey also investigates the potential ways in which quantum computing can be exploited to strengthen attacks on blockchains and emphasizes the importance of developing quantum-resistant defenses and exploring quantum and post-quantum blockchain architectures.

II. Overview of Blockchain

As of mid-2023, the global count of blockchain companies has surpassed 12,000 [166]. This number signifies a significant growth and widespread adoption of blockchain across various industries and sectors. It suggests that blockchain technology continues to gain momentum and attract a large number of companies interested in exploring its potential applications and benefits. Within this section, we present a succinct overview of the fundamental principles, characteristics, structure, and classification of blockchain technology.

Blockchain is a decentralized record-keeping system (or ledger) that allows immutable transactions between parties who do not necessarily trust each other, all without the need for a central authority or human involvement. In blockchain, transactions are collected and stored in an unalterable ledger and consensus is employed to achieve an agreement on the order of events within the chain. Moreover, a set of rules, known as transaction validation mechanism, is employed to ensure the correctness of every block and the transactions contained within it.

Blockchain presents opportunities for orchestrating various untrusted parties, as well as facilitating governance in a decentralized manner. Key features include decentralization, immutability, anonymity, transparency, auditability, autonomy and security. Decentralization allows transactions to be generated and validated by multiple nodes, breaking the reliance on central servers. Immutability is achieved through irreversible cryptographic hash functions, making records resistant to change. Anonymity is achieved by using pseudonymous addresses to protect identities and enhance privacy [25].

Transparency ensures all nodes have access to a complete transaction history. Auditability allows nodes to trace and verify transactions. Autonomy enables transaction operation and management without human interaction or third-party trust. Security is maintained through cryptographic mechanisms and network validation. The working procedure of blockchain can be summarized as follows:

1) Transaction Creation: Participants initiate transactions by creating digital records that contain relevant information, such as the sender, recipient, and transaction details. These transactions can involve various types of data, not just financial transactions.

2) Verification and Validation: Transactions are broadcasted to the network of nodes, which act as validators. These nodes collectively verify the validity and authenticity of each transaction using a specific set of rules that depends on the blockchain protocol being used.

3) Block Formation: Verified transactions are grouped together into blocks. Each block typically has a maximum size and can hold a certain number of transactions. Successive blocks are generated in order and connected to preceding blocks, creating a sequence of blocks known as the blockchain.

4) Consensus and Block Confirmation: Consensus mechanisms ensure that all nodes in the network agree regarding the order and legitimacy of transactions within every block. Once a block is confirmed and appended to the blockchain, modifying or tampering with recorded transactions becomes extremely difficult due to the application of cryptographic hash functions.

5) Distributed Ledger: The blockchain acts as a distributed ledger that is stored and replicated throughout multiple nodes in the network. This distributed nature ensures redundancy, security, and resilience, as the ledger is not reliant on a single central authority.

6) Mining (in some cases): In blockchain networks that utilize Proof of Work (PoW) consensus, mining nodes compete to solve complex mathematical puzzles. The initial node that successfully solves the puzzle introduces a fresh block to the blockchain and is rewarded with newly minted cryptocurrency as an incentive for their computational work.

7) Data Consistency and Security: When new blocks are incorporated into the blockchain, the ledger is continuously updated across all participating nodes. The decentralized and immutable nature of the blockchain ensures data consistency and security, making it highly resistant to fraud, tampering, and unauthorized modifications.

8) Access and Transparency: Depending on the kind of blockchain, retrieval of the stored data can be either public or restricted to authorized participants. Public blockchains, like Bitcoin and Ethereum, allow anyone to view and verify the transactions, while private or permissioned blockchains restrict access to a select group of participants.

A. Architecture of Blockchain

The architecture of blockchain encompasses the underlying structure, components, and protocols that enable its decentralized and secure operation. Understanding the architecture is crucial for comprehending the inner workings of blockchain technology. This section provides an overview of the key elements and layers involved in blockchain architecture.

There are two primary blockchain architectures: execute order validate (EOV) architecture, and order execute (OE) architecture. EOV, represented by Hyperledger Fabric, involves a transaction life cycle where the client generates a transaction sent to endorsement nodes. These nodes independently execute the transaction and send responses to the client. After collecting enough endorsements, the client forwards them, along with the transaction, to ordering service nodes (orderers). Orderers receive and pack transactions into blocks, distributing them to other full nodes for validation. Full nodes independently validate blocks, ensuring consistency by checking endorsements and signatures. Confirmed transactions receive a simple payment verification (SPV) from the full node.

In the OE architecture, represented by Bitcoin and Ethereum, transactions are executed after block producers generate valid blocks without endorsement nodes. The life cycle involves the client generating a transaction and sending it to a full node that verifies and broadcasts the transaction to neighboring nodes, which further verify and broadcast it. Block producers gather verified transactions and assemble them into a candidate block, aiming to add it to the blockchain through a competitive process. Successfully mined blocks are sent to other full nodes for validation. Full nodes verify the new block and provide an SPV to the client, confirming the transaction's addition to the blockchain.

Due to the similarities in network-layer operations across both architectures we focus on their building blocks. Based on the findings in [167] and [29], a generic blockchain system can be divided into six distinct layers, as depicted in Fig. 2. These layers, from top to bottom, include: application layer, contract layer, incentive layer, consensus layer, network layer, and the data layer. Each layer performs specific functions within the blockchain architecture. Below, we provide a concise overview of the roles of each layer.

The data layer primarily deals with transactions and blocks, wherein transactional data generated by various applications is stored. Blocks consist of a collection of transactions and are interconnected in a sequential manner, forming a sequence of blocks. Fig. 1 illustrates the two main components of a block: the main data and the block header. The main data section contains all executed transactions, where the type of data varies depending on the specific blockchain service.

The block header contains the hash values of the previous blocks and the present block, Merkle root, block version, timestamp, and other relevant information [25]. The block version indicates which set of rules for block validation should be adhered to. For Bitcoin, Version 1 was introduced with the genesis block in January 2009. Version 2, Version 3 and Version 4 were implemented through soft-forks in Bitcoin-Core 0.7.0, Bitcoin-Core 0.10.0 and Bitcoin-Core 0.11.2, which were released in September 2012, February 2015 and November 2015, respectively.

By utilizing the hash of the preceding block, it is possible to establish a irrefrangible connection between all blocks. As new blocks are appended to the blockchain, the most recent

block retains a hash pointer pointing to its preceding block. The hash value of the root node in the Merkle tree enables efficient verification of recorded transactions within the current block. The timestamp records the block generation time. It is important to note that in directed acyclic graph (DAG) networks, the new transaction directly references the prior transaction, and transaction blocks, as seen in conventional blockchain systems, are absent. The network layer encompasses the mechanisms employed in blockchain for tasks such as forwarding, broadcasting, verifying, and also auditing the produced data from the data layer. Typically, we model the blockchain network as a peer-to-peer (P2P) network in which blocks and transactions are distributed between nodes in an uncentralized fashion.

The consensus layer determines the consensus The consensus layer establishes the algorithm used to achieve agreement on certain data sharing among untrusted and distributed participants [53]. Numerous consensus protocols are utilized in blockchain systems, broadly categorized as consensus mechanisms with proof-of-concept (e.g., PoW[1] [22], Proof of Stake[2] (PoS) [168], Delegated PoS (DPoS) [169], Proof of Authority (PoA) [170]) and Byzantine Fault-Tolerant (BFT) replication protocols (e.g., Practical BFT (PBFT) [171], Delegated BFT (dBFT) [172], Ripple [173]. The selection of consensus protocols varies based on blockchain type. In permissionless blockchains (public blockchains), which exhibit loose control and limited synchronization, consensus schemes driven by incentives, like PoW and PoS are commonly employed. On the other hand, permissioned blockchains (private blockchains and consortium blockchains) typically adopt BFT consensus protocols like PBFT and dBFT. Since comprehensive surveys on consensus mechanisms already exist, our focus will be on providing an in-depth discussion of select representative consensus mechanisms.

PoW, as successfully employed in Bitcoin, represents a distributed and probabilistic consensus mechanism. PoW involves a complex computational process where competing nodes (miners) expend computational resources to solve a computational puzzle. Once a node discovers the solution, other nodes quickly verify its correctness, and the transactions within the present block are validated and stored on the ledger. This immutability prevents block modifications and Sybil attacks. However, PoW's energy consumption and scalability issues led to the development of PoS. PoS introduces a different approach to block verification by utilizing the coin holdings of participants, reducing the need for extensive computational work. Coin owners offer their coins as collateral, known as staking, in order to have the opportunity to validate blocks and receive rewards. Validators are chosen randomly to confirm transactions and validate block data. This approach eliminates the competitive rewards-based mechanism of PoW and instead employs a randomized selection process for fee collection. To become a validator, coin owners must stake a specific amount of coins. For example, in Ethereum, a user needs to stake 32 ETH to operate a node. Multiple validators validate blocks, and once a predetermined number of validators confirm the accuracy of a block, it is considered finalized and closed. While PoS reduces resource consumption, security concerns arise due to the low mining cost and the fact that stake is a virtual concept [174]. To address this, some blockchains combine PoW and PoS, such as Casper, which integrates PoS and BFT consensus theory [175].

DPoS is a stake-based consensus algorithm where nodes elect representatives to generate and validate blocks. This representative democracy, speeds up transaction verification in comparison with the direct democratic PoS mechanisms. Bitshares is an example of a blockchain that uses DPoS for efficient consensus and offers financial services [169].

PBFT, used in Hyperledger Fabric [176], is a Byzantine fault-tolerant replicating algorithm that can manage a maximum of $1/3$ fraudulent replicas [177]. PBFT requires nodes to know each other and relies on a primary node to order transactions. The consensus process involves pre-prepared phase, prepared phase, and commit phase. However, PBFT is not scalable for large networks due to increased communication costs. dBFT combines features of DPoS, where professional nodes achieve consensus and form blocks, while other nodes operate as regular nodes for block verification. For example, Antshares [169] and NEO [172] have implemented dBFT.

The topology of ledger ascertains how data is stored in the system. Most blockchain applications use a chain of blocks. However, new ledger topologies like DAG, sidechains, and off-chain have emerged to address scalability concerns. The incentive layer introduces financial incentives to encourage nodes to verify data in a decentralized blockchain system. The contract layer facilitates the ability to program blockchain systems and allows using smart contracts, script codes, and other programmable components for complex transactions. Platforms like Ethereum support smart contracts. In application layer, different applications, including edge computing, healthcare and IoT are encompassed. Significant applications in this layer include security services and digital identity, both of which have revolutionized their respective domains through enhanced, secure, and decentralized management.

B. Classification of Blockchains

In this section, we provide the classification of different types of blockchain technology based on various characteristics. The following general taxonomy can be used to classify blockchain systems:

1) Public Blockchain: A public blockchain is open to anyone who wants to participate. It is decentralized and permissionless, allowing anyone to join the network, validate transactions, and contribute to the consensus process. Examples include Bitcoin and Ethereum.

2) Private Blockchain: A private blockchain, also known as a permissioned blockchain, restricts access and participation

[1]Consensus protocols in blockchain technology can be categorized in two general styles: 1) the longest chain style which is also known as Nakamoto-style and 2) BFT-style. The longest chain protocol is probabilistic and prioritizes liveness over safety. BFT protocols offer strong safety guarantees, even in non-synchronous networks, but may deprioritize liveness compared to the longest chain protocol. In this context, when referring to PoW as a consensus algorithm, we specifically refer to the PoW in the longest chain style.

[2]For PoS, there are both longest-chain style and BFT-style implementations.

to a specific group of participants. It is typically used within organizations or consortia where participants are known and trusted. Private blockchains provide more control and privacy compared to public blockchains.

3) Consortium Blockchain: A consortium blockchain is a hybrid model that combines features of both public and private blockchains. It is operated by a group of organizations or consortium members who jointly govern the network. Consortium blockchains provide a balance between decentralization and control among the participating entities.

4) Hybrid Blockchain: A hybrid blockchain combines elements of public and private blockchains. It allows for both public and private transactions, where some data is publicly accessible and transparent while other data remains private and restricted to authorized participants. Hybrid blockchains provide flexibility in terms of privacy and scalability.

5) Permissioned Blockchain: A permissioned blockchain imposes restrictions on who can become part of the network and participate in the consensus protocol. Participants are required to obtain permission or credentials to access and interact with the blockchain. Permissioned blockchains offer higher scalability and transaction throughput compared to public blockchains.

6) Permissionless Blockchain: A permissionless blockchain, alternatively referred to as an open blockchain, allows anyone to become part of the network and participate in the consensus protocol without requiring permission or credentials. It provides a high degree of decentralization but may have limitations in terms of scalability and transaction speed.

7) Federated Blockchain: A federated blockchain is a form of consortium blockchain where a group of pre-selected entities or organizations are given the authority to validate transactions and maintain the blockchain network. It offers a higher level of scalability and performance compared to fully decentralized blockchains.

8) Blockchain Platforms: Blockchain platforms refer to the underlying infrastructure or software frameworks that enable the development and deployment of blockchain applications. Examples include Ethereum, Hyperledger Fabric, Corda, and EOS.

9) Blockchain Applications: This category includes various use cases and applications constructed atop the blockchain technology, like cryptocurrencies, supply chain management, voting systems, decentralized finance (DeFi), identity management, and more. The taxonomy of blockchains is provided is TABLE II. It should be noted that this taxonomy is not exhaustive, and the classification of blockchain systems can vary depending on different perspectives and criteria. Additionally, with the continuous evolution of blockchain technology, new variations and classifications may emerge [53], [55], [59].

TABLE II
TAXONOMY OF BLOCKCHAINS.

Criteria	Categories	Examples
Based on Access	Public Blockchain	Bitcoin, Ethereum
	Private Blockchain	Hyperledger Fabric, Corda
	Consortium Blockchain	Ripple, Quorum
Based on Permission	Permissionless Blockchain	Bitcoin, Ethereum
	Permissioned Blockchain	Hyperledger Fabric, Corda
Based on Consensus Mechanism	PoW	Bitcoin
	PoS	Cardano, Polkadot
	DPoS	EOS
	PBFT	Hyperledger Fabric
	Other Consensus Mechanisms	Proof-of-Authority (PoA), Proof-of-Elapsed-Time (PoET), etc.
Based on Use Case	Cryptocurrencies	Bitcoin, Litecoin
	Supply Chain	VeChain, IBM Food Trust
	Identity Management	Sovrin, uPort
	Smart Contracts	Ethereum, Cardano
	Decentralized Finance (DeFi)	Uniswap, Compound
	Internet of Things (IoT)	IOTA, Waltonchain
Based on Architecture	Layer-1 Blockchain	Bitcoin, Ethereum
	Layer-2 Blockchain	Lightning Network, Plasma
	Interoperable Blockchain	Polkadot, Cosmos

III. Overview of Quantum Computing

Quantum computing is a rapidly advancing field that aims to efficiently solve complex problems. Traditional computing methods are reaching their limits due to the size of transistors and quantum effects. Alternative computing approaches have limitations, which makes quantum computing essential to investigate. Google's Sycamore quantum device has demonstrated significant computational speedup, achieving quantum supremacy by outperforming classical supercomputers. However, the challenge lies in achieving quantum advantage for more practical applications, as current quantum hardware is still underpowered and faces various issues. The future goal is to develop fault-tolerant quantum devices capable of solving large-scale problems [112].

A. Fundamentals of Quantum Information

In quantum computers, information is manipulated by leveraging the laws of quantum mechanics. In this context, the unit of information is denoted by a quantum bit, often abbreviated as a *qubit*. In a physical sense, a qubit can be any quantum system with two distinguishable states or levels. In mathematical terms, we can correlate the state space of a single qubit with the complex projective line $\mathbb{CP}^1$. Nonetheless, qubit states are often thought of as elements denoted by $|\psi\rangle$, referred to as state vectors, which belong to a two-dimensional complex vector space. This consideration is constrained to those state vectors that adhere to the condition $\| |\psi\rangle \|^2 = 1$ and allows for the interchangeable use of $|\psi\rangle$ and $e^{i\theta}$. Using Dirac's "bra-ket" notation, a state vector is typically represented as a "ket" $|\psi\rangle$. The states $|0\rangle$ and $|1\rangle$, which are equivalent to classical bits 0 and 1, respectively, are instances of two single-qubit kets [112]

There exist alternative models of quantum computation beyond qubits, including qudits for $n > 2$, which are n-level quantum systems [178], and continuous-variable systems with infinite dimensions [179]. These models extend the concept of qubits and provide additional degrees of freedom for quantum information processing.

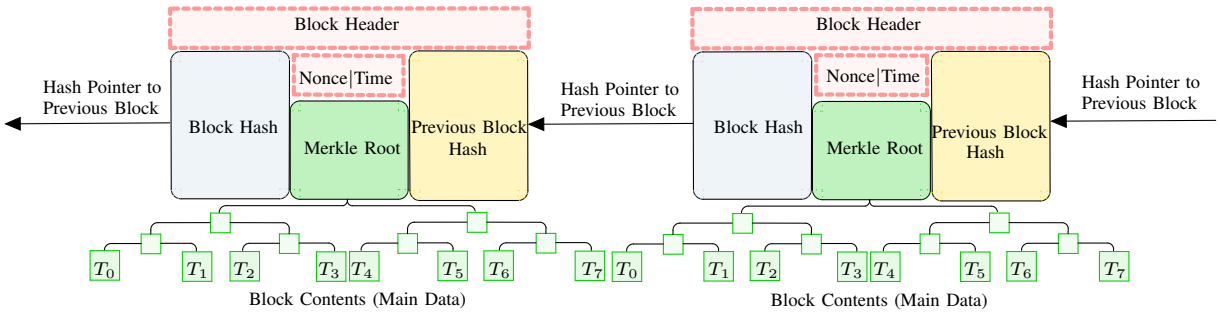

Fig. 1. Depiction of a sequence of interconnected blocks.

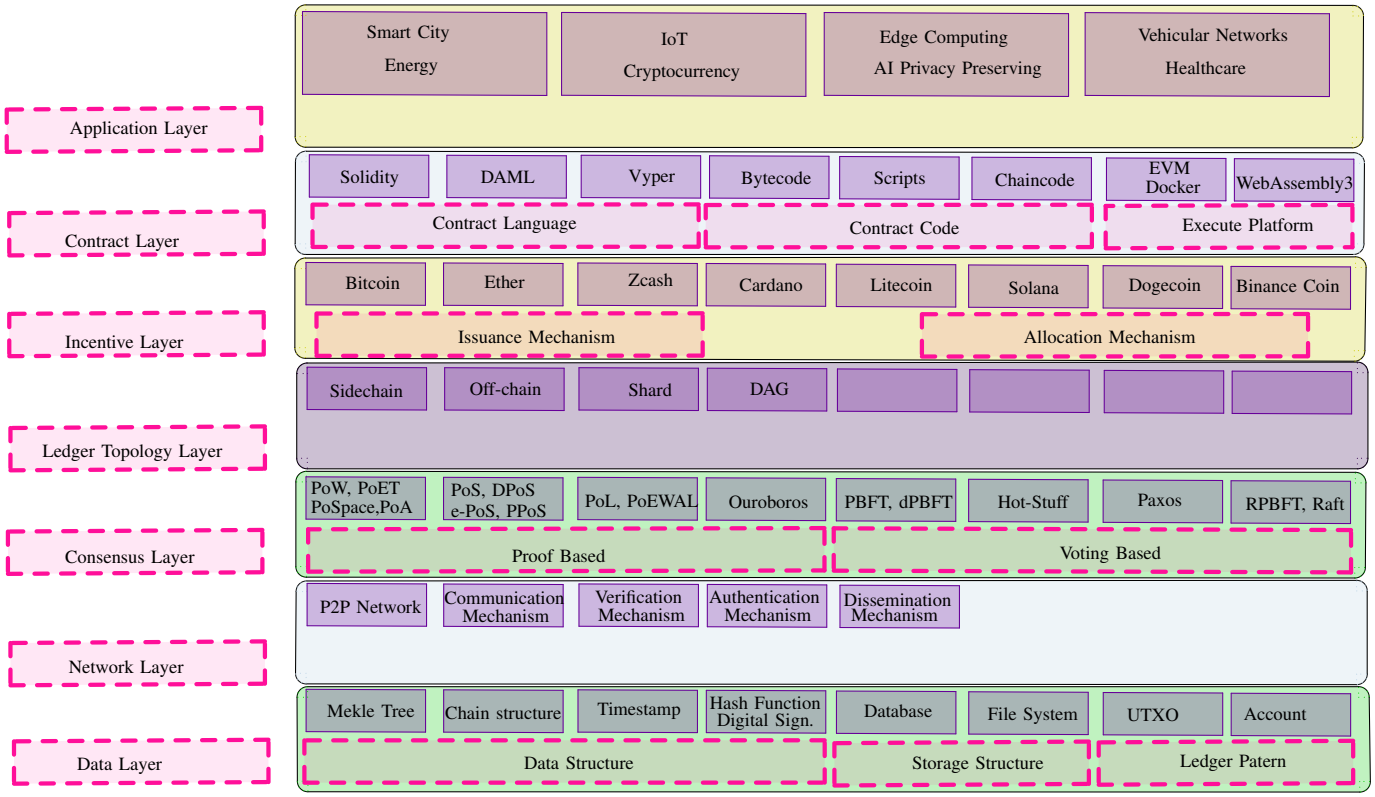

Fig. 2. An overview of the blockchain architecture.

By employing the tensor product of vector spaces, we can construct Multiqubit state spaces [112], which are 2^n-dimensional complex vector spaces for a system composed of n qubits. We indicate the tensor product of two state-vectors $|1\rangle$ and $|2\rangle$ by $|1\rangle \otimes |2\rangle$ or $|1\ 2\rangle$. This idea can naturally be expanded to encompass multiple qubits. Within multiqubit systems, there is a quantum phenomenon referred to as entanglement, wherein the description of the states of the subsystems cannot be provided independently. Mathematically, entangled states are represented as non-simple tensors, indicating that they cannot be factored over the subsystems involved. When certain subsystems can be independently described using a simple tensor, the quantum state is referred to as a product state of those subsystems. Regarding a specific basis, qubits are considered to be in a superposition state when their state-vector is a nontrivial linear combination of basis states. Unlike classical bits, which are limited to being in either the state 0 or 1, a qubit has the potential to exist in any superposition of basis states $|0\rangle$ and $|1\rangle$. The coefficients that define the superposition are referred to as amplitudes, and they are complex numbers.

Within quantum mechanics, measurements encompass the

act of probing a system in order to attain a numerical outcome. Quantum measurements are inherently probabilistic. Performing a projective measurement on a system, based on a Hermitian operator A (referred to as an observable), results in the system's state-vector being projected orthogonally onto the eigenspace determined by an orthogonal projector Π_λ. The resulting measurement outcome corresponds to the associated eigenvalue λ. The probability of obtaining a specific measurement outcome λ is given by the squared magnitude of the inner product between the state vector and the corresponding eigenvector, $\|\Pi_\lambda|\psi\rangle\|^2$. The expectation of the measurement using the operator A, denoted as $\langle A\rangle$, is equal to $\langle\psi|A|\psi\rangle$, where $\langle|$ represents the Hermitian adjoint, often referred to as a "bra".

In the realm of physics, the quantum-Hamiltonian represents the observable associated with the energy of a system. In this context, the ground-state of a quantum-Hamiltonian refers to the state-vector belonging to the eigenspace corresponding to the smallest eigenvalue, representing the system's lowest energy level. Any physical transformation applied to a quantum system can be characterized using a completely positive non-trace-increasing linear operator. Two notable cases within these operations are measurements and unitary operators. However, it's important to note that measurements are not unitary transformations.

B. Measurements

In a quantum system composed of n qubits, the state is represented by 2^n complex values fulfilling a normalization condition. However, the wave function, which encapsulates these parameters, cannot be directly accessed due to the principles of quantum mechanics. Information about the wave function can only be obtained through measurements, which inevitably affect the system's state. Measurements in the quantum circuit model are usually carried out within the computational basis, yielding probabilistic outcomes denoted as i (ranging from 0 to 2^n-1), and leaving the system in the corresponding state $|i\rangle$.

To delve deeper into this concept, let's consider the scenario of a single qubit ($n=1$). The qubit can exist in a general state of $a|0\rangle+b|1\rangle$. Performing a measurement in the computational basis leads to an outcome of 0 with a probability of $|a|^2$ and an outcome of 1 with a probability of $|b|^2$. When the outcome is 0, the state "collapses" to $|0\rangle$, while for an outcome of 1, it collapses to $|1\rangle$. Subsequent measurements will consistently produce the same outcome with a probability of 1 (unless quantum gates are applied to the state) [180].

The normalization requirement applied to coefficients a and b is essential since $|a|^2$ and $|b|^2$ represent the probabilities of the respective measurement outcomes and should sum to 1.

Similarly, for an n-qubit system in the state $|\psi\rangle = \sum_{i=0}^{2^n-1} a_i|i\rangle$, where a_i are complex coefficients, performing measurements on all qubits leads to an outcome i with a probability of $|a_i|^2$, causing the state to collapse to $|i\rangle$.

As an alternative, there's the option to measure a single qubit rather than measuring all qubits within the system. Suppose we measure the j-th qubit. The probability of obtaining 0 is determined by summing the squared magnitudes of coefficients a_i for all integers i in the set A_0, which comprises numbers between 0 and 2^n-1 with a 0 bit in the j-th position. In other words, we accumulate the probabilities of all compatible states where the j-th qubit measures 0. Following the measurement, the state collapses to $\frac{\sum_{i\in A_0} a_i|i\rangle}{\sum_{i\in A_0}|a_i|^2}$, representing a normalized state. Similarly, measuring the j-th qubit yields an outcome of 1 with a probability given by the sum of squared magnitudes of coefficients a_i for all integers i in the set A_1, that is $\frac{\sum_{i\in A_1} a_i|i\rangle}{\sum_{i\in A_1}|a_i|^2}$, where A_1 consists of numbers between 0 and 2^n-1 with a 1 bit in the j-th position [180].

C. Quantum Computing Models

Unlike classical computing, quantum computing explicitly leverages features like entanglement, superposition, and interference. Several models have been suggested to incorporate these traits, including quantum Turing-machines that are functional within superposition [180]. However, implementing such theoretical models in practice is highly challenging and seemingly impractical.

Therefore, in this section, we elaborate on the three types of quantum computing models that better represent the currently available and expected quantum information processing devices in the near to medium term. These types possess equal capabilities, on a par with the quantum Turing machine model, and they constitute the main methodologies for programming quantum computers [180].

1) Gate-Based Quantum Computing: This model is also recognized as the quantum circuit model, employs unitary operators (gates) arranged in a circuit to perform operations on fixed-state qubits. The circuit is a directed acyclic graph representing operations on qubits. Measurements in the computational basis can be performed, and operations conditioned on measurement results are possible. In this model, the circuit depth refers to the longest series of gates that cannot be further parallelized. Quantum gates are invertible, enabling reversible computation [112], [180].

We can employ this model to achieve universal quantum computation. It involves constructing circuits with n qubits using any form of single-qubit gate and a single type of two-qubit gate. Using this approach, any n-qubit unitary operation can be approximated with negligible error.

Two-qubit gates play a crucial role in establishing entanglement. A specific collection of gates capable of achieving universal quantum computation is known as a basis gate set. The quantum device's native gate set is the basis gate set realized by that particular device. It usually comprises a finite number of single-qubit gates as well as a two-qubit entangling operation. We can roughly decompose any single-qubit gate into a combination of the native single-qubit gates [112]. Frequent single-qubit gates consist of Pauli gates, Hadamard gate and Phase gate. In contrast, illustrations of two-qubit gates encompass SWAP gate and controlled-NOT gate. The time complexity of an algorithm is evaluated through the measurement of circuit depth. Majority of quantum computers, including those created by companies such as Google, Honeywell, IBM, IonQ and Rigetti, implemented the quantum circuit model [112], [180]. We can use classical hardware to

simulate gate-based quantum computers, but this approach is not computationally efficient and requires significant memory resources. Tensor network simulators can reduce memory requirements for certain computations. Classical simulation is commonly used for algorithm development, verification, and benchmarking [112], [180].

2) Adiabatic Quantum Computing and Quantum Annealers: Quantum annealing and adiabatic quantum computing (AQC) are alternative approaches to quantum computation, distinct from the traditional quantum circuit model. While the quantum circuit model applies discrete operators (gates) to modify qubit states, AQC relies on the uninterrupted evolution of a quantum state governed by a time-dependent Hamiltonian. In AQC, information is encoded in the initial state of a quantum system, and the system evolves under the influence of the Hamiltonian. The outcome state is subsequently measured to obtain the desired output [112], [180].

A key difference between AQC and the gate-based model lies in the nature of the evolution. In AQC, the Hamiltonian continuously influences the quantum state, whereas in digital quantum computers, the state evolves through discrete actions in sequential steps. Adhering to the adiabaticity condition, if the Hamiltonian changes gradually enough and the system begins in the ground state of the initial Hamiltonian, the system will always stay in a ground state throughout the process. By carefully selecting a final Hamiltonian whose ground state encodes the solution to a specific problem, measuring the final state enables problem solving. The equivalence of this approach to the quantum circuit model has been demonstrated [112], [180].

However, achieving adiabaticity and determining the appropriate rate of change for the Hamiltonian pose practical challenges. To address these difficulties, we introduce the quantum annealing as a heuristic technique which is inspired by adiabatic computing. Quantum annealing follows a similar scheme but does not generally ensure adiabaticity. Commercial quantum computers, such as those developed by D-Wave, are based on the concept of quantum annealing. These devices, known as quantum annealers, employ specific algorithms for solving combinatorial optimization problems. It is important to note that while quantum annealing is a practical implementation, it does not provide universal quantum computation capability [112], [180].

3) Measurement-Based Quantum Computing: Measurement-based quantum computing is a computation approach that involves initiating from an extensively entangled initial state and applying adaptive measurements on it. When the initial state is universal, like cluster states, this model enables the execution of various computations achievable in both the gate-based quantum computing model and AQC [180], [181]. Within measurement-based model, the simulation of any quantum circuit is straightforward [180], [181]. Indeed, preparing the initial highly-entangled state can be achieved through the utilization of two-qubit entangling gates and single-qubit gates. The measurements that are subsequently conducted can be implemented using only single-qubit gates and measurements in terms of the computational basis. Experimental progress has been made in creating cluster states and other resource states, showing promise for practical implementation of measurement-based quantum computation as an alternative to traditional circuit-based approaches [181].

D. Quantum Gates and Quantum Circuits

Within this section, the various forms of operations that can be applied to qubits to alter their states and perform practical computations, will be introduced. Broadly speaking, quantum system transformations correspond to solutions of the Schrödinger equation. When it comes to programming quantum computers, it is essential to understand whether the evolution of a quantum system adheres to the principles of quantum mechanics, which are defined by unitary transformations. These transformations are linear operations preserving the normalization condition of the state.

In gate-based quantum computing model, we perform operations on a finite set of qubits through discrete steps. We refer these operations as quantum gates which are denoted by square matrices of size $2^n \times 2^n$. For preserving the normalization constraints, these matrices are required to be unitary. This implies that their inverse is identical to their conjugate transpose. As a formal definition, a complex square matrix U fulfilling the condition $UU^\dagger = U^\dagger U = I$ is called a unitary matrix, where $U^\dagger$ is the conjugate transpose of U and I is the identity matrix. In gate-based quantum computing model, the quantum gates are matrices of this type. We can consider these matrices as transformations between two orthonormal bases [180]. In TABLE III the major quantum gates are provided. A quantum circuit is comprised of several parallel lines or wires representing the number of qubits in that circuit. At the beginning, the state of all qubits is $|0\rangle$ which results the whole system state to be the product state $|0\rangle \otimes |0\rangle \ldots \otimes |0\rangle$.

TABLE III
MOST IMPORTANT QUANTUM GATES.

Gate Name	Symbol	Matrix Representation
One-Qubit Gates		
Pauli-X gate	X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y gate	Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z gate	Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Hadamard gate	H	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Phase gate	S	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\pi/8$ gate	T	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
Two-Qubit Gates		
CNOT gate	CNOT	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
Controlled-Z gate	CZ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$
SWAP gate	SWAP	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Subsequently, the quantum gates will be applied in sequence to one or some of the wires and the final result will be obtained via the measurements of some of the qubits. When working with quantum circuits, there are several important considerations to keep in mind, as they can differ significantly from classical algorithms [180]:

- **Probabilistic behavior**: Quantum circuits are not deterministic, and results are obtained with certain probabilities. Quantum algorithms often involve multiple executions of circuits with statistical manipulation of the measurements.
- **Reversibility**: Quantum gates are reversible, except for measurements. We can simulate the classical circuits, which are constructed using irreversible gates, using Toffoli and X gates with ancillary qubits.
- **Hardness of classical simulation**: Simulating quantum circuits efficiently is challenging for classical computers due to the exponential size of the state vector. No known classical method can simulate general quantum circuits efficiently.
- **Impossibility of copying quantum information**: Quantum states cannot be independently copied. The no-cloning theorem states that there is no quantum gate that takes an arbitrary quantum state as input and outputs multiple copies of that state.

E. Some Well-known Quantum Algorithms

In this section, we will present a concise overview and description of several renowned quantum algorithms.

Deutsch-Jozsa's Algorithm: Deutsch-Jozsa's algorithm is a quantum algorithm designed to solve the Deutsch-Jozsa problem, which is a black-box problem that determines whether a given function $f : \{0,1\}^n \rightarrow \{0,1\}$ is constant or balanced [182]. The algorithm uses a quantum oracle U_f to perform the computation. It starts with $n+1$ qubits in the state $|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$, where $|0\rangle^{\otimes n}$ represents the n-qubit computational basis state. Then, the algorithm applies the Hadamard gate to all n input qubits, resulting in the superposition state $|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |1\rangle$. Next, the quantum oracle U_f is applied, yielding $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes |1\rangle$. Finally, another Hadamard gate is applied to the input qubits, and the final measurement is performed. If the measurement yields the all-zero result, the function $f(x)$ is constant; otherwise, it is balanced.

Shor's Algorithm: Shor's algorithm is a quantum algorithm for integer factorization [183]. It solves the problem of finding the prime factors of a large composite number N in polynomial time, whereas classical algorithms require exponentially more time. Given an input N, Shor's algorithm can find its prime factors p and q such that $N = p \times q$. The algorithm consists of two main steps: (1) Quantum Fourier Transform (QFT) [184]: It applies the QFT to a set of n qubits in the superposition state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$, where n is chosen appropriately based on the size of N. (2) Period Finding: It uses the QFT output to find the period r of a function $f(x) = a^x \mod N$, where a is a randomly chosen integer coprime to N. The algorithm then uses classical post-processing techniques to determine the factors p and q of N from the obtained period r.

As mentioned, the Shor's algorithm possesses the capacity to factorize large integers and solve the problem of finding the discrete logarithm in polynomial time. Specifically, it can factor an integer N in $O(\log^2 N \log\log N \log\log\log N)$ time (or more succinctly, $O(\log^3 N)$), requiring $O(\log N)$ space. Alternatively, when considering the input size $n = \log N$ in bits, Shor's algorithm runs in $O(n^2 \log n \log\log n)$ time (or more succinctly, $O(n^3)$), using $O(n)$ space [185].

This holds particular significance as a large portion of currently used public-key cryptosystems, such as ElGamal, RSA, Diffie-Hellman and elliptic curve cryptosystems depend on the computational complexity of either factoring large integers or solving the discrete logarithm problem. To grasp the extent of this concern, let's consider the case of RSA 2048 as an illustration. Through a straightforward calculation, it becomes evident that a classical computer equipped with a 5GHz CPU would require approximately 13.7 billion years to decipher an RSA 2048 cipher utilizing the most advanced current methods. In contrast, a quantum computer that performs operations at a rate of 10MHz would have the capability to accomplish this task in approximately 42 minutes [185]. However, to achieve this, a quantum device needs to have sufficient quantum memory capacity to represent both the input and output of the problem. It is estimated that a sufficiently large quantum computer capable of breaking RSA-2048 could potentially be developed by around the year 2035 [185].

Grover's Algorithm: The algorithm of Grover is a quantum search algorithm capable of effectively locating a particular item within an unordered database. [186]. Given a function $f : \{0,1\}^n \rightarrow \{0,1\}$ that maps $N = 2^n$ elements to a binary output, Grover's algorithm can find the input x such that $f(x) = 1$ with high probability. It starts with n qubits initialized to the superposition state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$. The algorithm then iteratively applies the following steps: (1) Apply the quantum oracle U_f that marks the states satisfying $f(x) = 1$ by applying a phase flip to them. (2) Apply the Grover diffusion operator D that amplifies the amplitude of the target state and suppresses the others. These steps are repeated approximately $\frac{\pi}{4}\sqrt{N}$ times, after which a measurement is performed, yielding the solution x with high probability.

Grover's algorithm enable finding a solution within any search space of size N in $O(\sqrt{N})$ time. In essence, this means that any NP-Complete problem is solvable with a quadratic speedup compared to any known classical algorithm. Although the speed-up is not as remarkable as in the previous case, the significance of these algorithms lies in their broad applicability. Specifically, we can gain a quadratic quantum speed-up for any problem for which the solution is efficiently verifiable, encompassing all problems within NP. Amplitude amplification algorithms, which are generalizations of Grovers search algorithm [187], hold particular relevance in this context since numerous consensus algorithms used in blockchain technologies depend on solving NP-Complete problems [185].

F. Challenges in Quantum Hardware

In the present era of quantum hardware, we are in the stage of noisy intermediate-scale quantum (NISQ) technology [188]. This signifies that the current quantum devices are relatively underpowered and encounter various challenges. On the other hand, the fault-tolerant era refers to a future period, yet to be realized, in which we can expect the existence of large-scale quantum devices that are resilient against errors. The existing quantum computers or NISQ devices, come in various physical implementations for qubit-based quantum computation. Major players in the industry, such as IBM, Google, D-Wave, and Rigetti, have manufactured superconducting-based quantum computers, while companies like IonQ, Quantinuum, and AQT have developed trapped atomic ion systems. These technologies have gained prominence in research due to their wide availability. However, several other promising technologies, including photonic systems, neutral-atoms, spins in silicon, molecular qubits, quantum dots and topological quantum systems, are being actively developed. It is important to note that most of these quantum devices follow the quantum circuit model, except for the D-Wave quantum annealers. While there is ongoing research and engineering to enhance these devices, they face significant technical challenges. These challenges impact the progress of quantum algorithms, which can be categorized into algorithms intended for near-term NISQ devices, and algorithms that require advanced hardware with a large number of high-fidelity quantum gates. It is worth mentioning that, at present, none of the aforementioned algorithms that are implemented on NISQ devices offer a definitive superiority compared to classical algorithms [112].

1) Noise: Qubits in quantum devices experience decoherence, leading to the loss of their quantum state over time. One of the crucial properties of a quantum device is the decoherence time of qubits. Different mechanisms contribute to qubit decoherence, including quantum noise depolarizing, the relaxation processes of quantum amplitude and phase, and external factors like cosmic rays for superconducting systems. While we have a good understanding about single-qubit decoherence, multiqubit decoherence, known as crosstalk, poses more significant challenges. For example, two-qubit operations have higher error rates compared to single-qubit operations, making it challenging to entangle multiple qubits without errors.

To mitigate the effect of errors in near-term quantum applications, several techniques have been proposed. However, in the long term, it will be necessary to develop quantum error-correction utilizing logical operations. Quantum error correction requires a significantly larger number of physical qubits than currently available in NISQ systems, and it is crucial for native operations to exhibit low error rates. As a result, algorithms executed on current hardware need to handle noise and are usually confined to circuits with limited depth. Presently, quantum error correction techniques primarily target local errors, and their effectiveness in dealing with non-local errors is an ongoing research area [112]. As a result, the noise is needed to be handled by algorithms implemented on current hardware which are basically low-depth circuits. Presently, quantum error-correction techniques primarily focus on mitigating local errors, and the adaptability of these techniques to address non-local errors is an area of ongoing exploration [112].

2) Connectivity: For optimal performance, quantum circuits must be efficiently mapped onto the topology of quantum devices to reduce the runtime and errors. Available quantum hardware has limitations on qubit connectivity, with fixed topologies in superconducting and trapped-ion processors. Trapped-ion devices can rearrange ion ordering to enable non-neighboring qubits to interact, while superconducting processors rely on additional SWAP gates for remote qubit operations. Connectivity issues also affect quantum annealers.

3) Gate Speed: Fast quantum gates are crucial for achieving quantum advantage with NISQ devices. However, certain quantum devices, like trapped-ion processors, can be slower compared to superconducting devices, despite potentially lower gate error rates. Balancing gate speed, fidelity, and space is essential, as reducing gate time below a certain duration can increase error rates.

4) Native Gates: The availability of a diverse set of native quantum gates is important for designing efficient and high-fidelity quantum circuits. Native gates are the physical operations that can be executed directly on a specific quantum device. The development of advanced quantum compilers plays a critical role in efficiently translating general quantum gates into the native gates of a specific quantum device.

In Table IV, we present the timeline of significant advancements and the evolution of quantum computing spanning over a century.

IV. Application of Blockchain in Cybersecurity

The world is currently witnessing rapid growth in cyberspace, which brings both opportunities and risks. The increasing accessibility of information has created a need to protect systems and technologies from malicious activities. Cybersecurity is essential for maintaining the integrity, confidentiality, and availability of computing assets within organizations and across networks. Due to the evolving nature of cyber threats, researchers emphasize the importance of educating cybersecurity concepts. Negligence in cybersecurity and lack of awareness among clients contribute to cybercrimes. Recent research highlights the introduction of threat intelligence frameworks in the US, which involve gathering information from various sources and analyzing threats using machine learning techniques. The UK has also implemented its own National Cyber Security Strategy 2016-2021, allocating a significant budget for cybersecurity programs. Numerous nations have addressed cybersecurity through national strategies and legal acts. Preplanning vulnerabilities, timely information exchange, and understanding situational incidents are crucial aspects of cybersecurity [189]. Cybersecurity encompasses a comprehensive range of measures aimed at preventing cyber attacks, data breaches, and managing risks [190], [191]. The security architecture defines characteristics of security, including active and passive attacks, and security objectives. Various threats exist in cyberspace, such as cyberbullying, identity, theft, autonomous systems vulnerabilities, and cyber terrorism.

TABLE IV
A COMPREHENSIVE QUANTUM COMPUTING EVOLUTION TIMELINE.

The Theoretical Foundations of Quantum Computing (1900–1980)	
1905	Albert Einstein explains the photoelectric effect, suggesting that light consists of individual quantum particles or photons.
1924	Max Born introduces the term "quantum mechanics" in a paper.
1925	Werner Heisenberg, Max Born, and Pascual Jordan develop matrix mechanics, providing a mathematically consistent formulation of quantum mechanics.
1925–1927	Niels Bohr and Werner Heisenberg formulated the Copenhagen interpretation, which is among the earliest explanations of quantum mechanics and continues to be extensively taught.
1930	Paul Dirac publishes "The Principles of Quantum Mechanics," a seminal textbook in the field.
1935	Albert Einstein, Boris Podolsky, and Nathan Rosen publish the EPR paper [192], highlighting the counterintuitive nature of quantum superpositions and questioning the completeness of quantum mechanics.
1935	Erwin Schrdinger introduces Schrdinger's cat thought experiment and the term "quantum entanglement" during discussions with Albert Einstein.
1947	In correspondence with Max Born, Albert Einstein refers to quantum entanglement as "spooky action at a distance".
The Emergence of Quantum Computing (1980–1994)	
1976	Roman Ingarden proposes one of the first attempts at creating a quantum information theory.
1980	Paul Benioff introduces the concept of a quantum Turing machine or a classical computer operating under quantum mechanical principles.
1981	Richard Feynman delivers a keynote speech titled "Simulating Physics with Computers," emphasizing the potential of quantum computers to simulate physical phenomena beyond the capabilities of classical computers.
1985	David Deutsch formulates a description for a quantum Turing machine, contributing to the theoretical framework of quantum computing.
The Development of Quantum Algorithms (1994–2000)	
1992	The Deutsch-Jozsa algorithm is proposed, demonstrating an exponential speedup of quantum algorithms over classical algorithms.
1993	The first paper describing the idea of quantum teleportation is published, introducing the concept of transmitting quantum information between qubits.
1994	Peter Shor develops a groundbreaking quantum algorithm for factoring integers, which has implications for breaking RSA encryption.
1994	The inaugural conference on quantum computing sponsored by the United States government is arranged by the National Institute of Standards and Technology (NIST), bringing together researchers and fostering collaboration in the field.
1996	The quantum database search algorithm (QSA) has been invented by Lov Grover, showing another example of quantum algorithms outperforming classical ones.
1996	Using Grover's algorithm, an algorithm called BBHT-QSA has been introduced by Boyer, Brassard, Høyer and Tapp to tackle search problems, where the sought value is the only known. This algorithm operates with a complexity of $O(\sqrt{N})$.
1996	The extended version of BBHT-QSA called DH-QSA, has been proposed by Durr and Høyer, to tackle the optimization problems, where a particular value is only assumed to be known. This algorithm operates with a complexity of $O(\sqrt{N})$.
1998	The first demonstration of quantum error correction is achieved, a crucial step towards building fault-tolerant quantum computers. Additionally, it is proven that certain classes of quantum computations can be efficiently emulated using classical computers.
1998	The quantum phase estimation algorithm (QPEA) as an extension of Shor's algorithm has been proposed by Cleve, Ekert, Macchiavello and Mosca to estimate the phase of a specific quantum eigenstate.
1998	The quantum counting algorithm (QCA) has been introduced by Brassard, Høyer and Tapp to count the quantum eigenstates exhibiting a particular characteristic. The QCA can be employed to ascertain the frequency of occurrence of a search value within a database, without revealing their respective positions in the database.
1998	The quantum phase algorithm (QPA) has been proposed by Abrams and Lloyd for evaluating both the eigenvectors and eigenvalues of a local Hamilotonian in polynomial time.
1999	Yasunobu Nakamura and Jaw-Shen Tsai demonstrate the use of a superconducting circuit as a qubit, advancing the experimental realization of quantum computing.
2000	The quantum amplitude estimation (QAE) algorithm has been proposed by Brassard, Høyer, Mosca and Tapp, utilizing the QPE and the QCA algorithms, to estimate the amplitude of a particular quantum eigenstate.
2000	A quantum heuristic algorithm has been proposed by Hogg for optimization, based on tunable and problem-specific quantum gates building the QSA circuit of Grover algorithm.
The Race to Build Quantum Computers (2000–present)	
2002	The first version of the Quantum Computation Roadmap is published, outlining the key challenges and milestones in quantum computing research and development.
2004	Jian-Wei Pan's group at the University of Science and Technology in China demonstrates five-photon entanglement, pushing the boundaries of entanglement experiments.
2008	DH-QSA has been amalgamated by Malossini, Blanzieri and Calarco using a classical genetic algorithm to provide enhanced heuristic optimization with the aid of quantum methods.
2009	A quantum algorithm has been proposed by Harrow, Hassidim and Lloyd to solve linear systems of equations that offers an exponential speed-up compared to the most rapid classical algorithms, albeit solely when the objective is to acquire particular features of the solution vector rather than the solution vector itself.
2011	D-Wave Systems becomes the first company to offer a commercially available quantum computer, providing access to quantum computing resources for researchers and organizations.
2011	The quantum mean algorithm (QMA) has been proposed by Brassard, Dupuis, Gamps and Tapp to calculate the average value of a database.
2012	1QB Information Technologies (1QBit) is founded as the first dedicated quantum computing software company, focusing on developing software tools and applications for quantum computers.
2013	The quantum weighted sum algorithm (QWSA), as an extension of QMA, has been proposed by Botsinis, Ng and Hanzo to calculate the accumulation of values in an unsorted dataset based on their respective weights.
2014	Scientists at the Kavli Institute of Nanoscience achieve the transfer of information between two quantum bits positioned approximately 10 feet apart, resulted a flawless error rate of zero percent, which was a significant milestone in quantum teleportation experiments.
2017	Chinese scientists announce the initial quantum teleportation of distinct single-photon qubits from a terrestrial observatory to a satellite in low Earth orbit, covering a distance of approximately 1400 km, demonstrating the feasibility of long-distance quantum communication.
2018	The National-Quantum-Initiative-Act is enacted in the United States, outlining a ten-year strategy to expedite advancements in quantum information science and the application of quantum technology.
2019	Google asserts that they have achieved quantum supremacy by executing a sequence of tasks in 200 seconds, a feat that would demand approximately 10,000 years for a supercomputer to accomplish. IBM disputes the claim, suggesting alternative classical computing techniques that could potentially reduce the computation time.
2019	IBM builds a 20-qubit quantum computer accessible through the cloud.
2020	Honeywell builds a 64-qubit quantum computer with low quantum error rates.
2021	IBM builds a 127-qubit quantum computer with low error rates.
2022	Google claims to achieve quantum supremacy with a 72-qubit quantum computer.
2023	Microsoft announces a topological qubit design for fault-tolerant quantum computing.

The advancement of science has led to more sophisticated cybercrimes, as exemplified by the Atlanta City government's ransomware attack in 2018 and other recent breaches [189]. In [189], the authors provide an overview of common attacks, historical background of cryptographic standards, advancements in asymmetric algorithms, key management schemes, and the emerging field of quantum cryptography. It also explores the threat of side-channel attacks and the need for quantum-resistant solutions. They have provided an overview of different types of attacks across various domains. The attacks are categorized as follows [189]:

- Cryptographic attack: Breaking cryptography protocols to retrieve plaintext without the encryption key.
- Access attack: Unauthorized access to a host's machine to manipulate information and access private data.
- Reconnaissance attack: Mapping targeted systems to identify vulnerabilities and gather information.
- Active attack: Altering transmitted data to cause damage and disruption.
- Passive attack: Monitoring information transmission without intrusion to collect data.
- Phishing attack: Sending deceptive messages to obtain sensitive information.
- Malware attack: Deliberately installing malicious software to infect computers and gain access to private data.
- Attack on quantum key distribution: Manipulating data transmission in quantum channels.

These attack types represent different strategies used by attackers to compromise systems and obtain unauthorized access to sensitive information. Understanding them is crucial for effective cybersecurity measures.

In [193], the author conducts a comprehensive evaluation of blockchain technology's role in strengthening cybersecurity and protecting privacy. The author compares blockchain with cloud-based solutions, highlighting its potential superiority in terms of security and privacy, particularly within the IoT ecosystem. The author emphasizes the decentralized nature of blockchain, which enhances resistance to manipulation and forgery, and explores how identity and access management systems based on blockchain tackle obstacles in IoT security and analyze its role in tracking insecurity sources in supply chains of IoT devices. The author discusses containing IoT security breaches through blockchain and evaluates relevant initiatives and policies. They propose several policy implications, such as mandating blockchain deployment in critical supply chain systems, promoting training and investment in blockchain for privacy protection, fostering public-private partnerships, and establishing legal clarity for enforceable smart contracts.

In [194] the authors propose a real-time blockchain-based solution to enhance security against cyber-attacks. The solution introduces the concept of Cyber-Soldiers collaborating to update an Artificial Neural Network (ANN) framework on the cloud, offering incentives to enterprises through a monthly subscription. The authors introduce their cryptocurrency, CyberCent, for the network and utilize smart contracts on a conditionally public blockchain for monetary transactions. The paper also includes an experimental analysis of the framework's compression using state-of-the-art techniques.

In [195], the authors explore the application of blockchain in Smart Grid (SG) cybersecurity across three levels: communication and field measurement, power generation and transmission, and power distribution and utilization. The study presents examples such as using blockchain-based smart meters to safeguard the privacy and accuracy of customers' power consumption data. It also highlights the integration of blockchain with optimization approaches to enhance security in network information transmission through smart contracts and Decentralized Application (dApp) services. The research demonstrates the utilization of various blockchains in the energy grid for real-time monitoring and energy bidding. Incorporating blockchain into SG cyber systems supports operations, improves transaction security, and enables secure machine-to-machine transactions, including auctions and payments. Notably, the primary blockchain network in SGs encompasses control and monitoring systems, such as the national energy grid, network operators, meters, and maintenance companies, serving as the higher monitoring system of the SCADA network. This technology enables users to access the main network, monitor and modify smart contracts, and securely exchange information with networks like the local area network.

Blockchain technology has gained popularity in addressing security challenges in vehicular networks, providing decentralization, transparency, tamper-proofing, and public audit capabilities. In [27], the authors examine 75 security schemes based on blockchain for vehicular networks by analyzing applications, security requirements, attacks, blockchain platforms, types, consensus mechanisms, simulation tools, and the role of emerging technologies. They also identify prevalent challenges and outline potential avenues for future research in this domain. In TABLE VI, we present examples of how blockchain techniques are utilized to enhance the security of vehicular networks [27]. Furthermore, in TABLE VII, we outline the security requirements specific to blockchain-based vehicular networks [27]. In [26], the authors review the approaches based on blockchain that address various security services including confidentiality, authentication, access control, resource and data provenance, privacy, and ensuring integrity. These services play a crucial role in distributed applications because of the extensive data processing and the utilization of cloud computing. Centralized controllers currently manage these services, making them vulnerable to attacks. However, blockchain offers a secure and decentralized ledger that can mitigate centralization issues. They provide insights into current security services, highlight state-of-the-art techniques, discuss challenges, and explore how blockchain technology can address these challenges. Additionally, a comprehensive comparison of blockchain-based security approaches is presented in [26].

In [5], the authors explain the structure and operation of blockchain and analyze its use in providing security and privacy in IoT. Additionally, they introduce the "stalker," a variant of selfish mining attack, as a case study. The stalker aims to hinder a node from successfully publishing its blocks

TABLE VI
CATEGORIZATION OF BLOCKCHAIN-BASED SECURITY WORKS ON VEHICULAR NETWORKS [27].

Application Area	Summary	Supporting Blockchain Techniques
Data Trading and Sharing	Blockchain enables the trading and sharing of data in vehicular networks. Data is categorized into messages exchanged, personal data and behavioral information of user, and user ratings.	Local DAGs for storing the shared models for updates, global permissioned blockchain to handle data sharing requests, smart contract (SCs) for ciphertext matching and data searches
Transportation	Blockchain facilitates real-time coordination and management of vehicles for efficient movement. Applications include ride sharing/carpooling, platooning, and smart parking.	SCs guarantee the accuracy of shared models, SCs prevent fraud, SCs realise fairness and matching and advance payment, blockchain stores travel-related information, bloom filters for location anonymity, blockchain stores the records for maintaining the conditional privacy
Smart Grid	Blockchain enhances the fault-tolerance and scalability of smart grids, focusing on secure EV charging and reward mechanisms for energy sharing.	Blockchain with fog computing to reduce latency, SCs decide remuneration, energy exchange occurs in exchange for secure payments using blockchain cryptocurrency, SCs set prices and maximize utility, SCs maximize social welfare, by optimizing revenue generation
Authentication	Blockchain technology provides secure and decentralized authentication for smart vehicles, ensuring tamper-proof vehicle identities, preventing fraud, and enabling trusted interactions among stakeholders in the automotive ecosystem. It offers immutable records, cryptographic authentication, and decentralized consensus for reliable and efficient vehicle authentication.	Blockchain is employed to store certificates in the form of transactions, consortium blockchain is utilized to retain records of vehicle authentication, blockchain keeps transactions related to accident information, SCs are employed to disseminate certificates across the blockchain network
Resource Sharing	Blockchain enables the exchange of computational resources in vehicular networks, utilizing a distributed open market system.	The requester utilizes blockchain currency to compensate vehicles for utilizing their computational resources and spectrum, blockchain technology facilitates the migration of containers to different edge nodes, personally identifiable information encrypted and stored in blockchain, SCs facilitate the interaction between requesters and performers/providers, SCs establish pricing by aligning demand and supply
Crowdsensing/ Crowdsharing	Blockchain optimizes aggregated data collection for crowdsensing applications, improving map and location-based services and incentivizing data contribution.	The selection of vehicle teams and payment methods is carried out through blockchain technology, blockchain based credit management system using a privacy preserving incentive mechanism, Sharing location data over blockchain
Blockchain-based Internet of Vehicles (BIoV) Architecture	Research focuses on optimizing blockchain and IoV technologies, addressing limitations and core features for vehicular networks.	Leveraging blockchain for secure management of network commands in the control plane, large energy consumption in blockchain enabled IoV, blockchain provides secure communication, replacing CAs with a blockchain network for key management

TABLE VII
SUMMARY OF SECURITY REQUIREMENTS IN BLOCKCHAIN-BASED VEHICULAR NETWORKS [27].

Security Requirement	Description
Decentralization	Blockchain removes the necessity for intermediaries, preserving privacy and facilitating identity management, data sharing, and decentralized communication.
Tamper resistance	Blockchain's data organization and distributed nature make it difficult to tamper with or modify data, ensuring irreversibility and immutability.
Unforgeability	The decentralized characteristic of blockchain, in conjunction with signed-transactions, stops malicious actors from counterfeiting data or digital signatures.
Traceability	Every block within the blockchain includes the cryptographic hash of the preceding block, enabling traceability and verification of data, helping detect malicious activities in vehicular networks.
Public audit	Blockchain's consensus mechanism allows for public audits, ensuring that blocks created by miners are verified by other nodes, enhancing authentication and publicly auditing transactions in vehicular environments.
Non-repudiation	Ensures senders cannot deny message transmission and facilitates easy identification of vehicle nodes in accidents, achieved through message signing, timestamping, and secure positioning solutions.
Privacy preservation	Protects the private information of participating nodes and drivers against unauthorized disclosure, achieved through anonymity (untraceability) and unlinkability using pseudonyms and cryptographic techniques.
Traceability (conditional privacy)	Links a vehicle's pseudonym with its actual identity, enabling traceability by trusted third parties in case of malicious behavior.
Wallet security	Ensures the security of users' e-wallets, protecting them against malicious attacks through secure wallet services, encrypted digital signatures, and proper key and certificate management.
Scalability	Ensures efficient operation with a large number of participating vehicles, achieved through low computational overhead, dynamic consensus algorithms, and decentralized architectures.
Low latency and high throughput	Refers to minimizing network delays and maximizing the number of transactions added to the blockchain in a limited time, reducing the opportunity for adversaries to execute attacks and ensuring network security.

on the main chain. This paper surveys the state-of-the-art articles on the application of blockchain for IoT security and privacy. Numerous studies have addressed the challenges and countermeasures related to security and privacy in the IoT domain, emphasizing the role of machine learning and blockchain technologies [92].

Blockchain finds another application in cybersecurity through its integration with reputation systems. Reputation systems aim to foster accountability in distributed applications by utilizing user feedback to compute an overall reputation score. However, concerns like fear of retaliation may deter users from providing honest feedback. To address this, privacy-preserving reputation systems allow users to provide feedback privately and without inhibition. The authors in their work [91] propose analysis frameworks used to assess and compare existing privacy-preserving reputation systems. The specific focus of their analysis is on blockchain-based approaches. These blockchain-based systems offer unique features such as trustlessness, transparency, and immutability, which are absent in previous systems. Through their analysis, the authors offer valuable insights and highlight future research directions, including leveraging the full potential of blockchain to develop genuinely trustless systems, enhancing security properties, and addressing commonly overlooked attacks in current systems.

V. Cybersecurity-related Progress in Quantum Computing

Recently, there have been significant advancements in quantum computing, showcasing its remarkable potential for exponential speed gains compared to classical computing systems. However, these advancements also pose a significant threat to current classical security systems. Traditional security systems rely on classical communication channels for secure key exchange, which can be easily compromised by commercial-grade quantum computers. Quantum cryptography, a quantum-based cryptographic system, offers a solution to this issue by providing near-impossible hacking resistance for communication channels. Quantum key distribution research emerged from Stephen Weisner's proposal for quantum money in 1970, building upon the concepts of the Einstein-Podolsky-Rosen experiment [192]. The breakthrough contribution of Bennett and Brassard in 1984 introduced the BB84 protocol [196], demonstrating secret key distribution using photon polarization over a quantum channel. Artur K. Ekert further expanded on BB84 in 1991, employing Bell's states, entanglement, and Clauser Horne-Shimony-Holt inequalities [197]. In 1992, the BBM92 algorithm was proposed as an extension of BB84, serving as a resource for quantum cryptography [198], [199].

In a different research paradigm, Peter Shor revolutionized the field by introducing a pioneering quantum algorithm for factorization in 1994, which surpasses the computational efficiency of any known classical factorization algorithms. Although commercial quantum computers are not yet available, notable progress has been made in this field by companies like D-Wave Systems, IBM, Google, and Honeywell. Once fully functional quantum computers become a reality, current asymmetric cryptographic techniques will become obsolete. NIST has identified code-based, lattice-based, supersingular elliptic curve isogeny-based and multivariate polynomial-based cryptosystems as potential quantum-resistant asymmetric approaches. However, some researchers caution that we cannot guarantee the security of these quantum-safe algorithms against future quantum algorithms [199].

In addition to exploring mathematical approaches in asymmetric cryptography, it is crucial to direct our attention towards leveraging the principles of quantum mechanics for key generation and distribution mechanisms in symmetric cryptography.

Generating highly secure keys in the real world poses significant challenges, as they are typically based on pseudo-random numbers. Such keys can be vulnerable to hacking with a quantum computer, thus lacking strong security. On the other hand, utilizing quantum random number generators (QRNGs) allows for the generation of keys with nearly perfect security, harnessing the intrinsic randomness inherent in quantum mechanics. QRNG approaches can be categorized into device-dependent and device-independent methods. The current commercial QRNG systems predominantly employ device-dependent approaches, which rely on a thorough understanding of the device's operation. These generators achieve high rates of random bit generation, reaching approximately 4 million random bits per second. On the other hand, device-independent approaches, while not requiring specific device information, offer enhanced security compared to device-dependent methods. However, their practical implementation is currently limited due to the complexities involved [199].

Quantum key distribution (QKD) offers a reliable solution for safeguarding against quantum attacks by leveraging the laws of quantum physics like the no-cloning theorem the uncertainty principle of Heisenberg. It guarantees the integrity and confidentiality of sensitive information during transmission. In this context, BB84 [196] and Ekert91 [197] are two influential algorithms. BB84, introduced by Bennett and Brassard in 1984, encodes secret keys using polarized photons, making it challenging for potential eavesdroppers to intercept the information. The protocol exploits the fundamental principle that the polarized state of a single photon cannot be measured without disturbing it, making any interception attempts detectable. Errors are introduced if the eavesdropper manipulates the photon's polarization [196], [199].

Ekert91, proposed by Artur Ekert in 1991, utilizes Bell states emitted from a shared source and transmitted between Alice and Bob. By randomly selecting polarization bases to measure the received photons, the protocol employs Bell's inequalities to verify the presence of eavesdroppers [197], [199].

Another variation, BBM92, simplifies the BB84 protocol by employing polarization-entangled photon pairs and utilizing two non-orthogonal complementary states: horizontal/vertical basis states or diagonal $(+/-)$ basis states. This simplification enhances the efficiency of the protocol while ensuring secure key distribution [198], [199].

These quantum key distribution protocols play a significant role in advancing quantum cryptography, providing enhanced security and data integrity during communication. Some key players operating in the global quantum key distribution mar-

ket are listed in TABLE VIII [200].

TABLE VIII
KEY PLAYERS IN THE GLOBAL QUANTUM KEY DISTRIBUTION MARKET.

Key Players	Key Players
Anhui Qasky Quantum Technology Co. Ltd.	AUREA Technology
Crypta Labs Ltd.	Hewlett-Packard Development Company L.P.
IBM Corporation	ID Quantique
Infineon Technologies AG	ISARA Corporation
MagiQ Technologies, Inc.	Microsoft Corporation
NEC Corporation	Nucrypt LLC
PQ Solutions Limited	QuantumCTek Co Ltd.
QuantumXchange, Inc.	Qubitekk, Inc.
QuintessenceLabs	QuNu Labs Pvt Ltd.
Qutools GmbH	Toshiba Corporation

In another taxonomy, the existing protocols in QKD has been classified into two subcategories: Discrete-Variable-QKD protocols (DV-QKD) and Continuous-Variable-QKD protocols (CV-QKD). In the case of DV-QKD protocols, we encode the quantum state onto polarization of the transferred photon which is detectable by employing a single-photon detector. On the other hand, in CV-QKD protocols, we encode continuous variables onto observable states corresponding to the pulses of light which are detectable by employing homodyne or heterodyne detectors [201]. General subcategories within quantum cryptography are provided in Fig. 3 [201].

QKD is the key motivation for quantum communication. There are three main scenarios for quantum communication: optical fiber-based, terrestrial free-space optical (FSO) channel-based, and satellite-based FSO channel-based communication. Each scenario has its advantages and limitations within the evolving worldwide quantum communication framework. Optical fiber offers the advantage of providing a stable point to point channel, as it is minimally affected by external conditions. Nonetheless, optical fiber encounters challenges related to signal loss and the preservation of polarization, which restrict its operational range to just a few hundred kilometers. It is possible to overcome these constraints by developing quantum repeaters. On the other hand, FSO channels, whether terrestrial or satellite-based, have lower losses and allow for flexible infrastructure establishment. Terrestrial FSO communication faces limitations due to the Earth's curvature, line-of-sight blockages, and atmospheric conditions. Satellite-based FSO communication offers the advantage of communication even without a direct line of sight and potentially longer ranges. It bypasses the terrestrial horizon limit and experiences lower losses at high altitudes. However, atmospheric turbulence-induced loss remains a challenge in satellite-based quantum communication [137].

The deployment of the Micius satellite with quantum capabilities has marked a significant advancement in long-range quantum communication. This development demonstrates that quantum protocols, previously limited to terrestrial experiments, can now be extended to global distances using low-orbit satellites and single-photon discrete-variable quantum states. In [137], the authors survey the next phase of space-based quantum communication, focusing on the continuous-variable regime. The continuous variable regime, which is tightly related to classical wireless communications, holds the promise of improved communication performance and represents a crucial progression for the global quantum Internet and quantum communications.

Optical fiber networks, which are widely deployed in various communication networks, carry a vast amount of information. Integrating QKD with these existing optical networks in place of employing distinct dark fibers is suggested as a cost-effective approach. Nonetheless, this integration presents new research hurdles. [106] provides an exhaustive examination of the cutting-edge in optical networks secured by QKD, which are expected to shape future communication networks. The survey examines the methods and protocols employed in optical networks secured by QKD, focusing on the key establishment procedures. In [106], different techniques suggested in the literature to tackle networking obstacles in optical networks secured by QKD, are described and compared, including: routing, wavelength and time-slot allocation (RWTA), resiliency, QKD for multicast-service, trusted-repeater-node (TRN) placement, and quantum-key-recycling. The survey introduces QKD and its benefits compared to traditional encryption techniques. It describes various quantum attacks on QKD systems and the countermeasures employed to avoid them. Next, the paper delves into the detailed description of the QKD through an optical fiber link utilizing the BB84 protocol. Different architectures of the optical networks secured by QKD are also discussed.

Significant progress has been made in point-to-point QKD protocols, devices, and systems, leading to commercially available QKD systems. However, the limitation of point-to-point links has hindered the widespread adoption of QKD. To address this, researchers have extended QKD to network settings, enabling its application in various scenarios beyond point-to-point connections. These networks consist of interconnected QKD nodes using optical fiber or free space links. This expansion has facilitated the deployment of fiber-based QKD networks like DARPA, SECOQC, Tokyo, SwissQuantum, Beijing-Shanghai, and Cambridge networks. There have also been demonstrations of satellite-based intercontinental QKD networks [136]. The potential of QKD networks extends beyond securing point-to-point connections, offering enhanced security for industrial and governmental networks. These networks have the potential to secure various applications in finance, banking, government, defense, cloud computing, data centers, critical infrastructure, and healthcare. [136] provides an overview of QKD, its network development, implementation, architecture, interfaces, and protocols. It also discusses the physical and network layer solutions, standardization efforts, application scenarios, and future research directions in QKD networks. Design guidelines for QKD networks are also presented.

The implementation and experimentation of QKD protocols in real-life scenarios are often hindered by practical limitations, which make them complex and expensive to utilize. To overcome these challenges and advance the development of new protocols while assessing the feasibility of existing ones, efficient simulation frameworks are necessary. In [201], the authors provide a comprehensive analysis of recent quantum

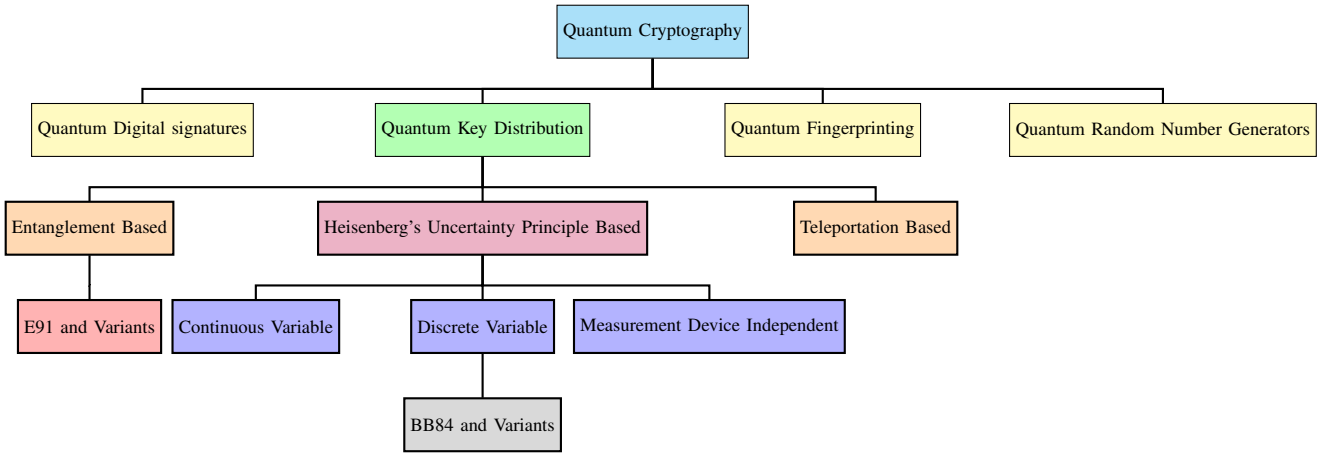

Fig. 3. General categories of quantum cryptography.

cryptographic networks and QKD simulation frameworks. There are different types of simulation frameworks available for QKD, catering to various needs. Some frameworks focus solely on simulating QKD protocols, while others are designed to simulate entire QKD networks along with the protocols. Examples of the former type include: QuCCs, qkdSim, EnQuad, QKD, CV-QKD, SeQUeNCe, QuNetSim, and NetSquid [201].

By examining fundamental studies on quantum cybersecurity, we realize that it can both pose a threat and offer solutions to critical cybersecurity issues. Through a systematic study, in [110], the authors conduct a comprehensive review of the latest advancements in the fields of quantum computing and cybersecurity, and also showcase the suggested methodologies that have been put forward up to this point. The findings highlight that while quantum computing holds the potential to enhance cybersecurity, it also introduces unexpected threats to the field. In TABLE IX, we have provided some recent papers in quantum cybersecurity from [110]. In the remainder of this section, we examine recent examples of utilizing quantum computing in cybersecurity that are not included in [110].

When discussing quantum cryptography, the focus is often on key distribution. However, there are other cryptographic applications to consider, such as bit commitment. The concept of a bit commitment protocol based on quantum mechanics was introduced by Brassard *et al.* [202]. Initially, the protocol was believed to have unconditional security, meaning its security was independent of computational resources. However, it was later proven to be insecure [203]. In a commitment protocol, one party (e.g., Alice) deposits a message that cannot be read or altered by anyone, including Alice herself. At a later point, Alice can reveal her message, and it can be demonstrated with high certainty that the revealed message matches the original deposit. To illustrate this scenario, consider an auction where participants can submit only one bid for a diamond ring. Each bidder writes their bid on a piece of paper, locks it in a personal safe, and gives the safe to the auctioneer, Bob. Only Bob has access to the committed safes, ensuring that bids cannot be seen or changed. After receiving all the safes, Bob compares the bids publicly, and only the highest bidder receives the diamond.

TABLE IX
SOME RESEARCH PAPERS IN QUANTUM CYBERSECURITY [110].

Ref.	Key Contribution
[204]	Cybersecurity applications of quantum-based random number generators
[205]	Presents quantum-resistant blockchain cryptography to counter quantum computing threats
[206]	A scalable and secure key management approach designed for quantum resistance
[207]	Quantum annealing based cybersecurity using restricted Boltzmann machine (RBM)
[208]	Quantum computing-centric cybersecurity addressing quantum-related vulnerabilities.
[209]	Utilizing quantum communication for enhancing cybersecurity in the post-pandemic era
[210]	Architecture for microgrid control utilizing quantum key distribution known as MDI-QKD
[211]	Quantum cryptography for the future internet and security
[212]	Combined quantum-classical deep learning model for use in cybersecurity
[213]	Security protocol for authentication and encryption using quantum-inspired quantum walks (QIQW)
[214]	Post-Quantum cybersecurity challenges associated with the Internet of Things
[215]	Quantum cryptography, quantum-key distribution
[216]	Utilizing RBM for quantum computing
[217]	Developing cybersecurity education curricula with a focus on quantum computation
[218]	Enhancing traffic flow through the utilization of a quantum annealer
[219]	Utilizing quantum computing to implement the Advanced Encryption Standard (AES) algorithm for secure encryption and decryption of cybersecurity files

In classical cryptography, one-way functions are used for commitment, including in public-key cryptography. In quantum cryptography, the goal is to leverage the laws of quantum mechanics to create a fair protocol for both parties. In [134], the authors provide an overview of essential protocols in quantum cryptography. They focus on two specific protocols: quantum key distribution using the BB84 protocol and its security analysis, and the quantum bit commitment protocol along with its proof of insecurity.

In [109], the authors investigate the impact of quantum computing on information security and provide insights into the potential consequences of quantum computers and the

existing measures taken to protect against quantum attacks. By analyzing various information security and privacy safeguards, the study also highlights the significant threat posed by quantum computers to information security.

In [220], a paradigm called "Cybersecurity via Determinism" is proposed for the future IoT, which will have control over critical infrastructure. This paradigm introduces a secure and straightforward sub-layer of "deterministic packet switches" (D-switches) at layer-3. It enables deterministic Software Defined Wide Area Networks (SD-WANs) and incorporates three new tools: Access Control, Rate Control, and Isolation Control, to enhance cybersecurity. The paradigm brings several benefits, including the elimination of congestion and attacks, reduction in buffer sizes, significant reduction in end-to-end IoT delays, support for the US NIST Zero Trust Architecture, implementation of quantum-safe encryption, and substantial cost savings in terms of capital, energy, and operational expenses.

There are lots of studies considering the application of quantum computing in different research areas. [221] considered the examination of the essential need to enhance quantum computing capabilities for homeland security and national defense. In [222], the focus is on exploring the collaboration of autonomous unmanned systems under the influence of cyber-physical attacks. The study takes inspiration from quantum entanglement as a conceptual framework. [223] presents a hybrid IoT (Quantum IoT) security infrastructure that incorporates an additional layer to ensure a quantum state. This quantum state acts as a safeguard against potential threats from eavesdroppers in the communication channel and cyber domain. The state is maintained and the key is protected using the quantum cryptography BB84 protocol. Additionally, an adapted version of the BB84 protocol is introduced specifically designed for the proposed IoT scenario. [224] demonstrated practical implementation of BB84 protocol using IBM QX software. The experimental results obtained differ from the expected theoretical outcomes of the BB84 protocol. To further understand these differences, the paper conducts a statistical analysis by comparing the standard deviation of the results. [225] examines the capabilities of quantum computers compared to classical alternatives in military applications. The paper focuses on four specific use cases of quantum computing in the military context, including recognizing hostile vehicles in drone footage, enhancing radar and sonar data processing, improving course of action determination, and decrypting communication.

There are also several well-established surveys available on quantum computing and algorithms [138], [142], [226]–[229]. In [226], the author provided an extensive explanation of how Grover's algorithm works and how it is utilized as a subroutine in various other quantum algorithms. [227] is focused on quantum walk-based search algorithms, highlighting their potential for solving search problems such as identifying unique entries in a list or determining commutativity among elements of a group. [228] reviewed efficient quantum algorithms that outperform classical counterparts, particularly in algebraic problems. [229] provided a review of various quantum algorithms by delving into their functionality and computational intricacies. Additionally, the website "Quantum Zoo" [230] compiled an exhaustive inventory of quantum algorithms, providing brief descriptions of their operation. [138] presented a compilation of optimization problems within the realm of wireless communications that could be tackled through the utilization of quantum computers. It also reviews quantum algorithms that have been applied previously to solve pre-existing challenges in conventional wireless communication systems. The paper aims to unveil the mysteries of quantum computing by showcasing the quantum circuits utilized within the presented quantum algorithms. The primary emphasis of the study is on algorithmic perspectives, highlighting potential performance gains and achievable complexity reductions. However, practical requirements like scalability, timing, hardware considerations, and integration between classical and quantum components are not addressed in this paper.

According to [142], the essential components of the quantum Internet include the classical Internet, quantum networks, quantum computers, quantum cryptography, and quantum applications. In TABLE X, the topics and challenges related to quantum computing are summarized [142].

The development of quantum Internet necessitates quantum communication through secure quantum channels using quantum cryptographic protocols. Quantum networks leverage the unique characteristics of qubits, like entanglement, superposition, and teleportation, which give them an advantage over traditional networks. However, the transmission of qubits across extended distances remains a challenging task, and ongoing investigation into quantum communication utilizing satellites aims to overcome this obstacle. [139] provides a comprehensive survey of quantum Internet technologies, applications, functionalities, and open challenges, offering readers insights into the necessary infrastructure for the global development of Quantum Internet. The authors of [139] delve into different capabilities of quantum Internet such as quantum channels, quantum memories, quantum repeaters, quantum teleportation, QKD, and terminal nodes.

The advent of quantum Internet holds immense potential for transforming various fields, particularly in strengthening encryption security. However, there is a need to carefully consider the strategic approach for its development. In a study discussed in [231], the authors delve into the strategic options available for a quantum Internet. They address the rise of remote work as a result of the COVID-19 pandemic which has not only impacted everyday activities but has also affected critical sectors like government and corporate businesses. This shift towards remote work has led to increased network usage, posing significant cybersecurity challenges, particularly at the mass scale. However, existing quantum communication technologies primarily focus on high-end applications that require robust encryption and specialized hardware. The intricate engineering involved in maintaining low error rates for qubits, ensuring reliable results, contributes to the high cost of such hardware. This situation presents a dilemma: while cybersecurity concerns are growing for mass applications, quantum technology predominantly caters to high-end requirements. As a result, there arises a question of how to navigate the development of quantum communication to address both

the high-end and mass segments of the Internet. Ultimately, this conundrum revolves around the influence of markets and governments on technological progress, with markets driving technological advancements and governments playing a role in pushing forward [231]. Three approaches can be considered to tackle this conundrum [231]:

1) Accept that quantum communication technology may not be suitable for the mass market.
2) Promote the overall development of the technology and allow it to find its own market niches.
3) Encourage the technology to adapt and cater to the mass market.

These strategic options reflect different perspectives on the role of quantum communication technology and how it should be directed to meet the diverse needs of both high-end and mass users. Among the strategic alternatives discussed, the authors of [231] lean towards the third option. This approach suggests a public-private collaboration to ensure the robustness of quantum communication technology and its broader accessibility. By implementing this approach, the benefits of quantum communication can be extended to individuals who are expected to remain connected even after the COVID-19 pandemic subsides. However, for the widespread adoption of quantum communication in mass cybersecurity, the economic resources primarily need to come from the markets themselves.

This strategic approach is recommended for several reasons. While securing highly sensitive links is important, the growing vulnerability of mass networks poses a national security problem that cannot be overlooked. Neglecting this issue could lead to significant economic losses and widespread information leaks, eroding public trust in accessing reliable information, the government's ability to protect it, and the overall health of democracy, including the integrity of elections [231].

TABLE X
RESEARCH TOPICS, ISSUES, AND POTENTIAL SOLUTIONS FOR QUANTUM COMPUTING.

Research Topics	**Details**	**Research Issues**	**Potential Solutions**
Hardware	Unreliability due to decoherence and noise, big hardware size, high design complexity, incomplete theory, etc.	Quantum computers	UQC or QA
Connectivity	Short distance (relatively), imperfect teleportation, lossy link, limited topology (end-to-end), trusted nodes, etc.	Quantum networks	Universal Quantum Computer (UQC)
Security	Low key rate, vulnerability to Denial of Service, low key efficiency, classical alternatives, etc.	Quantum cryptography	UQC
Data Analysis	Limited data type, low compatibility with classical approaches, no collaboration strategy, etc.	Quantum machine learning	Quantum Annealer (QA)
Pragmatism	High cost, big size, different programming styles, limited resources, etc.	General challenges in all topics	UQC or QA

According to TABLE X, the security of quantum computing and communication is highly related to quantum cryptography. As mentioned earlier, the important topics of quantum cryptography have been addressed in Figure 3. However, there is potential for further expansion in this classification. For instance, [145] provide an overview of the progress made in various branches of quantum cryptography, examining both theoretical advancements and experimental implementations. The reviewed branches include: quantum secure direct communication (QSDC), quantum secret sharing (QSS), quantum private query, quantum key distribution and quantum signature. Additionally, other branches that are currently in the theoretical research phase but have garnered significant attention from the academic community, encompass quantum sealed-bid auction, quantum anonymous voting, quantum dialogue, quantum secure multi-party summation, quantum identity authentication, quantum private comparison, quantum key agreement, and quantum public-key cryptosystem. These branches and their main research hotspots are summarized in TABLE XI.

In [232], the authors discuss the concept of the Quantum Random Oracle (QRO), which is a quantum counterpart to the classical Random Oracle Model used in cryptographic protocol design and security analysis. The QRO is important for post-quantum cryptography and quantum digital signatures. Designing and implementing an appropriate quantum hash function for the QRO is a challenging task. In this study, a QRO model is constructed specifically for quantum public-key encryption to defend against key-collision attacks. Two instantiation examples of the QRO using single-qubit rotation and quantum fingerprinting are provided, and their performances under key-collision attacks are compared. The results of [232] demonstrate the extension of the QRO model to analyze the security of quantum public-key encryption and its resistance to collision-type attacks.

While the cybersecurity community is currently focused on addressing the potential negative impacts of quantum computing, some individuals are raising concerns about a "quantum apocalypse" and the existential risks associated with artificial intelligence. There are two broad approaches to dealing with the quantum threat to conventional computers: 1) safeguarding individual Internet-connected computers against quantum attacks or 2) segregating quantum computing actions from the mainstream Internet [108].

Although the prevailing approach in the field is to protect individual computers using PQC algorithms, [108] proposes a different strategy. Instead of deploying PQC algorithms across the entire Internet, [108] suggests isolating quantum computing, which is evolving as a preferred business model called quantum-as-a-service (QaaS). QaaS providers, including Amazon and IBM, offer subscription-based quantum computing services for specific industry users. Subscribers of QaaS can be required to follow particular security procedures for obtaining access to these services. [108] refers to the concept of "zero-vulnerability computing (ZVC)" and explores whether its encryption-agnostic security protocol can make it quantum-safe. By utilizing ZVC's encryption-agnostic approach, unbreakable end-to-end security can potentially be achieved for accessing QaaS, effectively isolating it from the rest of the Internet. This approach diminishes the risk of legacy comput-

TABLE XI
CLASSIFICATION OF QUANTUM CRYPTOGRAPHY BRANCHES.

Branch	Revelation	Description	Main Research Hotspots
Quantum Key Distribution (QKD)	1984	A technology which enables two entities to jointly possess a shared key sequence for encryption.	QKD networks, measurement-device-independent (MDI) QKD, device-independent (DI) QKD, detector-device-independent (DDI) QKD, Discrete-Variable QKD (DV-QKD), Distributed-Phase Reference (DPR) QKD, Free-space-based QKD, Continuous-Variable QKD (CV-QKD), security proof for QKD, semi-QKD (SQKD), Fiber-based QKD
Quantum Secret Sharing (QSS)	1999	The process of segmenting messages through mathematical algorithms and distributing portions among two or more authorized users.	Circular QSS, semi-QSS, continuous-variable threshold QSS, QSS with verification function, full dynamic QSS
Quantum Secure Direct Communication (QSDC)	2002	Strives to transmit confidential information directly via quantum channels without the need for pre-established keys.	EPR-based, hyperentangled states-based, single photons-based, Bell states-based, W states-based, five-particle cluster states-based, six-qubit maximally entangled states-based, GHZ states-based, non-orthogonal states-based, seven-Qubit entangled states-based, pure entangled states-based, χ-type entangled states, cluster states-based, MDI-QSDC, DI-QSDC, semi-QSDC, DDI-QSDC
Quantum Signature (QS)	2002	A prevalent cryptographic technique employed to authenticate and ensure the integrity of messages.	Arbitrated quantum signature (AQS), blind quantum signature (BQS), quantum homomorphic signature (QHS), quantum digital signature (QDS), quantum proxy signature (QPS), quantum group signature (QGS)
Quantum Private Query (QPQ)	2008	A quantum scheme for symmetric-private-information-retrieval (SPIR).	QKD-based, multi-bit protocol, B92-based, DI QPQ, MDI QPQ
Quantum Private Comparison (QPC)	2009	Several participants, each one has the secret data, want to determine if their data matches while protecting the privacy of the data.	QPC protocol utilizing decoy photons and EPR pairs entangled with two photons, entangled GHZ states-based, χ-type states-based, cluster states-based, W states-based
Quantum Anonymous Voting (QAV)	2007	Allows participants to vote "yes" or "no" on some questions or cast votes for certain candidates, ensuring anonymity.	Entangled states have been used to guarantee the anonymity of the votes
Quantum Secure Multi-Party Summation (QSMS)	2007	Allows parties to compute a summation function on private data of parties.	Based on non-orthogonal states and various quantum states
Quantum Sealed-Bid Auction (QSBA)	2009	Includes a number of bidders, where the highest bidder wins the bidding.	QSDC based on GHZ states, protocols using single photons and Bell states, protocol based on four -particle cluster states, multi-particle superdense coding-based
Quantum Public Key Cryptosystem (QPKC)	2000	The expansion of the PKC concept in the quantum Turing machine (QTM) model.	Modeling all parties as quantum polynomial time Turing-machines, quantum entanglement-based, quantum asymmetric encryptions with symmetric-keys, non-orthogonal states-based, quantum walk-based, NP-complete problems-based, Bell states-based
Quantum Key Agreement (QKA)	2004	Allows distrustful parties to reach consensus on a key sequence via shared quantum channels.	Working on the number of parties involved (2 to n) and security of protocols
Quantum Dialogue (QD)	2004	This corresponds to the bidirectional quantum communication simultaneously conducted by both parties.	Single photons-based, Bell states-based, GHZ states-based, W states-based, four-qubit cluster states-based
Quantum Identity Authentication (QIA)	1995	Verifying the authenticity of the sender to safeguard the message from counterfeiting and denial.	Hybrid quantum authentication protocol, quantum information authentication protocols, protocol requiring a trusted authority, protocol without entanglement, multiparty simultaneous protocols, quantum deniable authentication protocols, protocols based on ping-pong technique, protocols based on entanglement swapping

ers encountering quantum algorithms capable of decrypting data, making recent PQC algorithms' failures less significant. These instances encompass a recent revelation that a post-quantum encryption algorithm (Rainbow), which had been validated and endorsed by NIST, could be readily breached using a conventional laptop. Furthermore, researchers at KU Leuven succeeded in breaking another encryption algorithm (SIKE) using a regular Intel Xeon CPU. SIKE was developed by a consortium including Infosec Global, Amazon, Texas Instruments, Microsoft Research, and several international universities.

As per a report by McKinsey Digital [233], and as depicted in Fig. 4, sectors need to ready themselves for post-quantum cryptography based on the longevity of data and the lifespan of systems. Data with extended shelf lives, such as corporate trade secrets, personal health records, or classified government documents, will remain valuable even after the advent of quantum computers. If such data, transferred over public networks today, remain relevant for a long time, they may face the threat of being intercepted and decrypted by future quantum computers. For instance, life insurance plans with extended terms or 30-year home mortgage loan agreements could potentially be susceptible to quantum-related risks as they will still be in effect when quantum computers become commercially accessible [108]. However, the ease with which PQC algorithms were cracked raises concerns about the outlook for cybersecurity in light of advancements in quantum computing [108]. In summary, due to the limited market share of PQC (currently about 2%), unproven protection from quantum and conventional threats and requiring more computing power and having higher latency, most organizations should wait for PQC technology to mature.

VI. Quantum Security of Blockchain's Building Blocks

Shor's algorithm, proposed in 1992, offers an exponential speedup compared to classical computers in the factorization of prime numbers and solving the discrete logarithm problem. By leveraging Shor's algorithm, an attacker equipped with a quantum computer could compute the private-key using information from a publicly available transaction's public-key. This compromises asymmetric cryptography and the blockchain's digital signature. The attacker could then publish new transactions using the victim's private-key, potentially leading to unauthorized access and fraudulent activities [234]. In the context of cryptocurrencies, Stewart *et al.* (2018) investigated the concept of transaction-hijacking enabled by Shor's algorithm [235]. The attacker could utilize the computed private-key to broadcast conflicting transactions prior to the original transaction is finalized in a block. By offering a higher fee, the attacker aims to increase the chances of miners including their transaction instead of the original one, thereby spending the same currency as the victim [234].

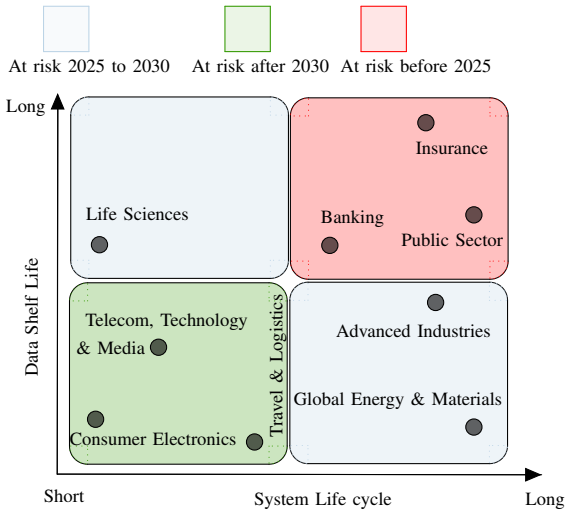

Fig. 4. The possibility of industries facing attacks utilizing quantum technology. (Source: McKinsey Digital)

Grover's algorithm, introduced in 1996, is mainly a threat to hash functions employed in symmetric cryptography. It enables a quantum computer to search unstructured data for the desired input value of a function, providing a quadratic speedup in computing a hash function inverse. This implies that a hash function with a length of k bits can be broken in just $2^{(k/2)}$ iterations using Grover's algorithm. As a result, the security level of hash functions is reduced by half in a post-quantum setting [234].

The implications of Grover's algorithm for blockchain security are twofold. Firstly, it allows for the search of hash collisions, making it possible to replace blocks without compromising the integrity of the blockchain. If an attacker can find a collision, where modified content combined with other block data results in the same hash as before, they have the ability to modify transactions within the block without causing disturbance to the entire chain. Secondly, the acceleration provided by Grover's algorithm empowers a quantum-equipped miner to substantially outpace the block mining process compared to a classical computer. In a scenario where a single entity possesses over 51% of the network's computational capacity. known as a 51%-attack, an attacker could monopolize the creation of new blocks. This grants them the power to decide which data gets added to the blockchain, potentially allowing them to hinder the recording of their own expenditure transactions [234].

Moreover, the attacker could "rewrite history" through the creation of a covert chain composed of chosen or altered blocks. Once this secret chain surpasses the length of the current main chain, the attacker can broadcast it to the network. As they dominate the larger portion of computational capacity, the forged chain would eventually be accepted as the new truth, replacing the original chain [234]. These vulnerabilities highlighted by Shor's and Grover's algorithms underscore the importance of developing and implementing quantum-resistant cryptographic solutions to ensure the long-term security of blockchain systems. In the rest of this section, we address the quantum threat posed to various components of blockchains.

A. Surveying Blockchain Signatures and Analyzing Their Vulnerability to Quantum Threats

Cryptographic algorithms play an essential role in guaranteeing the security, privacy, and performance of blockchain systems. Digital signatures are particularly important cryptographic primitives in blockchains. Bitcoin, for instance, utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA) to manage the ownership of coins, allowing assets to be spent only by their legitimate owners. ECDSA depends on the challenge of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Pollard's subexponential algorithm is currently the most efficient technique currently recognized for solving ECDLP but is impractical for attacks. However, Shor's algorithm can solve ECDLP in polynomial time and it can potentially expose the private-key using the public-key [236]. The following relationship can be used for estimating the time needed to solve the ECDLP via a quantum computer based on the time overhead c_τ, the error rate ρ_g of gate, and clock rate s [236]:

$$\tau \quad = \quad 1.28 \times 10^{11} \times \frac{c_\tau(\rho_g)}{s}, \tag{1}$$

with the needed qubit count being $n_Q = 2334 \times c_{nq}(\rho_g)$, in which c_{nq} is the overhead of space. For example, a quantum computer with 1.7×10^6 physical gates, a significant gate error, and processing clock frequency of 66.6MHz would take approximately 6.49 days to compromise the ECDSA signature. Furthermore, by employing a clock frequency of 10GHz and an error rate of 10^{-5}, signatures could be cracked within 30 minutes [236].

Based on a market cap snapshot of top 100 cryptocurrencies taken in February 2021, it was observed that 74 coins, including Bitcoin, Ethereum, and 48 ERC20 tokens,

TABLE XII
BLOCKCHAIN PLATFORMS AND WIDELY USED DIGITAL SIGNATURES THAT ARE AFFECTED BY THE QUANTUM THREAT.

Signing Algorithm	Curve / Parameters	Quantm Security	Cryptocurrency
ECDSA	secp256k1	Broken	Ethereum, Bitcoin Cash, Litecoin, Bitcoin SV, Binance Coin, Bitcoin, EOS, Tron, VeChain, Cosmos, Theta Network, Crypto.com Coin, DOGE, DASH, Filecoin, Avalanche, Ethereum Classic, ICON, Blockstack, Terra, DigiByte, Horizen, Qtum, Bitcoin Cash ABC, Energy Web Token, TerraUSD,
	NIST P-256	Broken	NEO, Ontology
EdDSA	curve25519	Broken	Cardano, Stellar, Elrond, Solana, Waves, Algorand, Siacoin
ECDSA, EdDSA	curve25519, secp256k1	Broken	XRP, Near, IOST
ECDSA, EdDSA	secp256k1, curve25519, NIST P-256	Broken	Tezos (tz1: EdDSA, tz2: ECDSA/secp256k1, tz3: ECDSA/NIST P-256)
ECDSA, Schnorr, EdDSA	ristretto25519, secp256k1, curve25519	Broken	Polkadot, Kusama
EdDSA, EC-Schnorr	curve25519, secp256k1	Broken	Decred
EdDSA, Bullet-proofs	curve25519	Broken (Bulletproofs is based on DL)	Monero (non-standard hashing algorithm, uses Keccak)
Winternitz OTS	-	No significant threat by quantum computer	IOTA
ECDSA, ZK-SNARKs	secp256k1, BLS12-381-JubJub	Broken	Zcash (BLS12-381-JubJub for shielded/anonymous transactions)
EC-Schnorr	secp256k1	Broken	Zilliqa
ECDSA, EdDSA, RSA	NIST P-384, curve25519, RSA 3072	Broken	Hedera Hashgraph
RSA	4096	Broken	Arweave

utilize the ECDSA algorithm with the secp256k1 curve. Additionally, 10 coins, such as Stellar, Cardano, and Elrond, employ the EdDSA algorithm with curve25519. There are also 8 coins, including Polkadot and Tezos, that make use of multiple signing algorithms and curves, often incorporating both ECDSA/secp256k1 and EdDSA/curve25519 [237]. Further information on the top cryptocurrencies and their quantum security, particularly regarding the transaction mechanism, is provided in TABLE XII.

A typical signature scheme comprises a public-key for verification and a private-key for signing, where the address of Bitcoin is derived from the verification key. Transactions transferring funds between Bitcoin addresses require signatures from corresponding signing keys [165]. With the evolution of blockchains, signatures possessing distinctive attributes and capabilities, called "exotic signatures", have been employed to address various issues. Prior to the emergence of blockchain, different signature schemes, such as blind signatures, were used in digital cash systems to prevent linkability between payees and transactions. In the blockchain context, additional signature schemes like adaptor signatures, multi-signatures, aggregate signatures, threshold signatures and ring signatures play vital roles, empowering blockchains in areas such as the efficiency of consensus, account management, scriptless blockchain capabilities, and the privacy of users [165].

In terms of managing accounts, Bitcoin employs a non-Turing complete script language that facilitates multi-signature addresses and jointly-owned asset management. However, multi-signature addresses have limitations in terms of scalability, transaction fees, and privacy. Threshold signature schemes have been put forward to improve the management of collectively owned assets by distributing the capability to generate a signature among multiple participants [165]. In terms of consensus efficiency, threshold signatures or aggregated signatures are utilized in blockchain consensus mechanisms to reduce communication complexity and improve scalability. Layer 2 protocols, like payment channels, strive to enhance blockchain throughput by summarizing a significant volume of transactions onto the blockchain. Adaptor signatures have been explored as a means to facilitate layer 2 protocols on blockchains that lack scripting capabilities. Adaptor signatures are a novel type of digital signatures introduced by Poelstra as scriptless scripts [265]. They involve generating a "pre-signature" based on a specific condition and then adapting it to create a complete signature using a witness for that condition. The resulting complete signature appears as a regular signature during verification, making it suitable for blockchain applications. Adaptor signatures offer enhanced functionality and the ability to incorporate conditions surpassing the limitations of the scripting languages of blockchains [165].

To protect blockchain privacy, blind signatures and ring signatures are employed. BlindCoin and CryptoNote are examples of using blind signatures and linkable ring signatures, respectively, to improve privacy in cryptocurrencies. Monero, with its market capitalization of $2.6 billion USD, is a prominent privacy-preserving cryptocurrency [165].

While the importance of cryptographic primitives is widely recognized, the emergence of quantum computing raises concerns about the resilience of existing cryptographic algorithms. Shor's algorithm, for instance, poses a threat to problems like large integer factorization and discrete logarithms. The achievement of "quantum supremacy" by Google and IBM further emphasizes the need for post-quantum secure blockchains [165].

In [165] the authors provided a comprehensive survey specifically focused on post-quantum exotic signatures re-

TABLE XIII
A CONCISE OVERVIEW OF CUTTING-EDGE POST-QUANTUM SIGNATURE SCHEMES [165]. THE SIZE OF AGGREGATE SIGNATURES CORRESPOND TO EACH INDIVIDUAL SIGNER WHEN THERE ARE N SIGNERS INVOLVED. ℓ IS THE LENGTH OF THE UNDERLYING LEARNING PARITY WITH NOISE (LPN) PROBLEM.

Type	Scheme	Post-quantum Type	Broken (Asymptotically or Practically)	Quantum Security (bits)	Signature Size (KB)
Multi- and Aggregate Signatures **Application:** Account Management	[238]	Lattice	No	120	0.49 ($N = 10$)
	[239]	Lattice	No	128	N/A
	MMSAT [240]	Lattice	Yes	128	0.036 ($N = 10^3$)
	MQSAS [241]	Multivariate Quadratic (MQ)	No	120	0.004 ($N = 10$)
Threshold Signatures **Application:** Consensus Efficiency	Falcon MPC [242]	Lattice	No	108	0.67
	De Feo-Meyer [243]	Isogeny	No	60	0.56
	Sashimi [244]	Isogeny	No	60	1.77
	LUOV MPC [242]	MQ	No	231	3.1
Adaptor Signatures **Application:** Scriptless Blockchain	LAS [245]	Lattice	No	128	1.58
	O-IAS [246]	Isogeny	No	60	19.0 (Pre-sig.) 0.956 (Sig.)
Blind Signatures **Application:** Privacy	[247]	Lattice	No	128	7730
	UBSS [248]	Isogeny	Yes	N/A	N/A
	DVBS [249]	Isogeny	Yes	128	≈1.75
	CFS [250]	Code	No	82	3100
	RankSign [250]	Code	No	100	200
	[251]	MQ	Yes	128	28.5
Ring Signature **Application:** Privacy	DualRing-LB [252]	Lattice	No	128	5
	MatRing [253]–[255]	Lattice	No	128	11
	SMILE [256]	Lattice	No	128	16
	Calamari [257]	Isogeny	No	60	7
	[258]	Hash	No	128	178
	[259]	Hash	No	128	2125
	[260]	Code	No	63.3	0.208 ($N = 10$)
	[261]	Code	No	80	0.587 ($N = 10, \ell = 9$)
	[262]	Code	No	128	397 ($N = 10$)
	Ringrainbow [263]	MQ	Yes	128	0.83 ($N = 10$)
	[264]	MQ	No	80	0.324 ($N = 10$)

quired by blockchain systems. Given the diverse range of real-life blockchain applications, only exotic signatures with significant existing blockchain applications are considered and the focus is on practical efficiency rather than theoretical results [165]. Furthermore, since post-quantum ordinary signatures have already been extensively surveyed in other studies like [266], they are not discussed in [165]. In TABLE XIII, the overview of cutting-edge post-quantum exotic signature schemes and their applications are provided.

As addressed earlier, by utilizing Shor's algorithm, an adversary equipped with a sufficiently powerful quantum computer can derive the ECDSA secret key K_s solely from the public-key K_p. This poses a significant security risk to blockchain systems, as the the attacker could successfully forge the identity of any wallet, validate themselves on the blockchain, and potentially initiate the transfer of assets from the breached wallet. Consequently, there is a clear need for a quantum-resistant algorithm as a substitute for ECDSA.

However, the process of directly replacing ECDSA with another compatible digital signature algorithm that is secure against quantum attacks, presents several challenges. The migration process itself is complex and time-consuming, raising concerns about compatibility and potential issues during the transition. Therefore, it is essential to consider these factors alongside the technical aspects of algorithm replacement. In [267], an in-depth analysis of the existing usage of ECDSA in blockchains is provided by examining the impact on applications and users if such a change were to occur. The authors also identified some approaches for the development of a quantum-resistant digital signature algorithm that can mitigate some of the migration-related challenges. In TABLE XIV, the impacts of replacing ECDSA with a post-quantum signature in different use cases are presented [267].

The majority of private-keys produced by wallet applications adhere to the Bitcoin Improvement Proposal 39 or BIP39 [268] procedure. In this process, we consider a sequence of randomly selected words from a wordlist containing 2048 human-readable words. We use these words as a deterministic Seed along with an optional password selected by user for deriving the final ECC secret-key (refer to TABLE XIV). The adoption of BIP39 has led to the emergence of the concept known as paper wallets or cold wallets. This empowers the users of blockchain to retain the Seed as an offline recovery phrase, ensuring physical security by isolating it from the Internet. Notably, employing BIP39 is essential to achieve backward compatibility [267].

While an adversary with quantum capabilities has the potential to analyze the public-key K_p of ECC to extract the secret-key K_s, the security of the BIP39 Seeds or recovery phrases held by current users remains intact due to the quantum-resistant properties of hashing. If we are able to design an alternative post-quantum algorithm that leverages the Seed to accommodate inactive users and preserve the address mapping, it could partially mitigate the impact of migration,

TABLE XIV
THE EFFECTS OF SUBSTITUTING ECDSA IN VARIOUS USE CASES [267]. BTC AND ETH DENOTE BITCOIN AND ETHEREUM CORRESPONDINGLY. K_s AND K_p REPRESENT THE PRIVATE AND PUBLIC-KEYS, RESPECTIVELY.

Scenario	Impacted entity	Consequence	Comments
Key Generation	Active user $\text{ECCKeyGen}() \Rightarrow \begin{cases} K_s = \text{PBKDF2}(\text{Seed} + \text{Pass}) \\ K_p = \text{ECC Pub Key}\,(K_s) \end{cases}$ $\text{Seed} = \text{“}s_1 s_2 \ldots s_n\text{”} : s_i \in \text{ Word-list}$ $\text{Word-list} = \{ \text{ abaciscus, abbreviate,}\ldots, \text{zone } \}$ $\text{Pass} = \text{Non-compulsory user password}$	The user must update their wallet for generating a fresh key.	Minimal impact
	Inactive cold wallet users	Users who fail to stay updated with technological advancements, or those who mistakenly perceive the fraudulent upgrade, might not produce a fresh key within the specified timeframe. Consequently, the nodes of blockchain lack the ability to distinguish such users' wallets and quantum-capable adversaries attempting to impersonate them.	Significant financial losses
Transaction signing	Active user $\text{ECCSign}\,(M, K_s) = \text{Secp}\,256k1\,(\text{Hash}(M), K_s)$ $M = \text{Blockchain transaction}$ $\text{Hash}() = \begin{cases} \text{RIPEMD160}\,(\text{SHA256}\,()) & \#\text{BTC} \\ \text{KECCAK256}() & \#\text{ETH} \end{cases}$	Users need to actively take part in the hard-fork process to transfer their assets.	Minimal impact
	Dormant user	There is a possibility that users may lack awareness of the hard-fork and end up with assets trapped in the outdated, quantum-vulnerable chain.	Significant financial losses
Consensus	Blockchain node	It is necessary to upgrade nodes with the new algorithm.	Minimal impact
	Previously committed blocks	In non Proof-of-work consensus, there may be a requirement to counter-sign some additional blocks using the new algorithm to thwart spoofing.	Minimal impact
Multi-Signature	All active users	For all active users, upgrading the wallet to produce a fresh key will be necessary.	Minimal impact
	Some inactive users	In the case where the count of dormant users who have not performed the upgrade is greater than $N - M$ in an M-of-N setting, transactions will not be granted approval.	Significant disruptions or financial losses
Off-chain signing	Side-chains	Upgrading nodes and wallets within the side-chains is necessary to ensure compatibility with signatures. However, due to the existence of multiple Ethereum-Virtual-Machine (EVM) Layer-2 side-chains, not every chain possesses the necessary community resources required to stay updated with the upgrade. Consequently, certain chains may be removed as a result.	Disruptions likely in Layer-2 chains
	Off-chain assets	To prevent compromise, assets must undergo a counter-signing process using the new algorithm. It should be noted that in certain implementations, it might be challenging to track the source of assets on the blockchain. Consequently, further analysis needs to be conducted individually for each case.	Unable to ascertain the impact comprehensively
Address Computation	User identity $\text{Addr}\,(K_p) = \text{Format}\,(\text{Hash}\,(K_p))$ $\text{Hash}() = \begin{cases} \text{RIPEMD160}\,(\text{SHA256}\,()) & \#\text{BTC} \\ \text{KECCAK256}() & \#\text{ETH} \end{cases}$ $\text{Format}() = \begin{cases} \text{ChecksumEncoding}() & \#\text{ BTC} \\ \text{Truncate20Bytes}() & \#\text{ETH} \end{cases}$	Certain digital identity implementations, like www.proofofhumanity.id, link users' identities to their wallet-addresses. Additionally, numerous users publicly share their wallet-addresses on social media. Consequently, these associations will require modification, which may result in disruptions and inconvenience for users.	Some disruption or inconvenience for users
	Smart Contract $\text{SCAddr(Script)} = \text{Format(Hash(Script))}$ $\text{Script } = \begin{cases} \text{ Bitcoin script} & \#\text{BTC} \\ K_p + \text{nonce} & \#\text{ETH} \end{cases}$ $\text{Hash}() = \begin{cases} \text{RIPEMD160}\,(\text{SHA256}\,()) & \#\text{BTC} \\ \text{KECCAK256}() & \#\text{ETH} \end{cases}$ $\text{Format}() = \begin{cases} \text{ChecksumEncoding}() & \#\text{BTC} \\ \text{Truncate20Bytes}() & \#\text{ETH} \end{cases}$	A considerable number of smart contracts often include fixed addresses to refer to other smart contracts or payment recipients. To avoid execution failures or asset lock-ups, these addresses must be reconstructed (assuming that the source codes are accessible) or updated accordingly.	Significant disruptions or financial losses

assuming the utilization of BIP39 by users for key-generation. In accordance with [267], there are two potential strategies available:

1) Adapting from a post-quantum algorithm standardized by NIST: After concluding its third round of evaluation [269], NIST has determined that CRYSTALS-KYBER will be the standardized public-key encryption and key-establishment algorithm. As for digital signatures, the standardized algorithms will be CRYSTALS-Dilithium, FALCON, and SPHINCS+. Although multiple signature algorithms were chosen, NIST recommends CRYSTALS-Dilithium as the primary algorithm for implementation. Additionally, four alternate key-establishment candidate algorithms, namely BIKE, Classic McEliece, HQC, and SIKE, will proceed to a fourth round of evaluation, with the potential for future standardization. These algorithms are chosen for standardization and are expected to be published by 2024. It is necessary to opt for an algorithm capable of utilizing the Seed for generating a fresh key. The post-quantum hash-based algorithm, SPHINCS+, is anticipated to offer greater flexibility in key generation and improved compatibility with BIP39 in contrast to lattice-based algorithms. A critical area of research would involve developing a secure bidirectional mapping function to establish a connection between the SPHINCS+ public-key and the legacy ECC public-key. This would enable the wallet to validate that both keys originate from the same BIP39 Seed, and blockchain nodes could subsequently reverse the process by mapping the legacy wallet address based on ECDSA to the new wallet address based on SPHINCS+.
2) Using zero knowledge proof for key generation: In the case of employing ECDSA for transaction signing, if the wallet can securely demonstrate that K_s is created from a BIP39 Seed without disclosing the Seed itself, it assures blockchain nodes that the incoming ECDSA signature has not been generated from a K_s obtained through cryptanalysis. This assurance can be established by integrating a post-quantum zero-knowledge proof-of-knowledge into the signature, like MPC-in-the-head [270], as exemplified in [271]. This approach ensures that the legacy ECC key remains in use, rendering address mapping a non-issue.

Major blockchain applications, such as Ethereum 2.0 and Algorand, have planned efforts to incorporate post-quantum cryptographic solutions. As an illustration, the Ethereum 2.0 update is anticipated to include support for quantum-resistant cryptographic solutions, while Algorand has considered state-proofs based on lattice problems, utilizing a post-quantum signature scheme. However, widespread adoption of post-quantum tools in the blockchain setting is not yet prevalent, aside from these notable instances [165].

The process of Blockchain migration necessitates the identification of solutions or algorithms with specific properties. One crucial factor to contemplate is how the size of signatures and public-keys affects the entire blockchain network. As each transaction requires validation from nodes adding their signatures to the block for consensus, larger signature sizes contribute to increased network bandwidth and higher costs associated with the consensus algorithm [236], [272].

Another crucial factor is the computational efficiency of signing and verification algorithms. Transaction validation is a mandatory aspect of the consensus process, and if the signing and verification algorithms are computationally complex, it can result in a slow and impractical network. To ensure scalability, it is essential to employ algorithms that can handle a significant number of transactions per second [236], [273]. Additionally, the chosen signature scheme must guarantee that no private information is exposed through its public parameters, ensuring the confidentiality of sensitive information [236], [273]. Numerous approaches have been proposed to address these requirements. One example is the introduction of a new post-quantum PoW (PQPoW) consensus model that solves a problem based on multivariate quadratic equations, which falls into the category of NP-Hard problems, instead of the traditional SHA256 hash problem [236], [272]. This approach aims to attain compact transaction blocks by utilizing the Rainbow scheme which is an identity-based signature [236], [274]. However, this approach faces challenges such as increased memory requirements and longer computation times as the complexity and number of equations grow.

Other research focuses on the development of efficient signature schemes based on lattice assumptions, aiming to address scalability and security concerns. For instance, the MatRiCT protocol proposed a highly effective ring confidential transaction (RingCt) protocol for blockchain, which utilizes a lattice-based assumption to shorten ring signatures without requiring computationally expensive Gaussian-sampling [236], [275].

The exploration of quantum-secure signatures is also a topic of interest, with proposed schemes transitioning from one-time-signatures to highly effective many-time-signatures. These approaches enable an endless number of signatures while keeping their sizes consistent. However, the repetitive inclusion of the signature with the public-key for authentication can lead to an increase in the public-key size, potentially impacting long-term efficiency [236], [276].

Researchers have also analyzed the suitability of signature schemes that have been selected as finalists of post-quantum cryptography by NIST for blockchain applications. For example, a new hash-based signature method, which merges a one-time-signature with Naor-Yung-chaining, has been introduced to attain more compact signatures and improved performance when contrasted with current hash-based signature techniques [236], [277]. However, this scheme had the drawback of being stateful, as the loss of key-state may result in a financial loss. Therefore, proper backup and security measures are crucial for its implementation.

Furthermore, investigations have been conducted on the security of lattice-based signature schemes, particularly concerning side-channel attacks. The identification of the attacks based on cache memory and discrete Gaussian sampling emphasizes the need for robust security measures in these schemes [236], [273].

Considering the nascent stage of research on both post-quantum hardness and quantum computing capabilities, hybrid primitives combining current cryptographic paradigms with post-quantum algorithms have been proposed to facilitate a smooth migration. Hybrid signatures offer a method of combining signature schemes and provide security definitions such as unforgeability and non-separability [236], [278].

Comparative benchmarking projects, such as PQFabric, have assessed the candidates of NIST in permissioned blockchains like Hyperledger Fabric. The analysis reveals that the size of public-keys and signatures impacts hashing time, which is dependent on signing and verification operations. This highlights the importance of selecting candidates with smaller public-key and signature sizes for improved performance [236], [279]. The work done on this frontier is reviewed in [236], and it is concluded that Crystals-Dilithium is a good candidate for quantum-secure blockchains. The Crystals-Dilithium signature scheme is a lattice-based construction that relies on the Shortest Vector Problem (SVP) for its security, utilizing Fiat-Shamir Transformations. Its suitability for blockchain applications lies in its compact and fast signature design, making it easily implementable with different security levels. The scheme incorporates a zero-knowledge design through Fiat-Shamir Transforms with aborts, ensuring leakage resistance and forgery-proof signatures. Crystals-Dilithium offers low public-key and signature sizes, making it suitable for transmission in blockchain networks. Additionally, by adjusting the parameters, the recommended quantum security level can be achieved while maintaining an acceptable block size for blockchain applications. For example, at the most stringent quantum security level, the size of block stays near 3.0 MB [236].

In the pursuit of developing alternative signatures, [280] provides an analysis of Hash-based digital signature schemes. These schemes are chosen for their reliance on hash functions and their metaheuristic nature. The study provides an analysis of hash-based stateful signatures, including the Winternitz one-time signature scheme (W-OTS), Lamport one-time signature scheme, and the Merkle signature scheme (MSS). A stateful signature scheme involves signing a message by accessing the message and a secret key, resulting in a signature that incorporates the updated secret key. This implies that the signer needs to maintain a state that is altered with each issuance of a signature. These stateful schemes share common features and are designed for a limited number of signatures. The analysis of [280] covers key generation, signature generation, signature verification, and security levels of each scheme. Based on the analysis, MSS is identified as the most suitable candidate for the Bitcoin PoW protocol due to its security and the ability to sign multiple messages [280].

In [281], two hash-based signature schemes, namely W-OTS and MSS, were examined and compared with ECDSA and RSA commonly used in bitcoin transaction security. The comparison focused on evaluating the key generation time, signature generation time, and signature verification time of these schemes. W-OTS demonstrated superior performance with fast times for key generation (0.002s), signature generation (0.001s), and signature verification (0.0002s) compared to ECDSA (0.1378s, 0.0187s, 0.0164s) and MSS (16.290s, 17.474s, 13.494s). Given these findings, W-OTS has been suggested for enhancing the security of bitcoin transactions, primarily because of its efficiency and its capacity to withstand potential quantum computer attacks on the bitcoin network.

In another study, [282] compares ECDSA and post-quantum signature schemes based on key size, signature size, and performance metrics. Results indicate lattice-based schemes Falcon and Dilithium have smaller key sizes but Dilithium has the largest signature size. Among the schemes in the third round of NIST evaluation, Dilithium 3 excels in terms of rapid key generation, whereas Rainbow I leads in fast signature generation and verification. However, Rainbow I's key generation process is lengthy and energy-intensive, raising concerns for blockchain systems. Falcon, based on the SIS problem, shows promising performance comparable to RSA and ECDSA, with shorter key sizes and signature lengths among lattice-based schemes. Considering these factors, Falcon is considered a promising choice for blockchain applications [282]. This study was conducted prior to the discovery of vulnerabilities in the Rainbow scheme.

TABLE XV
SECURITY AND PERFORMANCE REQUIREMENTS FOR BITCOIN [283].

Feature	Necessity	Offered by Bitcoin
Signing Algorithm	128 (bits)	ECDSA with curve secp256k1
Size of private-key	256 (bits)	256 (bits)
Size of public-key	Small	64 (bytes)
Size of signature	Small	64 (bytes)
Size of hash	Small	256 (bits)
Size of address	Small	2536 (bytes)
Size of block	Small	14 (MB)
Time of key-generation	Offline	0.10 (ms)
Time of signing	Fast	0.34 (ms)
Time of verification	Fast	0.25 (ms)

Security and performance requirements for Bitcoin is provided in TABLE XV. Considering this requirements, a separate comparison was conducted to evaluate the application of NIST finalists and alternate candidates of digital signature schemes, such as Dilithium, Falcon, GeMSS128, Picnic2-FS, SPHINCS-s, AQTA, qTESLA-I, XNYSS, NOTS, and Rainbow, in the Bitcoin network [283]. The timings for signing and verifying are provided and normalized concerning the timings of the classical ECC curve P-256, and alternate candidates are found to be unsuitable for Bitcoin due to issues related to the size of public-key and signature, and also timing performance. While Rainbow shows excellent timing performance, it suffers from a large public-key size and a recent attack. Among the analyzed candidates, Falcon and Dilithium-2 exhibited faster verification times than ECC. Given the significance of verification in cryptocurrencies, implementing these algorithms for quantum resistant version of Bitcoin should not pose timing performance issues. However, the increased size of public-keys and signatures of Falcon and Dilithium-2 continue to be a matter of concern [283].

Some cryptocurrencies, such as IOTA, Bitcoin Post-Quantum, and Quantum-Resistant Ledger (QRL), employ hash-based digital signature schemes that can resist quantum attacks, although they are not standardized. However, the

size of the signature remains a critical concern for their adoption [283]. Other blockchain platforms are also taking steps towards quantum resistance. For instance, Ethereum 3.0 intends to incorporate quantum-resistant components like zero-knowledge scalable transparent arguments of knowledge (ZK-STARKs) [284]. Abelian [285], another blockchain platform, has proposed the utilization of lattice-based post-quantum cryptosystems as a means of safeguarding against quantum attacks. Additionally, experiments are being conducted on certain blockchains like Corda, exploring the application of post-quantum algorithms such as SPHINCS [286].

The most comprehensive survey available on the evaluation of post-quantum cryptography for blockchain applications is [148]. The survey explores the current state of post-quantum cryptosystems and their relevance to blockchain technology and distributed ledger technologies (DLTs). It also investigates the prominent post-quantum blockchain systems and the challenges they face. The article provides detailed comparisons of the attributes and efficiency of the most favorable post-quantum public-key encryption and digital signature systems for integration with blockchains.

Additionally, the article compares all the candidates from the second round of NIST and analyzes their quantum security and performance when implemented on blockchains. This survey was conducted prior to the third round of NIST PQC, and it is important to mention that part of the evaluated cases in [148] are now considered insecure. In TABLE XVI and TABLE XVII, a comparison of post-quantum digital signatures, selected as finalists by NIST and analyzed by [148] for blockchain applications, is presented.

B. Surveying Blockchain Hashes and Assessing Their Quantum Security Level

In contrast to digital signatures and public-key cryptosystems, conventional hash functions are generally considered to be resilient against quantum attacks, as developing quantum algorithms for NP-hard problems appears unlikely [287]. However, recent academic proposals have introduced new hash functions specifically designed to withstand quantum attacks [288]. Nonetheless, it is commonly suggested to augment the size of output for conventional hash functions as a precaution. This recommendation stems from the potential utilization of Grover's algorithm to expedite brute force attacks with a quadratic speedup. There are two ways in which Grover's algorithm can be leveraged to exploit vulnerabilities in a blockchain.

Firstly, it can be employed to seek out instances of hash collisions, enabling the replacement of entire blockchain blocks. For example, a study [289] suggests employing the algorithm of Grover to identify collisions within hash functions, which indicates that a hash function should produce $3 * n$ bits of output to offer a security level of n bits. Consequently, many existing hash functions might not be adequate in the era of quantum computing, whereas options like SHA-2 and SHA-3 might require expanding their output sizes. Secondly, the algorithm of Grover can expedite the mining process of blockchains such as Bitcoin by speeding up the generation of nonces, which could result in the rapid recreation of entire blockchains, compromising their integrity [148].

Furthermore, hash functions are also susceptible to attacks using Shor's algorithm. If a blockchain's hash function is compromised, an individual with a sufficiently powerful quantum computer could exploit Shor's algorithm to impersonate users within the blockchain, counterfeit digital signatures, and pilfer their digital assets [148].

TABLE XVIII provides the key attributes of the most widely used hash functions in prominent blockchains and illustrates how quantum computing affects their security level [148]. Moreover, [290] provides a comprehensive examination of hashing algorithms used in cryptocurrencies. It covers basic information about hashing, which serves as the foundation for these algorithms. The study focuses on cryptographic hashing algorithms such as SHA256, Ethash, Scrypt, Equihash, RandomX, X11, Lyra2Z, and Lyra2REv2. Each algorithm is discussed individually, highlighting their specific use in certain cryptocurrencies or their significant role in multiple cryptocurrencies. The study concludes by exploring the creators of these algorithms, their intended purposes, features, structures, working methods, and areas of application.

Hash functions have played a significant role in shaping blockchain technology by introducing hash-based signatures, which have been thoroughly explored and analyzed in the preceding sections. For instance, commercial distributed ledger technologies such as IOTA's Tangle [291] assert their higher resilience against quantum attacks compared to Bitcoin, particularly in processes involving nonce search [292]. Notably, IOTA leverages one-time hash-based signatures (Winternitz signatures) instead of relying on ECC. Moreover, IOTA leveraged ternary hardware, diverging from the conventional binary hardware, to implement a novel hash function called CURL-P.

Curl-P, also known as Curl, is a cryptographic hash function specifically designed for use in the IOTA blockchain. It serves various purposes within the IOTA ecosystem, including generating transaction addresses, creating message digests, performing proof of work, and facilitating hash-based signatures. While Curl-P follows the general structure of a Sponge Construction, it differs from other hash functions in certain aspects. It operates on trits in balanced ternary, which is distinct from the typical binary-based operations of most cryptographic hash functions. It is important to note that the IOTA project has not provided an official specification or analysis of Curl-P. Therefore, the description of Curl-P is mainly based on the open-source implementation made available by the IOTA developers.

In [293], vulnerabilities have been discovered in the cryptography previously used in the IOTA blockchain, including the capability to counterfeit signatures under specific conditions. Practical attacks were developed against Curl-P-27, the hash function of IOTA, enabling the efficient generation of short messages with identical hash values. Such collisions occur even when the messages have identical lengths. Taking advantage of these vulnerabilities in Curl-P-27, the security of the former IOTA Signature Scheme (ISS) was compromised, and the ability to counterfeit signatures or multi-signatures for legitimate spending transactions or bundles was demonstrated

TABLE XVI
COMPARISON OF POST-QUANTUM DIGITAL SIGNATURES (NIST FINALISTS) FOR BLOCKCHAIN APPLICATIONS [148].

Scheme	Category	Subcategory	Level of Quantum Security	Public-Key Size	Private-Key Size	Size of Signature
DILITHIUM-1280x1024+SHAKE	Lattice based	Fiat-Shamir-with-Aborts	128 (bits)	1472 (bytes)	-	2701 (bytes)
DILITHIUM-1280x1024+AES	Lattice based	Fiat-Shamir-with-Aborts	128 (bits)	1472 (bytes)	-	2701 (bytes)
FALCON 512	Lattice based	SIS-over-NTRU-lattices and FFT	103 (bits)	897 (bytes)	1314.56 (bytes)	657.38 (bytes)
FALCON 1024	Lattice based	SIS-over-NTRU-lattices and FFT	230 (bits)	1,793 (bytes)	2546.62 (bytes)	1273.31 (bytes)
SPHINCS+, SHAKE256-128f-simple	Hash based	Stateless-signature	128 (bits)	32 (bytes)	64 (bytes)	16976 (bytes)
SPHINCS+, SHAKE256-192f-simple	Hash based	Stateless-signature	192 (bits)	48 (bytes)	96 (bytes)	35664 (bytes)
SPHINCS+, SHAKE256-256f-simple	Hash based	Stateless-signature	256 (bits)	64 (bytes)	128 (bytes)	49216 (bytes)
SPHINCS+, SHA256-128f-simple	Hash based	Stateless-signature	128 (bits)	32 (bytes)	64 (bytes)	16976 (bytes)
SPHINCS+, SHA256-192f-simple	Hash based	Stateless-signature	192 (bits)	48 (bytes)	96 (bytes)	35664 (bytes)
SPHINCS+, SHA256-256f-simple	Hash based	Stateless-signature	256 (bits)	64 (bytes)	128 (bytes)	49216 (bytes)
SPHINCS+, Haraka-128f-simple	Hash based	Stateless-signature	128 (bits)	32 (bytes)	64 (bytes)	16976 (bytes)
SPHINCS+, Haraka-192f-simple	Hash based	Stateless-signature	192 (bits)	48 (bytes)	96 (bytes)	35664 (bytes)
SPHINCS+, Haraka-256f-simple	Hash based	Stateless-signature	256 (bits)	64 (bytes)	128 (bytes)	49216 (bytes)

TABLE XVII
PERFORMANCE COMPARISON OF POST-QUANTUM DIGITAL SIGNATURES [148].

Algorithm	Evaluation Platform	Key-Generation (cycles)	Signing (cycles)	Verification (cycles)
DILITHIUM-1280x1024+SHAKE	Intel-Core-i7-6600U-(Skylake)-2.6GHz, Optimized AVX.2	156,777	437,638	155,784
DILITHIUM-1280x1024+AES	Intel-Core-i7-6600U-(Skylake)-2.6GHz, Optimized AVX.2	99,907	350,465	109,782
FALCON 512	Intel-Corei7-6567U-3.3GHz	7.26ms	-	-
FALCON 1024	Intel-Corei7-6567U-3.3GHz	21.63ms	-	-
SPHINCS+, SHAKE256-128f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	3,909,682	133,452,230	9,468,278
SPHINCS+, SHAKE256-192f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	6,303,298	171,354,532	14,758,202
SPHINCS+, SHAKE256-256f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	16,898,344	416,398,690	15,383,888
SPHINCS+, SHA-256-128f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	3,257,486	116,197,711	6,094,962
SPHINCS+, SHA-256-192f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	2,280,172	140,223,132	9,723,976
SPHINCS+ SHA-256-256f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	5,594,338	145,433,610	9,384,544
SPHINCS+, Haraka-128f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	654,294	25,178,368	1,333,172
SPHINCS+, Haraka- l92f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	2,317,102	58,491,132	3,714,942
SPHINCS+, Haraka-256f-simple	Intel-Core-i7-4770K-3.5GHz, Optimized AVX.2	2,510,894	65,870,866	1,949,510

in a chosen-message setting.

While the discovery of such attacks undermines IOTA's claim of superior security compared to Bitcoin, it is essential to acknowledge alternative blockchain solutions developed to succeed Bitcoin in the post-quantum era. One such solution is the Quantum-Resistant Ledger (QRL) [294], which replaces secp256k1 with XMSS (eXtended Merkle Signature Scheme) [148]. These alternatives aim to address the challenges posed by quantum computing and enhance the security of cryptographic operations in the blockchain context.

C. Surveying Consensus Mechanisms in Blockchains and Analyzing Their Quantum Security

The cryptocurrency application of modern blockchains consist of two main parts: a consensus protocol for generating fresh blocks and a digital signature scheme for verifying the transactions. The blockchain performs as a distributed consensus storage system, utilizing consensus mechanisms among nodes to reach an agreement on the storage contents and maintain ledger consistency across the distributed network. Consensus mechanisms, along with cryptographic schemes like public-key cryptography and hash functions, ensure security in an open and untrusted network. Various consensus models, including PoW, PBFT, PoS, delegated proof of DPoS, etc., have been proposed. The PoW model involves solving a mathematical problem to achieve consensus, utilizing algorithms like SHA256, Scrypt, Cryptonight, Equihash and etc. Difficulty adjustment algorithms (DAA) are used to stabilize block generation time, although the original Bitcoin PoW model lacks such an algorithm [147]. The main objective of a blockchain consensus protocol is to establish unanimous agreement among participating nodes regarding the transaction history stored in the blockchain. This is achieved by satisfying several requirements for blockchain consensus. These requirements include [53], [297]:

1) Safety (or Consistency): If all nodes generate identical and valid outputs, adhering to the protocol's rules, the consensus protocol can be deemed secure.
2) Liveness: If all participating nodes that are not faulty, generate a result, the consensus mechanism will be seen as ensuring liveness.
3) Termination: Each truthful node is expected to either accept or discard fresh transactions within a block, ensuring their inclusion in the blockchain.
4) Agreement: All truthful nodes must unanimously accept or discard new transactions and their corresponding blocks. Additionally, every honest node should assign the same sequence number to accepted blocks.
5) Validity: In the event that all nodes receive an identical valid block or transaction, it ought to be incorporated

TABLE XVIII
BLOCKCHAIN PLATFORMS AND WIDELY USED HASH FUNCTIONS THAT ARE AFFECTED BY THE QUANTUM THREAT.

Scheme	Main Impacted DLTs or Blockchains	Classical Security Level	Post-Quantum Security Level (Grover)	Hash Size (bits)
SHA-256	Ethereum, Bitcoin, Dash, Litecoin, Zcash, Morrero, Ripple, NXT, Byteball	256 bits	128 bits	256
Ethash (Keccak-256, Keccak-512)	Ethereum	256/512 bits	128/256 bits	256/512
Scrypt	Litecoin, NXT, Verge	256 bits	128 bits	256
RIPEMD160	Bitcoin, Ethereum, Litecoin, Monero, Ripple, Bytecoin	160 bits	80 bits	160
Keccak-256	Bytecoin, Monero	256 bits	128 bits	256
Keccak-384	IOTA	384 bits	192 bits	384
SHA-3 256	-	256 bits	128 bits	256
X11 (Multiple rounds of 11 different hashes: blake, jh, bmw, groestl, skein, keccak, shavite, cubehash, echo, simd)	Dash, luffa, Petro	256 bits	128 bits	256
CryptNight	Monero (Replaced in November 2019)	256 bits	128 bits	256
RandomX	Monero	256 bits	128 bits	256
X17 (17 rounds of hashing functions: Blake, Bmw, Groestl, Jh, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, Echo, Hamsi, Fugue, Shabal, Whirlpool, Loselose, Djb2)	Verge			
groestl (512 or 1024 bits), blake2s, lyra2	Verge	256 bits	128 bits	256
Verthash	Vertcoin	256 bits	128 bits	256
ETChash or Thanos (Updated version of Ethash after a series of 51% attacks on the Ethereum Classic network in 2020, based on Keccak-256)	Ethereum Classic	256 bits	128 bits	256
Blake2 (Blake2b)	Nano	512 bits	256 bits	512
Equihash (A memory-oriented PoW algorithm designed to be resistant to specialized mining hardware such as ASICs. It has three parameters (n, k, d) and finds distinct, n-bit values $i_1, \ldots, i_{2^k}$ satisfying $H(i_1) \oplus \cdots \oplus H(i_{2^k}) = 0$ that $H(i_1 \parallel \cdots \parallel i_{2^k})$ has d leading zeros, where H is a chosen hash function.)	Zcash and Bitcoin Gold	N/A	N/A	N/A
Eaglesong	Nervos CKB	256 bits	128 bits	256

TABLE XIX
AVAILABLE SURVEYS ON CONSENSUS ALGORITHMS.

Ref.	Title	Year
[295]	A Review on Consensus Algorithm of Blockchain	2017
[296]	Blockchain Consensus: An Introduction to Classical, Blockchain, and Quantum Consensus Protocols	2022
[45]	A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions	2019
[65]	A Survey of Blockchain Consensus Protocols	2023
[297]	A Survey of Distributed Consensus Protocols for Blockchain Networks	2020
[49]	A Survey on Consensus Protocols and Attacks on Blockchain Technology	2023
[298]	A Taxonomic Hierarchy of Blockchain Consensus Algorithms: An Evolutionary Phylogeny Approach	2023
[53]	A taxonomy of blockchain consensus protocols: A survey and classification framework	2021
[43]	A Comparative Study of Blockchain Consensus Algorithms	2020
[299]	A Review: Consensus Algorithms on Blockchain	2022
[62]	Survey of Consensus Algorithms for Proof of Stake in Blockchain	2022
[300]	Quantum Consensus: an overview	2021
[301]	Blockchain Consensus Mechanisms: A Primer For Supervisors	2022
[158]	A Survey on Consensus Algorithms in Blockchain based on Post Quantum Cryptosystems	2022
[302]	Comparative Analysis of Blockchain Consensus Algorithms	2018
[303]	Consensus Algorithms in Blockchain Technology: A Survey	2019
[304]	Study of Blockchain Based Decentralized Consensus Algorithms	2019
[305]	A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks	2019
[306]	Analysis of the Consensus Protocols used in Blockchain Networks An overview	2022
[307]	A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues	2023
[308]	Survey on Private Blockchain Consensus Algorithms	2019
[309]	A Survey and Ontology of Blockchain Consensus Algorithms for Resource-Constrained IoT Systems	2022

into the blockchain.
6) Integrity: At every truthful node, there should be coherence among all accepted transactions to deter double spending. Furthermore, approved blocks must be generated accurately and chained in order of occurrence.

A blockchain consensus protocol consists of five core components [297]:

1) Block proposal: This involves generating blocks and providing generation proofs. Available scenarios include: client operation request, any server can propose transactions, PoW, PoS, PoS with stake delegation, PoS-based committee election, PoR and etc.
2) Information propagation: Blocks and transactions are disseminated throughout the network to verify all nodes are aware of the latest updates. Available scenarios include: broadcast, broadcast among BFT committee, broadcast among committee, broadcast among validators, Broadcast among delegates and etc.
3) Block validation: Blocks are checked for proof of generation and validity of transactions. Available scenarios include: signature check, PoW check, PoS check, delegate eligibility check, tip approval check, proposer eligibility check and etc.
4) Block finalization: Agreement is reached among nodes regarding the acceptance of validated blocks. Available scenarios include: mutual agreement on the same state, longest-chain rule, BFT, PBFT, stake-weighted voting, variations of GHOST rule, accepting more than 80% voted transactions and etc.
5) Incentive mechanism: This component promotes honest participation in the consensus process and encourages the creation of network tokens. Available scenarios include: block reward and transaction fee, getting qualified to issue fresh transactions, commissions acquired from storage charges, and etc.

Additionally, two more features, namely transaction processing capability and fault tolerance, are important considerations in a blockchain consensus protocol [297]. Fault tolerance ensures the protocol can withstand failures or malicious attacks, while transaction processing capability focuses on maximizing throughput and minimizing transaction confirmation latency. The authors in [297] conducted a comparison of different blockchains based on these metrics and features. There are also numerous comprehensive surveys available on consensus algorithms, which are listed in TABLE XIX and we highly recommend for more detailed information.

Blockchain transactions occur whenever a user aims to transfer blockchain assets (or coins) to another user. The user signs a hash of the prior transaction and sends the public-key of the recipient. A selected miner verifies and broadcasts the transaction to the blockchain network, eventually collecting valid transactions into a new block. The user who successfully adds a new block confirms all transactions within that block until the next six blocks are verified and added. Signature schemes used in transactions vary based on efficiency, functionality, and other blockchain requirements. Examples include ECDSA for higher transactions-per-second (TPS) in Bitcoin and linkable-ring-signature schemes for privacy protection in Monero. Block time intervals and block sizes are typically fixed, with Bitcoin producing a block every 10 minutes and each block being 1MB in size. As the ledger accumulates historical transactions, its size grows over time and may require expansion [147].

Quantum computing attacks on blockchain involve targeting the consensus model and signature schemes. For instance, quantum computers can attack the core hash function SHA256, reducing its complexity from $O(N)$ to $O(\frac{\pi}{4}\sqrt{10N})$. Similarly, ECDSA can be vulnerable to quantum attacks, with complexity estimated as $9n + 2\left[\log_2(n)\right] + 10$, for $n = 160$, using the fastest known method [147].

The first proposed solution for a consensus mechanism in a post-quantum environment introduced a new PoW algorithm [310] utilizing a system of multivariate quadratic equations to create a hard problem based on hashing. Solutions, in the context of the mining procedure, are obtained through exhaustive enumeration. Nevertheless, this algorithm does not take into account storage usage, ultimately reducing it into a simplified Bitcoin-like proof-of-work algorithm with post-quantum characteristics [147]. From the other point of view, one more solution gaining attention is the Post-Quantum Blockchain (PQB) [148], which focuses on enhancing the security of processing transactions within the blockchain. Notably, [311] and [312] have presented post-quantum signature algorithms, obtained using lattice-based cryptography, for processing transactions within blockchain systems.

In [147], the authors proposed the construction of a post-quantum blockchain. Specifically,

1) They proposed a novel PoW consensus mechanism designed for the post-quantum era. The main idea behind constructing a PoW framework like this is using alternative challenging problems to substitute for SHA-256, which is employed by PoW model of Bitcoin. To be more specific, their PoW consensus mechanism introduces the task of finding solutions for quadratic multivariate equations, which falls into the category of NP-hard problems. The miners employ a solution finding method based on Grobner bases (either F4 or F5 algorithms) for solving the stochastic multivariate quadratic equations. The suggested mechanism offers the following advantages: i) The tasks performed by the miner incorporates both computation capability and storage capacity, and ii) DAA algorithms are integrated into the consensus construction.
2) They introduced a new mechanism for constructing lightweight post-quantum blockchain transactions. This mechanism incorporates an identity-based post-quantum signature scheme and the Inter Planetary File System (IPFS). At the time of publication, the authors asserted that their scheme achieved the most compact public-keys and signatures for blockchain transactions. The authors provided an elaborate explanation of how to construct these transactions, highlighting the proposed signature scheme's ability to protect against quantum attacks.

As mentioned earlier, blockchain technologies can be simplified into two fundamental components: the consensus proto-

TABLE XX
QUANTUM VULNERABILITIES OF WELL-KNOWN BLOCKCHAINS [185].

Blockchain	Level of Risk	Objective	Susceptibilities
Bitcoin	High	Transactions recorded to the network	Transactions recorded to the network are susceptible to quantum attacks, particularly concerning their signature scheme. The primary identified form of attack targets transactions which are disclosed to the network but have not yet been incorporated into a block. A quantum-attacker can take advantage of the public-key declared by the transaction sender to derive the private-key, enabling them to replicate the transaction with any destination of their choice.
Ethereum	High	Re-use of public-keys	Ethereum, operating on an account-centric system, commonly experiences public-key reuse. The identified attack mechanism focuses on accounts that have earlier broadcasted transactions to the network while retaining Ether-tokens. By employing the algorithm of Shor to solve the public-key and acquire the private-key, a quantum assailant could create transactions under the user's identity by producing a legitimate transaction signature.
Litecoin	High	Transactions recorded to the network	Litecoin, having a considerable part of its technical framework in common with Bitcoin, exhibits equivalent vulnerability to quantum attacks. The most impactful attack technique, similar to Bitcoin, targets transactions broadcasted to the network but not yet included in the blockchain.
Bitcoin Gold	High	Transactions recorded to the network	Because of its cryptographic components resembling those of Bitcoin, Bitcoin Gold is exposed to the same vulnerabilities.
Bitcoin Core	High	Transactions recorded to the network	Given its resemblance to Bitcoin's cryptographic components, Bitcoin Core is susceptible to identical vulnerabilities.
Bitcoin Cash	High	Transactions recorded to the network	Because of its resemblance to Bitcoin's cryptographic components, Bitcoin Cash is exposed to the same vulnerabilities.
Monero	Medium	Obfuscated transactions and transactions recorded to the network	Monero employs a signature scheme called Monero-EdDSA, which is potentially susceptible to quantum-attacks because its security is based on the discrete logarithm problem. Nevertheless, Monero does have some built-in capabilities to withstand quantum attacks owing to the anonymity of its users and transaction amounts. While the Bulletproof protocol used in Monero to obfuscate transaction amounts can also be susceptible to quantum attacks, an attacker would need a stroke of luck to target a high-value transaction. Additionally, Monero has recently updated its consensus protocol with the introduction of RandomX, further bolstering its resistance against quantum-attacks, especially in cases where adversaries try to carry out a 51% attack using the algorithm of Grover.
BEAM	Medium	Obfuscated transactions and transactions recorded to the network	The signature scheme of BEAM, along with the employed technique for obfuscation known as Mimblewimble, is quantum-vulnerable. Quantum attacks can capture broadcasted transactions to the network and compromise the anonymity of concealed transactions. Nonetheless, similar to Monero, concealing the values of transaction and account reduces the motivation for quantum-attackers.
Grin	Medium	Obfuscated transactions and transactions recorded to the network	The signature scheme of Grin, along with the employed technique for obfuscation known as Mimblewimble, is quantum-vulnerable. Quantum attacks can capture broadcasted transactions to the network and compromise the anonymity of concealed transactions. Nonetheless, similar to Monero, concealing the values of transaction and account reduces the motivation for quantum-attackers.
ZCash	Very High	Public parameter generated during the ZK-SNARK ceremony	ZCash is exposed to significant risks from quantum-attacks targeting its consensus mechanism and signature algorithm. Nonetheless, the most critical vulnerability identified in ZCash lies in its protocol for zero-knowledge proofs called ZK-SNARKS. This protocol relies on a trusted setup process that involves generating a public-parameter, which serves as a public-key. If a quantum attacker manages to obtain the private-key for this public-parameter, they would gain the ability to generate tokens without restriction. This implies a significant risk to the integrity and security of ZCash.

col and the transaction mechanism. To the best of our knowledge, there is a limited number of thorough and comprehensive analyses (i.e., considering the both fundamental components) on the vulnerability of blockchains to quantum attacks. The first such study was conducted by Aggarwal and colleagues regarding Bitcoin security [313]. Their work represents the initial effort to thoroughly analyze the potential weaknesses of cryptocurrencies, when exposed to quantum attacks, in a more comprehensive manner.

The project Bitcoin Post-Quantum [314] emerged in response to the threat of quantum attacks. It involved a hard fork commencing at block height 555,000 within the Bitcoin network, implementing a post-quantum hash-based digital signature scheme (XMSS) and a quantum resistant PoW mechanism (Equihash96x3) based on the birthday paradox like Z-Cash and provides quantum-safe privacy based on post-quantum zero-knowledge proofs (ZKB++/Picnic [315] and zk-STARKs [316]). However, since this project is a fork, it does not provide any actual security advantages to the original Bitcoin blockchain.

In the study conducted by Kearney et al. [185], the same analysis was performed on five major cryptocurrencies, namely Ethereum, Monero, Litecoin, ZCash, and Bitcoin, along with some of their variants. Litecoin, being a hard fork in the blockchain of Bitcoin, shares many similarities in its infrastructure. Although there is less dedicated research on Litecoin, its protocol architecture has been thoroughly documented in terms of security standpoint, including analysis of the Equihash PoW algorithm it employs. Ethereum, on the other hand, has a distinct protocol and has no origin from another blockchain. Its security analysis largely revolves around its novel feature of smart contracts, with extensive research conducted on its classical security aspects [185]. Monero and ZCash, despite having smaller user bases compared to other blockchains, have received significant security analysis due to their unique utilization of confidential transactions [185].

While extensive analysis has been conducted on the protocols and cryptographic security of many cryptocurrencies, the majority of them do not have publicly available rigorous post-quantum vulnerability assessments. However, existing research on classical cybersecurity attacks provides some insights for understanding the quantum vulnerabilities. There are also analyses that encompass the security of multiple blockchains simultaneously [93], [317], acknowledging the similarities in their structures and cryptographic protocols. For example, the use of ECDSA or its variants for cryptographic signatures and PoW as the predominant consensus mechanism is common among many blockchains. While this type of analysis is valid for classical security analyses, it may not hold true for quantum security analysis. Even though small protocol differences may have minimal impact on classical security, they can yield a substantial effect on the severity of an attack on the network using quantum technology, as evidenced in [185].

For each selected blockchain technology in [185], the vulnerabilities to quantum attacks are presented and ranked. The

attack with the highest potential for causing reputational or financial loss to the network is also described. The authors also considered the feasibility of removing or mitigating these vulnerabilities when applicable. These factors are subsequently merged into an overall vulnerability score, representing the overall vulnerability of the blockchain. This enables the ranking of blockchains based on their comparative vulnerability, ranging from low vulnerability for those with a diminished risk of a quantum-attack to very high vulnerability rendering a blockchain entirely unsuitable for utilization with the advent of quantum technologies. On the other hand, blockchains that are susceptible to quantum-attacks but employ technologies that might deter or render attacks more challenging, receive a medium rating [185]. A summary of this information can be found in TABLE XX. It presents the blockchain name, the determined risk level, the specific cryptographic technology that is vulnerable, and a brief summary of the corresponding attack.

Bitcoin, along with numerous other cryptocurrencies, implement PoW mechanism known as Hashcash, which was developed by Adam Back [318]. The hashcash PoW involves discovering a valid block-header satisfying the condition $h(\text{block-header}) \leq t$, where t is a threshold and $h(\cdot)$ denotes the SHA256(SHA256($\cdot$)) hash function. Considering that the range of h consists of 2^{256} possibilities, the anticipated count of attempted hashes required to achieve the hashcash PoW with parameter t is $2^{256}/t$. In the context of Bitcoin PoW, however, it is typically expressed in relation to the difficulty level D, which is defined as $D = 2^{224}/t$. This represents the projected number of hashes necessary to complete the PoW, divided by 2^{32}, which corresponds to the number of available nonces.

The security of a PoW-based blockchain relies on the probability of any agent solving the PoW task before others exceeding 50%. The time required for executing the Grover algorithm and achieving successful block mining is [313]

$$\tau = \pi 2^{14}\sqrt{10 \cdot D} \times \frac{\mathcal{G}_{\mathcal{O}}}{s}, \quad (2)$$

$$\mathcal{G}_{\mathcal{O}} = 297784 \times c_\tau(D, p_g), \quad (3)$$

where $\mathcal{G}_{\mathcal{O}}$ represents the number of cycles required for a single call of oracle, s denotes the clock-speed of the quantum computer. The term c_τ corresponds to the time overhead factor associated with quantum error-correction. It measures the quantity of clock cycles needed for each logical T gate operation and relies on the difficulty D and the physical gate error rate p_g. Considering the parallelization of the Grover algorithm across d quantum processors, gives the time expected for finding a solution as $\tau_{||} = 0.39 \times \tau/\sqrt{d}$ with the effective-hash-rate as

$$h_{QC,||} = 2.56 \times h_{QC}\sqrt{d}, \quad (4)$$

$$h_{QC} = \frac{0.28 \times s\sqrt{D}}{c_\tau(D, p_g)}. \quad (5)$$

If we maintain a constant requirement of 2402 logical qubits for the Grover algorithm, irrespective of its complexity, the quantity of physical qubits needed would be [313]

$$n_Q = 2402 \times c_{n_Q}(D, p_g), \quad (6)$$

where c_{n_Q} represents the space overhead, which refers to the additional physical qubits required for quantum error correction. This overhead is dependent on the difficulty level and the gate error rate. Considering a maximum achievable gate speed of $s = 66.7$MHz, gate error rate of $p_g = 5\times10^{-4}$, along with a difficulty level close to $D = 10^{12}$, the corresponding overheads are $c_\tau = 538.6$ and $c_{n_Q} = 1810.7$. This implies an effective-hash-rate of $h_{QC} = 13.8\text{GH}/s$ using $n_Q = 4.4\times10^6$ physical-qubits. However, this hash rate corresponds to a speed that is over a thousand times less compared to commercially available ASIC devices that operate at hash rates of $14\text{TH}/s$ [313].

By utilizing Grover algorithm, a quantum computer is able to perform the hashcash-PoW with significantly lower number of hash computations compared to a conventional computer. Nevertheless, the current rate of dedicated ASIC hardwares used for hashcash-PoW, combined with the lower speed of gates in the existing quantum-architectures, effectively nullifies this quadratic speedup. Given the existing difficulty level, there is no advantage for employing quantum computers. Although future advancements in quantum technology, enabling gate speeds as high as 100GHz, may potentially make quantum computers approximately 100 times faster than current technology in solving the PoW, such progress is unlikely within the next decade. By that time, classical hardware may have become significantly faster, and quantum technology could be so widely adopted that no individual quantum-capable entity could establish dominance over the PoW problem [313].

The desired properties for a PoW system can be summarized as follows [313]:

1) Difficulty: The ability to adjust the difficulty of the problem based on the available computing power in the network.
2) Asymmetry: The verification of the PoW should be significantly easier than actually performing the PoW.
3) No quantum advantage: The proof-of-work should not provide a significant advantage to quantum computers over classical computers.

While the Bitcoin PoW satisfies properties (1) and (2), there is a need to explore alternative PoW mechanisms that address property (3) more effectively. Several authors have explored alternative PoW approaches that aim to address the limitation of being accelerated by ASICs, rather than focusing on quantum advantage (property 3). One approach is to consider memory-intensive-PoW methods. Several noteworthy candidates are available, including Momentum [319], which relies on the collision discovery in a hash function, Equihash [320], which relies on the generalized birthday-problem, and Cuckoo Cycle [321], which involves identifying constant-sized subgraphs in a random graph These candidates not only exhibit promising characteristics for resistance against quantum attacks but also provide alternatives to ASIC acceleration [313]. These schemes are built upon the hashcash-style PoW and follow a similar template as follows. A secure hash function, denoted as h_1 is employed to calculate the hash $H = h_1(\text{block-header})$ of the block-header. The objective is finding a nonce x that satisfies the predicate P, with $h_1(H||x) \leq t$ and $P(H, x)$. This

approach introduces a departure from the traditional sequential iteration through nonces and allows for the flexibility of adjusting the difficulty by varying the parameter t [313].

Zcash adopts the Equihash PoW algorithm as its consensus mechanism. Equihash is a memory-hard PoW scheme that is derived from the generalized birthday problem. It is specifically designed to be computationally intensive on memory, making it resistant to ASIC mining. It has been revealed that ZCash's consensus mechanism and signature system can be vulnerable to quantum-attacks [185]. However, the most critical vulnerability found in ZCash is related to its zero-knowledge proof protocol, ZK-SNARKS. To address this issue, [328] examines the limitations of existing zero-knowledge proof (ZKP) implementations in cryptocurrencies like Monero and Zcash, which are vulnerable to quantum attacks due to their reliance on discrete logarithm assumptions. To address this, the paper focuses on lattice-based cryptography as a promising post-quantum solution. Unfortunately, the costs associated with lattice-based solutions are significantly higher compared to discrete logarithm settings. For instance, the proof of the lattice-based scheme in [329] occupies nearly 200KB, whereas the Bulletproofs protocol employed in Monero only requires less than 1KB [330]. In Monero, the Ring Confidential Transaction (RingCT) protocol is employed, which utilizes a range proof to demonstrate that all amounts are positive and that the disparity between outputs and inputs is zero, ensuring a balanced state. Due to the separate commitment of amounts in the RingCT protocol, available efficient aggregations cannot be utilized. However, a breakthrough in lattice-based RingCT protocols called MatRiCT [331] has successfully addressed this issue by optimizing the proof size within a blockchain environment. Currently, MatRiCT is implemented in Hcash, marking the first practical application of a lattice-based RingCT protocol. MatRiCT optimizes proof size by employing a balance proof with hashed-message commitments (HMC). MatRiCT also incorporates techniques like batched commitments and rejection sampling to enhance the efficiency of ring signatures.

Building upon MatRiCT, [328] proposes two novel techniques: linear equation satisfiability and unbalanced linear sum proof. The linear equation satisfiability technique reduces proof size and verification time by generalizing balance proofs to linear equations, overcoming overflow issues in inner-product relations under lattice settings. The unbalanced linear sum proof replaces the binary proof component in existing ring signatures with a more efficient approach based on relaxed relations. The results show that their solutions can reduce the proof size of [329] by about 25%, and achieve up to 70% reduction in proof size, 30% reduction in proving time, and 20% reduction in verification time compared to [331].

Ethereum, which previously relied on PoW, has transitioned to a proof-of-stake consensus protocol. The previous PoW mechanism used by Ethereum, known as EthHash, employed one round of SHA-3 (Keccak-265) hashing for crafting the PoW problem, much like what is done in Bitcoin. However, like Bitcoin, Ethereum's PoW consensus mechanism could be vulnerable to quantum attacks utilizing Grover's algorithm. Even without advancements in the technology of ASIC, a quantum-enabled adversary would need a clock rate of approximately 5000 GHz to launch a 51% attack on consensus algorithm of Ethereum. Despite shorter block time of Ethereum in comparison with Bitcoin, its vulnerability to quantum attacks is significantly higher because of its transaction system based on accounts [185]. The authors in [74] provide a systematic analysis of the security of the Ethereum system, examining vulnerabilities, attacks, and defenses from a classical perspective. For example, random selection of block block-proposers in Ethereum is addressed as an issue. Random selection of winners in gambling and lottery contracts often relies on generating pseudorandom numbers using initial private seeds, such as block information. However, since these seeds are manipulatable by miners, a malicious miner can exploit this vulnerability and manipulate the outcome in their favor. Various proposals have been made to address this issue, each with its own advantages and disadvantages. The Oracle Random Number Generator (RNG) scheme suggests off-chain random number generation by employing external services and return them to the contract. However, this approach introduces a single point-of-failure in the Oracle RNG. Another proposal, RANDAO, involves multiple participants using a distributed cryptographic commitment scheme for generating a random number. However, it remains susceptible to the last-revealer attack, in which the final participant can introduce bias by deciding whether to reveal their committed entropy or not [74]. To mitigate this issue, Verifiable-Delay-Functions (VDFs) have been introduced to ensure that participants cannot compute the random seed before submitting their own entropy. In Ethereum 2.0, there is contemplation of employing a combination of the RANDAO protocol and VDFs to randomly select block-proposers on the beacon chain, aiming to create non-exploitable randomness. However, it is worth noting that existing VDFs are intricate and lack post-quantum security.

Litecoin, a fork of Bitcoin, utilizes a distinct PoW scheme called Scrypt. Similar to Bitcoin, Litecoin aims to require computational resources to solve a problem and authorize the creation of the subsequent block in the blockchain. However, Scrypt differs from other PoW schemes by emphasizing the utilization of RAM for mining-nodes as an additional resource, instead of relying exclusively on processing power. While Scrypt might have a vulnerability to quantum-leveraged 51% attack using the algorithm of Grover, Litecoin presently maintains a hash rate of 320 THz. Hence, to even contemplate such an attack at the current hash rates, a quantum computer would have to run at a clock frequency of 2.4 THz. Additionally, future advancements in ASIC technology further diminish the likelihood of such attacks in the foreseeable future. In comparison to Bitcoin, Litecoin exhibits slightly improved resistance against quantum attacks [185].

Monero employs the CryptoNight v8 PoW mechanism, which is designed to be resistant to ASIC mining and is derived from the Egalitarian PoW used in CryptoNote. This method is based on slow memory access over random-intervals, which results in a high memory demand, necessitating 2 Mb per instance. However, Monero has recently transitioned from CryptoNight to a new PoW scheme called RandomX. RandomX is based on executing random programs

TABLE XXI
ASSESSMENT OF CONSENSUS ALGORITHMS UTILIZING POST-QUANTUM CRYPTOGRAPHY [158].

Consensus	Post-quantum system/UsedTechnique	Persistence	Security	Scalability	Efficiency	Quantum resistant	Used-Resources
[322]	Multivariate based/Threshold signature, Generation of coefficients using Unbalanced Vinegar & Oil scheme	Yes	Yes	Like	Moderate	Yes	Moderate
[323]	Multivariate quadratic equations, Generation of coefficients using PRNG & SHA-256	Yes	Yes	Like PoW	High	Yes	Moderate
[310]	Multivariate based/MQ problem, Generation of coefficients using SHA-256 & SHA-512	Yes	Yes	Like PoW	High	Yes	Moderate
[324]	Hash based/Serial-Mining-Puzzle (SMP) and Mining-Credibility-System (MCS)	Yes	Yes	Like PoW	Moderate	Yes	Moderate
[320]	Hash based/Generalized Birthday Problem	Yes	Yes	Like PoW	Moderate	No	High
[325]	Hash based/Toeplitz Signature	Yes	Yes	Like BFT	Moderate	Yes	Moderate
[326]	Lattice based/Hermite SVP Problem	Yes	Yes	Like PoW	High	Yes	Low
[327]	Code based/Low Density Parity Check Decoder	Yes	Yes	Like PoW	Moderate	No	Moderate

with a specialized instruction-set consisting of floating point math, integer math, and branches. The aim of RandomX is to minimize the advantage of GPUs in PoW mining and potentially enhance quantum resiliency indirectly. As of the time of composing this paper, there is no known method to attain a quantum superiority in RandomX. This suggests that Monero's PoW system is currently free from known quantum vulnerabilities. However, it is important to note that Monero transactions remain susceptible to quantum attacks, although the transaction anonymization features of networks make them less appealing targets compared to transactions on other blockchain networks [185].

In addition to signing algorithms, post-quantum cryptography systems can also be utilized to strengthen the security of established blockchain networks by adjusting the functioning of consensus mechanisms. To create a post-quantum blockchain, the first step is to select a difficult NP-Hard problem. This problem can be solved using post-quantum techniques, such as multivariate quadratic equations. The solution obtained from solving the problem is then used to alter an available consensus mechanism, such as PoW, or to provide a new consensus algorithm. In the rest of this section, we provide a review of modified consensus algorithms used in blockchain systems, categorized based on the post-quantum techniques they utilize [158].

In [323], a post-quantum consensus mechanism is introduced that replaces the traditional SHA256 hashing scheme with an NP-Hard problem and introduces a DAA to adapt the computational difficulty of blocks. The algorithm supports memory mining and incorporates an identity-based post-quantum signature for lightweight transactions. It addresses the challenge of solving Multivariate Quadratic (MQ) Equations using a system of quadratic multivariate equations over a finite field.

In [310], a modified consensus algorithm is presented, based on solving random quadratic multivariate equations over $\mathrm{GF}(2)$. This algorithm utilizes the NP-hard MQ problem and assigns multiple hash values to coefficients of multivariate polynomials during block mining. By finding a random vector, the consensus scheme progresses. The algorithm attains characteristics such as public verifiability of solutions, intrinsic hardness, difficulty adjustability and homogeneous hardness.

The paper [324] introduces GSCS, an improved consensus mechanism for decentralized Blockchain systems. GSCS utilizes Serial-Mining-Puzzle (SMP) and Mining-Credibility-System (MCS) techniques to resist quantum attacks, ensuring quantum safety. SMP prevents resource coalition, outsourced mining, and parallel mining, while MCS evaluates mining actions based on participants' credibility and records them in a blockchain.

In [320], an asymmetric consensus mechanism is proposed, focusing on achieving ASIC resistance. It tackles the generalized birthday-problem or k-XOR problem by making proof generation difficult and verification easier. The algorithm binding method prevents cost amortization and limits parallel implementations through memory bandwidth restrictions.

The paper [325] suggests a new consensus mechanism, QSYAC, which integrates YAC algorithm with an Unconditionally-Secure-Signature (USS) scheme. USS overcomes quantum threats by using hashing techniques for signature creation, while YAC operates as a consensus protocol reliant on voting. The protocol employs the Toeplitz hash message authentication code, with quantum key distribution ensuring quantum safety. It substitutes the public-key signature employed by the original YAC.

In [326], a lattice-based consensus algorithm called LPoW is proposed. It solves the NP-hard Hermite-SVP problem using lattice systems to achieve quantum safety in hash-based PoW. Different algorithms and heuristic lattice sieves with favorable quantum complexity are used. The parameters of LPoW are adjustable to fine-tune the difficulty, with higher dimensions requiring more computational resources.

The paper [327] presents ECCPoW, a consensus protocol that addresses the issue of mining centralization caused by ASICs. ECCPoW combines a low-density parity-check decoder with a hash function to achieve ASIC resistance in Blockchain systems. In TABLE XXI, we have provided the evaluation of consensus algorithms utilizing post-quantum cryptography [158].

The paper [298] presents a detailed classification of 38 consensus algorithms and 41 mainnets.

TABLE XXII: Classification of available consensus algorithms in the literature.

Failure Models	Level of Decentralization	Modes of Decision-making	Consensus Algorithms	Quantum Security	Mainnets
Crash Fault Tolerance	Centralized	-	Kafka	N/A	-
Authentication detectable Byzantine Fault Tolerance	Centralized	Feudalism	Delegated Proof of Stake (DPoS)	Voting-based, independent of computing power. Quantum version QDPoS exists [332].	EOS
					Lisk
					aelf
					Ark
					BitShares
			Raft	N/A	Quorum
			Proof of Elapsed Time	Trusted component for random wait time generating can be affected by quantum computing.	Hyperledger Sawtooth
			BFT-SMaRt	N/A	-
		Despotism	Ripple Protocol Consensus Algorithm	N/A	Ripple
		Democracy	Governance Council	N/A	Klaytn
			Masternode Proof of Stake	N/A	Ether Zero, Dash
		Liquid	Liquid Proof of Stake	Seems to be like PoS. Allows token holders to loan their validation rights without losing token ownership.	Tezos
	Decentralized	Plutocracy	Proof of Stake	Hashrate-based consensus vulnerable to Grover. Staking vulnerable to Shor's attack. Stealth uses Quantum Proof-of-Stake (qPoS) [333]. QRL has post-quantum secure Proof-of-Stake.	Ethereum
					QTUM
					Peercoin
					Stratis
			Burn and Earn Delegated Proof of Stake (B&E DPoS)	Seems to be like DPoS. Participants can burn their tokens to earn the right to validate transactions.	EOS Chrome
			Proof of Trading	N/A	F Coin
			Proof of Burn (PoB)	N/A	Slimecoin
		Oligarchy	Tendermint	N/A	Cosmos
			Proof of Authority (PoA)	Pre-selected validators or authorities validate transactions and add them to the blockchain. It is based on identity and reputation rather than cryptographic puzzles or computations.	Luniverse
			Istanbul Byzantine Fault Tolerance (IBFT)	N/A. Quantum Secured-Byzantine Fault Tolerance (QS-BFT) consensus exists [334].	-
			Asynchronous Byzantine Fault Tolerance(ABFT)	Two post-quantum asynchronous Byzantine fault tolerance (aBFT) protocols SodsBC and SodsBC++ have been proposed [335].	Hedera
			Redundant Byzantine Fault Tolerance (RBFT)	Like BFT. Multiple instances of the same BFT protocol executing on different machines. Quantum BFT raises the upper bound on the fraction of malicious nodes from $\frac{1}{3}$ to $\frac{1}{2}$ [336].	-
			Ouroboros Byzantine Fault Tolerance	Ouroboros has a mechanism called "security parameter" that can adjust the network's security to defend against quantum computing attacks as they become more powerful [337].	Cardano (Claimed quantum resistance)
		Republicanism	Proof of Brain	N/A	Steemit
			Proof of Anonymous Stake	N/A	Spectre
			Proof of Believability (PoB)	N/A	IOST
			Proof of Flow	Combines Proof of Stake (PoS) and HotStuff.	Flow blockchain
		Algocracy	Dual Delegated Proof of Stake (DDPoS)	N/A	Sigmachain
			Artificial Intelligence Delegated Proof of Stake	N/A	Velas
			Proof of Formulation (PoF)	PoF does not require excessive computing resources or depend on the amount of stake that someone possesses.	Fleta
			Proof of Performance (PoP)	It rewards participants based on their performance or contribution to the network. Quantum supremacy may be a threat.	High Performance Blockchain (HPB)
			Proof of Storage	Quantum proof of space exists [338].	Storj, Burst, Chia, SpaceMint
Byzantine Fault Tolerance	Decentralized	Socialism	Proof of Work	Based on hashrate, Grover vulnerable. Quantum versions exist [339], [340]. A PoW design in a random-beacon model exists believed to be post-quantum but not integrated into consensus protocols [341].	Bitcoin
					Bitcoin Cash
					Dogecoin
					Litecoin
			KawPoW	It is hashrate-based but developers alternate between X15 and SHA512 algorithms and is protected against ASICs.	Raven
			Ethash	ASIC-resistant.	EthereumPoW
			Cuckoo Cycle	Requiring memory-intensive PoW based on locating constant-sized subgraphs within random graphs and believed to be quantum resistant [342].	Cortex
			Dual Proof of Work	DPoW provides additional protection against 51% attacks by combining two different PoW algorithms.	Grin Coin
			Proof of Useful Work (PoUW)	Assumes solving instances of real-life combinatorial optimization (CO) problems. The potential impact of DWAVE quantum computers, which can solve certain optimization problems, should be thoroughly analyzed.	ANKR

			ProgPoW	Programmatic PoW is designed to minimize the opportunity for efficiency gains of GPUs or ASICs. For example, changes keccak with 64-bit words to 32-bit words.	-
		Anocracy	equilibrium Proof of Work	N/A	Hdac
			Spectre	N/A	Hycon
		Demarchy	Pure Proof of Stake (PPos)	Quantum resistant	Algorand (Using Falcon and state proofs makes it quantum resistant.) [343]
	Centralized	–	Practical Byzantine Fault Tolerance (PBFT)	N/A	Hyperledger Fabric (Its quantum-resistant version is PQFabric [344].)
	De-Centralized	–	Federated Byzantine Agreement (FBA)	N/A	Stellar and Ripple

TABLE XXIII
CONSENSUS ALGORITHMS IN THE LITERATURE WITHOUT A SPECIFIC CLASSIFICATION.

(Part I)

Consensus Algorithms	Quantum Security	Mainnets
Delegated Byzantine Fault Tolerance (dBFT)	N/A	NEO
Hybrid Proof of Work (HPoW)	N/A	Lynx
Proof of Work time (PoWT)	N/A	Vericoin, Verium
Delayed Proof of Work (dPoW)	More secure Compared to PoW	Komodo (Quantum Secure Blockchain integrating Dilithium)
Proof of Edit Distance	Find a hash with minimum edit distance compared to previous block. Edit distance of strings x, y can be computed in $O(n^2)$, $n = \max\{\|x\|, \|y\|\}$. Subquadratic quantum algorithm available [345].	Block Collider
ePoW: equitable chance and energy-saving	N/A	HDAC (It uses quantum random number generators.)
Semi-Synchronous Proof of Work (SSPoW)	N/A	Purple
Delegated Proof-of-Contribution (DPoC)	N/A	ICON
Secure Proof of Stake (SPoS)	Deterministic approach based on stake and rating, eliminates computational waste.	Elrond
Hybrid PBFT/Aurand	N/A	Polkadot
Proof of Stake Time (PoST)	N/A	PostCoin, Vericoin
Proof of stake Boo (PoS Boo)	N/A	SHIELD
High Interest Proof of Stake (HiPoS)	N/A	Positron, BitBean, EdgeCoin, GRAVITYBITS
Asset PoS (APoS)	N/A	MarcoPolo Protocol (MAP)
Traditional Proof of Stake / Tiered Proof Of Stake (TPOS)	N/A	XSN
Casper the Friendly Finality Gadget (FFG)	N/A	Casper the Friendly GHOST
Variable Delayed Proof of Stake (vDPOS)	N/A	CryptoCircuits
Proof of Stake Velocity	N/A	Reddcoin
Magi's Proof of Stake (mPoS)	N/A	MAGI
Leased Proof of Stake (LPoS)	N/A	NXT, Waves
Delegated Proof of Importance (DPoI)	Similar to DPoS but DPoI calculates importance score using stake, financial transfer activity, and social activity enhancing security.	U$^\circ$OS
Proof of Process	N/A	Stratum
Proof of capacity (PoC)	N/A	Signum, SpaceMint, Permacoin

(Part II)

Consensus Algorithms	Quantum Security	Mainnets
Proof of Signature (PoSign)	N/A	XBY
Proof of Retrievability (POR)	N/A	PermaCoin
Proof of Location	N/A	FOAM
Proof of Reputation (PoR)	In PoR, reputation serves as the incentive for both good behavior and block publication instead of digital coins, therefore no miners are needed. A provably secure PoR has been proposed in [346] that uses Nakamoto ledger as fallback.	GoChain
Proof of Proof (PoP)	PoP consensus protocol allows blockchains to inherit PoW security from established blockchains like Bitcoin, enabling a secure ecosystem. Like PoW, it will be affected by Grover.	VeriBlock
Proof of History	PoH utilizes time to establish an immutable and auditable record of all transactions and reduces the amount of computing power necessary to secure the network. PoH offers speed, efficiency, and enhanced security against quantum attacks [337].	Solana (It is exploring the use of post-quantum cryptography to further enhance its resistance to quantum attacks.)
Proof of Existence	Proof of Existence integrates and verifies validator identities and works in conjunction with other consensus mechanisms like PoS and PoC and enhance security.	HeroNode, DragonChain, XIDEN
Proof of Research (DPoR)	N/A	GridCoin
Proof of Weight (PoWeight)	Broad classification of consensus algorithms, centered around the Algorand consensus, including PoST and PoR.	Algorand, Filecoin, Chia
Proof of Zero (PoZ)	N/A	ZCrypt
Proof of Importance	N/A	New Economy Movement (NEM)
Proof of Care (PoC)	N/A	Quantstamp, TomoCoin
Proof of Value (PoV)	N/A	LTBcoin
Proof of Stake (POS) / Proof of Presence (PoP)	N/A	HEAT
Proof of Devotion	N/A	Nebula
HotStuff	N/A	Cypherium
LibraBFT (Variant of HotStuff)	N/A	LibraBFT
Proof of Activity	N/A	Espers, Coinbureau, Decred
Nexus Proof of State (nPoS) or Nexus Proof of Holding (nPOH)	N/A	Nexus

The classification categorizes the consensus algorithms and mainnets based on five taxonomic ranks, representing their hierarchical relationship. In their classification, the Kafka algorithm is included separately. Kafka-Streams, which is a client library for developing stream applications, utilizes fault-tolerant features native to Kafka, but in [298] it is classified as crash fault tolerance (CFT). Other consensus algorithms are classified based on their ability to solve the Byzantine generals problem and are further categorized as authentication-detectable Byzantine fault tolerance or Byzantine fault tolerance (BFT).

In authentication-detectable Byzantine fault tolerance, the decision rank represents the level of centralization. Feudalism is the most centralized, followed by Despotism, Democracy, and Liquid. Feudalism-based consensus algorithms, such as DPoS, Raft, PoET, and BFT-SMaRt, involve stakeholders exercising voting rights to elect representatives who make decisions through consensus. Examples of mainnets using DPoS include EOS, Lisk, aelf, Ark, and Bitshares. The Raft consensus algorithm maintains the same state across all nodes and ensures system functionality even if some nodes fail. It is categorized as centralized within the BFT rank. Decentralized BFT is further classified into Socialism, Anocracy, and Demarchy. Socialism employs a distributed environment where workers democratically own the means of production. PoW algorithms, such as PoW consensus, are used to validate work participation through mining and solve complex formulas to find hash values. All nodes verify and approve the hash value before storing transaction details in a block. PoW is considered the consensus method that best embodies blockchain decentralization [298]. In TABLE XXII and TABLE XXIII, we present the classification of consensus algorithms and their respective quantum security status. The quantum security column in these tables indicates whether there have been efforts to enhance or diminish the security of the consensus algorithm using quantum technology. The "N/A" entry in these tables indicates that no information regarding the impact of quantum computing on the respective consensus algorithm has been found. In Fig.5, the taxonomy of consensus algorithms is presented [45].

According to our evaluation, voting-based consensus algorithms are generally considered to be less vulnerable to quantum attacks compared to compute-Incentive-based algorithms, which are at a higher risk.

D. Exploring Additional Building Blocks of Blockchains

Apart from the components discussed earlier, there are additional integral components within blockchains. Among them, smart contracts play a crucial role. Smart contracts are self-executing agreements that incorporate predetermined rules and conditions within software code. They autonomously carry out actions and transactions triggered by predefined conditions, thereby eliminating the requirement for intermediaries. Smart contracts aim to achieve several objectives, including minimizing the reliance on trusted intermediaries, lowering arbitration expenses, mitigating fraud losses, and minimizing both deliberate and unintentional exceptions [347].

The concept of smart contracts originated in 1994 when Nick Szabo introduced it to the world. Ethereum's invention played a crucial role in the advancement of smart contracts, allowing users to deploy applications on the public Ethereum blockchain. While Ethereum initially focused on currency exchange, the Hyperledger Fabric project diverged from Ethereum's path and aimed at serving as an enterprise blockchain. Various platforms are now under development to meet the requirements of enterprises, and research is concentrated on legalizing smart contracts and exploring their position in emerging computer science research topics [347].

Blockchain-based smart contracts inherit features from the underlying blockchain, making them applicable across diverse domains. They operate in a peer-to-peer mode without requiring for a centralized third entity and ensure service availability without relying on centralization. They enable automated transaction execution based on predefined conditions. The following are the primary characteristics of smart contracts based on blockchain technology [347]:

1) Eliminating the need for a trusted third party and self-execution: Integrating a system with blockchain-based smart contracts allows for the elimination of trusted intermediaries like agents, brokers, or service providers. This removal of the reliance on a trusted third party results in reduced transaction costs, diminished centralized authority, and guarantees precision in operations without human errors or biased interventions.

2) Forge resistance and immutability: Transaction records in a distributed ledger are verified through digital signatures, ensuring the integrity of the data. Smart contract code deployed on the blockchain is also immutable, preventing tampering. The code can be updated if necessary, with agreement from the nodes in the blockchain network. This guarantees that the smart contract and its executed code are trustworthy for all involved parties.

3) Transparency: Transparency is a significant feature inherited by smart contracts from the blockchain. The code and transactions in smart contracts are transparent, allowing intervening parties and the public to inspect and verify them.

The deployment and execution of blockchain-based smart contracts involves initializing the smart contracts, installing them on the network, and connecting them with external business systems through various interfacing techniques. The blockchain network receives transactions, verifies their legitimacy, and triggers smart contract execution. Legitimate transactions are added to blocks, which are then approved by the nodes in the network based on consensus rules. Once the consensus is reached, the blocks are appended to the blockchain [347].

Scientific research on blockchain-based smart contracts has explored various technical aspects, leading to improved security, scalability, and optimal operation. In [347], the authors conduct a thorough survey with an emphasis on various technical aspects of smart contracts. They address concerns related to the privacy, security, gas cost, and concurrency of current programming languages for smart contracts. The authors provide an overview of different attacks and vulnerabilities that arise from programming errors, language restrictions,

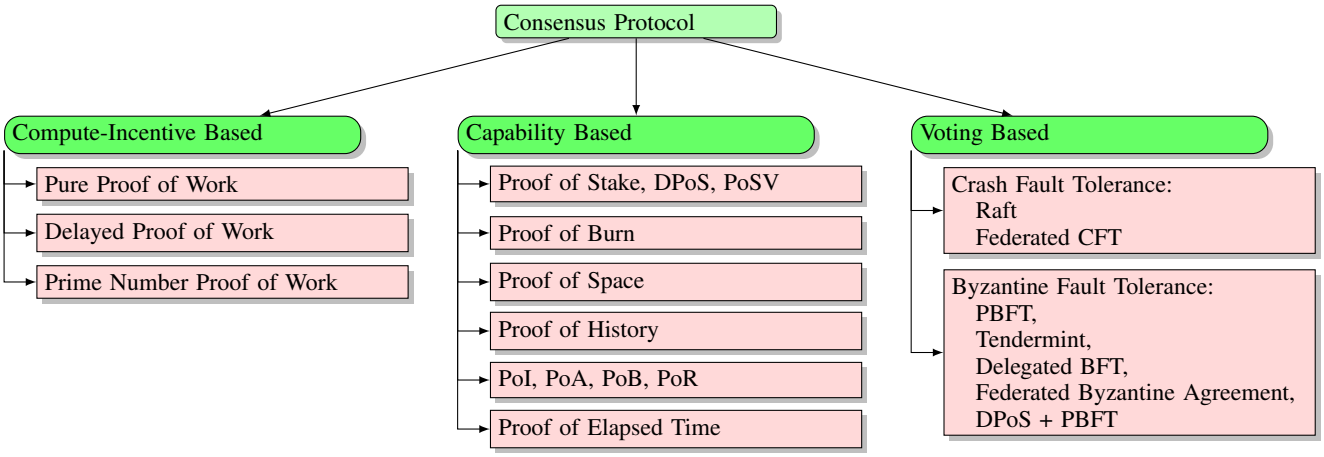

Fig. 5. Taxonomy of consensus algorithms.

and security loopholes. They emphasize that such attacks can disrupt blockchain networks, leading to accuracy issues, loss of cryptocurrency, and system unavailability. The attacks discussed include underflow/overflow errors, re-entrancy vulnerability, Sybil attacks, majority attacks, double spending attacks, exception disorder, destroyable contracts, call stack vulnerability, bad randomness, and unbounded computational power intensive operations. The authors highlight the importance of addressing these vulnerabilities to safeguard the integrity and reliability of smart contracts within blockchain networks. Furthermore, they offer potential solutions to mitigate these security concerns.

To enhance smart contract security, researchers have focused on the following key areas [348]:

1) Verification Mechanism: Establishing an automatic information verification mechanism for smart contracts is essential. This ensures that trading activities are verified according to the contract and that blockchain business data is publicly accessible. Some scholars have utilized anti-counterfeiting technology to create decentralized ledgers on each block, enabling intelligent recording of fund flows. Smart contracts can connect these distributed ledgers to verify relevant data. Researchers have also worked on improving the security of transaction information verification mechanisms, such as utilizing role-based access mechanisms to ensure security and traceability [348].

2) Privacy Protection Mechanism: Implementing privacy protection mechanisms within smart contracts is crucial. Techniques like robust control and anonymity have been employed to enhance anti-jamming capabilities and protect user privacy in payment systems. Anonymous technology has been utilized to prevent banks or blockchains from accessing users' historical consumption records. Anti-counterfeiting technology has been applied to record verification information on the blockchain, allowing public access while preserving the privacy of individual transactions [348].

3) Data Signature Mechanism: Building a robust data signature mechanism is important for secure smart contracts. Researchers have proposed schemes such as secure attribute-based and ID-based signatures to ensure safe and orderly execution of transaction processes. Multi-signature schemes have been developed to assist multiple parties in processing transactions based on predefined conditions. Additional research, including blockchain security detection models and grid-based hidden attribute signatures, has been conducted to further enhance smart contract security [348].

However, the security improvements mentioned above are based on algorithm complexity, and more secure schemes may introduce implementation burdens under quantum attack environments. To address this, [348] proposes a lightweight quantum blind signature scheme for smart contracts that does not rely on a trusted arbitrator and is unconditionally secure regardless of algorithm complexity. The scheme aims to improve the security performance of blockchain smart contracts against quantum attacks. The authors present a smart contract architecture, analyze the information processing and transmission for quantum blind signatures, introduce the lifecycle and signature rules for quantum blind signatures in smart contracts, and propose protocols for both single and multi-signer scenarios. The proposed scheme utilizes quantum entanglement characteristics and offers improved security without the need for a trusted third party. Comparison of signature algorithms used for smart contract security is provided in TABLE XXIV.

Smart contracts have diverse applications in the field of multi-party cryptographic primitives, such as secure multi-party computation, secure lotteries, and card game protocols. One major challenge faced by blockchains in achieving widespread adoption is scalability, which involves increasing transaction throughput while maintaining resource requirements and security against adversarial attacks. Current blockchain systems like Bitcoin and Ethereum can handle only a limited number of transactions per second compared to traditional financial systems like Visa [354].

In [354], the authors propose a quantum solution to the scalability problem by combining smart contracts with tools from quantum cryptography. They specifically address the scalability issue for payment transactions, not general smart contract transactions. The key quantum component used is a concept called *quantum lightning*, which builds upon the notion of collision-resistant quantum money. Quantum lightning enables the creation of quantum banknotes with unique serial

TABLE XXIV
COMPARISON OF SIGNATURE ALGORITHMS FOR SMART CONTRACT SECURITY [348].

Model	# Signatures	Security	Privacy	Dispute Arbitration	Security vs. Complexity
Security Attribute Signature [10]	Single	Relatively Safe	No Privacy Protection	Decentralization	Depends on complexity
ID-based Signature [349]	Single	Relatively Safe	No Privacy Protection	Decentralization	Depends on algorithm complexity
Multi-signature [350]	More than 2	Relatively Safe	No Privacy Protection	Decentralization	Depends on complexity
Lattice Attribute Signatures [351]	Single	Relatively Safe	No Privacy Protection	Arbitration Required	Depends on complexity
Optical Signature [352]	Single	Absolutely Safe	No Privacy Protection	Arbitration Required	Depends on complexity
Quantum Multi-signature [353]	More than 2	Absolutely Safe	No Privacy Protection	Arbitration Required	Independent of complexity
Quantum Blind Signature	More than 2	Absolutely Safe	Blind Message	Arbitration Required	Independent of complexity
Lightweighted Quantum Blind Signature [348]	Any number	Absolutely Safe	Blind Message	Decentralization	Light-weighted, independent of algorithm complexity

numbers, preventing the production of multiple banknotes with the same serial number. However, challenges such as trustless minting and deterioration of quantum states over time need to be addressed for a practical implementation of such a quantum money scheme [354]. To tackle these challenges, the authors leverage smart contracts to provide a mechanism for minting money, validating serial numbers, and addressing the issues associated with deteriorating quantum states. This represents the first application of smart contracts in conjunction with quantum tools, and it suggests the potential for smart contracts to find further utility in quantum cryptography. The authors propose that classical blockchains and smart contracts can serve as valuable primitives not only in classical cryptography but also in quantum cryptography. They present a hybrid classical-quantum payment system that combines a classical blockchain capable of handling stateful smart contracts with quantum lightning as a means of implementing decentralized and efficient payments while ensuring the recovery of lost value in case of damaged or lost quantum banknotes.

The advantages of smart contracts are attributed to the infrastructure provided by existing blockchain platforms. While procedural languages are commonly used, logic-based languages offer several advantages over the procedural approach. These advantages, as highlighted in [355], include:

1) Formal Verification: Logic-based programs (smart contracts), are more appropriate for formal verification compared to procedural programs. For procedural programs, it is common practice to construct a formal calculus with precise semantics and represent a program as a collection of expressions within that calculus. Logic itself serves as a formal calculus, eliminating the requirement for adaptation to different systems and simplifying the verification process [5,6].

2) Compactness: Logical contracts are typically more concise than their procedural counterparts. They focus solely on what needs to be accomplished without specifying how to achieve it.

3) Error-Prone Reduction: Expressing contracts in a logical language reduces the likelihood of errors as they closely align with user-friendly specifications, unlike procedural programming languages [7].

The authors of [355] conduct investigations into the utilization of logic and logic-based programming in designing smart contracts, starting from the logic-based programming language employed by the Logicontract (LC) framework [325]. They expand upon the logical framework utilized in Logicontract using answer-set-programming (ASP), a contemporary method for declarative logic-based programming. By utilizing ASP, the authors are able to develop several intriguing smart contracts. The precisely defined syntax and semantics of the ASP language contribute to the contracts' enhanced understandability and formal verifiability.

The study assumes a permissioned-blockchain which is quantum-secured, such as LC, as the underlying blockchain framework. Specifically, it assumes the presence of a quantum communication network where each node is a classical computer. Although having quantum computers as nodes provides unconditional security for certain problems like voting, lotteries, and auctions, the research focuses on solving a wide range of interesting problems on a blockchain secured against quantum technology but operated by classical computers. Nodes are linked via quantum and classical channels, facilitating the establishment of unconditionally secure keys between each pair of nodes. Nodes also act as participants in transactions, where the sender of each transaction signs it using a signature scheme based on quantum key distribution, ensuring unconditional security. Each node retains a record of entire transactions, and the blockchain's consensus mechanism guarantees consistent transaction records across different nodes.

In the current implementation of LC, there is only an Unconditionally-Secure-Signature (USS) without a public-key signature. Whereas USS effectively protects messages exchanged between different nodes, it poses challenges in protecting distinct users on the identical node. To address this limitation, the authors of [355] integrate cryptographic techniques for the post-quantum era, like public-key signature schemes based on lattices [312], [356], [357], [357], into ASP. This integration enables users of a node to distinguish themselves from others using their unique public-keys. The inclusion of post-quantum cryptographic primitives enhances the power of the logical language beyond ordinary ASP. The authors validate the practical feasibility of this approach through recent experimental work by Wang et al. [358], which demonstrates the effectiveness of a quantum communication network secured using post-quantum cryptographic authentication.

The instances provided in this section serve as examples showcasing the impact of quantum technology on smart contracts, which are essential components of blockchains. However, it is important to note that the literature contains numerous additional contributions in this field.

VII. Quantum Attack Surface of Blockchains

While blockchain technology has garnered considerable attention and is undergoing exploration in diverse fields, it is crucial to comprehend its weaknesses, especially those pertaining to security. To address the research questions and identify potential solutions to blockchain problems using quantum computing, researchers have divided them based on different layers of the blockchain, each with different security requirements. By doing so, we gain insights into the specific challenges and issues associated with each layer which are summarized here [157]:

1) Hardware and infrastructure layer: This layer focuses on the creation of virtual resources such as storage, networks, and servers. Nodes, which are hardware devices connecting to the network, play a vital role in achieving consensus in the blockchain. Improvements at the infrastructure level are necessary to ensure the proper implementation of quantum or post-quantum blockchain.

2) Data layer: This layer involves the storage and management of blockchain data. Different blockchain types have varying data requirements. Blockchain networks add data to the blockchain once consensus is reached among nodes. Digital signatures and hash functions ensure data integrity and security. However, quantum attacks pose a significant threat to this layer due to the reliance on cryptographic algorithms vulnerable to quantum computers.

3) Network layer: This layer handles communication and propagation of blocks, transactions, and information among nodes. Nodes in a peer-to-peer network collaborate to achieve common goals. The use of quantum networks in this layer can enhance security and facilitate secure interactions and synchronization among nodes.

4) Consensus layer: The consensus layer ensures that transactions are validated according to established rules and that blocks comply with those rules. Consensus mechanisms have a pivotal role in preserving the integrity and synchronization of blockchain networks. However, quantum computers can exploit vulnerabilities in this layer, such as searching for hash collisions or quickly mining blocks, which may enable attackers to modify the blockchain undetected.

5) Application layer: This layer encompasses chaincode, smart contracts, and decentralized applications (dApps). Smart contracts are automatically executed when specific events or conditions are met. dApps, running on a blockchain network, provide user privacy, developer independence, and lack of censorship. Quantum-resistant smart contracts become crucial to maintain their security, as quantum computers could potentially manipulate or modify deployed smart contracts.

By organizing the challenges and solutions according to these layers, [157] identifies the vulnerabilities and risks that arise in each layer of the blockchain ecosystem when quantum computing becomes practical. TABLE XXV presents various types of attacks categorized by their respective layers in the blockchain architecture. Each layer represents a different aspect of the blockchain system, and the attacks listed highlight the vulnerabilities and potential threats within each layer [55]. Previous surveys have also examined the attack surface of blockchains, but they have certain limitations. Some surveys focused on specific blockchain applications like Bitcoin, Ethereum, and Monero, evaluating their robustness against popular attacks without exploring countermeasures [26], [49], [317], [359]. Others discussed the use of blockchain for providing security services or analyzed specific applications like smart contracts [360]. The study [23] systematically analyzes different attack vectors, explores their relationships, and surveys countermeasures and defenses against these attacks. By addressing these challenges, the research aims to contribute to the design of more secure and robust blockchain solutions [23] .

TABLE XXV
Attacks on blockchains by layer.

Layer	Attack Name
Data Layer	Malleability attack, Replay attack, Time Hijacking attack, Fault injection attack, Quantum attack, Upgraded attack, Modification attack
Network Layer	51% attack, DDoS attack, Eclipse attack, Sybil attack, Phishing attack, Blockchain ingestion attack, BGP Hijacking attack, Liveness attack, Man-in-the-middle (MITM) attack, Routing attack
Consensus Layer	Double spending attack, Cryptojacking attack, Stake bleeding attack
Incentive Layer	Block withholding attack, Selfish mining attack, Refund attack, Balance attack, Bribery attack
Smart Contract Layer	Mishandling exceptions attack, Integer overflow attack, Gas cost attack, Re-Entrancy attack, Timestamp dependency attack, Criminal smart contract attack, Transaction ordering dependency attack, Short address attack
Application Layer	Money laundering attack, Private-key compromise attack, Location cheating attack, Collusion attack, Ballot stuffing attack, Badmouthing attack, Guess attack, Linking attack, Impersonation attack, Chosen ciphertext attack

In contrast to other surveys, this work goes beyond the existing literature by specifically examining the quantum effect on existing attacks and their implications. While previous surveys have analyzed various attack vectors and countermeasures in blockchain systems, this research takes it a step further by considering the potential impact of quantum computing on these attacks. By incorporating the quantum perspective, the study provides valuable insights into the vulnerabilities and risks that may arise in blockchain systems in the era of quantum computing.

In TABLE XXVI and TABLE XXVII, we have provided an overview of attacks on blockchains and their implications in presence of quantum computing.

VIII. Examining Existing Solutions

Quantum computers are currently not powerful enough to break existing encryption schemes, but advancements are expected within the next two decades. However, noise and error accumulation pose significant challenges in quantum calculations, limiting the number of qubits and the size of factored integers [234].

Specialized mining hardware in cryptocurrencies outperform early quantum computers. Grover's algorithm can break hashing algorithms with fewer tries than classical computers, but the required number of qubits is currently unattain-

TABLE XXVI
OVERVIEW OF ATTACKS ON BLOCKCHAINS AND THEIR IMPLICATIONS IN THE ERA OF QUANTUM COMPUTING (PART 1).

Attack Surface	Attacks	Affected Components/Explanations	Implications	Quantum Impact
Blockchain Structure	Forks	Blockchain	Chain Splitting, Revenue Loss	Forking can increase or decrease security. For example Bitcoin is exploring the possibility of implementing a hard fork to introduce quantum-resistant. The chances of finding a fork grow as a quadratic function in terms of applied number of Grover iterations [361].
	Orphaned blocks	Blockchain, Miners, Mining Pools	Revenue Loss	No information disclosed
Peer to Peer System	DNS hijacks	Miners, Mining Pools, Exchanges, Users	Revenue Loss, Partitioning, Theft	DNS Security Extensions (DNSSEC) use digital signatures and are vulnerable to quantum threat.
	BGP hijacks	Miners, Mining Pools, Users	Revenue Loss, Partitioning, Theft	Border Gateway Protocol (BGP) is insecure and susceptible to hijacking attacks. RPKI with network routes signing is an attempt to enhance security, but current signatures are vulnerable to quantum attacks [362].
	Eclipse attack	Miners, Users	Partitioning	No information disclosed
	Majority attack	Blockchain, Miners, Application	Chain Splitting, Revenue Loss, Malicious Mining	Quantum computers could be used to launch a majority attack on a blockchain.
	Selfish mining	Blockchain, Miners, Mining Pools	Revenue Loss, Malicious Mining	It is suggested to change Bitcoin protocol by requiring quantum miners to decide the Grover iterations upfront [361], but it clashes with proposed fixes for selfish mining insecurities [363].
	DDoS attacks	Blockchain, Miners, Mining Pools	Malicious Mining, Theft	Researchers have proposed using quantum computing to detect and prevent DDoS attacks [364].
	Consensus Delay	Miners, Mining Pools, Users	Delay, Info Loss	Quantum computers can potentially reduce consensus time in blockchains and delay depends on the consensus algorithm and quantum computational power.
	Block Withholding	Miners, Mining Pools	Revenue Loss, Malicious Mining	No information disclosed
	Time jacking attacks	Miners, Mining Pools, Application	Chain Splitting, Revenue Loss, Malicious Mining, Delay	No information disclosed
	Finney attacks	Miners, Mining Pools, Users	Revenue Loss	Quantum computers have the potential to affect Finney attacks, which involve a dishonest miner creating a forged transaction (forge signature) and block with a 50% chance of their block being accepted as the valid chain. This attack is a form of double-spending [365].
Blockchain Application	Blockchain Ingestion	Blockchain	Info Loss	No information disclosed
	Wallet theft	Exchanges, Application, Users	Revenue Loss, Theft	Wallet security is related to digital signatures, this is where quantum computers pose a more realistic threat [366].
	Double-spending	Blockchain, Users	-	Quantum computers can simultaneously make multiple attempts at finding the hash and gain the authority to validate a transaction. This introduces the risk of potential double-spending attempts [367].
	Cryptojacking	Application, Users	Chain Splitting, Malicious Mining, Theft	No information disclosed
	Smart contract DoS	Blockchain, Application, Users	Revenue Loss, Delay, Theft	No information disclosed
	Reentrancy attack	Application, Users	Revenue Loss, Theft	No information disclosed
	Overflow attack	Application, Users	Theft	No information disclosed
	Replay attacks	Blockchain, Mining Pools, Application, Users	Revenue Loss, Info Loss	Quantum cryptography can solve replay and passive attacks [368].
	Short address attacks	Application, Users	Revenue Loss, Theft	No information disclosed
	Balance attacks	Application, Users	Revenue Loss, Theft	No information disclosed

able. Increasing the hash length or altering the consensus in blockchain networks can mitigate these risks [234]. Furthermore, there are additional solutions that should be taken into account to enhance the security of blockchains against quantum threats.

Post-quantum cryptography aims to develop quantum-resistant algorithms for encryption and digital signatures. Until recently, NIST had been evaluating different algorithms for standardization, with lattice and hash-based algorithms considered suitable options [234]. Alternative proof-of-work algorithms and secure key generation practices can reduce vulnerabilities to quantum computers. Preventing the reuse and exposure of public-keys is also crucial to mitigate brute-force attacks [234]. In another direction of research, Quantum cryptography, based on the laws of physics, provides unbreakable security against quantum computers. Quantum key distribution enables secure key sharing, while quantum secure direct communication (QSDC) allows for secure message sharing without a secret key. However, scalability and network size remain challenges for quantum cryptography [234].

Quantum blockchains and quantum cryptocurrencies have emerged as innovative approaches that harness quantum features to enhance security. The establishment of ground-to-satellite communication is of paramount importance for the development of potential global quantum networks. Moreover, quantum cryptocurrencies make use of the no-cloning theorem to guarantee secure transactions and minimize the blockchain's size, as highlighted by Kappert et al. [234]. In the remainder of this section, we present specific examples that align with each research direction.

TABLE XXVII
OVERVIEW OF ATTACKS ON BLOCKCHAINS AND THEIR IMPLICATIONS IN THE ERA OF QUANTUM COMPUTING (PART 2).

Attacks	Affected Components/Explanations	Implications	Quantum Impact
Brute Force	Computing Power	Data Encryption	A brute force attack can be targeted at various components, such as private-keys, wallet addresses, or even consensus algorithms. Quantum computers can perform certain calculations much faster.
Refund	Payment Protocol	Lose Reputation	Refund attacks exploit verification vulnerabilities and unsecure transaction links. Quantum attackers can manipulate transaction details, complicating the identification of legitimate refund requests from fraudulent ones.
Long Range	Database	Changes the Transaction History	Long Range Attack is a threat to PoS consensus, similar to the 51% attack in PoW. An adversary with a significant stake in the token balance can take advantage of quantum computing's ability to break cryptographic algorithms used in securing past transactions and deceive nodes by creating a false chain starting from the Genesis block. This false chain appears indistinguishable from the real chain, allowing the adversary to take over the blockchain and potentially manipulate transactions.
Sybil	Network	Pseudonymous Identities	Sybil attacks involve creating multiple fake identities to gain control over a network. In blockchain technology, digital identities are used to verify transactions. Verifiable Anonymous Identities have been proposed to prevent fake identities, relying on zero-knowledge proofs and public-key cryptography [369]. However, their quantum security analysis must be taken into account due to the potential impact of quantum computing on these cryptographic mechanisms.
DAO	Computing Power	Fake Transaction	The DAO, a decentralized autonomous organization built on Ethereum, aimed to revolutionize venture capital through blockchain technology. However, it was hacked within months of its launch, resulting in the loss of $60 million worth of Ether. The attack exploited a vulnerability in The DAO's smart contract, known as a reentrancy attack. The Ethereum community responded by implementing a hard fork to reverse the attack and return the stolen funds. This led to the creation of two separate Ethereum blockchains: Ethereum and Ethereum Classic. The DAO attack was primarily a result of a code vulnerability rather than a quantum-related vulnerability.
Nothing at Stack	Block	Slow Consensus	The nothing-at-stake problem is a theoretical security hole in PoS systems. The problem can occur anytime there is a fork in the blockchain [370]. Since Grover iterations can increase the chance of forking [361], it can increase the chance of Nothing at Stack.
Pool Mining	Block	Slow Verification Time	Hash rate advantage could allow the quantum-powered pool to mine blocks faster and earn a higher proportion of the block rewards which is against the decentralization in blockchain . Quantum computers may pose a threat by breaking the cryptographic mechanisms used to secure the communication channels and authentication protocols between the pool participants.
Spam	Network	Slow Transaction Network	Spam attacks involve overwhelming the network with a large number of illegitimate transactions, causing congestion and slowing down transaction processing. With quantum computing, attackers can leverage its computational power to generate a significantly larger volume of spam transactions compared to traditional computing methods.
51% attack	A single entity or organization controlling 50% or more of the hashing rate computation power, leading to the attacker consistently winning mining.		An unexpected quantum speedup could, if hidden, lead to vast centralization of mining and possible 51% attacks [371].
Liveness attack	Attacks causing delay, preparation, and denial of target transaction acknowledgment. The attacker aims to establish an isolated blockchain and slow down transaction growth rate.		No information disclosed
Transaction malleability	Attack on transaction signature to sabotage the transaction and render it invalid.		By compromising the integrity of transaction signatures like ECDSA, quantum computers could enable attackers to manipulate and render transactions invalid. This poses the potential threat of transaction malleability in the era of quantum computing [372].
The middle protocol attack	Attacks on smart contracts and node communication, utilizing network communication attacks (e.g., Sybil, eclipse, DDoS) and compromising user privacy.		No information disclosed
Attack of consensus excitation	Attacker tampering with block consensus outcome, employing block withholding, selfish mining attacks, and pool hopping for generating additional proceeds.		No information disclosed

A. Post-quantum Blockchains

The use of ECDSA in blockchain involves the calculation of a public-key from a private-key using a one-way function. This function makes it computationally easy to derive the public-key, but reversing the process to obtain the private-key is extremely difficult due to the mathematical complexity of solving discrete logarithm problems. However, the security of ECDSA can be compromised by quantum computers using Shor's algorithm, which can break the underlying cryptographic assumptions. As a result, there is a demand for quantum-resistant signature algorithms [24].

Another aspect to consider is the security of addresses in blockchain. The use of hash functions ensures that it is mathematically infeasible to drive the public-key from a given P2PKH address. However, when funds are sent from a P2PKH-address, its public-key is exposed during transaction verification, making it vulnerable to quantum attacks. Approximately 25% of all Bitcoins have addresses that could potentially suffer from such attacks [24].

To address the impact of quantum computing on blockchain, the community started to explore post-quantum cryptography. Research efforts are focused on applying post-quantum cryp-

tography to build robust and quantum-resistant blockchains. This would require a hard fork, such as the development of a new blockchain version, which implements the new post-quantum cryptography protocol [24].

For instance, Ethereum developers face a challenge as their current PoS protocol relies on a signature scheme called BLS, which is efficient but vulnerable to quantum computers. The quantum-resistant alternatives, although more secure, are not as efficient. The use of "KZG" commitment schemes in Ethereum is known to be vulnerable to quantum attacks. Currently, this is addressed through trusted setups where multiple users generate randomness that cannot be reverse-engineered by quantum computers. However, the ideal solution would be to incorporate quantum-safe cryptography directly. Two promising approaches, STARK-based and lattice-based signing, are being researched and prototyped as potential replacements for the BLS scheme, aiming to achieve both efficiency and quantum resistance [373]. In [374], the authors introduced modifications to the Ethereum platform. They implemented a multivariate-based cryptosystem known as the Rainbow signature scheme and conducted an efficiency comparison with the existing version of Ethereum.

Blockchain is a subclass of a wider family, namely distributed ledger technologies (DLTs). DLTs can be classified based on various factors, including their data structures, consensus algorithms, permissions, and whether they involve mining. In terms of data structures, DLTs range from linear structures like blockchains to more intricate structures like directed acyclic graphs (DAGs) and hybrid approaches. Consensus algorithms in DLTs include compute-incentive-based and capability-based approaches like PoW and PoS, along with DAG-based consensus-building and voting algorithms. DLTs can also generally be categorized as either permissioned (private) or permissionless (public). PoW-based cryptocurrencies can be further categorized as mined or non-mined, with the latter referring to cryptocurrencies that are typically pre-mined, such as XRP or IOTA. PoS-based cryptocurrencies, such as Cardano or Solana, do not rely on miners but instead validate transactions among cryptocurrency owners. DLTs based on DAG data structures or hybrid blockchain-DAG approaches offer advantages such as reduced transaction data size, lower transaction costs, and faster transaction speeds. Examples of DAG-based DLT cryptocurrencies include IOTA and HBAR (Hedera Hashgraph). IOTA is a post-quantum blockchain, identified as the leading DAG-based blockchain protocol [291], serves as a scalable and publicly accessible distributed ledger specifically designed for IoT. IOTA implements Tangle technology, which adapts the DAG structure to facilitate decentralized storage of immutable and transparent data/transactions within a distributed network [375]. Tangle also encompasses the necessary capabilities to establish micro-payment protocols between machines [375]. In the IOTA network, all nodes maintain a copy of the Tangle and collectively agree on its content through consensus. Additionally, IOTA employs one-time signatures that are resilient to quantum computers, thereby ensuring robust security [60]. DAG-based blockchains offer enhanced throughput without transaction costs. In contrast to traditional blockchains like Bitcoin, DAG-based blockchains eliminate the need for miners and remain resilient against attacks from quantum computers. Nevertheless, DAG-based blockchains exhibit certain limitations. They are susceptible to double spending attacks, and several DAG-based blockchains, such as IOTA, rely on statistical analysis, like Monte Carlo simulations, for transaction confirmation. However, there is a lack of analysis to determine the required number of sample simulations for a given transaction confirmation [60].

In [376], the authors focused on the integration of secure cryptographic primitives into blockchain technology through the advancements in PQC. It explores the influence of quantum computing on blockchains and examines the integration of PQC primitives into different blockchain platforms. It presents the state-of-the-art in PQC, covering PQC signing algorithms, public-key PQC cryptosystems and NIST's 3rd round PQC candidates. It highlights the blockchain-platforms that endorse PQC primitives and conducts a performance comparison of PQC primitives that made it to the 3rd round of the NIST's call and discusses the resilience of PQC algorithms against various cryptographic attacks.

In [152], the authors provide a comprehensive survey of blockchain schemes in the context of the post-quantum era. They begin by presenting an overview of the algorithms and procedures that have advanced quantum computing and the different categories of post-quantum cryptosystems. The paper also includes a discussion on the current state of quantum capabilities and their impact on the need for post-quantum research. Furthermore, the authors provide an introduction to the fundamentals of blockchain technology and the security primitives currently employed. They analyze the most prominent cryptocurrencies based on their market capitalization, considering the potential threats posed by quantum computing. Lastly, the paper reviews proposals for post-quantum blockchain (PQB) schemes, highlighting their significance in addressing quantum-related challenges.

In another research [156], a unique analysis of the relationship between blockchain post-quantum security, law, and the creation of money is conducted. It challenges conventional assumptions about blockchain's decentralizing impact and argues that it fails to offer a legal and secure peer-to-peer payment system. It also explores the implications of post-quantum computing on blockchain security.

The available evidence suggests that numerous blockchains have taken proactive measures to enhance the security of their networks against quantum threats. They have accomplished this by implementing unique and customized post-quantum solutions. In TABLE XXVIII, the provided list showcases available post-quantum blockchain projects. In the sequel, we present several examples of the application of post-quantum blockchains.

In [377], the authors address the fundamental transition from the pre-quantum era to the post-quantum era by proposing a framework for achieving quantum-resistant decentralization within blockchain. Their approach leverages polynomial-based lattices for identity-based-encryption (IBE) and employs aggregate-signatures for consensus, ensuring effectiveness and appropriateness for post-quantum blockchain applications. The

TABLE XXVIII
POST-QUANTUM BLOCKCHAIN PROJECTS.

Project	Brief Explanation	Website
Quantum Resistant Ledger (QRL)	A blockchain platform designed to be resistant to quantum attacks, utilizing the XMSS signature scheme.	https://theqrl.org/
Hcash (HyperCash)	A blockchain platform focused on privacy and interoperability, aiming to incorporate post-quantum technology.	https://h.cash/
Nexus	A blockchain platform with quantum-resistant cryptography and multidimensional chain structure.	https://nexus.io/
QAN Blockchain Platform	A blockchain platform providing quantum-resistant cryptography and scalable infrastructure.	https://qanplatform.com/
Hashgraph	A distributed ledger technology utilizing a DAG for consensus.	https://www.hedera.com/
Aidos Kuneen	A privacy-focused blockchain platform aiming to incorporate post-quantum cryptography for security.	https://aidoskuneen.com/
IOTA	A distributed ledger technology utilizing the Tangle, exploring post-quantum cryptography solutions (uses WOTS).	https://iota.org/
Ouroboros	The consensus protocol used by the Cardano blockchain, researching post-quantum cryptography solutions.	https://cardano.org
Algorand	Algorand is an open-source quantum-resistant blockchain.	https://algorand.com/about/
Solana	Solana is exploring the use of postquantum cryptography to further enhance its resistance to quantum attacks.	https://solana.com/validators/
Komodo	Quantum secure blockchain integrating Dilithium signature.	https://komodoplatform.com/en/
Bitcoin Post-Quantum	It uses hash-based XMSS signature scheme, post-quantum zero-knowledge proofs and quantum resistant PoW algorithm Equihash96x3.	https://bitcoinpq.org/
Abelian	Abelian is a post-quantum privacy-preserving blockchain network, which adopts the NIST standardized lattice-based cryptography, and is cryptographically proven secure. Its cryptocurrency ABEL is also anonymous and untraceable.	https://www.abelian.info/home/
Corda	Corda uses BPQS signature (BPQS is essentially an adapted version of the XMSS scheme, utilizing a single path of authentication, i.e., it is based on a chain and not a tree) which makes it a post-quantum-enabled blockchain.	https://corda.net/
PQFabric	The initial release of the Hyperledger Fabric enterprise-grade permissioned blockchain introduces hybrid signatures, combining quantum-resistant and classical digital signatures. The creators conducted performance evaluations of their PQ-Fabric system, comparing it with various NIST candidates and alternatives, such as Dilithium-2, Falcon-512, Dilithium-3, Falcon-1024, Dilithium-4, and qTesla-p-I.	[279]

authors conducted experiments to evaluate their proposed approach, considering factors such as delay, throughput, energy consumption, and complexity.

In [378], the authors propose a cryptocurrency scheme based on a post-quantum blockchain. The authors first propose a signature scheme based on lattice problems. They utilize a lattice basis delegation algorithm for secret key generation, which involves choosing a random value, and employing a preimage sampling algorithm for message signing. Additionally, they introduce the concept of a double-signature, consisting of the first and last signatures, to minimize the correlation between the signature and the message. Next, the authors combine the suggested signature scheme with blockchain technology to construct the post-quantum blockchain and present their cryptocurrency scheme. The security of this scheme is reduced to the lattice short-integer-solution (SIS) problem. Using investigation, the authors demonstrate that compared to previous signature schemes, the signature and secret key sizes in their scheme are relatively shorter, resulting in decreased computational complexity.

In [379], the authors address the emerging security challenges posed by quantum technologies and the increasing need for data sharing in the IoT domain. They introduce a blockchain-based system specifically designed for sharing data securely in the post-quantum age. Their system utilizes a private blockchain to facilitate sharing data among several organizations while ensuring regulatory and compliance necessities are met. The authors put the suggested framework into practice by employing three blockchain networks, namely Ethereum, Quorum, and Hyperledger Fabric. The authors have considered NTRU as their quantum-secure cryptographic scheme to analyze and contrast the parallelization efficiency of Karatsuba's and Toom-Cook's computational approaches.

In [335], the authors present a new framework for an asynchronous permissioned blockchain that offers high performance and post-quantum security. Their framework includes two quantum-secure aBFT protocols, SodsBC and SodsBC++. They utilize concurrent preprocessing to accelerate the preparation of cryptographic objects needed for the consensus process. These objects resist quantum attacks and include random coins, encryption keys, and hash values. The authors evaluate their protocols against competitors in a typical setting with 100 participants and 20,000 transactions per block. The results show that SodsBC and SodsBC++ outperform quantum-sensitive competitors, reducing latency by 53% and 6%, respectively.

In [380], the authors propose a post-quantum blockchain with segregation witness. This approach aims to improve throughput by reducing the proportion of signatures in the block size. By leveraging the hardness assumption of SIS problem, they demonstrate the existential unforgeability of their proposed scheme against adaptive chosen-message attacks in the random oracle model. The authors emphasize that their scheme offers better performance in terms of handling capacity compared to existing solutions.

In [381], the author introduces the concept of Social Internet of Things (SIoTs), which combines IoT technology with social networks. Existing SIoT systems are centralized and fail to adequately protect user security and privacy. To address these challenges, the author proposes a privacy protection system based on post-quantum techniques. The proposed system includes a post-quantum ring signature scheme and a post-quantum blockchain system. The ring signature scheme is built on multivariate polynomials, providing improved privacy

protection in SIoTs by leveraging a security approach based on solving multivariate quadratic equations. The post-quantum blockchain, built on the ring signature scheme, offers enhanced security against both traditional and quantum computers.

In [382], the authors explore the utilization of post-quantum blockchains in the context of smart grids. These grids rely on data collected by sensors to facilitate informed decision-making. However, the current systems are centralized and raise privacy and security concerns among multiple users. To address these challenges, the authors propose a blockchain architecture for smart grids, leveraging ring signatures to ensure security in the post-quantum era.

In [383], the authors propose a lattice-based blockchain infrastructure for artificial intelligence that is quantum-resistant. Their infrastructure addresses the issue of throughput by utilizing a lattice-based aggregate signature, which efficiently reduces the proportion of signatures in the block size. The proposed scheme is proven to be secure in the random oracle model and demonstrates better efficiency compared to similar schemes.

The authors of [384] propose a lattice-based redactable consortium blockchain scheme that allows for the rewriting or repeal of block content. This scheme employs a consensus-based election mechanism and utilizes a lattice-based chameleon hash function. With the knowledge of a secret trapdoor, participants can efficiently find hash collisions, enabling them to edit the blockchain's history. Each member of the consortium blockchain is granted the right to modify the content. This approach addresses the increasing demand for post-quantum security in blockchain applications.

B. Quantum Blockchains

The utilization of quantum mechanics properties can be employed not only to exploit blockchain but also to safeguard it from quantum computers. Unlike post-quantum cryptography, which relies on software, quantum cryptography takes a hardware-based approach. This renders it invulnerable to quantum computers as it is rooted in the laws of physics rather than computational assumptions. Quantum cryptography encompasses various methods for secure message transmission, including QKD, QSDC, QSS, and QDS. QKD, for instance, focuses on securely generating and sharing keys in a network, offering advantages such as the production of random, unbreakable keys and perfect forward secrecy. Furthermore, the measurement-disturbance principle in quantum physics ensures that eavesdroppers are immediately detected when attempting to intercept a connection. QKD employs a quantum channel to establish a pre-shared symmetric key between two parties, enabling subsequent message exchange over a classical channel inaccessible to others. However, QKD is currently limited to small-scale networks. QSDC, on the other hand, involves message sharing without a secret key, employing encryption methods like Kak's three-stage protocol [150].

In 2018, Ikeda and Kazuki developed a peer-to-peer quantum cash-system that employed quantum digital signatures [385]. Similarly, in 2018, Kiktenko *et al.* introduced a quantum-secured blockchain by incorporating QKD in place of digital signatures typically used in classical blockchains. They also proposed a decentralized method for generating blocks [386]. In 2019, Rajan and Visser proposed a method called quantum blockchain, aiming to protect blockchain from hacking using quantum computers [387]. They applied entanglement for applications involving time and space and introduced a hardware composition for the quantum computer. The authors presented a framework for a quantum blockchain that facilitates the incorporation of reusable modules to develop quantum blockchain applications. The framework emphasizes characteristics like transparency, consistency, availability, confidentiality, and performance. They explored architectural patterns, with a layered approach for building computational components and securing mechanisms for transactions in the quantum blockchain. The architectural patterns involve the physical layer responsible for quantum network device interaction, the link layer for generating network states, the network layer for enabling interconnected network states, the transport layer for qubit transmission, and the application layer for quantum network applications and message exchange. To support their framework, considering both hardware functionality and software components is crucial, and the authors emphasize the need for tools to support quantum computing, such as simulators, resource estimators, optimization tools, and verification tools.

While quantum cryptography provides a general solution, there have been specific proposals for quantum blockchains and quantum cryptocurrencies. However, the implementation of these proposals is constrained by the current limitations of quantum networks in terms of size. Ground-to-ground and ground-to-satellite communication are the two key approaches for key distribution, with ground-to-satellite QKD being the potential means for realizing global quantum networks. As for quantum cryptocurrencies, they leverage the concept of quantum blockchain and exploit the no-cloning theorem, ensuring the impossibility of duplicating a quantum state. This property serves as a built-in copy protection mechanism, guaranteeing secure transfer of coins without the need for transaction storage and verification. By storing key-value pairs matching a coin's serial number to the user's public-key, the blockchain's size can be significantly reduced compared to traditional cryptocurrencies [150].

In order to enhance comprehension of quantum blockchain, it is important to grasp the concept of quantum consensus. The definition of consensus for quantum systems must consider the inherent variations between classical and quantum networks. Whereas we can define quantum consensus by employing its classical counterpart, we need to consider the stochastic nature of quantum measurement [300]. In a study by the authors [388], a systematic exploration of consensus in quantum networks was conducted. They have categorized quantum consensus algorithms into four classes: reduced state consensus, σ-expectation consensus, symmetric state consensus, and single σ-measurement consensus, utilizing symmetries and invariants of the system for their definitions. These definitions can be applied to classical random-variables or probability distributions of state-values, aligning with the principles of classical consensus. The authors also identified hierarchies

within their definitions and explored the implications arising from them. Furthermore, they discussed methods for detecting consensus in quantum networks, highlighting the challenges introduced by entanglement and the need to consider the impact of permutations on the overall state [300].

Researchers have put forward quantum protocols and algorithms for achieving consensus across quantum networks. These approaches can be categorized into four groups, each leveraging a specific quantum mechanical feature to attain consensus [300]:

- Invariance of state in relation to permutations,
- Correlations arising from entangled-states,
- State evolution through quantum measurements,
- Evolution of states through QKD protocols.

Recently, a new group of quantum consensus approaches has emerged, drawing inspiration from classical consensus methods, such as QDPoS or QPoW.

1) Symmetric-state consensus: Researchers have explored various aspects of symmetric-state consensus in several papers. Shi *et al.*, in [389], [390], [390], focus on achieving consensus on symmetric-state in a quantum network. They utilize a Lindblad master equation [391] to depict the network's state evolution, employing continuous-time swapping operators. Additionally, they establish a correspondence between quantum consensus involving n qubits and a consensus process within a classical graph. In another work, Mazzarella *et al.* introduce a quantum gossip-type mechanism in [388], which achieves convergence to symmetric-state consensus states while preserving the expected values of permutation-invariant observables. Meanwhile, Takeuchi *et al.* explore the feedback control of quantum networks in a distributed way using local quantum observation and feedback [392]. They demonstrate that quantum consensus algorithms can generate W-state entanglement. Jafarizadeh [393] investigates the optimization of the rate at which a quantum consensus algorithm converges within a quantum network with n qudits. Ticozzi [394] introduces two algorithms that enhance the gossip-like consensus and offer a new dynamic for quantum consensus. These algorithms aim to achieve consensus on statistical properties rather than individual local measurements. The first algorithm improves the purity of the output state while ensuring symmetric-state consensus, while the second algorithm strives for an outcome more akin to classical consensus, where subsequent measurements in different subsystems yield the same outcome.

2) Entanglement-based Consensus: Quantum consensus algorithms have been investigated and compared with classical consensus algorithms, particularly in the context of the Byzantine Generals Problem, which deals with faulty participants in the consensus process. Quantum properties have shown potential in enhancing classical results and addressing problems that were previously considered unsolvable. The authors of [395] presented a fast quantum Byzantine agreement algorithm. Their algorithm, combining classical and quantum channels, achieves Byzantine consensus within $O(1)$ expected communication rounds, even against powerful dynamic adversaries. It can tolerate up to $n/3$ faulty participants in synchronous systems and as much as $n/4$ faulty participants in asynchronous systems. Another algorithm is proposed in [396] for the same problem. The focus was on indicating the unfeasibility of distributed consensus within asynchronous settings, known as the FLP impossibility [397]. This algorithm claimed to resolve the consensus challenge in a fully asynchronous environment without needing for classical forms of communication. However, in [398], the authors raised questions regarding the possibility of reaching consensus using the proposed protocol [396]. They pointed out that the quantum algorithm lacks deterministic agreement and validity, which raised concerns about its practical applicability for certain scenarios.

3) Measurement-based Consensus: The postulates of quantum mechanics state that when a quantum state is measured, it collapses into an eigenstate of the measured operator. In other words, the act of measurement determines the subsequent state of the system. Building upon this principle, [399] propose and analyze a consensus protocol for a quantum hybrid network. Within this network model, each node holds a qubit, and consensus is achieved through classical communication channels.

The protocol involves performing measurements on the qubits, and the measurement outcomes are exchanged between nodes via classical messages. The goal is to drive all the qubits in the quantum hybrid network to a common state, thereby reaching consensus. To address the challenges associated with a centralized solution that involves a large number of messages, the authors also present a distributed Pairwise-Qubit-Projection (PQP) algorithm. The research demonstrates that the proposed quantum hybrid network protocol, along with the PQP algorithm, ensures that the network is convergent almost surely to a consensus state for every qubit. By leveraging quantum measurements and classical communication, this approach offers a promising method for achieving consensus in quantum hybrid networks [300], [399].

4) QKD-based Consensus: In [400], a quantum communication protocol is proposed for achieving Byzantine consensus among several entities, without the need for entanglement. Their protocol leverages the unconditional security provided by QKD. The authors use sequences of numbers with correlation which is shared among semi-honest parties distributing quantum-keys, as the foundation of their protocol. By utilizing this approach, the protocol aims to establish consensus among the parties involved. To enhance the protocol further, future advancements could explore the use of low-dimensional entanglement as a substitute for the reliance on semi-honest participants in the key distribution process [300].

5) Quantum Consensus Approaches Inspired by Classical Consensus Methods: The quantum blockchain scheme of [387] utilizes temporal entanglement, where GHZ states encode the quantum blockchain and every quantum-block represents two classical bits. In 2020, Banerjee *et al.* introduced a quantum-based blockchain protocol employing the states of weighted hypergraph to store information from classical blocks [401]. Other approaches for integrating the quantum technologies with blockchain have also been suggested [163], [402]–[406]. However, many of these quantum blockchains lack effective verification methods and specific consensus algorithms, leading to potential issues regarding unverified

transactions and implementation inefficiency.

To address these challenges, it is essential to consider consensus mechanisms suitable for quantum blockchains, as traditional approaches like PoW and PoS that rely on computational power are not appropriate. Instead, DPoS, which relies on voting and is independent of node computing power, aligns better with quantum blockchains. Additionally, digital signatures have been successfully integrated into classical blockchains, and the utilization of quantum digital signatures can effectively ensure transaction authenticity in quantum blockchains [332].

In [332], the authors present a novel quantum blockchain scheme by introducing the QDPoS consensus mechanism, which utilizes quantum voting to facilitate agreement among normal nodes and enable representative nodes to efficiently create corresponding blocks. The proposed scheme employs single qubits as quantum blocks and connects them through entanglement, leveraging either weighted-graph-states or weighted-hypergraph-states. Furthermore, existing quantum digital signature methods are integrated into the quantum blockchain scheme and its security and effectiveness are also evaluated [332]. In TABLE XXIX, the comparison of aforementioned quantum blockchains is provided [332].

In [407], a novel blockchain consensus mechanism is designed, leveraging the stochastic nature, irreversibility, and uncertainty of quantum measurement. The proposed mechanism eliminates the need for complex calculations and intractable mathematical problems, resulting in significant savings in computing resources, reduced energy consumption, shorter time delays, and increased throughput. Additionally, the proposed quantum consensus mechanism demonstrates resilience against 51% attacks. The proposed consensus mechanism, utilizing quantum encryption technology, offers improved fault tolerance and resistance against attacks compared to traditional mechanisms. Additionally, the utilization of quantum entanglement enables the implementation of the Byzantine consensus protocol, where entangled states are used to establish mutual communication information.

In response to the future quantum threat to Bitcoin, researchers have proposed various quantum blockchain schemes. Ikeda introduced qBitcoin, a peer-to-peer quantum-cash-system that utilizes quantum methods to build a Bitcoin-like system. Each qBitcoin consists of classical and quantum states, with the quantum information being unknown to everyone. The No-Cloning theorem prevents the copying and forgery of qBitcoin, ensuring its security. Quantum reporting is employed to transmit the quantum information of qBitcoin, using QKD protocol BB84 to establish a secure key [385].

Jorgenfors proposed Quantum Bitcoin, a secure and anonymous cryptocurrency based on the No-Cloning theorem. Quantum Bitcoin adopts the quantum-state as the currency unit, combined with classical information for verification. It operates on a blockchain and offers advantages such as immediate transactions and independence from a central bank. However, the challenge of untrusted miners and the possibility of quantum double mining arise. To address this, the protocol records coinage in the Quantum Bitcoin system, while it incurs some overhead [404], [408].

The authors of [409] propose a practically realizable fully quantum blockchain model to address the security threats posed by quantum computers to classical blockchains. Their model employs a generalized-Gram-Schmidt process with dimensional lifting. The transactions' information is recorded within a multi-qubit-state and then encoded by employing the generalized-Gram-Schmidt procedure to generate the blockchain. The authors consider different scenarios of forking and provide preventive measures for their proposed model. It is demonstrated that the model remains secure even in the presence of quantum computing attacks, leveraging the no-cloning theorem and the non-democratic aspect of generalized-Gram-Schmidt orthogonalization. Additionally, the authors sketch a blueprint for a quantum token that utilizes the identical architecture as their quantum blockchain.

In [410], the author presents an approach to address the challenges related to block validation and assignment in a blockchain system. By leveraging concepts from Complexity Theory, Quantum Mechanics, and Relativistic Mechanics, the approach offers insights into addressing important questions within the context of blockchain, such as ensuring democracy and randomness in the selection of block validators and the assignment of new blocks.

These quantum blockchain schemes aim to counter the quantum threat and provide enhanced security and efficiency compared to classical cryptocurrencies like Bitcoin. However, the implementation of such solutions requires the establishment of a new security infrastructure, specifically for access control and authentication. [146] focuses on the theoretical analysis of quantum blockchain technologies for decentralized identity authentication. It presents a conceptual design for a quantum blockchain identity framework and reviews the technical evidence supporting its feasibility and effectiveness. While there are limitations and challenges associated with these quantum blockchain technologies, the article emphasizes the importance of exploring decentralized quantum applications despite the current constraints.

Quantum blockchains have also found applications in various fields, including healthcare. For instance, [411] surveys the potential applications of quantum blockchain technology, particularly in healthcare and the fight against COVID-19. Blockchain can enhance data acquisition, patient monitoring, and secure data storage in healthcare systems. Quantum blockchain further enhances these benefits by leveraging quantum computing for thermal imaging and rapid patient location and monitoring. The combination of quantum computing and blockchain can improve the speed and privacy of processing medical records. The paper investigates the advantages of combining blockchain and quantum technologies alongside other state-of-the-art communications and information technologies like artificial intelligence and machine learning. Blockchain, records and shares all digital events with confirmation from multiple parties. The quantum blockchain, which relies on quantum information theory and quantum computing, ensures data integrity and remaining unalterable after recording. With quantum technology's progress, research into quantum blockchain has also increased. Quantum blockchain technologies is actively involved in blockchain technology research

TABLE XXIX
COMPARISON OF QUANTUM BLOCKCHAIN SCHEMES [332].

	QDPoS Scheme [332]	Kiktenko Scheme [386]	Rajan Scheme [387]	Banerjee Scheme [401]
Communication complexity for verifying transactions	One-way communication performed $O\left(n^2\right)$ times	Two-way communication performed $O\left(n^2\right)$ times	Two-way communication performed $O\left(n^2\right)$ times	N/A
Nodes' undeniability	Yes	No	No	N/A
Consensus algorithm	QDPoS	Byzantine agreement	θ-protocol	Relative phase consensus
Time complexity of consensus	$O(n)$	$O\left(n^{f+1}\right)$	$O\left(n^2\right)$	$O(n)$
Byzantine fault tolerance	Yes ($\frac{n}{2}$)	Yes ($\frac{n}{2}$)	No (0)	No (0)
Quantum resource loss during the consensus procedure	No	N/A	$2n$ qubits	n qubits
Resource needs for generating a block	One 1-qubit state $\|+\rangle$	c classical bits	One 2-qubit Bell state	One 1-qubit state $\|+\rangle$
Amount of information in a single block	c-bits	c-bits	two bits	c-bits
Chain structure	Weighted-graph-state or weighted-hypergraph-state	Classical-chain	GHZ state	Weighted-hypergraph-state
Resistance against hashrate-attacks	Yes	No	Yes	Yes

TABLE XXX
THE COMPARISON AND ANALYSIS OF RELEVANT WORKS IN THE AREA OF QUANTUM BLOCKCHAIN [411]. A: QUANTUM COMPUTING B: BLOCKCHAIN C: QUANTUM BLOCKCHAIN D: HEALTHCARE E: QUANTUM DRONES

Author	Year	A	B	C	D	E	Major Findings
[412]	2022	✓	✓	✓	✓	✗	The researchers proposed an attribute-based authentication method resistant to quantum attacks to tackle the challenges related to protected Electronic Medical Records (EMRs) sharing with Blockchain.
[413]	2021	✓	✓	✓	✓	✗	Blockchains are considered a crucial solution to various challenges in the context of 5G, such as mobile IoT security and Electronic Health Record (EHR) exchange. The researchers examined post-quantum hash-based authentication as a means to enhance blockchain security.
[414]	2022	✗	✓	✗	✓	✗	It provides a thorough investigation of modern solutions based on blockchain for security of medical data, utilizing cloud computing and in the absence of cloud computing. Various strategies are built and analyzed using blockchain in this study. The findings include identifying gaps, addressing challenges, and proposing a future roadmap, all contributing to the advancement of Healthcare 4.0 innovation.
[415]	2022	✓	✓	✓	✓	✗	It introduces a cloud-as-a-service platform with quantum capabilities for advanced smart healthcare computations, offering efficiency, scalability, and enhanced security. What sets this model apart is the utilization of blockchain technology and quantum terminal machines , which significantly improves the anonymity and feasibility of the suggested approach.
[416]	2022	✓	✓	✓	✗	✓	The authors proposed a defense strategy against quantum attacks by leveraging lattice-based cryptography. Additionally, they demonstrated the use of a reliable blockchain system to guarantee the reliability of vehicles in batch data verification.
[417]	2019	✓	✓	✓	✗	✗	The proposed quantum signature strategies utilize quantum entanglement characteristics that can be employed by either a single signer or multiple signers. These strategies aim to improve the security of smart contracts on blockchain against quantum threats, while preserving a lightweight design and eliminating the necessity for a trusted third party.
[410]	2021	✓	✓	✓	✗	✗	In this study, a novel negotiation technique is introduced to establish the transaction's validity and assign a fresh block within the architecture of blockchain. The negotiation process relies on an extended likelihood framework to accomplish the allocation and verification of block.

and development, incorporating quantum computing and AI deep learning for innovative applications. Overall, blockchain and quantum technologies have the potential to revolutionize various sectors, including medicine, pharmacy, and healthcare systems. TABLE XXX provides the comparison and analysis of previous studies in the quantum blockchain domain [411].

IX. CONCLUSION

This survey paper has thoroughly examined the significant threat that quantum computers pose to the security of blockchain technology. The reliance of blockchain on hash functions and public-key cryptography, based on large odd prime numbers and discrete logarithms, renders it susceptible to compromise by quantum algorithms such as Grover's and Shor's algorithms. Throughout the paper, we conducted a thorough analysis of the impact of quantum computers on blockchain security, starting with a review of the existing literature on blockchains and quantum computing to establish the current state of research. We then provided an overview of blockchain, highlighting its key components and functionalities, while also exploring the preliminaries and key definitions of quantum computing to establish a foundation for understanding the implications on blockchain security. The application of blockchains in cybersecurity was thoroughly explored, considering their strengths and vulnerabilities in the context of evolving quantum computing capabilities. Our survey focused specifically on the quantum security of blockchain's fundamental building blocks, such as digital signatures, hash functions, consensus algorithms, and smart contracts. We analyzed the vulnerabilities introduced by quantum computers, addressing potential countermeasures and enhancements to ensure the integrity and confidentiality of blockchain systems.

Additionally, we conducted a thorough exploration of the quantum attack surface of blockchains, meticulously iden-

tifying potential pathways through which quantum computing could be leveraged to enhance existing attack strategies. Recognizing the urgency, we emphasized the need for the development of quantum-resistant defenses and explored solutions to mitigate the threat of quantum computers to blockchains. These solutions involve adopting quantum and post-quantum blockchain architectures to improve the robustness and security of blockchain systems against advancing quantum computing technology.

By providing insights into vulnerabilities and discussing mitigation strategies, our survey aims to guide researchers, practitioners, and policymakers in their efforts to develop secure and resilient blockchain systems capable of withstanding the ever-evolving landscape of quantum computing. It is crucial to act proactively and ensure that blockchain technology remains trustworthy and resilient in the era of quantum computing.

REFERENCES

[1] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121.

[2] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 839–858.

[4] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Zanella-Béguelin, "Formal Verification of Smart Contracts: Short Paper," in *ACM Workshop on Programming Languages and Analysis for Security*, Vienna, Austria, Oct. 2016.

[5] E. Ferreira Jesus, V. R. L. Chicarino, C. V. N. de Albuquerque, and A. A. de A. Rocha, "A survey of how to use blockchain to secure internet of things and the stalker attack," *Security and Communication Networks*, vol. 2018, 2018. [Online]. Available: https://doi.org/10.1155/2018/9675050

[6] P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park, "Distblocknet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Communications Magazine*, vol. 55, no. 9, pp. 78–85, 2017.

[7] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.

[8] P. K. Sharma, S. Rathore, and J. H. Park, "DistArch-SCNet: Blockchain-based distributed architecture with Li-Fi communication for a scalable smart city network," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 55–64, 2018.

[9] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2018.

[10] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11 676–11 686, 2018.

[11] D. Rakic, "Blockchain technology in healthcare," in *Proceedings of the 4th International Conference on Information and Communication Technologies for Ageing Well and e-Health*, Funchal, Madeira, Portugal, March 2018, pp. 13–20.

[12] H. Hyvärinen, M. Risius, and G. Friis, "A blockchain-based approach towards overcoming financial fraud in public sector services," *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 441–456, 2017.

[13] F. Holotiuk, F. Pisani, and J. Moormann, "The impact of blockchain technology on business models in the payments industry," in *Towards Thought Leadership in Digital Transformation*, Feb 2017. [Online]. Available: http://aisel.aisnet.org/wi2017/track09/paper/6

[14] F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 983–986.

[15] F. S. Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, "E-voting with blockchain: An E-Voting protocol with decentralisation and voter privacy," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1561–1567.

[16] E. Heilman, F. Baldimtsi, and S. Goldberg, "Blindly signed contracts: Anonymous on-blockchain and off-blockchain bitcoin transactions," in *Financial Cryptography and Data Security - International Workshops, BITCOIN, VOTING, and WAHC*, Christ Church, Barbados, Feb 2016, pp. 43–60.

[17] N. Fotiou and G. C. Polyzos, "Decentralized name-based security for content distribution using blockchains," in *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2016, pp. 415–420.

[18] M. Zhang and Y. Ji, "Blockchain for healthcare records: A data perspective," *PeerJ PrePrints*, vol. 6, p. e26942, 2018. [Online]. Available: https://doi.org/10.7287/peerj.preprints.26942v1

[19] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2016, pp. 1–3.

[20] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, 2015, pp. 180–184.

[21] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Tim'on, and P. Wuille. (2014) Enabling blockchain innovations with pegged sidechains. [Online]. Available: http://kevinriggen.com/files/sidechains.pdf

[22] S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[24] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100067, 2022.

[25] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. M. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[26] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, 2019.

[27] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 1212–1239, 2022.

[28] A. A. Monrat, O. Scheln, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[29] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2794–2830, 2019.

[30] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[31] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018.

[32] A. Khanna, A. Sah, V. Bolshev, A. Burgio, V. Panchenko, and M. Jasiski, "Blockchain-cloud integration: A survey," *Sensors*, vol. 22, no. 14, 2022.

[33] S. Sarker, A. K. Saha, and M. S. Ferdous, "A survey on blockchain & cloud integration," in *2020 23rd International Conference on Computer and Information Technology (ICCIT)*, 2020, pp. 1–7.

[34] S. Megha, H. Salem, E. Ayan, M. Mazzara, H. Aslam, M. Farina, M. R. Bahrami, and M. Ahmad.

[35] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of Bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[36] M. Belotti, N. Boi, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019.

[37] M. Ul Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 289–318, 2023.

[38] K. Gai, J. Guo, L. Zhu, and S. Yu, "Blockchain meets cloud computing: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2009–2030, 2020.

[39] B. Cao, Z. Wang, L. Zhang, D. Feng, M. Peng, L. Zhang, and Z. Han, "Blockchain systems, technologies, and applications: A methodology perspective," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 353–385, 2023.

[40] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[41] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Integration of blockchain and cloud of things: Architecture, applications and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2521–2549, 2020.

[42] Z. Shi, C. de Laat, P. Grosso, and Z. Zhao, "Integration of blockchain and auction models: A survey, some applications, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 497–537, 2023.

[43] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, and L. He, "A comparative study of blockchain consensus algorithms," *Journal of Physics: Conference Series*, vol. 1437, no. 1, p. 012007, Jan 2020. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1437/1/012007

[44] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2017, pp. 2567–2572.

[45] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *Symmetry*, vol. 11, no. 10, 2019. [Online]. Available: https://www.mdpi.com/2073-8994/11/10/1198

[46] A. Altaf, F. Iqbal, R. Latif, B. M. Yakubu, S. Latif, and H. Samiullah, "A survey of blockchain technology: Architecture, applied domains, platforms, and security threats," *Social Science Computer Review*, vol. 0, no. 0, 2022. [Online]. Available: https://doi.org/10.1177/08944393221110148

[47] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surv.*, vol. 54, no. 8, oct 2021.

[48] H. T. M. Gamage, H. D. Weerasinghe, and N. G. J. Dias, "A survey on blockchain technology concepts, applications, and issues," *SN Computer Science*, vol. 1, no. 2, p. 114, 2020.

[49] A. Guru, B. K. Mohanta, H. Mohapatra, F. Al-Turjman, C. Altrjman, and A. Yadav, "A survey on consensus protocols and attacks on blockchain technology," *Applied Sciences*, vol. 13, no. 4, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/4/2604

[50] T. T. Huynh, T. D. Nguyen, and H. Tan, "A survey on security and privacy issues of blockchain technology," in *2019 International Conference on System Science and Engineering (ICSSE)*, 2019, pp. 362–367.

[51] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.

[52] G. Wang, S. Zhang, T. Yu, and Y. Ning, "A systematic overview of blockchain research," *Journal of Systems Science and Information*, vol. 9, no. 3, pp. 205–238, 2021. [Online]. Available: https://doi.org/10.21078/JSSI-2021-205-34

[53] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Systems with Applications*, vol. 168, p. 114384, 2021.

[54] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," *Ledger*, vol. 4, no. 0, pp. 1–39, 2019. [Online]. Available: https://ledger.pitt.edu/ojs/ledger/article/view/140

[55] K. Hameed, M. Barika, S. Garg, M. B. Amin, and B. Kang, "A taxonomy study on securing blockchain-based industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues," *Journal of Industrial Information Integration*, vol. 26, p. 100312, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2452414X21001060

[56] S. Perera, F. Leymann, and P. Fremantle, "A use case centric survey of blockchain: Status quo and future directions," *PeerJ Preprints*, vol. 7, p. e27529v1, 2019. [Online]. Available: https://peerj.com/preprints/27529/

[57] M. Garriga, S. Dalla Palma, M. Arias, A. Renzis, R. Pareschi, and D. A. Tamburri, "Blockchain and cryptocurrencies: A classification and comparison of architecture drivers," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 8, p. e5992, April 2021.

[58] M. Krichen, M. Ammi, A. Mihoub, and M. Almutiq, "Blockchain for modern applications: A survey," *Sensors*, vol. 22, no. 14, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/14/5274

[59] M. C. Ballandies, M. M. Dapp, and E. Pournaras, "Decrypting distributed ledger designtaxonomy, classification and blockchain community evaluation," *Cluster Computing*, vol. 25, no. 3, pp. 1817–1838, Jun 2022.

[60] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125 244–125 262, 2020.

[61] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digital Communications and Networks*, vol. 7, no. 3, pp. 295–307, 2021.

[62] M. A. Khan, L. Ge, J. Wang, and G. Zhang, "Survey of consensus algorithms for proof of stake in blockchain," *Security and Communication Networks*, vol. 2022, p. 2812526, 2022. [Online]. Available: https://www.hindawi.com/journals/scn/2022/2812526/

[63] S. Trivedi, K. Mehta, and R. Sharma, "Systematic literature review on application of blockchain technology in e-finance and financial services," *Journal of technology management & innovation*, vol. 16, pp. 89–102, 12 2021.

[64] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?-a systematic review," *PLoS One*, vol. 11, no. 10, p. e0163477, 2016. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/27695049/

[65] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Comput. Surv.*, Jan 2023.

[66] E. u. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Comput. Surv.*, vol. 53, no. 2, Mar 2021.

[67] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of iot applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, Feb 2021.

[68] P. Tolmach, Y. Li, S.-W. Lin, Y. Liu, and Z. Li, "A survey of smart contract formal specification and verification," *ACM Comput. Surv.*, vol. 54, no. 7, Jul 2021.

[69] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains: Theories, modelings, and tools," *ACM Comput. Surv.*, vol. 54, no. 2, Mar 2021.

[70] J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Transactions on Services Computing*, vol. 15, no. 4, pp. 2490–2510, 2022.

[71] X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," *Applied Sciences*, vol. 9, no. 22, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/22/4731

[72] D. Dasgupta, J. M. Shrein, and K. D. Gupta, "A survey of blockchain from security perspective," *Journal of Banking and Financial Technology*, vol. 3, no. 1, pp. 1–17, 2019.

[73] Y. Wen, F. Lu, Y. Liu, and X. Huang, "Attacks and countermeasures on blockchains: A survey from layering perspective," *Computer Networks*, vol. 191, p. 107978, 2021.

[74] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks, and defenses," *ACM Comput. Surv.*, vol. 53, no. 3, Jun 2020.

[75] Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the internet of things: A survey," *ACM Comput. Surv.*, vol. 52, no. 6, Nov 2019.

[76] X. Wang, S. Duan, J. Clavin, and H. Zhang, "Bft in blockchains: From protocols to use cases," *ACM Comput. Surv.*, vol. 54, no. 10s, Sep 2022.

[77] P. Sharma, R. Jindal, and M. D. Borah, "Blockchain technology for cloud storage: A systematic literature review," *ACM Comput. Surv.*, vol. 53, no. 4, Aug 2020.

[78] S. Suhail, R. Hussain, R. Jurdak, A. Oracevic, K. Salah, C. S. Hong, and R. Matulevičius, "Blockchain-based digital twins: Research trends, issues, and future challenges," *ACM Comput. Surv.*, vol. 54, no. 11s, Sep 2022.

[79] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing internet of things: A comprehensive survey," *ACM Comput. Surv.*, vol. 55, no. 9, Jan 2023.

[80] X. Li, Z. Wang, V. C. M. Leung, H. Ji, Y. Liu, and H. Zhang, "Blockchain-empowered data-driven networks: A survey and outlook," *ACM Comput. Surv.*, vol. 54, no. 3, Apr 2021.

[81] J. Zhu, J. Cao, D. Saxena, S. Jiang, and H. Ferradi, "Blockchain-empowered federated learning: Challenges, solutions, and future directions," *ACM Comput. Surv.*, vol. 55, no. 11, Feb 2023.

[82] Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood, "Blockchain-enabled federated learning: A survey," *ACM Comput. Surv.*, vol. 55, no. 4, Nov 2022.

[83] B.-J. Butijn, D. A. Tamburri, and W.-J. v. d. Heuvel, "Blockchains: A systematic multivocal literature review," *ACM Comput. Surv.*, vol. 53, no. 3, Jul 2020.

[84] A. Pasdar, Y. C. Lee, and Z. Dong, "Connect api with blockchain: A survey on blockchain oracle implementation," *ACM Comput. Surv.*, vol. 55, no. 10, Feb 2023.

[85] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Comput. Surv.*, vol. 53, no. 1, Feb 2020.

[86] M. Fahmideh, J. Grundy, A. Ahmad, J. Shen, J. Yan, D. Mougouei, P. Wang, A. Ghose, A. Gunawardana, U. Aickelin, and B. Abedin, "Engineering blockchain-based software systems: Foundations, survey, and future directions," *ACM Comput. Surv.*, vol. 55, no. 6, Dec 2022.

[87] G. Wang, Q. Wang, and S. Chen, "Exploring blockchains interoperability: A systematic survey," *ACM Comput. Surv.*, Feb 2023.

[88] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? a survey," *ACM Comput. Surv.*, vol. 55, no. 7, Dec 2022.

[89] J. Zou, D. He, S. Zeadally, N. Kumar, H. Wang, and K. R. Choo, "Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges," *ACM Comput. Surv.*, vol. 54, no. 8, Oct 2021.

[90] V. Dwivedi, V. Pattanaik, V. Deval, A. Dixit, A. Norta, and D. Draheim, "Legally enforceable smart-contract languages: A systematic literature review," *ACM Comput. Surv.*, vol. 54, no. 5, Jun 2021.

[91] O. Hasan, L. Brunie, and E. Bertino, "Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey," *ACM Comput. Surv.*, vol. 55, no. 2, Jan 2022.

[92] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures," *ACM Comput. Surv.*, vol. 53, no. 6, Dec 2020.

[93] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, Jul 2019.

[94] A. J. Varela-Vaca and A. M. R. Quintero, "Smart contract languages: A multivocal mapping study," *ACM Comput. Surv.*, vol. 54, no. 1, Jan 2021.

[95] Q. Wang, J. Yu, S. Chen, and Y. Xiang, "SoK: DAG-based blockchain systems," *ACM Comput. Surv.*, vol. 55, no. 12, Mar 2023.

[96] M. Dotan, Y.-A. Pignolet, S. Schmid, S. Tochner, and A. Zohar, "Survey on blockchain networking: Context, state-of-the-art, challenges," *ACM Comput. Surv.*, vol. 54, no. 5, May 2021.

[97] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K. R. Choo, "The application of the blockchain technology in voting systems: A review," *ACM Comput. Surv.*, vol. 54, no. 3, Apr 2021.

[98] M. Barborak, A. Dahbura, and M. Malek, "The consensus problem in fault-tolerant computing," *ACM Comput. Surv.*, vol. 25, no. 2, p. 171220, Jun 1993.

[99] A. Lohachab, S. Garg, B. Kang, M. B. Amin, J. Lee, S. Chen, and X. Xu, "Towards interconnected blockchains: A comprehensive review of the role of interoperability among disparate blockchains," *ACM Comput. Surv.*, vol. 54, no. 7, Jul 2021.

[100] W. Deng, T. Huang, and H. Wang, "A review of the key technology in a blockchain building decentralized trust platform," *Mathematics*, vol. 11, no. 1, 2023. [Online]. Available: https://www.mdpi.com/2227-7390/11/1/101

[101] A. I. Sanka, M. Irfan, I. Huang, and R. C. Cheung, "A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research," *Computer Communications*, vol. 169, pp. 179–201, 2021.

[102] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61 048–61 073, 2021.

[103] C. Yan, C. Zhang, Z. Lu, Z. Wang, Y. Liu, and B. Liu, "Blockchain abnormal behavior awareness methods: a survey," *Cybersecurity*, vol. 5, no. 1, p. 5, 2022.

[104] S. Wu, J. Li, F. Duan, Y. Lu, X. Zhang, and J. Gan, "The survey on the development of secure multi-party computing in the blockchain," in *2021 IEEE Sixth International Conference on Data Science in Cyberspace (DSC)*, 2021, pp. 1–7.

[105] W. Ma, W. J. Chen, and W. Paweenbampen, "Survey of whether blockchain can replace other online-payment," in *2019 2nd International Conference on Hot Information-Centric Networking (HotICN)*, 2019, pp. 84–89.

[106] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum key distribution secured optical networks: A survey," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2049–2083, 2021.

[107] M. Krelina, "Quantum technology for military applications," *EPJ Quantum Technology*, vol. 8, no. 1, p. 24, 2021.

[108] F. Raheman, "The future of cybersecurity in the age of quantum computers," *Future Internet*, vol. 14, no. 11, 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/11/335

[109] J. E. Raya, A. S. Yahya, and E. K. Ahmad, "Protection from a quantum computer cyber-attack: survey," *Technium: Romanian Journal of Applied Sciences and Technology*, vol. 5, pp. 1–12, Jan. 2023. [Online]. Available: https://techniumscience.com/index.php/technium/article/view/8293

[110] M. J. Hossain Faruk, S. Tahora, M. Tasnim, H. Shahriar, and N. Sakib, "A review of quantum cybersecurity: Threats, risks and opportunities," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, pp. 1–8.

[111] A. Vaishnavi and S. Pillai, "Cybersecurity in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods," *Journal of Physics: Conference Series*, vol. 1964, no. 4, p. 042002, Jul 2021. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/1964/4/042002

[112] D. Herman, C. Googin, X. Liu, A. Galda, I. Safro, Y. Sun, M. Pistoia, and Y. Alexeev, "A survey of quantum computing for finance," 2022.

[113] M. A. Serrano, J. A. Cruz-Lemus, R. Perez-Castillo, and M. Piattini, "Quantum software components and platforms: Overview and quality assessment," *ACM Comput. Surv.*, vol. 55, no. 8, dec 2022.

[114] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[115] P. B. Upama, M. J. H. Faruk, M. Nazim, M. Masum, H. Shahriar, G. Uddin, S. Barzanjeh, S. I. Ahamed, and A. Rahman, "Evolution of quantum computing: A systematic survey on the use of quantum computing tools," 2022.

[116] M. Caleffi, M. Amoretti, D. Ferrari, D. Cuomo, J. Illiano, A. Manzalini, and A. S. Cacciapuoti, "Distributed quantum computing: a survey," 2022.

[117] M. H. Ullah, R. Eskandarpour, H. Zheng, and A. Khodaei, "Quantum computing for smart grid applications," *IET Generation, Transmission & Distribution*, vol. 16, no. 21, pp. 4239–4257, 2022. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/gtd2.12602

[118] R. Allaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Lnger, N. Ltkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "Using quantum key distribution for cryptographic purposes: A survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.

[119] V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, "The impact of quantum computing on present cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018.

[120] E. Osaba, E. Villar-Rodriguez, and I. Oregi, "A systematic literature review of quantum computing for routing problems," *IEEE Access*, vol. 10, pp. 55 805–55 817, 2022.

[121] S. Ghosh, S. Upadhyay, and A. A. Saki, "A primer on security of quantum computing," 2023.

[122] R. Ur Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, and Z. Anwar, "Quantum computing for healthcare: A review," *Future Internet*, vol. 15, no. 3, 2023. [Online]. Available: https://www.mdpi.com/1999-5903/15/3/94

[123] J. Singh and K. S. Bhangu, "Contemporary quantum computing use cases: Taxonomy, review and challenges," *Archives of Computational Methods in Engineering*, vol. 30, no. 1, pp. 615–638, 2023.

[124] M. Njorbuenwu, B. Swar, and P. Zavarsky, "A survey on the impacts of quantum computers on information security," in *2019 2nd International Conference on Data Intelligence and Security (ICDIS)*, 2019, pp. 212–218.

[125] S. S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, and R. Buyya, "Quantum computing: A taxonomy, systematic review and future directions," *Software: Practice and Experience*, vol. 52, no. 1, pp. 66–114, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.3039

[126] U. Kaiser, "A short survey of quantum computing," *Journal of Knot Theory and Its Ramifications*, vol. 26, no. 03, p. 1741004, 2017.

[127] M. M. Savchuk and A. V. Fesenko, "Quantum computing: Survey and analysis," *Cybernetics and Systems Analysis*, vol. 55, no. 1, pp. 10–21, 2019.

[128] C. Ciliberto, M. Herbster, A. D. Ialongo, M. Pontil, A. Rocchetto, S. Severini, and L. Wossnig, "Quantum machine learning: a classical perspective," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 474, no. 2209, p. 20170551, 2018. [Online]. Available: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.2017.0551

[129] A. Laghari, H. Shah, R. Laghari, K. Kumar, A. Waqan, and A. Jumani, "A review on quantum computing trends & future perspectives," *EAI Endorsed Trans Cloud Sys*, vol. 7, no. 22, p. e1, May 2022.

[130] A. A. Khan, A. Ahmad, M. Waseem, P. Liang, M. Fahmideh, T. Mikkonen, and P. Abrahamsson, "Software architecture for quantum computing systems a systematic review," *Journal of Systems and Software*, vol. 201, p. 111682, 2023.

[131] F. D. Albareti, T. Ankenbrand, D. Bieri, E. Hnggi, D. Ltscher, S. Stettler, and M. Schngens, "A structured survey of quantum computing for the financial industry," 2022.

[132] G. Pilato and F. Vella, "A survey on quantum computing for recommendation systems," *Information*, vol. 14, no. 1, 2023. [Online]. Available: https://www.mdpi.com/2078-2489/14/1/20

[133] D. Chawla and P. S. Mehra, "A survey on quantum computing for internet of things security," *Procedia Computer Science*, vol. 218, pp. 2191–2200, 2023.

[134] D. Bruss, G. Erdélyi, T. Meyer, T. Riege, and J. Rothe, "Quantum cryptography: A survey," *ACM Comput. Surv.*, vol. 39, no. 2, p. 6es, Jul 2007.

[135] F. V. Massoli, L. Vadicamo, G. Amato, and F. Falchi, "A leap among quantum computing and quantum neural networks: A survey," *ACM Comput. Surv.*, vol. 55, no. 5, Dec 2022.

[136] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[137] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881–919, 2019.

[138] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2019.

[139] A. Singh, K. Dev, H. Siljak, H. D. Joshi, and M. Magarini, "Quantum internetapplications, functionalities, enabling technologies, challenges, and research directions," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2218–2247, 2021.

[140] S. Koudia, A. S. Cacciapuoti, K. Simonov, and M. Caleffi, "How deep the theory of quantum communications goes: Superadditivity, superactivation and causal activation," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 1926–1956, 2022.

[141] Z. Babar, D. Chandra, H. V. Nguyen, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo, "Duality of quantum and classical error correction codes: Design principles and examples," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 970–1010, 2019.

[142] Z. Yang, M. Zolanvari, and R. Jain, "A survey of important issues in quantum computing and communications," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1059–1094, 2023.

[143] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018.

[144] A. Raya and K. Mariyappn, "Diffie-hellman instantiations in pre- and post- quantum world: A review paper," in *2020 Fifth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 2020, pp. 130–136.

[145] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Communications*, vol. 16, no. 10, pp. 1–36, 2019.

[146] Z. Yang, T. Salman, R. Jain, and R. D. Pietro, "Decentralization using quantum blockchain: A theoretical analysis," *IEEE Trans. on Quantum Engineering*, vol. 3, pp. 1–16, 2022.

[147] J. Chen, W. Gan, M. Hu, and C.-M. Chen, "On the construction of a post-quantum blockchain," in *2021 IEEE Conference on Dependable and Secure Computing (DSC)*, 2021, pp. 1–8.

[148] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020.

[149] S. Brotsis, N. Kolokotronis, and K. Limniotis, *Towards Post-Quantum Blockchain Platforms*. Now Publishers, 2022, pp. 106–130.

[150] N. Kappert, E. Karger, and M. Kureljusic, "Quantum computing - the impending end for the blockchain?" in *Pacific Asia Conference on Information Systems (PACIS), Dubai, UAE*, 2021. [Online]. Available: https://ssrn.com/abstract=4075591

[151] R. K. Dhanaraj, V. Rajasekar, S. K. H. Islam, B. Balusamy, and C. H. Hsu, *Quantum Blockchain: An Emerging Cryptographic Paradigm*. Wiley, 2022.

[152] A.-T. Ciulei, M.-C. Creu, and E. Simion, "Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective," Cryptology ePrint Archive, Paper 2022/026, 2022. [Online]. Available: https://eprint.iacr.org/2022/026

[153] T. G. Tan and J. Zhou, "Migrating blockchains away from ecdsa for post-quantum security: A study of impact on users and applications," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham: Springer International Publishing, 2023, pp. 308–316.

[154] B. Yokubov and L. Gan, "Comprehensive comparison of post-quantum digital signature schemes in blockchain," in *2021 International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*, 2021, pp. 158–161.

[155] M. D. Noel, O. V. Waziri, M. S. Abdulhamid, A. J. Ojeniyi, and M. U. Okoro, "Comparative analysis of classical and post-quantum digital signature algorithms used in bitcoin transactions," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, 2020, pp. 1–6.

[156] B. S. Haney, "Blockchain: Post-quantum security & legal economics," 24 N. C. Banking Inst. 117, 2020, available at https://scholarship.law.unc.edu/ncbi/vol24/iss1/8.

[157] A. R. Faridi, F. Masood, A. H. T. Shamsan, M. Luqman, and M. Y. Salmony, "Blockchain in the quantum world," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, 2022. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2022.0130167

[158] J. M. Jose and P. V, "A survey on consensus algorithms in blockchain based on post quantum cryptosystems," in *2022 5th International Conference on Computational Intelligence and Networks (CINE)*, 2022, pp. 1–6.

[159] S. P. and D. Boscovic, "A survey on quantum-safe blockchain system," in *Proceedings of Annual Computer Security Applications Conference (ACSAC)*. Austin, TX, USA: ACM, 2022. [Online]. Available: https://www.acsac.org/2022/workshops/web3sec/Swathi2022.pdf

[160] Y. Zhu, Q. Ni, R. Jiang, A. Bouridane, and C.-T. Li, *Quantum Bitcoin: The Intersection of Bitcoin, Quantum Computing and Blockchain*. Springer International Publishing, 2022, pp. 223–234. [Online]. Available: https://doi.org/10.1007/978-3-031-04424-3_12

[161] J. Dey and R. Dutta, "Progress in multivariate cryptography: Systematic review, challenges, and research directions," *ACM Comput. Surv.*, vol. 55, no. 12, Mar 2023.

[162] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surv.*, vol. 51, no. 6, Jan 2019.

[163] K. Ikeda, "Security and privacy of blockchain and quantum computation," in *Blockchain Technology: Platforms, Tools and Use Cases*, ser. Advances in Computers, P. Raj and G. C. Deka, Eds. Elsevier, 2018, vol. 111, pp. 199–228. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0065245818300160

[164] T. Srivastava, B. Bhushan, S. Bhatt, and A. K. M. B. Haque, *Integration of Quantum Computing and Blockchain Technology: A Cryptographic Perspective*. Springer Singapore, 2022, pp. 197–228.

[165] M. Buser, R. Dowsley, M. Esgin, C. Gritti, S. Kasra Kermanshahi, V. Kuchta, J. Legrow, J. Liu, R. Phan, A. Sakzad, R. Steinfeld, and J. Yu, "A survey on exotic signatures for post-quantum blockchain: Challenges and research directions," *ACM Comput. Surv.*, vol. 55, no. 12, Mar 2023.

[166] Golden Research Engine, "List of blockchain companies and projects," https://golden.com/query/list-of-blockchain-companies-W9Z, 2023, accessed: May 30, 2023.

[167]

[168] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *Self-published paper*, vol. 19, Aug. 2012.

[169] D. Larimer, "Delegated proof-of-stake (dpos)," *Bitshare whitepaper*, 2014.

[170] Parity Technologies. (2018) Proof of authority chains. https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains. Accessed 2023-05-31.

[171] M. Castro, B. Liskov, and et al., "Practical byzantine fault tolerance," in *OSDI*, vol. 99, 1999, pp. 173–186.

[172] Neo, "Neo White Paper," Accessed 2023-05-31. [Online]. Available: {http://docs.neo.org/en-us/whitepaper.html}

[173] D. Schwartz, N. Youngs, A. Britto, and et al., "The ripple protocol consensus algorithm," Ripple Labs Inc, Tech. Rep. 5, 2014.

[174] S. Deb, S. Kannan, and D. Tse, "Posat: Proof-of-work availability and unpredictability, without the work," 2021.

[175] V. Buterin and V. Griffith, "Casper the friendly finality gadget," 2019.

[176] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, vol. 310, 2016.

[177] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, pp. 382–401, 1982.

[178] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, "Qudits and high-dimensional quantum computing," *Frontiers in Physics*, vol. 8, 11 2020.

[179] S. Buck, R. Coleman, and H. Sargsyan, "Continuous variable quantum algorithms: an introduction," *arXiv preprint arXiv:2107.02151*, 2021.

[180] E. F. Combarro, *Quantum Computing Foundations*. Springer International Publishing, 2022.

[181] T.-C. Wei, "Measurement-based quantum computation," https://doi.org/10.1093/acrefore/9780190871994.013.31, 2021, retrieved from https://oxfordre.com/physics/view/10.1093/acrefore/9780190871994.001.0001/acrefore-9780190871994-e-31.

[182] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 439, no. 1907, pp. 553–558, 1992.

[183] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings of FOCS*, 1994, pp. 124–134.

[184] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th ed. Cambridge University Press, 2011.

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

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

[187] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," *Contemporary Mathematics*, vol. 305, pp. 53–74, 2002.

[188] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, August 2018.

[189] J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, Part B, pp. 5766–5781, 2022.

[190] "Guidelines for cyber security," http://www.iso27001security.com/html/27032.html, accessed August 18, 2018.

[191] "X. 1205: Overview of cyber security," https://www.itu.int/rec/T-REC-X.1205-200804-I, accessed August 20, 2018.

[192] A. Einstein, B. Podolsky, and N. Rosen, "D. bohm, quantum theory (prentice hall, englewood ciias, nj, 1951)," *Phys. Rev.*, vol. 47, p. 777, 1935.

[193] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[194] S. K. Yadav, K. Sharma, C. Kumar, and A. Arora, "Blockchain-based synergistic solution to current cybersecurity frameworks," *Multimedia Tools and Applications*, vol. 81, no. 25, pp. 36 623–36 644, 10 2022.

[195] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, 2023.

[196] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175–179. [Online]. Available: http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf

[197] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661

[198] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557

[199] A. K. Bishwas and J. Advani, "Managing cyber security with quantum techniques," in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 2021, pp. 1–7.

[200] Transparency Market Research, "Quantum key distribution market," Retrieved from https://www.transparencymarketresearch.com/quantum-key-distribution-market.html, accessed: June, 14, 2023.

[201] A. Aji, K. Jain, and P. Krishnan, "A survey of quantum key distribution (qkd) network simulation platforms," in *2021 2nd Global Conference for Advancement in Technology (GCAT)*, 2021, pp. 1–8.

[202] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties," in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, 1993, pp. 362–371.

[203] D. Mayers, "The trouble with quantum bit commitment," Computing Research Repository (CoRR), Tech. Rep. quant-ph/9603015v3, 1995. [Online]. Available: http://arxiv.org/abs/quant-ph/9603015

[204] C. Abellan and V. Pruneri, "The future of cybersecurity is quantum," *IEEE Spectrum*, vol. 55, no. 7, pp. 30–35, 2018.

[205] T. M. Fernandez-Carames and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020.

[206] M. Y. Al-darwbi, A. A. Ghorbani, and A. H. Lashkari, "Keyshield: A scalable and quantum-safe key management scheme," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 87–101, 2021.

[207] V. Dixit, R. Selvarajan, T. Aldwairi, Y. Koshka, M. A. Novotny, T. S. Humble, M. A. Alam, and S. Kais, "Training a quantum annealing based restricted boltzmann machine on cybersecurity data," *IEEE Trans. on Emerging Topics in Computational Intelligence*, vol. 6, no. 3, pp. 417–428, 2022.

[208] N. Kilber, D. Kaestle, and S. Wagner, "Cybersecurity for quantum computing," 2021.

[209] M. C. Libicki and D. Gompert, "Quantum communication for post-pandemic cybersecurity," in *2021 13th International Conference on Cyber Conflict (CyCon)*, 2021, pp. 371–386.

[210] R. Yan, J. Dai, Y. Wang, Y. Xu, and A. Qun Liu, "Quantum-key-distribution based microgrid control for cybersecurity enhancement," in *2021 IEEE Industry Applications Society Annual Meeting (IAS)*, 2021, pp. 1–7.

[211] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future internet and the security analysis," *Security and Communication Networks*, vol. 2018, pp. 1–7, February 2018.

[212] H. Suryotrisongko and Y. Musashi, "Evaluating hybrid quantum-classical deep learning for cybersecurity botnet dga detection," *Procedia Computer Science*, vol. 197, pp. 223–229, 2022, sixth Information Systems International Conference (ISICO 2021). [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921023590

[213] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in iot-based smart cities," *Information Processing & Management*, vol. 58, no. 4, p. 102549, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0306457321000546

[214] O. S. Althobaiti and M. Dohler, "Cybersecurity challenges associated with the internet of things in a post-quantum world," *IEEE Access*, vol. 8, pp. 157 356–157 381, 2020.

[215] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[216] V. Dixit, Y. Koshka, T. Aldwairi, and M. Novotny, "Comparison of quantum and classical methods for labels and patterns in restricted boltzmann machines," *Journal of Physics: Conference Series*, vol. 2122, no. 1, p. 012007, Nov 2021. [Online]. Available: https://dx.doi.org/10.1088/1742-6596/2122/1/012007

[217] H. Albataineh and M. Nijim, "Enhancing the cybersecurity education curricula through quantum computation," in *Advances in Security, Networks, and Internet of Things*, K. Daimi, H. R. Arabnia, L. Deligiannidis, M.-S. Hwang, and F. G. Tinetti, Eds. Springer International Publishing, 2021.

[218] F. Neukart, G. Compostella, C. Seidel, D. v. Dollen, S. Yarkoni, and B. Parney, "Traffic flow optimization using a quantum annealer," *Frontiers ICT*, vol. 4, p. 29, 2017.

[219] K.-K. Ko and E.-S. Jung, "Development of cybersecurity technology and algorithm based on quantum computing," *Applied Sciences*, vol. 11, no. 19, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/19/9085

[220] T. H. Szymanski, "The "cyber security via determinism" paradigm for a quantum safe zero trust deterministic internet of things (iot)," *IEEE Access*, vol. 10, pp. 45 893–45 930, 2022.

[221] D. Rosch-Grace and J. Straub, "Analysis of the necessity of quantum computing capacity development for national defense and homeland security," in *2021 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2021, pp. 1–8.

[222] F. Khoshnoud, C. W. de Silva, and I. I. Esat, "Quantum entanglement of autonomous vehicles for cyber-physical security," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2017, pp. 2655–2660.

[223] M. S. Rahman and M. Hossam-E-Haider, "Quantum iot: A quantum approach in iot security maintenance," in *2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST)*, 2019, pp. 269–272.

[224] D. AL-Mubayedh, M. AL-Khalis, G. AL-Azman, M. AL-Abdali, M. Al Fosail, and N. Nagy, "Quantum cryptography on ibm qx," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6.

[225] N. M. P. Neumann, M. P. P. van Heesch, F. Phillipson, and A. A. P. Smallegange, "Quantum computing for military applications," in *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, 2021, pp. 1–8.

[226] C. P. Williams, "Quantum search algorithms in science and engineering," *Comput. Sci. Eng.*, vol. 3, no. 2, pp. 44–51, Mar./Apr. 2001.

[227] M. Santha, *Quantum Walk Based Search Algorithms*. Heidelberg, Germany: Springer, 2008.

[228] A. M. Childs and W. van Dam, "Quantum algorithms for algebraic problems," *Rev. Mod. Phys.*, vol. 82, pp. 1–52, Jan. 2010.

[229] M. Mosca, *Quantum Algorithms*. New York, NY, USA: Springer, 2012.

[230] S. Jordan, "Quantum algorithm zoo," [Online], 2011. [Online]. Available: http://math.nist.gov/quantum/zoo/

[231] M. C. Libicki and D. Gompert, "Quantum communication for post-pandemic cybersecurity," in *2021 13th International Conference on Cyber Conflict (CyCon)*, 2021, pp. 371–386.

[232] T. Shang, R. Chen, and Q. Lei, "Quantum random oracle model for quantum public-key encryption," *IEEE Access*, vol. 7, pp. 130 024–130 031, 2019.

[233] B. Lennart, K. Benjamin, M. Niko, P. Anika, and S. Henning, "Whenand howto prepare for post-quantum cryptography," McKinsey Digital, May 2022, accessed on 16 June 2023. [Online]. Available: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography

[234] N. Kappert, E. Karger, and M. Kureljusic, "Quantum computing - the impending end for the blockchain?" in *Pacific Asia Conference on Information Systems (PACIS)*, Dubai, UAE, 2021. [Online]. Available: https://ssrn.com/abstract=4075591

[235] I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, and W. J. Knottenbelt, "Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack," *Royal Society open science*, vol. 5, no. 6, p. 180410, 2018.

[236] L. Sharma and A. Mishra, "Analysis of crystals-dilithium for blockchain security," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, 2021, pp. 160–165.

[237] "Cryptography behind the top 100 cryptocurrencies," http://ethanfast.com/top-crypto.html, accessed on June 26, 2023.

[238] R. El Bansarkhani and J. Sturm, "An efficient lattice-based multisignature scheme with applications to bitcoins," in *International Conference on Cryptology and Network Security*. Springer, 2016, pp. 140–155.

[239] I. Damgård, C. Orlandi, A. Takahashi, and M. Tibouchi, "Two-round n-out-of-n and multisignatures and trapdoor commitment from lattices," in *PKC'21, Part I*, 2021, pp. 99–130.

[240] Y. Dorç, J. Hoffstein, J. H. Silverman, and B. Sunar, "Mmsat: A scheme for multimessage multiuser signature aggregation," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 520, 2020.

[241] R. El Bansarkhani, M. S. E. Mohamed, and A. Petzoldt, "Mqsas - a multivariate sequential aggregate signature scheme," in *Information Security (ISC'16), Proceedings (LNCS)*, M. Bishop and A. C. A. Nascimento, Eds., vol. 9866. Springer, 2016, pp. 426–439.

[242] D. Cozzo and N. P. Smart, "Sharing the luov: Threshold post-quantum signatures," in *Cryptography and Coding - 17th IMA International Conference (IMACC'19), Proceedings*, 2019, pp. 128–153.

[243] L. De Feo and M. Meyer, "Threshold schemes from isogeny assumptions," in *Public-Key Cryptography (PKC'20)*, A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, Eds. Springer International Publishing, 2020, pp. 187–212.

[244] D. Cozzo and N. P. Smart, "Sashimi: Cutting up csi-fish secret keys to produce an actively secure distributed signing protocol," in *Post-Quantum Cryptography*, J. Ding and J.-P. Tillich, Eds. Springer International Publishing, 2020, pp. 169–186.

[245] M. F. Esgin, O. Ersoy, and Z. Erkin, "Post-quantum adaptor signatures and payment channel networks," in *ESORICS (2) (LNCS)*, vol. 12309. Springer, 2020, pp. 378–397.

[246] E. Tairi, P. Moreno-Sanchez, and M. Maffei, "Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments," 2020.

[247] E. Hauck, E. Kiltz, J. Loss, and N. K. Nguyen, "Lattice-based blind signatures, revisited," in *Advances in Cryptology (CRYPTO'20)*, D. Micciancio and T. Ristenpart, Eds. Springer International Publishing, 2020, pp. 500–529.

[248] S. S. M. and V. Chandrasekaran, "Isogeny-based quantum-resistant undeniable blind signature scheme," *International Journal of Network Security*, vol. 20, no. 1, pp. 9–18, 2018.

[249] R. A. Sahu, A. Gini, and A. Pal, "Supersingular Isogeny-Based Designated Verifier Blind Signature," 2019.

[250] O. Blazy, P. Gaborit, J. Schrek, and N. Sendrier, "A code-based blind signature," in *2017 IEEE International Symposium on Information Theory (ISIT'17)*. IEEE, 2017, pp. 2718–2722.

[251] A. Petzoldt, A. Szepieniec, and M. S. E. Mohamed, "A practical multivariate blind signature scheme," in *Financial Cryptography and Data Security (FC'17), Revised Selected Papers (LNCS)*, A. Kiayias, Ed., vol. 10322. Springer, 2017, pp. 437–454.

[252] T. H. Yuen, M. F. Esgin, J. K. Liu, M. H. Au, and Z. Ding, "DualRing: Generic construction of ring signatures with efficient instantiations," in *CRYPTO (1) (Lecture Notes in Computer Science)*, vol. 12825. Springer, 2021, pp. 251–281.

[253] M. F. Esgin, R. Steinfeld, J. K. Liu, and D. Liu, "Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications," in *CRYPTO (1) (LNCS)*, vol. 11692. Springer, 2019, pp. 115–146.

[254] M. F. Esgin, R. Steinfeld, and R. K. Zhao, "Matrict+: More efficient post-quantum private blockchain payments," in *IEEE Symposium on Security and Privacy*, 2022, pp. 1281–1298.

[255] M. F. Esgin, R. K. Zhao, R. Steinfeld, J. K. Liu, and D. Liu, "Matrict: Efficient, scalable and post-quantum blockchain confidential transactions protocol," in *ACM CCS 2019, Proceedings*. ACM, 2019, pp. 567–584.

[256] V. Lyubashevsky, N. K. Nguyen, and G. Seiler, "SMILE: Set membership from ideal lattices with applications to ring signatures and confidential transactions," 2021.

[257] W. Beullens, S. Katsumata, and F. Pintore, "Calamari and falafl: Logarithmic (linkable) ring signatures from isogenies and lattices," in *Advances in Cryptology (ASIACRYPT'20)*, S. Moriai and H. Wang, Eds. Springer International Publishing, 2020, pp. 464–492.

[258] J. Katz, V. Kolesnikov, and X. Wang, "Improved non-interactive zero knowledge with applications to post-quantum signatures," in *ACM SIGSAC CCS 2018, Proceedings*, 2018, pp. 525–537.

[259] D. Derler, S. Ramacher, and D. Slamanig, "Post-quantum zero-knowledge proofs for accumulators with applications to ring signatures from symmetric-key primitives," in *International Conference on Post-Quantum Cryptography*. Springer, 2018, pp. 419–440.

[260] D. Zheng, X. Li, and K. Chen, "Code-based ring signature scheme," *Int. J. Netw. Secur.*, vol. 5, no. 2, pp. 154–157, 2007.

[261] L. Dallot and D. Vergnaud, "Provably secure code-based threshold ring signatures," in *Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009. Proceedings (LNCS)*, M. G. Parker, Ed., vol. 5921. Springer, 2009, pp. 222–235.

[262] P. Branco and P. Mateus, "A code-based linkable ring signature scheme," in *Provable Security (ProvSec'18), Proceedings (LNCS)*, J. Baek, W. Susilo, and J. Kim, Eds., vol. 11192. Springer, 2018, pp. 203–219.

[263] M. S. E. Mohamed and A. Petzoldt, "Ringrainbow-an efficient multivariate ring signature scheme," in *Progress in Cryptology (AFRICACRYPT'17), Proceedings (LNCS)*, M. Joye and A. Nitaj, Eds., vol. 10239, 2017, pp. 3–20.

[264] A. Petzoldt, S. Bulygin, and J. Buchmann, "A multivariate based threshold ring signature scheme," *Appl. Algebra Eng. Commun. Comput.*, vol. 24, no. 3–4, pp. 255–275, 2013.

[265] A. Poelstra, "Scriptless scripts," Presentation Slides, 2017, accessed on 14 December 2021. [Online]. Available: https://download.wpsoftware.net/bitcoin/wizardry/mw-slides/2017-05-milan-meetup/slides.pdf

[266] N. Di Chiano, R. Longo, A. Meneghetti, and G. Santilli, "A survey on nist pq signatures," *CoRR*, vol. abs/2107.11082, 2021.

[267] T. G. Tan and J. Zhou, "Migrating blockchains away from ecdsa for post-quantum security: A study of impact on users and applications," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Cham: Springer International Publishing, 2023, pp. 308–316.

[268] M. Palatinus, P. Rusnak, A. Voisine, and S. Bowe. (2013) BIP 0039: mnemonic code for generating deterministic keys. Accessed Aug 2022. [Online]. Available: https://en.bitcoin.it/wiki/BIP0039

[269] G. Alagic and et al., "Status report on the third round of the nist post-quantum cryptography standardization process," National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep., 2022.

[270] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Zero-Knowledge from Secure Multiparty Computation," in *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*. ACM, 2007, pp. 21–30.

[271] T. G. Tan and J. Zhou, "Layering Quantum-Resistance into Classical Digital Signature Algorithms," in *ISC 2021*, ser. LNCS, vol. 13118. Cham: Springer, 2021, pp. 26–41.

[272] 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*, vol. 58, p. 102780, 2021.

[273] L. G. Bruinderink, T. Lange, A. Hulsing, and L. Bonebakker, "Towards post-quantum bitcoin," Master's thesis, Eindhoven University of Technology, 2016.

[274] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *Applied Cryptography and Network Security*, pp. 164–175.

[275] M. F. Esgin, R. K. Zhao, R. Steinfeld, J. K. Liu, and D. Liu, "Matrict: Efficient, scalable and post-quantum blockchain confidential transactions protocol," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 567–584.

[276] S. Vives, "Synced hash-based signatures: Post-quantum authentication in a blockchain."

[277] W. van der Linde, P. Schwabe, A. Hulsing, Y. Yarom, and L. Batina, "Post-quantum blockchain using one-time signature chains," Radboud Univ., Nijmegen, The Netherlands, Tech. Rep., 2018.

[278] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a quantum-resistant public key infrastructure," in *International Workshop on Post-Quantum Cryptography*. Springer, 2017, pp. 384–405.

[279] B. Das, A. Holcomb, M. Mosca, and G. Pereira, "Pqfabric: A permissioned blockchain secure from both classical and quantum attacks," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[280] M. D. Noel, O. V. Waziri, M. S. Abdulhamid, and A. J. Ojeniyi, "Stateful hash-based digital signature schemes for bitcoin cryptocurrency," in *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, 2019, pp. 1–6.

[281] M. D. Noel, O. V. Waziri, M. S. Abdulhamid, A. J. Ojeniyi, and M. U. Okoro, "Comparative analysis of classical and post-quantum digital signature algorithms used in bitcoin transactions," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, 2020, pp. 1–6.

[282] B. Yokubov and L. Gan, "Comprehensive comparison of post-quantum digital signature schemes in blockchain," in *2021 International Conference on Electronic Communications, Internet of Things and Big Data (ICEIB)*, 2021, pp. 158–161.

[283] M. Á. León-Chávez, L. P. Perin, and F. Rodríguez-Henríquez, *Post-Quantum Digital Signatures for Bitcoin*. Cham: Springer International Publishing, 2023, pp. 251–270.

[284] "Ethereums official roadmap," https://github.com/ethereum/wiki/wiki/Sharding-roadmap, 2019, accessed: Nov. 2, 2019.

[285] "Abelian," https://www.abelianfoundation.org, 2019, accessed: Nov. 2, 2019.

[286] "Cordas supported security suites," https://docs.corda.net/cipher-suites.html, 2019, accessed: Nov. 2, 2019.

[287] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, October 1997.

[288] S. Krendelev and P. Sazonova, "Parametric hash function resistant to attack by quantum computer," in *Proceedings of the Federated Conference on Computer Science and Information Systems*. IEEE, September 2018, pp. 387–390.

[289] G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," in *Proceedings of the Latin American Symposium on Theoretical Informatics*. IEEE, March 2006, pp. 163–169.

[290] E. ÜNSAL, H. KAHRAMANLI ÖRNEK, and c. TAŞDEMİR, "A review of hashing algorithms in cryptocurrency," in *International Conference on Frontiers in Academic Research*, vol. 1, Feb. 2023, p. 544550. [Online]. Available: https://as-proceeding.com/index.php/icfar/article/view/161

[291] "Iota," https://www.iota.org, accessed: Jun. 2, 2023.

[292] S. Popov, "The Tangle, Version 1.4.3," IOTA Foundation, White Paper, Apr. 2018. [Online]. Available: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf

[293] E. Heilman, N. Narula, G. Tanzer, J. Lovejoy, M. Colavita, M. Virza, and T. Dryja, "Cryptanalysis of Curl-P and other attacks on the IOTA cryptocurrency," *IACR Transactions on Symmetric Cryptology*, vol. 2020, no. 3, pp. 367–391, Sep. 2020. [Online]. Available: https://tosc.iacr.org/index.php/ToSC/article/view/8707

[294] "Qrl-the quantum resistant ledger," https://theqrl.org/, accessed: Jun. 2, 2023.

[295] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2017, pp. 2567–2572.

[296] I. Bashir, *Blockchain Consensus*. Apress Berkeley, CA, 2022.

[297] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[298] H. Kim and D. Kim, "A taxonomic hierarchy of blockchain consensus algorithms: An evolutionary phylogeny approach," *Sensors*, vol. 23, no. 5, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/5/2739

[299] J. Yusoff, Z. Mohamad, and M. Anuar, "A review: Consensus algorithms on blockchain," *Journal of Computer and Communications*, vol. 10, pp. 37–50, 2022.

[300] M. Marcozzi and L. Mostarda, "Quantum consensus: An overview," 2021.

[301] P. Bains, *Blockchain Consensus Mechanisms: A Primer for Supervisors*. International Monetary Fund, 2022. [Online]. Available: https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/25/Blockchain-Consensus-Mechanisms-511769

[302] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018, pp. 1545–1550.

[303] K. Sharma and D. Jain, "Consensus algorithms in blockchain technology: A survey," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1–7.

[304] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, "Study of blockchain based decentralized consensus algorithms," in *TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)*, 2019, pp. 908–913.

[305] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019.

[306] B. S. Anupama and N. R. Sunitha, "Analysis of the consensus protocols used in blockchain networks an overview," in *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*, 2022, pp. 1–6.

[307] S. Islam, M. J. Islam, M. Hossain, S. Noor, K.-S. Kwak, and S. M. R. Islam, "A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues," *IEEE Access*, vol. 11, pp. 39 066–39 082, 2023.

[308] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on private blockchain consensus algorithms," in *2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT)*, 2019, pp. 1–6.

[309] M. Khan, F. den Hartog, and J. Hu, "A survey and ontology of blockchain consensus algorithms for resource-constrained iot

systems," *Sensors*, vol. 22, no. 21, 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/21/8188
[310] J. Ding, "A new proof of work for blockchain based on random multivariate quadratic equations," in *International Conference on Applied Cryptography and Network Security*. Springer, 2019, pp. 97–107.
[311] W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.
[312] C. Li, X. Chen, Y. Chen, Y. Hou, and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2019.
[313] D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum attacks on bitcoin, and how to protect against them," *Ledger*, vol. 3, Oct. 2018. [Online]. Available: https://ledger.pitt.edu/ojs/ledger/article/view/127
[314] N. Anhao, "Bitcoin post-quantum," https://bitcoinpq.org/#whitepaper, 2018.
[315] M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger, D. Slamanig, and G. Zaverucha, "Post-quantum zero-knowledge and signatures from symmetric-key primitives," https://eprint.iacr.org/2017/279.pdf, 2017.
[316] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," https://eprint.iacr.org/2018/046.pdf, 2018.
[317] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, vol. 107, pp. 841–853, 2020.
[318] A. Back, "Hashcash–a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
[319] D. Larimer, "Momentum - a memory-hard proof-of-work via finding birthday collisions," http://www.hashcash.org/papers/momentum.pdf, 2014.
[320] A. Biryukov and D. Khovratovich, "Equihash: Asymmetric proof-of-work based on the generalized birthday problem," *Ledger*, vol. 2, pp. 1–30, 2017.
[321] J. Tromp, "Cuckoo cycle: A memory bound graph-theoretic proof-of-work," in *Financial Cryptography and Data Security: BITCOIN*, 2015, pp. 49–62.
[322] H. Yi, Y. Li, M. Wang, Z. Yan, and Z. Nie, "An efficient blockchain consensus algorithm based on post-quantum threshold signature," *Big Data Research*, vol. 26, p. 100268, November 2021.
[323] 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*, vol. 58, p. 102780, 2021.
[324] J. Wang, Y. Ding, N. Xiong, W.-C. Yeh, and J. Wang, "Gscs: General secure consensus scheme for decentralized blockchain systems," *IEEE Access*, vol. 8, pp. 125 826–125 848, 2020.
[325] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, p. 887, 2019.
[326] R. Behnia, E. Postlethwaite, M. Ozmen, and A. Yavuz, "Lattice-based proof-of-work for post-quantum blockchains," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 2022, pp. 310–318.
[327] H. Jung and H.-N. Lee, "Eccpow: Error-correction code based proof-of-work for asic resistance," *Symmetry*, vol. 12, no. 6, p. 988, 2020.
[328] S. GAO, T. ZHENG, Y. GUO, and B. XIAO, "Efficient and post-quantum zero-knowledge proofs for blockchain confidential transaction protocols," Cryptology ePrint Archive, Paper 2021/1674, 2021, https://eprint.iacr.org/2021/1674. [Online]. Available: https://eprint.iacr.org/2021/1674
[329] M. F. Esgin, R. Steinfeld, J. K. Liu, and D. Liu, "Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications," in *Advances in Cryptology – CRYPTO 2019*. Cham: Springer International Publishing, 2019, pp. 115–146.
[330] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, "Bulletproofs: Short proofs for confidential transactions and more," in *Proc. of the IEEE Symposium on Security and Privacy (Oakland)*. IEEE, 2018.
[331] M. F. Esgin, R. K. Zhao, R. Steinfeld, J. K. Liu, and D. Liu, "Matrict: Efficient, scalable and post-quantum blockchain confidential transactions protocol," in *Proc. of the ACM Conference on Computer & Communications Security (CCS)*. ACM, 2019.
[332] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism qdpos," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3264–3276, 2022.
[333] "Stealth's quantum-proof-of-stake."
[334] R. Chang, Z. Hong, and J. Hua, "Quantum secured-byzantine fault tolerance blockchain consensus mechanism," *Computer Science*, vol. 49, no. 5, pp. 333–340, 2022. [Online]. Available: https://www.jsjkx.com/EN/abstract/article_20718.shtml
[335] S. Dolev, B. Guo, J. Niu, and Z. Wang, "Sodsbc: A post-quantum by design asynchronous blockchain framework," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–16, 2023. [Online]. Available: https://eprint.iacr.org/2020/205
[336] X. Gao, J. Xu, and J. Fan, "A novel quantum byzantine consensus protocol based on malicious node prevention mechanism," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 2022, pp. 202–205.
[337] "Cardano: Quantum resistant?" https://coinwut.com/cardano-quantum-resistant/, accessed: June 27, 2023.
[338] J. Maxfield, "Quantum proofs of space," Available online: http://users.cms.caltech.edu/~vidick/reports/maxfield-final-report.pdf, 2020.
[339] D. Singh, B. Fu, G. Muraleedharan, C.-M. Cheng, N. R. Newton, P. P. Rohde, and G. K. Brennen, "Proof-of-work consensus by quantum sampling," 2023.
[340] M. Y. Shalaginov and M. Dubrovsky, "Quantum proof of work with parametrized quantum circuits," 2022.
[341] S. Park and N. Spooner, "The superlinearity problem in post-quantum blockchains," Cryptology ePrint Archive, Paper 2022/1423, 2022. [Online]. Available: https://eprint.iacr.org/2022/1423
[342] R. Fernàndez-València, "Post-quantum cryptography," https://medium.com/iovlabs-innovation-stories/post-quantum-cryptography-e48c2e54967b, accessed: June 27, 2023.
[343] A. Foundation, "Pioneering falcon post-quantum technology on blockchain," https://www.algorand.foundation/news/pioneering-falcon-post-quantum-technology-on-blockchain, accessed: June 27, 2023.
[344] A. Holcomb, G. C. C. F. Pereira, B. Das, and M. Mosca, "Pqfabric: A permissioned blockchain secure from both classical and quantum attacks," 2020.
[345] M. Boroujeni, S. Ehsani, M. Ghodsi, M. Hajiaghayi, and S. Seddighin, "Approximating edit distance in truly subquadratic time: Quantum and mapreduce," *Journal of the ACM*, vol. 68, no. 3, pp. 19:1–19:41, 2021.
[346] L. Kleinrock, R. Ostrovsky, and V. Zikas, "Proof-of-reputation blockchain with nakamoto fallback," in *Progress in Cryptology – INDOCRYPT 2020*. Cham: Springer International Publishing, 2020, pp. 16–38.
[347] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on blockchain-based smart contracts: Technical aspects and future research," *IEEE Access*, vol. 9, pp. 87 643–87 662, 2021.
[348] Z. Cai, J. Qu, P. Liu, and J. Yu, "A blockchain smart contract based on light- weighted quantum blind signature," *IEEE Access*, vol. 7, pp. 138 657–138 668, 2019.
[349] Q. Lin, H. Yan, Z. Huang, and et al., "An id-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20 632–20 640, 2018.
[350] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions On Dependable And Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.
[351] J. Chen, Y. Hu, and W. Gao, "Lattice-based threshold ring signature with message block sharing," *KSII Transactions On Internet And Information Systems*, vol. 13, no. 2, pp. 1003–1019, 2019.
[352] E. Stinaff, M. Scheibner, A. Bracker, and et al., "Optical signatures of coupled quantum dots," *Science*, vol. 311, no. 5761, pp. 636–639, 2006.
[353] X.-J. Wen, Y. Liu, and Y. Sun, "Quantum multi-signature protocol based on teleportation," *Zeitschrift Fur Naturforschung Section A-A Journal of Physical Sciences*, vol. 62, no. 3-4, pp. 147–151, 2007.
[354] A. Coladangelo, "Smart contracts meet quantum cryptography," 2019.
[355] X. Sun, P. Kulicki, and M. Sopek, "Logic programming with post-quantum cryptographic primitives for smart contract on quantum-secured blockchain," *Entropy*, vol. 23, no. 9, 2021. [Online]. Available: https://www.mdpi.com/1099-4300/23/9/1120
[356] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*. ACM, 2008, pp. 197–206.
[357] L. Ducas and D. Micciancio, "Improved short lattice signatures in the standard model," in *Advances in Cryptology—CRYPTO 2014—34th Annual Cryptology Conference*, vol. 8616. Springer, 2014, pp. 335–352.

[358] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu *et al.*, "Experimental authentication of quantum key distribution with post-quantum cryptography," *NPJ Quantum Information*, vol. 7, no. 1, p. 67, 2021.

[359] L. Anderson, R. Holz, A. Ponomarev, P. Rimba, and I. Weber, "New kids on the block: An analysis of modern blockchains," *CoRR*, vol. abs/1606.06530, 2016. [Online]. Available: http://arxiv.org/abs/1606.06530

[360] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts SOK," in *Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204*. New York, NY, USA: Springer-Verlag New York, Inc., 2017, pp. 164–186. [Online]. Available: https://doi.org/10.1007/978-3-662-54455-6_8

[361] O. Sattath, "On the insecurity of quantum bitcoin mining," *International Journal of Information Security*, vol. 19, no. 3, pp. 291–302, mar 2020.

[362] Cloudflare, "Welcome to crypto week 2019," https://blog.cloudflare.com/welcome-to-crypto-week-2019/, 2019.

[363] R. R. Nerem and D. R. Gaur, "Conditions for advantageous quantum bitcoin mining," *Blockchain: Research and Applications*, p. 100141, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720923000167

[364] D. Rajan, "Quantum analogue of entropy based ddos detection," 2022.

[365] B. Magazine. (2013) Bitcoin is not quantum-safe, and how we can fix it. Accessed: June 27, 2023. [Online]. Available: https://bitcoinmagazine.com/technical/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150

[366] Braiins, "Can quantum computers 51% attack bitcoin?" https://fa.braiins.com/blog/can-quantum-computers-51-attack-bitcoin, accessed: June 27, 2023.

[367] "Quantum computing and blockchain," https://moralismoney.com/blog/quantum-computing-and-blockchain, accessed: June 27, 2023.

[368] L. Kumar and B. Chinnaiah, "Prevention of authentication problems using quantum cryptography," *International Journal of Research in Electronics and Computer Engineering*, vol. 6, no. 2, pp. 929–931, 2018.

[369] T. Hardjono and A. Pentland, "Verifiable anonymous identities and access control in permissioned blockchains," 2019.

[370] "Nothing-at-stake problem," https://golden.com/wiki/Nothing-at-stake-problem-639PVZA, accessed on July 3, 2023.

[371] "Quantum crypto," https://www.mach37.com/blog/quantum-crypto, accessed: July 3, 2023.

[372] "A fair look into abcmint: A quantum-resistant cryptocurrency," https://medium.com/@pqcwoof/a-fair-look-into-abcmint-a-quantum-resistant-cryptocurrency-6c03f28c1307.

[373] "Ethereum future proofing," https://ethereum.org/de/roadmap/future-proofing/.

[374] R. Shen, H. Xiang, X. Zhang, B. Cai, and T. Xiang, "Application and implementation of multivariate public key cryptosystem in blockchain (short paper)," in *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2019, pp. 419–428.

[375] P. Serguei, "The tangle," Tech. Rep., 2016.

[376] S. Brotsis, N. Kolokotronis, and K. Limniotis, "Towards post-quantum blockchain platforms," in *Security Technologies and Methods for Advanced Cyber Threat Intelligence, Detection and Mitigation*. Now Publishers, 2022, pp. 106–130.

[377] R. Saha, G. Kumar, T. Devgun, W. J. Buchanan, R. Thomas, M. Alazab, T. Hoon-Kim, and J. J. P. C. Rodrigues, "A blockchain framework in post-quantum decentralization," *IEEE Transactions on Services Computing*, vol. 16, no. 1, pp. 1–12, 2023.

[378] 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*, vol. 6, pp. 27 205–27 213, 2018.

[379] E. Zeydan, Y. Turk, S. B. Ozturk, H. Mutlu, and A. A. Dundar, "Post-quantum blockchain-based data sharing for iot service providers," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 96–101, 2022.

[380] B. Li and F. Wu, "Post quantum blockchain with segregation witness," in *2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS)*, 2021, pp. 522–527.

[381] H. Yi, "Secure social internet of things based on post-quantum blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 3, pp. 950–957, 2022.

[382] B. Khan, I. Ul Haq, S. Rana, and H. Ul Rasheed, "Secure smart grids: Based on post-quantum blockchain," in *2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2022, pp. 653–658.

[383] B. Yuan, F. Wu, W. Qiu, W. Wang, H. Zhu, and D. Zhou, "Blockchain-based infrastructure for artificial intelligence with quantum resistant," in *2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD)*, 2021, pp. 627–631.

[384] C. Peng, H. Xu, and P. Li, "Redactable blockchain using lattice-based chameleon hash function," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 2022, pp. 94–98.

[385] K. Ikeda, "qbitcoin: A peer-to-peer quantum cash system," in *Proc. Sci. Inf. Conf.*, 2018, pp. 763–771.

[386] E. O. Kiktenko *et al.*, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, p. 035004, 2018.

[387] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *Quantum Rep.*, vol. 1, no. 1, pp. 3–11, 2019.

[388] L. Mazzarella, A. Sarlette, and F. Ticozzi, "Consensus for quantum networks: Symmetry from gossip interactions," *IEEE Transactions on Automatic Control*, vol. 60, no. 1, pp. 158–172, 2015.

[389] G. Shi, D. Dong, I. R. Petersen, and K. H. Johansson, "Consensus of quantum networks with continuous-time Markovian dynamics," in *Proceeding of the 11th World Congress on Intelligent Control and Automation*. IEEE, 2014, pp. 307–312.

[390] G. Shi, S. Fu, and I. R. Petersen, "Reaching quantum consensus with directed links: Missing symmetry and switching interactions," in *Proceeding of the 11th World Congress on Intelligent Control and Automation*. IEEE, 2015, pp. 307–312.

[391] G. Lindblad, "On the generators of quantum dynamical semigroups," *Communications in Mathematical Physics*, vol. 48, no. 2, pp. 119–130, 1976.

[392] R. Takeuchi and K. Tsumura, "Distributed feedback control of quantum networks," *IFAC-PapersOnLine*, vol. 49, no. 22, pp. 309–314, 2016.

[393] S. Jafarizadeh, "Optimizing the convergence rate of the quantum consensus: A discrete-time model," *Automatica*, vol. 73, pp. 237–247, 2016.

[394] F. Ticozzi, "Symmetrizing quantum dynamics beyond gossip-type algorithms," *Automatica*, vol. 74, pp. 38–46, 2016.

[395] M. Ben-Or and A. Hassidim, "Fast quantum byzantine agreement," in *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, 2005, pp. 481–485.

[396] L. K. Helm, "Quantum distributed consensus," in *PODC*, 2008, p. 445.

[397] M. J. Fischer, N. A. Lynch, and M. S. Paterson, "Impossibility of distributed consensus with one faulty process," *Journal of the ACM (JACM)*, vol. 32, no. 2, pp. 374–382, 1985.

[398] W. Golab and H. Tan, "A closer look at quantum distributed consensus," in *Proceedings of the 32nd ACM Symposium on Parallelism in Algorithms and Architectures*, 2020, pp. 539–541.

[399] G. Shi, B. Li, Z. Miao, P. M. Dower, and M. R. James, "Reaching agreement in quantum hybrid networks," *Scientific Reports*, vol. 7, no. 1, pp. 1–9, 2017.

[400] X. Sun, P. Kulicki, and M. Sopek, "Multi-party quantum byzantine agreement without entanglement," *arXiv preprint arXiv:2003.09120*, 2020.

[401] S. Banerjee, A. Mukherjee, and P. K. Panigrahi, "Quantum blockchain using weighted hypergraph states," *Physical Review Research*, vol. 2, no. 1, p. 013322, 2020.

[402] Y.-L. Gao, X.-B. Chen, G. Xu, K.-G. Yuan, W. Liu, and Y.-X. Yang, "A novel quantum blockchain scheme based on quantum entanglement and dpos," *Quantum Information Processing*, vol. 19, no. 12, pp. 1–15, December 2020.

[403] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732, pp. 465–467, 2018.

[404] J. Jogenfors, "Quantum Bitcoin: An anonymous and distributed currency secured by the no-cloning theorem of quantum mechanics," 2016.

[405] S. Singh, N. K. Rajput, V. K. Rathi, H. M. Pandey, A. K. Jaiswal, and P. Tiwari, "Securing blockchain transactions using quantum teleportation and quantum digital signature," *Neural Processing Letters*, pp. 1–16, June 2020.

[406] B. K. Behera, A. Banerjee, and P. K. Panigrahi, "Experimental realization of quantum cheque using a five-qubit quantum computer," *Quantum Information Processing*, vol. 16, no. 12, pp. 1–12, December 2017.

[407] D. Zhang, H. Wang, and J. Yu, "A blockchain consensus protocol based on quantum attack algorithm," *Computational Intelligence and Neuroscience*, vol. 2022, p. 1431967, 2022. [Online]. Available: https://doi.org/10.1155/2022/1431967

[408] J. Jogenfors, "Quantum Bitcoin: An anonymous, distributed, and secure currency secured by the no-cloning theorem of quantum mechanics," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 245–252.
[409] K. Nilesh and P. K. Panigrahi, "Quantum blockchain based on dimensional lifting generalized gram-schmidt procedure," *IEEE Access*, vol. 10, pp. 103 212–103 222, 2022.
[410] G. Iovane, "Murequa chain: Multiscale relativistic quantum blockchain," *IEEE Access*, vol. 9, pp. 39 827–39 838, 2021.
[411] K. Kaushik and A. Kumar, "Demystifying quantum blockchain for healthcare," 2022.
[412] X. Chen, S. Xu, T. Qin, Y. Cui, S. Gao, and W. Kong, "Aqabs: Anti-quantum attribute-based signature for emrs sharing with blockchain," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2022, pp. 1176–1181.
[413] L. Mirtskhulava, M. Iavich, M. Razmadze, and N. Gulua, "Securing medical data in 5g and 6g via multichain blockchain technology using post-quantum signatures," *pp. 72–75*, Feb. 2022.
[414] H. B. Mahajan and et al., "Integration of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems," *Applied Nanoscience (Switzerland)*, vol. 1, pp. 1–14, Feb. 2022.
[415] A. EL Azzaoui, P. K. Sharma, and J. H. Park, "Blockchain-based delegated quantum cloud architecture for medical big data security," *Journal of Network and Computer Applications*, vol. 198, Feb. 2022.
[416] D. S. Gupta, A. Karati, W. Saad, and D. B. Da Costa, "Quantum-defended blockchain-assisted data authentication protocol for internet of vehicles," *IEEE Trans Veh Technol*, vol. 71, no. 3, pp. 3255–3266, Mar. 2022.
[417] Z. Cai, J. Qu, P. Liu, and J. Yu, "A blockchain smart contract based on light-weighted quantum blind signature," *IEEE Access*, vol. 7, pp. 138 657–138 668, 2019.
[418] J. H. Mosakheil, "Security threats classification in blockchains," *Culminating Projects in Information Assurance*, vol. 48, 2018. [Online]. Available: https://repository.stcloudstate.edu/msia_etds/48
[419] Coindesk. Quantum computers vs. crypto mining: Separating facts from fiction. Accessed: June 27, 2023. [Online]. Available: https://www.coindesk.com/learn/quantum-computers-vs-crypto-mining-separating-facts-from-fiction/