Applying Post-Quantum Cryptography Algorithms to a DLT-Based CBDC Infrastructure: Comparative and Feasibility Analysis

Daniel de Haro Moraes,[*] João Paulo Aragão Pereira, PhD,[†] Bruno Estolano Grossi, MSc,[‡]
Gustavo Corrêa Mirapalheta,[§] George Marcel Monteiro Arcuri Smetana,[¶] Wesley Rodrigues,[||]
Courtnay Nery Guimarães Jr.,[**] Bruno Domingues,[††] Fábio Saito,[‡‡] Marcos Simplício[§§]

Abstract

This article presents an innovative project for a Central Bank Digital Currency (CBDC) infrastructure. Focusing on security and reliability, the proposed architecture: (1) employs post-quantum cryptography (PQC) algorithms for long-term security, even against attackers with access to cryptographically-relevant quantum computers; (2) can be integrated with a Trusted Execution Environment (TEE) to safeguard the confidentiality of transaction contents as they are processed by third-parties; and (3) uses Distributed Ledger Technology (DLT) to promote a high level of transparency and tamper resistance for all transactions registered in the system. Besides providing a theoretical discussion on the benefits of this architecture, we experimentally evaluate its components. Namely, as PQC algorithms, we consider three signature schemes being standardized by the National Institute of Standards and Technology (NIST), CRYSTALS-Dilithium, Falcon, and SPHINCS+. Those algorithms are integrated into the Hyperledger Besu (DLT) and executed both inside and outside an Intel SGX TEE environment. According to our results, **CRYSTALS-Dilithium-2** combined with classical secp256k1 signatures leads to the shortest execution times when signing blocks in the DLT, reaching 1.68ms without the TEE, and 2.09ms with TEE. The same combination also displays the best results for signature verifications, achieving 0.5ms without a TEE and 1.98ms with a TEE. We also describe the main aspects of the evaluation methodology and the next steps in validating the proposed infrastructure. The conclusions drawn from our experiments is that the combination of PQC and TEE promises highly secure and effective DLT-based CBDC scenarios, ready to face the challenges of the digital financial future and potential quantum threats.

Keywords: *CBDC, Security, PQC, DLT, TEE*

[*] Computer Engineer (UNICAMP-2006) - Head of Emerging Technologies at Venturus: daniel.moraes@venturus.org.br

[†] AI/ML researcher at POLI/USP, Head of Innovation applied in Financial Services at Microsoft: jopereira@microsoft.com

[‡] Computer Scientist (UFOP-2002, MSc. UFMG-2005), Head of Emerging Technologies at Inter & Co: bruno.grossi@inter.co

[§] Professor of Technology and Data Science at FGV: gustavo.mirapalheta@fgv.br

[¶] Innovation leader at Bradesco: george.smetana@bradesco.com.br

[||] Sr. Security Architect at Microsoft and Master's degree student at IPT-SP – wrodrigues@microsoft.com.br

[**] CTO Financial Services Industry at Avanade – courtnayguima@gmail.com

[††] CTO Financial Services Industry at Intel – bruno.domingues@intel.com

[‡‡] Sr. Architect at Microsoft – fabio.saito@gmail.com

[§§] Professor at USP (security and blockchain) – mjunior@larc.usp.br

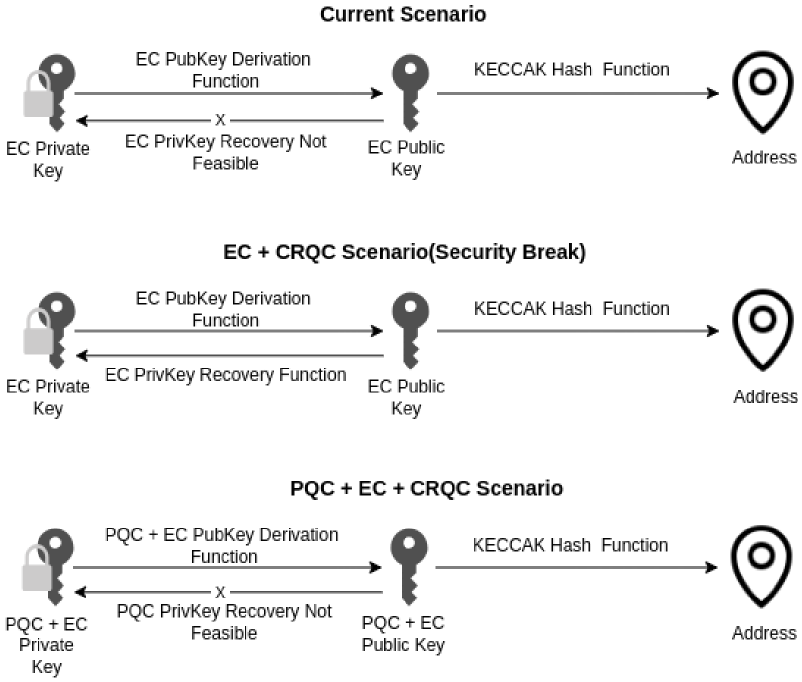
1 Introduction

As the world transitions toward a digital economy, Central Bank Digital Currencies (CBDCs) [12] have emerged as a critical component of modern financial systems. On the one hand, these digital representations of national currencies offer efficiency, transparency, and accessibility. On the other hand, ensuring the security and integrity of CBDC transactions is paramount.

In this context, the adoption of post-quantum cryptography within Distributed Ledger Technology (DLT) [31] is commonly seen as an important step toward long term secure and transparent systems. Specifically, CBDCs leverage DLTs to record transactions in a decentralized, tamper-resistant ledger.

Digital signatures play a pivotal role in CBDC transactions, ensuring authenticity, non-repudiation, and data integrity. However, quantum computers, with their immense computational power, pose a significant threat to classical cryptographic algorithms. Shor's algorithm [57], in particular, can efficiently factor large numbers and solve discrete logarithms, breaking widely used public-key cryptosystems like RSA (Rivest–Shamir–Adleman) [54] and ECC (Elliptic Curve Cryptography) [20]. As quantum computing matures, the need for cryptographic solutions that can withstand quantum attacks becomes urgent. After all, it is hard to foresee when a cryptographically relevant quantum computer (CRQC) [26, 35, 51, 4] will become a reality. When it does, however, any blockchain infrastructure that is not protected by quantum-resistant cryptographic algorithms will be at risk, as illustrated in Figure 1.

Figure 1: *Blockchain scenarios related to keys and address derivation.*


Current Scenario
EC PubKey Derivation Function
KECCAK Hash Function
x
EC PrivKey Recovery Not Feasible
EC Private Key
EC Public Key
Address
EC + CRQC Scenario(Security Break)
EC PubKey Derivation Function
KECCAK Hash Function
EC PrivKey Recovery Function
EC Private Key
EC Public Key
Address
PQC + EC + CRQC Scenario
PQC + EC PubKey Derivation Function
KECCAK Hash Function
x
PQC PrivKey Recovery Not Feasible
PQC + EC Private Key
PQC + EC Public Key
Address

In the current scenario, Ethereum [25] utilizes elliptic curves (EC) for key derivation and address generation. The process involves using a private key to derive the corresponding public key through the PubKey Derivation Function. This public key is then hashed using the Keccak hash function [46] to generate the Ethereum address. The security of this method relies on the mathematical difficulty of deriving the private key from the public key (or, equivalently, finding discrete logarithms in elliptic curves), a process that is currently infeasible with classical computing methods. However, the EC + CRQC scenario highlights a significant potential vulnerability with the advent of quantum computing. In this scenario, the same EC cryptographic process is used to derive the public key from the private key. However, quantum computers could potentially exploit the EC PrivKey Recovery Function to recover the private key from the public key. This represents a critical security breach, as the classical cryptographic assumptions no longer hold in the face of quantum capabilities. Such a breach could compromise the security of Ethereum addresses and transactions, emphasizing the need for a more secure approach.

To address these emerging threats, this work proposes the PQC + EC + CRQC scenario that is a hybrid cryptographic approach. This scenario involves combining PQC and EC private keys to derive a PQC + EC public key. The hybrid public key is then hashed using the Keccak hash function to produce the Ethereum address. This approach ensures that the private key recovery remains infeasible even with the advent of quantum computing, providing an additional layer of security. While this hybrid method introduces potential performance overhead due to the complexity of integrating PQC, it offers a future-proof solution that balances enhanced security with operational efficiency. This scenario underscores the importance of transitioning to post-quantum cryptographic methods to secure blockchain systems against both classical and quantum threats.

In this context, post-quantum cryptography is important because:

1. **Quantum Resistance**: Post-quantum cryptography offers secure algorithms even against quantum adversaries. Lattice-based, code-based, and multivariate polynomial-based schemes are promising candidates. These algorithms resist attacks from both classical and quantum computers, safeguarding CBDC transactions;
2. **Long-Term Security**: CBDCs are designed to last for decades. The cryptographic algorithms used today must withstand advances in quantum computing during this period. Post-quantum cryptography ensures the longevity of digital signatures, preventing vulnerabilities from emerging quantum technologies;
3. **Smooth Transition**: Implementing post-quantum cryptography early allows CBDC systems to adapt seamlessly to quantum-safe algorithms. Waiting until quantum computers are widespread could lead to rushed transitions, potentially compromising security. By integrating post-quantum techniques now, central banks can ensure a gradual and secure migration;
4. **Public Confidence**: CBDCs rely on public trust. Demonstrating a commitment to quantum-safe security reassures users that their digital transactions are protected. Post-quantum signatures enhance confidence in CBDCs, fostering adoption and acceptance.

Central banks must plan for a gradual transition [48]. Hybrid systems supporting classical and post-quantum signatures during the migration period are essential. The NIST (National Institute of Standards and Technology) Post-Quantum Cryptography Standardization project [50] aims to identify robust algorithms, such as CRYSTALS-Dilithium, Falcon, and SPHINCS+. CBDC systems, like DREX in Brazil, should align with these standards to ensure interoperability and future-proofing. In this way, our initial approach is to have a hybrid test environment with a classical signature added to a post-quantum encryption algorithm to analyze performance, as some post-quantum algorithms are computationally intensive, and balancing security and efficiency is crucial. In the era of quantum computing, CBDCs must prioritize security. Post-quantum cryptography provides a path forward, ensuring that digital signatures remain resilient against quantum attacks. By adopting these quantum-safe algorithms within DLT-based CBDCs, central banks can build a secure foundation for the future of digital finance. This work covers the importance of building a secure foundation and performance analysis about three algorithms: CRYSTALS-Dilithium, Falcon, and SPHINCS+.

1.1 Objectives and Motivation

The aim of this study is to demonstrate that a hybrid approach, integrating post-quantum and classical cryptography, can effectively defend against block and transaction signature attacks in a DLT-based CBDC environment, offering resistance to key-breaking attempts through quantum computing, with a specific focus on infrastructure transaction signature rather than individual user transaction signature. And, the main driver of this study is related to the growth of studies related to CBDC, with more than 130 countries [22], and many based on DLT with EVM (Ethereum Virtual Machine) compatibility, including the use of Hyperledger Besu in Brazil (DREX pilot).

1.2 Expected Contributions

The main contribution of this work is to prove the feasibility of implementing a hybrid approach to protect a DLT-based CBDC environment against key-cracking attacks with quantum computing, without compromising performance in a Wholesale and Retail environment, and consequently to maintain the security of the national financial ecosystem.

1.3 Document Structure

The document is structured into a series of chapters that collectively lay the groundwork, dissect methodologies, and culminate in a synthesis of findings and forward-looking insights. Session 1 outlines the demands and objectives of the study. Session 2 provides an overview of the fundamental concepts necessary for understanding the subject matter, and presents the algorithms selected by NIST for digital signatures. Session 3 delves into the research methodology employed. Session 5 presents the proposed implementation of this research and the approach taken. Session 6 presents the findings and interprets their significance within the context of the study. Session 7 presents a comparative analysis of performance between CRYSTALS-Dilithium and Falcon for post-quantum cryptography (PQC). Session 8 presents a comprehensive assessment to determine the viability of a proposed implementation across technical, economic and legal dimensions. As the document draws to a close, the Conclusion section in Session 9 offers a concise summary of the identified use cases, research conclusions, and potential future research avenues stemming from this study's findings.

2 Literature Review

2.1 Central Bank Digital Currencies (CBDCs)

Central Bank Digital Currency (CBDC) [12], which can also be a tokenized deposit [11], represents a new form of money, a digital extension of the fiat currency issued by a country. According to the World Economic Forum, 98% of global central banks are exploring CBDC to determine how to modernize the capabilities of and improve access to central bank money [64]. Twenty-four CBDCs are projected to go live by 2030.

Atlantic Council tracks CBDC projects worldwide [22] showing the advancement of interest in developing digital currencies. It shows that three countries have fully launched a CBDC: the Bahamas, Jamaica and Nigeria. Nineteen of the Group of 20 (G20) countries are now in the advanced stages of CBDC development. In most countries with an advanced retail CBDC project, the access to CBDCs is intermediated, meaning they are distributed through banks, financial institutions, and payment service providers.

2.2 Distributed Ledger Technology (DLT) and Blockchain

Recent years have seen the emergence of blockchain and Distributed Ledger Technologies (DLTs), which are transforming data storage and transaction processing. It's crucial to recognize that although related, blockchain technology and DLT are distinct entities. DLT is a comprehensive term covering various technologies that facilitate secure, transparent, and decentralized record-keeping across a network of participants [2]. It involves the use of diverse mathematical structures to register transactions in a distributed database. The most used alternative to blockchain as DLT technology is the Directed Acyclic Graph (DAG) [23].

Blockchain is a fault-tolerant distributed ledger platform that achieves consensus in a large, decentralized network of distrustful parties, enhancing security and transparency in transactions and digital interactions [34]. Originating with Bitcoin, introduced by Satoshi Nakamoto in 2008 as a peer-to-peer cryptocurrency mechanism without intermediaries [42], blockchain reduces fraud and data manipulation risks. Smart Contracts on Blockchain, defining token characteristics and governance, are self-executing contracts activated upon consensus, ensuring transaction security and reliability [28, 61]. The exploration of DLTs reveals their vast potential in facilitating and regulating transactions, extending to real-world objects and rights. This integration enhances the value and accessibility of these objects by providing improved record-keeping security, transparency, and ease of fractionation.

2.3 CBDC Infrastructure and Security Concepts

Wholesale CBDC infrastructure requires a security infrastructure that supports the high demand for interbanks and large-volume transactions. This includes implementing secure and efficient consensus protocols, rigorous authentication and authorization, and the ability to integrate with existing payment and settlement systems. On the other hand, Retail CBDC should focus on consumer protection and data privacy. This involves creating secure digital wallets, identity protection mechanisms, and implementing advanced encryption technologies to secure personal transactions.

Regardless of the type of CBDC, there are essential security components that must be incorporated. These include: **1) Robust Encryption**: Using cutting-edge encryption algorithms to protect data in transit (TLS) and at rest; **2) Multifactor Authentication**: Implementation of multiple layers of authentication to access critical resources; **3) Key Management**: A secure key management system is vital to maintain control over who can access and carry out transactions on the network; **4) Monitoring and Anomaly Detection**: Intrusion detection and continuous monitoring systems to identify and respond to suspicious activities in real-time; **5) Resilience**

to Failures: Design the network to be resistant to failures and attacks, ensuring continuity of services even in the face of adverse incidents. There are some specific challenges worth highlighting regarding security for DLT-based CBDCs:

1. **Digital identity and authentication**: to have a robust digital identity and authentication system to ensure transaction security. This involves using multi-factor authentication methods such as facial recognition, fingerprints or one-time passwords. Furthermore, it is essential to implement a reliable and decentralized digital identity infrastructure to ensure the integrity of transactions.
2. **End-to-end encryption, including hybrid or PQC-based**: requires the use of end-to-end encryption. This ensures that transactions are protected and that only authorized parties have access to sensitive information. End-to-end encryption is essential for both the wholesale and retail environments, as it prevents interception and fraud during transactions.
3. **Distributed consensus**: use of a distributed consensus mechanism. This ensures that all transactions are validated by a network of distributed nodes, thus avoiding the risk of a single entity having control over transactions. Consensus algorithms such as Proof of Work (PoW) or Proof of Stake (PoS) are widely used to ensure the integrity and security of the DLT network.
4. **Protection against cyber attacks**: to protect against cyber attacks, it is necessary to implement advanced security measures. This includes implementing firewalls, intrusion detection systems, and strong encryption to protect both transactions and data stored on the network. Additionally, it is important to perform regular audits and penetration tests to identify and fix potential vulnerabilities.
5. **Privacy and anonymity**: Ensuring the privacy and anonymity of transactions in a DLT-based CBDC is crucial, for example, using Microsoft Zero Knowledge Proof (ZKP) Nova [40]. While it is necessary to track and investigate suspicious activity, it is critical to strike a balance between necessary transparency and protecting users' privacy.

Thus, in addition to all these components, including the use of PQC algorithms, there is also the possibility of running the CBDC environment in confidential computing.

2.4 Trusted Execution Environment (TEE)

A Trusted Execution Environment (TEE) is a secure area of a main processor that guarantees code and data loaded inside to be protected with respect to confidentiality and integrity. TEEs are designed to be isolated from the main operating system, providing a strong defense against malware and other malicious attacks. One prominent example of TEE is Intel's Software Guard Extensions (SGX), which was selected for use in these tests. It introduces a set of security-related instruction codes that enable the creation of secure enclaves. These enclaves are protected areas of execution in memory, ensuring that the data and code inside them cannot be accessed or modified by any process outside the enclave, including those with higher privilege levels like the operating system or hypervisor [33].

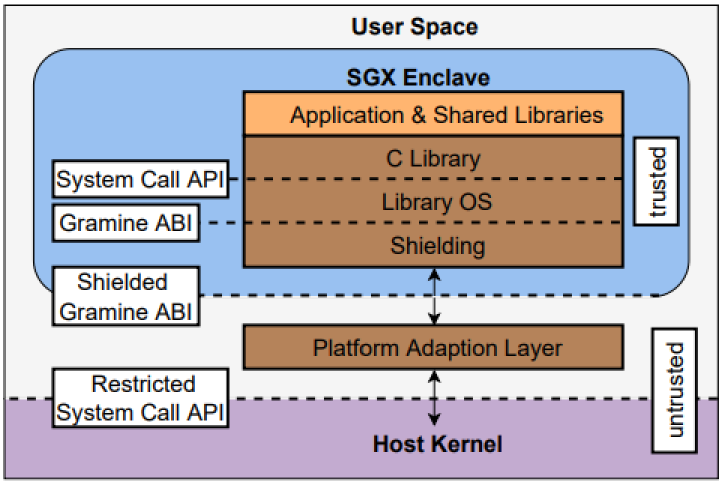
The primary benefits of Intel SGX lie in its robust security mechanisms and broad applicability in various sensitive computing tasks. Firstly, SGX provides hardware-based isolation, which is inherently more secure than software-based security solutions. This hardware-level protection ensures that even if the entire system is compromised, the enclave remains secure, thus providing a strong defense against a wide range of attack vectors, including those targeting privileged system software. Secondly, SGX supports secure remote attestation, which allows users to verify that the enclave is genuine and has not been tampered with. This capability is crucial for building trust in distributed systems, such as cloud computing, where users need assurance that their data is processed in a secure environment. Remote attestation enhances the credibility and trustworthiness of cloud services by providing verifiable proof of enclave integrity.

2.4.1 Gramine Library OS

Gramine is an open-source library operating system designed to facilitate the deployment of unmodified Linux applications within Intel SGX enclaves. By providing a lightweight and flexible framework, Gramine allows developers to execute their applications in a secure environment without the need to modify the original code. This compatibility is particularly advantageous for CBDC application, as it avoids lock-in with the platform while taking advantage of the security robustness of a hardware-based secure enclave. Gramine supports a wide range of applications, including those involving data-intensive computations as required by cryptographic algorithms. These ease of use and minimal overhead make Gramine an attractive option for hosting CBDC cryptographic operations.

From a security perspective, Gramine enhances the capabilities of Intel SGX by providing a comprehensive runtime environment that supports secure execution. It manages the interaction between the application and the SGX hardware, ensuring that sensitive data remains protected throughout its lifecycle. Gramine also implements security measures such as encrypted I/O operations, secure memory management, and controlled access to system resources, which further fortify the security guarantees of SGX enclaves. By isolating the application within an enclave, Gramine prevents unauthorized access and tampering from the underlying operating system or other applications. Additionally, Gramine supports remote attestation, allowing for the verification of the enclave's integrity and authenticity by external parties. This feature is crucial for applications deployed in cloud environments, where trust and data privacy are paramount such as CBDC [21].

Figure 2: *Gramine SGX Design.*



2.5 Post-Quantum Cryptography (PQC)

Post-quantum cryptography (also known as quantum-resistant cryptography or quantum computing-proof cryptography) is a research area that aims to create cryptographic algorithms resistant to attacks by quantum computers [52]. To understand the relevance of post-quantum cryptography, it is essential to first understand the current scenario. Conventional cryptography takes advantage of the existing difficulty in solving certain mathematical problems, such as the factorization of prime numbers or the discrete logarithm, to create ways to protect communication, such as RSA and elliptic curve keys [27].

The problems mentioned, which are complex for conventional computers, can be easily solved on quantum computers, which operate on a different principle. Shor's algorithm, for example, can factor large integers in polynomial time, which would compromise the security of current cryptographic systems [58]. Regev's algorithm can do the same as proposed by Shor but with even lower complexity [56]. Large companies, such as Microsoft and IBM are investing in research and development of quantum computers, with plans to have them operational before the next decade [38]. In light of this perspective, there is a need to find secure alternatives to current cryptography.

The National Institute of Standards and Technology (NIST) led a process to identify post-quantum cryptographic algorithms [44]. This effort involved the evaluation of several proposals, including schemes based on lattices, and function hashes, among others. NIST selected four algorithms in 2022 as the first group of winners. They are CRYSTALS-Kyber for Key Encapsulation Mechanism (KEM), and CRYSTALS-Dilithium, Falcon, and SPHINCS+ for digital signatures [47].

2.6 Post-Quantum Digital Signature Cryptography Algorithms

In this section, the algorithms selected by NIST for digital signatures are presented. Two are lattice-based (CRYSTALS-Dilithium, Falcon), and only SPHINCS+ is based on a different technology – a stateless hash-based signature scheme, according to Table 1.

Table 1: *Investigated post-quantum cryptography algorithms by NIST.*

Algorithm	Type	Family	NIST Round	Recommended
CRYSTALS-Dilithium	Digital Signature	Lattice	Standardization	Time sensitive
Falcon	Digital Signature	Lattice	Standardization	Signature size
SPHINCS+	Digital Signature	Hash	Standardization	Long term security

NIST selected SPHINCS+ (despite its inferior performance in most applications) with the intention of maintaining a contingency in the case a severe vulnerability is found with lattices [45]. Each algorithm present its own defined size for keys, signatures and also different security levels, as shown in Table 2.

Table 2: *Security analysis of post-quantum cryptography algorithms [55]*

Method	Public key size	Private key size	Signature size	Security level
CRYSTALS-Dilithium 2	1,312	2,528	2,420	1 (128-bit) Lattice
CRYSTALS-Dilithium 3	1,952	4,000	3,293	3 (192-bit) Lattice
CRYSTALS-Dilithium 5	2,592	4,864	4,595	5 (256-bit) Lattice
Falcon 512	897	1,281	690	1 (128-bit) Lattice
Falcon 1024	1,793	2,305	1,330	5 (256-bit) Lattice
SPHINCS+ SHA256-128f	32	64	17,088	1 (128-bit) Hash-based
SPHINCS+ SHA256-192f	48	96	35,664	3 (192-bit) Hash-based
SPHINCS+ SHA256-256f	64	128	49,856	5 (256-bit) Hash-based

2.6.1 CRYSTALS-Dilithium

CRYSTALS-Dilithium-2 [5, 39] is a digital signature scheme that is part of the Cryptographic Suite for Algebraic Lattices (CRYSTALS). It is built upon the hardness of lattice problems over module lattices, specifically leveraging the Learning with Errors (LWE) and Short Integer Solution (SIS) problems. The scheme employs the "Fiat-Shamir with Aborts" technique, which uses rejection sampling to ensure compact and secure lattice-based Fiat-Shamir schemes. Notably, CRYSTALS-Dilithium-2 avoids Gaussian sampling, opting instead for a uniform distribution, which contributes to its secure implementation against side-channel attacks. This design choice also results in optimized public key sizes, which is a significant improvement over previous designs. The security of CRYSTALS-Dilithium-2 is proven in the Random Oracle Model (ROM), and it is considered Strong Unforgeability under Chosen Message Attacks (SUF-CMA) secure, with a non-tight reduction. The algorithm is recognized for its efficiency and is comparable to the best current lattice-based signature schemes.

- Public-Key Sizes (bits) 10496-20736.
- Private-Key Sizes (bits) 20224-38912.
- Ciphertext Size (bits) 19360-36760.
- Hardness Module Small Integer Problem (MSIS) and Module Learning with Errors (MSIS).
- Further Comments: A public-key encryption counterpart, CRYSTALS-KYBER is also a NIST selected algorithm.
- Supported Security Levels 1, 3, 5.
- It is quantum-secure.

2.6.2 Falcon

Falcon [5] is a state-of-the-art post-quantum cryptographic signature algorithm, designed to provide secure digital signatures in the era of quantum computing. Submitted to the NIST Post-Quantum Cryptography Project in 2017, Falcon stands for "Fast Fourier lattice-based compact signatures over NTRU (Number Theory Research Unit). The algorithm is grounded in the hardness of NTRU lattice problems and employs a unique "fast Fourier sampling" technique for its trapdoor sampler. Falcon's design ensures that it remains secure against quantum computer attacks, which can break traditional number theory-based cryptographic systems like RSA and ECC. It offers several advantages, such as security with negligible information leakage on the secret key, compactness with substantially shorter signatures, and high performance with thousands of signatures per second achievable on common computers. Falcon's efficiency and scalability make it a promising candidate for securing digital communications in the forthcoming quantum era.

- Public-Key Sizes (bits) 7176-14264.
- Private-Key Sizes (bits) 10248-18440.
- Ciphertext Size (bits) 5328-10240.
- Hardness Short integer solution problem over NTRU lattices.
- Further Comments: Falcon uses floating-point arithmetic, which is uncommon in cryptography.
- Supported Security Levels 1, 3, 5.
- It is quantum-secure.

2.6.3 SPHINCS+

SPHINCS+ [5] is an advanced stateless hash-based signature framework that is part of the broader cryptographic initiative to develop quantum-resistant algorithms. It represents an evolution of the earlier SPHINCS scheme, offering enhancements in terms of speed, signature size, and security. SPHINCS+ operates on the principle of using a "hyper-tree" structure, which allows for the generation of signatures through a few-time signature scheme, significantly reducing the total tree height required for secure operations. One of the key modifications in SPHINCS+ is the addition of multi-target attack resilience, which fortifies the algorithm against various forms of cryptographic attacks. The framework provides fixed-length signatures, which are easier to compute than variable-size signatures, and it does not rely on Gaussian sampling, thus simplifying its implementation and reducing its vulnerability to side-channel attacks. SPHINCS+ is recognized for its collision- and multi-target attack resilience, making it a robust candidate for securing digital communications against the potential threats posed by quantum computing.

- Public-Key Sizes (bits) 32-64.
- Private-Key Sizes (bits) 64-128.
- Ciphertext Size (bits) 7856-49856.
- Hardness Collision Resistance.
- Further Comments: SPHINCS+ is selected as a NIST draft standard.
- Supported Security Levels 1, 3, 5.
- It is quantum-secure.

3 Methodology

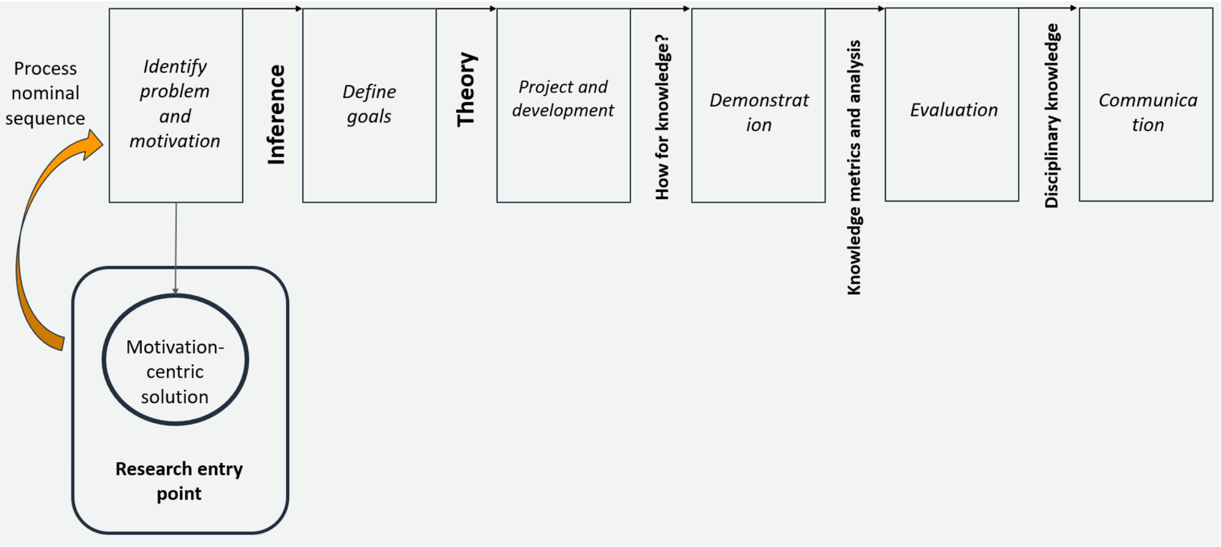
The method adopted to support the making of this article is the Design Science Research Methodology (DSRM) [53] in its nominal sequence. This method includes six steps: (1) problem identification and motivation; (2) definition of the objectives of a solution; (3) design and development; (4) demonstration; (5) evaluation; and (6) communication, as we can see in Figure 3. The method allows the search to start at any of steps (1), (2), (3), or (4), and therefore the nominal sequence of the process may not be followed. For this work, the solution sought is centered on motivation and, therefore, its first nominal activity was number one, based on growing and market demand, in addition to the regulator BCB (Brazilian Central Bank).

This chapter describes the applicability of DSRM to research about utilizing a hybrid approach of classical and post-quantum computing for digital signature protection to a DLT-based CBDC infrastructure environment, from demand confirmation to communication.

3.1 Demand confirmation

The demand for post-quantum cryptography has grown exponentially as quantum computing advances, bringing with it the threat of breaking traditional cryptographic algorithms, in convergence with the BIS (Bank for International Settlement) Leap [9] and Tourbillon [10] projects. In a process of digitally signing blocks and transactions, such as those used in DLT/blockchain, the security of the keys is paramount because quantum supremacy [26, 35, 51, 4]. Post-quantum cryptography offers a robust solution against attacks from quantum computers, which could easily decrypt keys created by conventional methods. The implementation of algorithms resistant to quantum attacks is essential to guarantee the integrity and authenticity of digital records, protecting them against adversaries who may have access to quantum technology in the future. Therefore, the transition to post-quantum cryptography is not just a preventative measure, but an imminent necessity for long-term cybersecurity for a country's financial ecosystem.

Figure 3: *Nominal sequence of Design Science Research Methodology (DSRM).*



3.2 Definition of goals

Fundamental objectives addressed in this white paper for applying post-quantum cryptography algorithms in a DLT-based CBDC environment:

- **Hybrid Approach** - evaluate whether the hybrid approach combined with classical cryptography (secp256k1 elliptic curve[ECC]) is feasible to be applied, for example, in a CBDC environment that uses Hyperledger Besu (DLT).
- **Performance** - to evaluate performance in terms of transaction duration, and feasibility of application in a Wholesale and Retail CBDC environment, as was done with PIX (Brazilian Instant Payment System) [17].

3.3 Design

The Motivation-Centered Solution was triggered by a real demand and can be treated with the development of a test environment with the use of the secp256k1 elliptic curve combined alternately with three digital signatures: CRYSTALS-Dilithium, Falcon (both lattice-based) and SPHINCS+ (hashed based). The same confidential computing environment was used (Microsoft Azure VM DCsV3 - Intel SGX processor [TEE - Confidential computing]) [7] for testing. However, one test using the segregated area of memory and CPU protected from the rest of the CPU using encryption such as Figure 4 (app enclave) [41], and another without using TEE, for performance comparison purposes.

3.4 Demonstration

This activity consists of defining and sharing of standard environment based on Hyperledger Besu, materialized in performance tests with the defined PQC algorithms and comparisons with the use of traditional computing and embedded TEE.

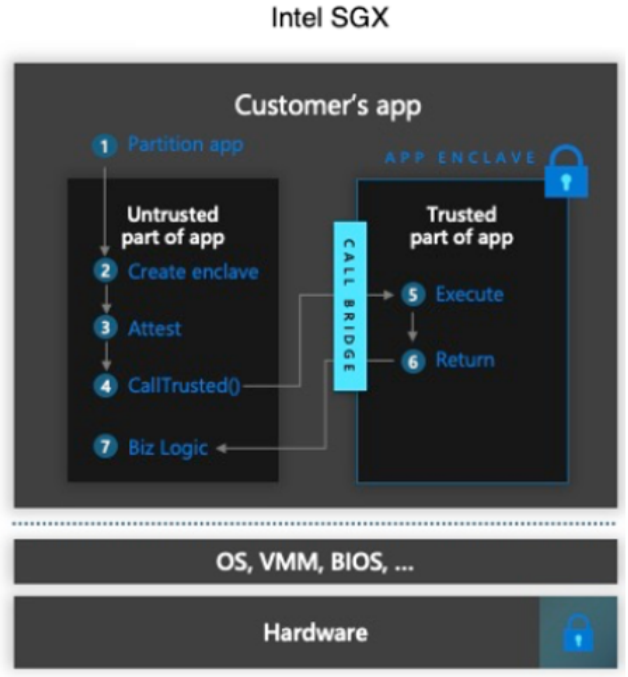
3.5 Evaluation

The assessment of the applicability of the integration will be carried out together with Inter&Co and Bradesco commercial banks beyond BCB and other financial institutions. It can be carried out later, through a pilot with them to implement the proposed approach, determine the integration flow, and determine which processes will be fully automated, in addition to the programmability, decentralization, and privacy.

3.5.1 CBDC Infrastructure Selection

The infrastructure of a Central Bank Digital Currency (CBDC) has crucial requirements such as running on reliable hardware and operating systems, ensuring privacy and confidentiality of transactions, and

Figure 4: *App enclave in Encrypted Protected Cache (EPC) within a VM.*



integrating technology for secure and immutable record-keeping. These requirements led to the architecture for experiments being a CBDC infrastructure utilizing distributed ledger technology which operates transactions through zero-knowledge proofs and runs its nodes in trusted execution environments.

Security is paramount in a CBDC infrastructure. To ensure a highly secure environment, we opted to implement a Trusted Execution Environment (TEE) across all network nodes. The TEE provides a hardware-protected, isolated environment where critical CBDC processes like cryptographic key generation and transaction execution can occur safely and reliably. This significantly reduces the attack surface and protects sensitive data from external threats. The DLT nodes run on Azure cloud using confidential virtual machines, which include Intel SGX processor providing a secure enclave. To maintain a secure and immutable record of all CBDC transactions, we integrated Distributed Ledger Technology (DLT). DLT is responsible for recording all transactions in chained blocks, ensuring records are transparent, tamper-resistant, and broadly distributed across the network. This adds an extra layer of security and trust, as each transaction is validated and recorded by multiple nodes in the network, making it nearly immune to malicious attacks. The DLT selected for testing is Hyperledger Besu, currently used in DREX, Brazilian CBDC.

3.5.2 Evaluation of Comparison Parameters

In the quest for quantum-resistant cryptographic solutions, three promising candidates stand out: CRYSTALS-Dilithium, Falcon, and SPHINCS+. These algorithms are at the forefront of securing digital communications against the looming threat of quantum computing. To effectively compare them, we must consider several critical parameters, each offering insights into their performance, security, and practicality. Understanding how these parameters correlate with traditional elliptic curve algorithms further enriches our analysis:

1. **Time to Sign and Verify Signatures**: One of the most direct measures of a cryptographic algorithm's efficiency is the time it takes to sign and verify signatures. These metrics are crucial for real-world applications where rapid authentication is necessary. CRYSTALS-Dilithium and Falcon, being structured lattice-based schemes, generally offer faster signing and verification times compared to SPHINCS+, a stateless hash-based signature algorithm. This efficiency closely relates to elliptic curve algorithms, where the balance between speed and security is also vital. However, it's important to note that post-quantum algorithms tend to have longer key generation times due to their complex structures.
2. **Signature and Key Sizes**: The size of signatures and keys is a significant factor, especially in environments with limited bandwidth or storage capacity. SPHINCS+ signatures, for instance, are notably larger than those produced by CRYSTALS-Dilithium and Falcon, which might be a drawback for certain applications. In comparison, elliptic curve algorithms are known for their compact keys and signatures, a feature

that post-quantum algorithms strive to achieve through various optimizations without compromising security.

3. **Difficulty to Break**: The resistance of an algorithm to cryptographic attacks, especially those leveraging quantum computers, is perhaps its most critical attribute. CRYSTALS-Dilithium, Falcon, and SPHINCS+ are designed to be resistant to both classical and quantum attacks, with security levels often compared to or exceeding those of elliptic curve cryptography (ECC). The "difficulty to break" is quantified by the work factor, representing the computational effort required to compromise the system. While ECC's security relies on the hardness of the elliptic curve discrete logarithm problem, post-quantum algorithms base their security on problems believed to be hard even for quantum computers, such as the shortest vector problem (SVP) for lattice-based schemes or the pre-image resistance of hash functions for SPHINCS+.
4. **Correlation with Elliptic Curve Algorithms**: When correlating these parameters with elliptic curve algorithms, it's essential to consider the underlying mathematical problems and their perceived hardness in a post-quantum world. While ECC provides efficient and secure solutions for today's cryptographic needs, its reliance on problems vulnerable to quantum attacks necessitates the transition to quantum-resistant alternatives. The evaluation of time to sign, verify, and the sizes of keys and signatures offer a direct comparison in terms of performance and efficiency. Meanwhile, the difficulty of breaking parameters provides a common ground to assess and ensure the long-term security of cryptographic systems in the face of quantum advancements.

In conclusion, comparing CRYSTALS-Dilithium, Falcon, and SPHINCS+ through these parameters not only highlights their respective strengths and potential limitations but also situates them within the broader context of cryptographic evolution from elliptic curve algorithms to quantum-resistant solutions. As the field progresses, these comparisons will guide the selection and standardization of algorithms that ensure the confidentiality, integrity, and authenticity of digital communications in the quantum era.

3.5.3 Selection of the Post-Quantum Cryptography algorithm

Selecting the appropriate post-quantum cryptography (PQC) algorithm to be used alongside secp256k1 in a DLT for block and transaction signatures is a crucial step in ensuring the security and efficiency of the system. The National Institute of Standards and Technology (NIST) has been at the forefront of evaluating PQC algorithms to address the growing threat posed by quantum computers. One of the significant challenges highlighted by NIST is the difficulty in comparing PQC algorithms with classical algorithms. Classical algorithms, such as those based on elliptic curve cryptography (ECC) like secp256k1, have been extensively studied and optimized over the years. In contrast, PQC algorithms are relatively new and vary widely in their structure and performance characteristics. To address this, NIST has considered several factors to ensure a fair comparison, including security level, key sizes, and computational efficiency.

When selecting a PQC algorithm, it is crucial to maintain the same level of security as classical algorithms. This involves ensuring that the PQC algorithm provides a comparable security margin against both classical and quantum attacks. Smaller key sizes are particularly advantageous as they reduce the storage and transmission overhead, which is vital in DLT/blockchain environments where efficiency and scalability are paramount. Additionally, the time required to sign and verify transactions is a critical factor, as these operations are performed frequently in DLT/blockchain networks and directly impact overall performance.

In line with NIST's recommendations, two PQC algorithms stand out for consideration: CRYSTALS-Dilithium and Falcon. Both algorithms have been designed to offer strong security guarantees while maintaining practical performance levels. CRYSTALS-Dilithium is known for its simplicity and ease of implementation, making it a robust choice for DLT/blockchain applications. It provides efficient key generation, signing, and verification processes, which are crucial for maintaining high transaction throughput. Following the NIST's comparisons between classical and post-quantum cryptographic algorithms, CRYSTALS-Dilithium-2 was selected because it maintains the same security level as secp256k1.

Falcon, on the other hand, is recognized for its compact key sizes and signatures, which make it an attractive option for systems with stringent space and bandwidth constraints. Its performance in terms of signing and verification times is competitive, ensuring that it can handle the demands of a high-frequency transaction environment typical of DLT/blockchain systems. Falcon-512 was considered the appropriate algorithm to keep the secp256k1 level of security as proposed by NIST but exists a work that claims that the complexity of breaking a Falcon lattice of rank "n" can be reduced to rank "n/2" [8]. This fact influenced the decision to use Falcon-1024 as the appropriate algorithm to keep the security level.

SPHINCS+ algorithm was considered only for research purposes, acknowledging NIST's explanation that it is not suitable for this kind of online signature. Despite this limitation, SPHINCS+ offers an intriguing alternative to lattice-based algorithms, providing a distinct method for digital post-quantum safe signatures. The parameters used with SPHINCS+ were SHA2 as the hash function, 128 bits of security level, and the fast form. Ultimately, the selection of a PQC algorithm for use with secp256k1 in DLT/blockchain must balance security, performance, and practicality. By considering the recommendations and evaluations provided by NIST, and focusing on algorithms like CRYSTALS-Dilithium and Falcon, DLT/blockchain developers can make informed decisions that safeguard their systems against future quantum threats while maintaining efficient and scalable operations.

3.6 Communication

This white paper was prepared to be presented to the BCB. In this way, the practical results of this white paper will be shared with the BCB, primarily, before it is proposed for publication in Nature Journey [43].

4 Related Work

The looming threat of quantum computers poses a significant challenge to existing public-key cryptography (PKC) schemes used in digital signatures as demonstrated by Shor's Algorithm [57]. Often PKC schemes based on Elliptic Curve Cryptography (ECC), like Blockchains, are not safe [63]. BIS reinforced the importance of quantum-resistance algorithms applied in financial ecosystem and addressed on Project Leap [9] the threat that future quantum computers represent to financial stability, even in a VPN tunnel environment, and demonstrates, on Project Tourbillon [10], that implementing quantum-safe cryptography on CBDCs is possible, but that it requires specialized expertise and scalability improvements. Allende et al. proposed quantum resistance adaption of existing public blockchains (EVM compatible) and on-chain verification using Falcon-512 post-quantum keys. However, our work is off-chain and compares the three PQC algorithms for digital signature, listed by NIST: Falcon, CRYSTALS-Dilithium and SPHINCS+, and demonstrates, in terms of execution time, that the CRYSTALS-Dilithium algorithm was the fastest.

Hupel and Rafiee in 2024 [29] studied typical assets in a CDBC system to understand which ones are most amenable to post-quantum cryptography, proposing an upgrade framework focusing on user wallets. Even though recent studies have explored various aspects of quantum resistance algorithms integration, focusing on feasibility, performance, key management, and interoperability — essential metrics for the successful deployment of PQC in CBDC systems —, to date it has not been possible to find a significant amount of relevant literature related to PQC algorithms applied to DLT-based CBDCs and its implementation in real software like Hyperledger Besu.

The work referenced in [3] is quite comprehensive regarding the introduction of post-quantum security into a blockchain. It has many aspects related to this project since it also uses Besu as a basis for modifications. A differentiator of our work is that we assume a direct off-chain change must be made in the block signature process within the implementation of nodes and wallets, rather than through on-chain contracts dealing with post-quantum signatures. The approaches of the reference work for on-chain signature incur both "gas" and processing costs for layer 1 operations of the network and do not transparently handle operations that should not be considered in these layers, including mixing responsibilities of the layers. However, it is important to highlight the care taken regarding the communication tunnels between the nodes with TLS and retro-compatibility, already considering algorithms and certificates with post-quantum support. Another factor to consider are the algorithms tested in each project; in the referenced work, only Falcon was considered, whereas in this project we are working with Crystals-Dilithium, Falcon, and SPHINCS+.

The global financial ecosystem, including BIS and Central Banks, and academic beyond WEF (World Economic Forum) [62] discourse on PQC in DLT-based CBDCs underscore the importance of a multifaceted approach considering feasibility, performance, key management, and interoperability. PQC two-key signatures offer a promising approach to securing CBDCs built on Hyperledger Besu, based on a hybrid digital signature environment. While challenges exist regarding performance optimization, interoperability, and integration, ongoing research efforts hold the potential to overcome these hurdles. By actively exploring PQC integration and collaborating on standardization efforts, the Hyperledger Besu community can contribute to the development of secure and future-proof CBDC systems. This article provides an implementation and roadmap for developing robust and secure CBDC systems that can withstand the quantum threat.

5 Implementation

The implementation of Post-Quantum Cryptography (PQC) for the Central Bank Digital Currency (CBDC) utilized version 24.1.2 of the open-source project Hyperledger Besu [31], incorporating the robust capabilities of the Bouncy Castle Java library [60]. This choice ensures the cryptographic backbone of our infrastructure is grounded in secure, up-to-date standards crucial for protecting the CBDC against existing and emerging threats. Our specific implementation of the cryptography algorithm is outside the scope of this work.

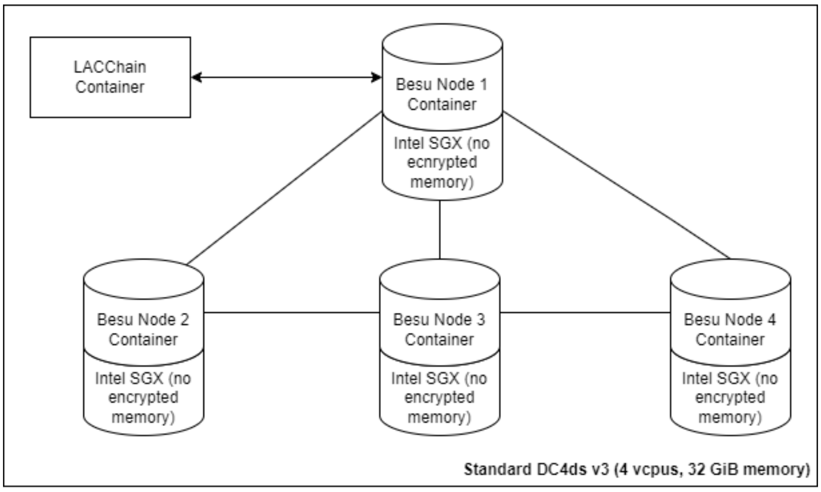
To integrate PQC into Hyperledger Besu, we made necessary modifications to handle the demands of quantum-resistant algorithms, including adapting cryptographic modules to the increased complexity and unique paradigms of PQC. The process was thoroughly documented to ensure reproducibility and support further development and audits by the community and experts. This strategic integration not only bolsters the security of the CBDC platform against quantum computing threats, but also underscores our commitment to employing cutting-edge technology to secure digital assets. This groundwork lays the foundation for future enhancements as quantum computing advances and new quantum-resistant algorithms emerge.

5.1 Architecture

The architecture of cryptographic signing and verification in Hyperledger Besu, like in many Ethereum-based platforms, is deeply intertwined with the use of the secp256k1 elliptic curve. This curve is pivotal for generating public-private key pairs, which are fundamental for security and identity verification within the DLT. The process primarily involves two critical operations: signing transactions with a private key and verifying these transactions by recovering the public key from the signature. Let's delve into the architecture and then discuss where and how Post-Quantum Cryptography (PQC) can be integrated into this framework.

To thoroughly evaluate the performance and feasibility of integrating PQC into a DLT environment, it was developed a test DLT architecture based on multiple nodes. This architecture was designed to test the signing and verification functions under conditions that closely mimic real-world operations. The test setup involves four DLT nodes configured to handle transactions and maintain consensus using QBFT (Quorum Byzantine Fault Tolerance) protocol [30], thereby providing a robust platform for assessing the impact of PQC on DLT performance. The testing framework leverages the LACChain Ethereum Benchmark [36], a well-established tool for evaluating DLT transaction rates and performance metrics. By using this benchmark, it was able to systematically test the transaction rates and precisely measure the time consumption of sign and verify operations across different cryptographic configurations. This approach was able to gather comprehensive data on the performance overhead introduced by PQC algorithms when integrated with the classical secp256k1 algorithm in a hybrid cryptographic system.

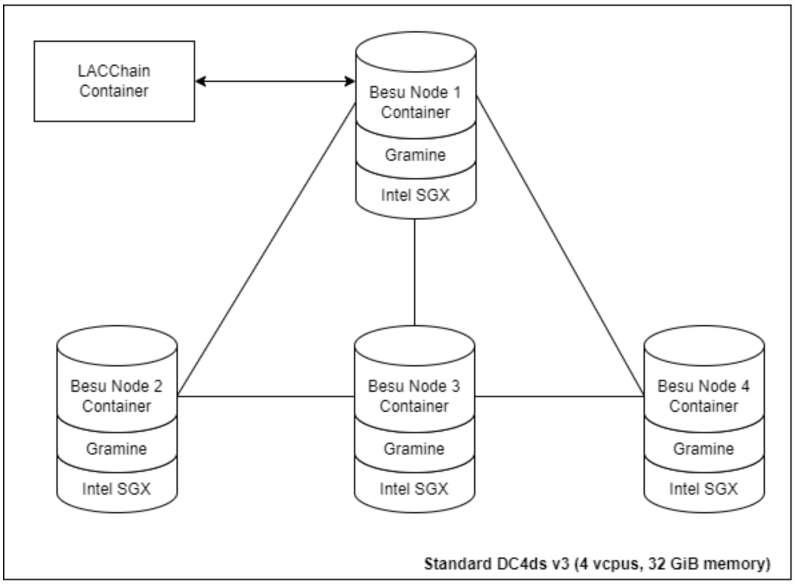
Figure 5: *Test environment architecture without TEE (SGX enclave + Gramine).*


LACChain Container
Besu Node 1 Container
Intel SGX (no ecnrypted memory)
Besu Node 2 Container
Intel SGX (no encrypted memory)
Besu Node 3 Container
Intel SGX (no encrypted memory)
Besu Node 4 Container
Intel SGX (no encrypted memory)
Standard DC4ds v3 (4 vcpus, 32 GiB memory)

The architecture of the test environment is illustrated in the accompanying Figure 5. It showcases the interconnected nodes, each equipped with the necessary cryptographic libraries to perform hybrid signing and verification operations. The nodes are configured to simulate typical DLT transactions, enabling it to measure the impact of different cryptographic algorithms on transaction throughput and latency. This setup ensures that the findings are relevant and can be directly applied to real-world DLT systems. By analyzing the data collected from this environment, this work aims to provide insights into the practical implications of adopting PQC in DLT technology.

To enhance the security of each node in the test DLT architecture an extra layer of security was implemented using a TEE. This additional layer was provided by Gramine and Intel SGX as explained before. This enhanced security architecture is depicted in Figure 6, which illustrates the deployment of TEEs across the DLT nodes, highlighting how communication and execution in secure enclaves are encapsulated to prevent unauthorized access and tampering.

Figure 6: *Test environment architecture with TEE (SGX enclave + Gramine).*



5.1.1 Transaction verification

The verification process in Hyperledger Besu is a critical component that ensures the authenticity and integrity of transactions within the network. This process leverages the unique properties of the secp256k1 elliptic curve, enabling the recovery of the signer's public key from the digital signature itself. This section delves into the mechanics of signature verification, highlighting its significance in maintaining the security and trustworthiness of the DLT. A distinguishing feature of Hyperledger Besu's cryptographic framework is its ability to extract the signer's public key directly from the transaction's digital signature. This is facilitated by the mathematical properties of the secp256k1 curve, which allow for the derivation of the public key from the signature components (r, s) and the transaction hash. This key recovery mechanism is instrumental in the verification process, as it eliminates the need to store public keys on the DLT, thereby optimizing storage and enhancing privacy.

Once the public key is recovered, the next step is to verify the digital signature against the transaction data. This involves a series of mathematical operations that confirm the holder of the corresponding private key indeed generated the signature. The verification process employs the Elliptic Curve Digital Signature Algorithm (ECDSA), utilizing the recovered public key and the original transaction data. If the signature is valid, it unequivocally demonstrates that the transaction was created and approved by the possessor of the private key, thereby affirming its authenticity and integrity. The signature verification process is paramount in preventing fraudulent transactions and ensuring each transaction is traceable to a specific entity. This reinforces the security of the Hyperledger Besu network and upholds the principle of non-repudiation, which is essential in maintaining trust among participants in the DLT ecosystem.

5.1.2 Block signing

Block generation within the Hyperledger Besu architecture is a critical component, ensuring the integrity and continuity of the DLT. This process is underpinned by the consensus mechanism employed by the network, such as Proof of Authority (PoA), each dictating the specific conditions under which a new block is proposed and accepted by the network. Central to the block generation process is the role of digital signatures, not only for individual transactions but also for the block itself, enhancing the security and verifiability of the entire DLT structure.

In the context of Besu, each block comprises a header, a set of transactions, and a block signature. The block header includes several pieces of critical information, such as the reference to the previous block hash, a timestamp, and the Merkle root of the transaction tree, which collectively ensure the immutability and chronological ordering of blocks. The transactions within the block are individually signed by the senders as previously described, employing the ECDSA over the secp256k1 elliptic curve, which provides a robust framework for transaction authentication. The block signature is a further augmentation of security, particularly relevant in PoA consensus mechanisms where blocks are minted by authorized validators. In such systems, the block proposer signs the block header, embedding a signature that can be publicly verified against the proposer's known public key. This signature serves as a non-repudiable proof of the block's origin, ensuring that the block was indeed created by a legitimate validator within the network. The verification of this block signature involves extracting the public key from the signature and comparing it against a predefined list of valid proposer public keys, thus affirming the block's validity.

The integration of block signatures within the Besu architecture necessitates meticulous attention to the security of private keys used by block proposers. A compromised key could lead to unauthorized block generation, undermining the network's integrity. As such, key management practices, including secure key storage and periodic key rotation, become paramount in maintaining the DLT's security posture. In conclusion, the block generation and signature verification process in Hyperledger Besu embodies a multi-faceted approach to security, leveraging digital signatures at both the transaction and block levels to ensure the integrity and authenticity of the DLT. This dual-layered application of cryptographic principles fortifies the network against tampering and unauthorized alterations, cementing the foundational trustworthiness of the DLT.

5.2 PQC Integration

Integrating post-quantum cryptography into a DLT is a complex task due to the requirement for independent addresses separate from the signature keys. This challenge is particularly evident in the Ethereum protocol, which derives addresses directly from public keys. The Ethereum protocol uses these public keys in operations to verify the authenticity of transactions, making the integration of PQC algorithms more difficult. As a result, it was only possible to simulate the use of PQC algorithms for signatures. To fully implement PQC, it would need to decouple the account from its verification process, as proposed in EIP-7702 Account Abstraction [24]. This separation is not a trivial task and would require considerable time and effort, which is beyond the scope of this paper.

While a full implementation integrating PQC with Ethereum's existing account structure would be ideal, it involves extensive modifications to the protocol. These modifications include redefining how addresses and public keys interact within the DLT, a process that is intricate and time-consuming. Therefore, this work was focused on simulating PQC within the current framework to evaluate its feasibility and performance impact. By simulating PQC signatures was possible to assess the performance and confirm that it is feasible to achieve post-quantum security without rendering the system inefficient. In this integration, it was crucial to adhere to NIST's advice on using hybrid signatures [49]. Since PQC algorithms have not yet been fully tested and proven, combining them with classical algorithms allows us to maintain security. Therefore, secp256k1 was still used alongside PQC algorithms. If the PQC algorithm fails, the system can fall back on the classical algorithm, ensuring continuous security. Once PQC algorithms have their security fully verified, the classical component can be removed.

This hybrid approach, while increasing the signature time, introduces an additional layer of security to the DLT. Leveraging both classical and PQC methods can enhance the resilience of the system against potential quantum attacks while retaining the reliability of established classical algorithms. The increase in signature time is a necessary trade-off for the enhanced security provided by this dual-layer approach. This method ensures that even during the transition to post-quantum security, the DLT remains protected, mitigating risks associated with the relatively untested nature of PQC algorithms. It is possible to implement the hybrid approach signature in three ways [37]: nested, concatenated, and true hybrid. The concatenated way was used in this project due to it is the easiest way to implement and test.

Figure 7 illustrates the architecture of the test designed to evaluate the performance of signing functions, in a DLT node with QBFT for consensus algorithm, using both classical and PQC algorithms. The diagram shows the process flow for message signing and the time measurements involved, integrating both secp256k1 and PQC signing functions. This flow has two main parts and can be described as below:

1. Message Signing with secp256k1 (Figure 7):
   (a) The *QBFT Consensus Module* sends a message to the *secp256k1 sign function* to be signed.
   (b) The signing time for secp256k1 is measured (secp256k1 measured time).
   (c) The function returns the signed message (using secp256k1) back to the *QBFT Consensus Module* and to the *PQC Sign Simulation module*.
2. Simulating PQC Signing (Figure 7):
   (a) The signed message from the *secp256k1 sign function* is sent to the *PQC Sign Simulation module* to simulate signing with PQC.
   (b) The *PQC sign function* signs the message, and the signing time for PQC is measured (PQC measured time).
   (c) The signed message with both secp256k1 and PQC signatures is generated but is discarded as indicated by the 'X', indicating that it is not used further in this simulation.

Figure 7: *PQC sign simulation architecture.*

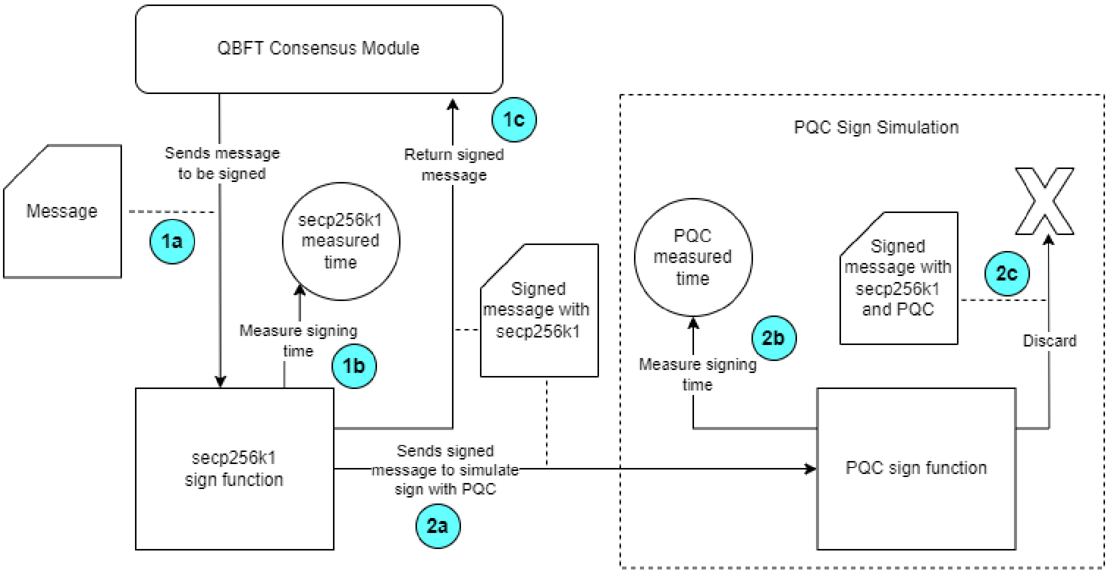
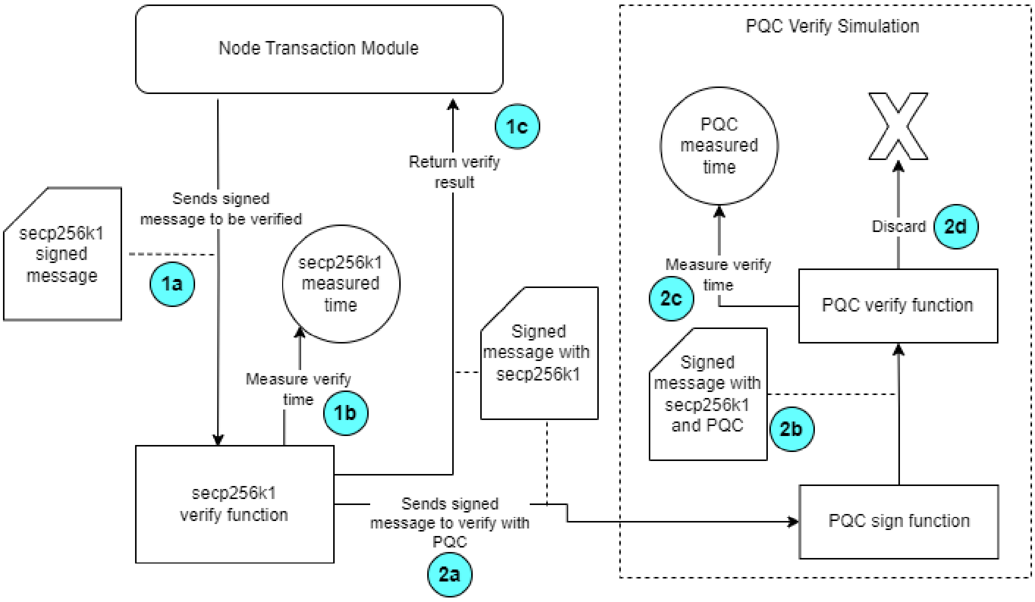


Figure 8 is another architecture that was designed to evaluate the verify process on the same DLT infrastructure. There is still a two main steps flow, but in this process the PQC signing time is not considered as only the verify time is being evaluated. The flow is described below:

1. Message Verification with secp256k1 (Figure 8):
   (a) The *Node Transaction Module* sends the signed message to the *secp256k1 verify function* to verify the signature.
   (b) The verification time for SECP256k1 is measured (secp256k1 measured time).
   (c) The function returns the verification result back to the *Node Transaction Module* and a copy to the *PQC Verify Simulation module*.
2. Simulating PQC Verification (Figure 8):
   (a) The signed message from the SECP256k1 function is sent to the *PQC Verify Simulation module* to simulate verification with PQC.
   (b) The *PQC Sign Function* generates a PQC signature for the signed message simulating it came PQC signed from the wallet.
   (c) The *PQC Verify Function* verifies the message, and the verification time for PQC is measured (PQC measured time).
   (d) The signed message with both secp256k1 and PQC signatures is generated but is discarded as indicated by the 'X', signifying that it is not used further in this simulation.

The insights gained from this study lay the groundwork for future research and development, paving the way for more robust integration of PQC in DLT systems, once the necessary protocol adjustments, such as those suggested in EIP-7702, can be systematically addressed.

Figure 8: *PQC verify simulation architecture.*



5.2.1 Security resources

The Bouncy Castle project offers open-source and multi-language APIs that support cryptography and cryptographic protocols [60]. They cover many security areas, such as public key infrastructure, digital signatures, authentication, and secure communication. It is widely used in the development of secure applications that require robust cryptographic functions. This library is known for its versatility and scalability, making it suitable for a wide range of cryptographic applications, and is a reference for the implementation of NIST PQC Competition Algorithms [45] in Java. However, it's crucial to acknowledge that the PQC algorithms implemented are still in the developmental phase, with published standards not expected before mid-2024. As of now, the Key Encapsulation Algorithms (KEMs) are suitable for use with hybrid cryptography using short-term keys. Given the possibility of ongoing changes, discretion is advised when considering their suitability for long-term usage.

5.3 Scalability Considerations

The integration of a hybrid PQC signature method within Hyperledger Besu introduces several scalability considerations that must be meticulously evaluated. The inherent complexities and resource requirements of PQC algorithms, compared to their classical counterparts, necessitate a thorough analysis of their impact on the DLT's performance, particularly in terms of block size, transaction throughput, and consensus efficiency.

Firstly, PQC signatures typically exhibit larger sizes than Elliptic Curve Digital Signature Algorithm (ECDSA) signatures. The inclusion of both signature types in a transaction would inherently increase the transaction size, potentially leading to larger block sizes. This increase could exert additional pressure on network bandwidth and storage requirements, particularly for nodes tasked with maintaining a complete copy of the DLT. The expanded block size may also affect block propagation times, a critical factor in maintaining network synchrony and reducing the likelihood of fork occurrences.

Secondly, the computational complexity of generating and verifying PQC signatures must be considered. PQC algorithms, while offering enhanced security against quantum attacks, often require more substantial computational resources. This increased computational demand could lead to longer transaction processing times, impacting the overall transaction throughput of the network. For validators, especially those with limited computational resources, this could raise the barrier to participation, potentially affecting the decentralization and security of the network.

Furthermore, the consensus mechanism employed by the Besu network requires careful examination in the context of PQC integration. In consensus protocols such as Proof of Authority (PoA), where block validation is performed by a set of authorized validators, the increased time required to verify hybrid signatures could introduce delays in the block finalization, affecting network throughput and latency.To mitigate these scalability challenges, several strategies could be explored. Optimizations in the implementation of PQC algorithms could reduce their computational overhead, making them more viable for DLT applications. Additionally, the development of more efficient hybrid signature schemes, which minimize the additional size and computational requirements, could alleviate the impact on transaction and block sizes. Finally, adaptive block generation and consensus mechanisms that dynamically adjust parameters in response to network conditions could help in balancing security with performance needs.

In conclusion, the integration of a hybrid PQC signature method in Hyperledger Besu necessitates a comprehensive analysis of scalability implications, focusing on block and transaction sizes, computational demands, and consensus efficiency. Addressing these considerations is paramount in ensuring that the enhanced security provided by PQC does not compromise the DLT's performance and scalability.

6 Results and Discussions

6.1 Analysis of signing

In the comparative analysis of hybrid PQC algorithms, we enveloped the classical secp256k1 algorithm inside each PQC algorithm to evaluate their performance in terms of signing speed. The goal was to determine which algorithm combination offers the best balance of security and efficiency for DLT applications.

The results indicate that **CRYSTALS-Dilithium-2** emerged as the best-performing PQC algorithm to be combined in terms of signing speed. As anticipated, CRYSTALS-Dilithium-2 efficiently handled the signing operations, maintaining a speed that makes it a practical choice for real-time and near-real-time applications within a DLT environment. Its performance in hybrid mode, combining the security of PQC with the proven robustness of secp256k1, confirms its suitability for securing DLT transactions without significant performance degradation.

Falcon-1024, while showing commendable performance, was found to be approximately five times slower than CRYSTALS-Dilithium-2. Despite this slower signing speed, Falcon-1024 offers the advantage of significantly smaller signature sizes, as discussed before, which can be beneficial in scenarios where storage and bandwidth are constrained. The trade-off between signing speed and signature size makes Falcon-1024 an interesting option for applications where minimizing data transmission overhead is critical.

SPHINCS+ demonstrated the slowest signing speed among the evaluated algorithms. This is consistent with its design, which prioritizes security and robustness over speed. SPHINCS+ is based on a fundamentally different cryptographic family, utilizing hash-based signatures, which inherently require more computational effort. However, the distinct advantage of SPHINCS+ lies in its security properties, being resistant to a wide range of cryptographic attacks. This unique aspect makes SPHINCS+ a valuable candidate for further research, particularly if performance optimizations can be realized. Enhancements in computational efficiency for SPHINCS+ could make it a more viable option for broader use in DLT applications.

In conclusion, for the signing process as observed in times as shown in Table 3, the comparative analysis highlights that CRYSTALS-Dilithium-2 is the most efficient hybrid PQC algorithm in terms of speed, making it highly suitable for integration into DLT systems, such as Hyperledger Besu. Falcon-1024 offers a compelling alternative with smaller signature sizes, albeit at a slower signing speed. SPHINCS+ remains a secure, albeit slower, option with potential for future performance improvements. This analysis provides a clear direction for selecting and optimizing PQC algorithms to ensure secure and efficient DLT operations in the post-quantum era.

Table 3: *Times of each tested algorithms for one signing operations involved in the creation of a DLT block.*

Algorithm PQC + secp256k1	P90 (sec)	P95 (sec)	P99 (sec)	Average (sec)
CRYSTALS-Dilithium-2	0,00105	0,00168	0,00566	0,00078
Falcon-1024	0,00578	0,00944	0,01917	0,00342
SPHINCS+	0,20428	0,27813	0,44733	0,10916

6.2 Analysis of signature verification

In the analysis of the signature verification using a hybrid approach, the performance of combination of algorithms is compared in Table 4. The hybrid method involves verifying both the PQC and secp256k1 signatures to ensure robust security against both classical and quantum threats. The evaluation still focused on the three PQC algorithms treated in this work: CRYSTALS-Dilithium-2, Falcon-1024, and SPHINCS+.

Table 4: *Ttimes of each tested algorithms for one transaction verify operations.*

Algorithm PQC + secp256k1	P90 (sec)	P95 (sec)	P99 (sec)	Average (sec)
CRYSTALS-Dilithium-2	0,00035	0,00056	0,00625	0,00038
Falcon-1024	0,00036	0,00058	0,00880	0,00046
SPHINCS+	0,02807	0,04297	0,07908	0,01258

The results of the analysis revealed that CRYSTALS-Dilithium-2 and Falcon-1024 exhibit comparable performance in terms of signature verification speed. Both algorithms demonstrated the ability to verify signatures efficiently, making them suitable candidates for hybrid implementation in DLT systems. CRYSTALS-Dilithium-2, in particular, showed verification speeds nearly on par with Falcon-1024, highlighting its potential for practical deployment in real-world applications where fast verification is critical. This efficiency ensures that the added security of post-quantum algorithms does not come at the cost of significant performance degradation. In contrast, SPHINCS+ was found to be approximately 30 times slower in verification compared to CRYSTALS-Dilithium-2 and Falcon-1024. This substantial difference in verification speed is attributable to the inherent design and computational requirements of SPHINCS+, which relies on hash-based cryptographic principles. While SPHINCS+ offers strong security guarantees and resilience against quantum attacks, its slower verification speed poses challenges for its use in high-frequency transaction environments, such as DLT networks for retail environments.

6.3 Analysis using TEE environment

In this study is integrated an additional layer of classical security in DLT nodes to address concerns related to execution time and security. This layer is referred to as the Trusted Execution Environment (TEE), Intel SGX Enclave with Gramine being the implementation used. The inclusion of TEE aims to enhance the security of node operations by isolating sensitive computations and protecting them from potential vulnerabilities.

However, the introduction of TEE resulted in time overheads during the signing and verification operations of PQC algorithms, detailed in Tables 5 and 6. Specifically, algorithms such as CRYSTALS-Dilithium-2 and Falcon-1024 experienced increased execution times due to the additional security measures imposed by the TEE. The overhead is attributed to the complex processes involved in maintaining an isolated and secure environment for cryptographic operations, which inherently require more computational resources and time.

Table 5: *Times of each tested algorithms for one signing operations involved in the creation of a DLT block on a node running over TEE.*

Algorithm PQC + secp256k1	P90 (sec)	P95 (sec)	P99 (sec)	Average (sec)
CRYSTALS-Dilithium-2	0,00145	0,00209	0,00826	0,00102
Falcon-1024	0,00837	0,01353	0,03457	0,00500
SPHINCS+	0,27984	0,37024	1,46751	0,15755

Interestingly, SPHINCS+ proved to be less susceptible to the time overhead introduced by the TEE layer. Despite its inherently slower performance in cryptographic operations compared to CRYSTALS-Dilithium-2 and Falcon-1024, SPHINCS+ showed relatively consistent execution times even when subjected to the additional TEE layer. This consistency suggests that the performance of hash-based algorithms like SPHINCS+ might be more stable under the constraints imposed by TEE, potentially due to its different cryptographic structure.

Table 6: *Times of each tested algorithms for one transaction verify operation on a node running over TEE.*

Algorithm PQC + secp256k1	P90 (sec)	P95 (sec)	P99 (sec)	Average (sec)
CRYSTALS-Dilithium-2	0,00049	0,00198	0,01683	0,00086
Falcon-1024	0,00063	0,00416	0,03178	0,00158
SPHINCS+	0,02302	0,05922	0,16130	0,01251

Our observations indicated that TEE occasionally generates longer execution times, with significant differences appearing at higher percentiles. These fluctuations highlight that while the average performance impact might be manageable, there are instances where the TEE layer induces substantial delays. This variability warrants further investigation to identify the underlying causes of these delays. Potential factors could include the interaction between TEE and specific hardware configurations, the nature of the workload, or inefficiencies in the current implementation of TEE. The measured times impacts of the TEE layer on different PQC algorithms are detailed in Table 5 for sign operations and Table 6 for verify operations. These tables provide a comprehensive overview of the execution times, illustrating the performance overhead introduced by TEE across various algorithms. The data highlight the trade-offs between enhanced security and operational efficiency, emphasizing the need for careful consideration when integrating TEE layers into DLT nodes.

In conclusion, while the use of TEE enhances the security of DLT nodes, it also introduces performance overhead (around milliseconds), particularly for certain PQC algorithms, but without compromising a near real-time environment, such as a Retail CBDC environment and so little of Wholesale. Understanding and mitigating these impacts are crucial for optimizing both security and efficiency in DLT systems.

7 Comparative Analysis

A comparative analysis of performance between CRYSTALS-Dilithium-2 and Falcon for post-quantum cryptography (PQC), both with and without the use of SGX enclave with Gramine providing a Trusted Execution Environment (TEE). This analysis is crucial to understanding the overhead introduced by these PQC algorithms compared to the pure secp256k1 algorithm. Evaluating the performance impact, including key generation, signing, and verification times, help determine the feasibility of integrating these PQC algorithms into DLT systems like Ethereum. The inclusion of TEE adds another layer of security, but it is essential to measure the additional computational overhead it imposes to ensure the overall system remains efficient and practical for real-world applications.

7.1 Evaluation metrics

When evaluating post-quantum cryptography (PQC) algorithms for integration into a DLT like Ethereum, several key metrics must be considered to ensure both security and performance are maintained. These metrics provide a comprehensive framework for assessing the feasibility and effectiveness of PQC algorithms in a DLT environment:

- **Security Level**: The primary metric for evaluating PQC algorithms is their security level. This involves assessing the algorithm's resistance to both classical and quantum attacks. It is crucial to ensure that the PQC algorithm provides a security level at least equivalent to existing classical algorithms, such as secp256k1, to protect against future quantum threats. Additionally, the algorithm's robustness against potential vulnerabilities and its ability to withstand various types of cryptographic attacks must be rigorously tested.
- **Key Sizes and Signature Sizes**: The size of the keys and signatures generated by PQC algorithms is a critical factor. Smaller key and signature sizes are preferable as they reduce storage and transmission overhead, which is particularly important in a DLT environment where efficiency and scalability are vital. Larger sizes can lead to increased latency and higher costs for data storage and transmission. Therefore, it is essential to strike a balance between security and practicality in key and signature sizes.
- **Computational Efficiency**: The computational efficiency of PQC algorithms, including the time required for key generation, signing, and verification, is another important metric. In Ethereum, where transactions occur frequently, it is imperative that these operations are performed quickly to maintain high throughput and low latency. Algorithms with high computational efficiency help ensure that the DLT can handle a large number of transactions per second without significant delays.
- **Performance Impact**: Finally, the overall performance impact of the PQC algorithm on the DLT must be assessed. This includes measuring the increase in signature and verification times, the additional computational load on network nodes, and any potential bottlenecks introduced by the new cryptographic processes. It is important to ensure that the adoption of PQC does not degrade the performance of the DLT to the point where it becomes impractical for real-world use.

By carefully evaluating these metrics, we can select the most suitable PQC algorithms for integration into DLT, ensuring a secure and efficient transition to post-quantum cryptographic standards.

7.2 Performance comparison

Elliptic Curve Cryptography (ECC) with the secp256k1 curve is widely used in DLT and other digital security applications due to its efficient performance and strong security properties. ECC's efficiency comes from the relatively small key sizes required to achieve high levels of security, which results in faster computation times for both signing and verifying operations. This makes it an excellent choice for applications where performance is critical, such as real-time financial transactions and mobile applications.

CRYSTALS-Dilithium-2 is a lattice-based post-quantum algorithm that offers strong security with reasonable performance. It provides a good balance between security and performance, making it a strong candidate for post-quantum secure applications. Its relatively efficient performance makes it suitable for many of the same applications as ECC, with the added benefit of quantum resistance. **Falcon-1024** is another lattice-based post-quantum algorithm known for its compact signatures and efficient performance. Its smaller signature sizes make it particularly appealing for applications where minimizing data transmission overhead is crucial, such as in low-bandwidth or high-frequency transaction environments. **SPHINCS+** is a hash-based post-quantum algorithm that emphasizes security but with a trade-off in performance. It provides robust security through its hash-based construction, which is highly resistant to both classical and quantum attacks. However, its large signature sizes and high computational requirements make it less suitable for real-time applications, although it remains valuable for applications requiring high security where performance is a secondary concern.

Figure 9: *Log10 of secp time histogram for algorithms and two types of transaction.*

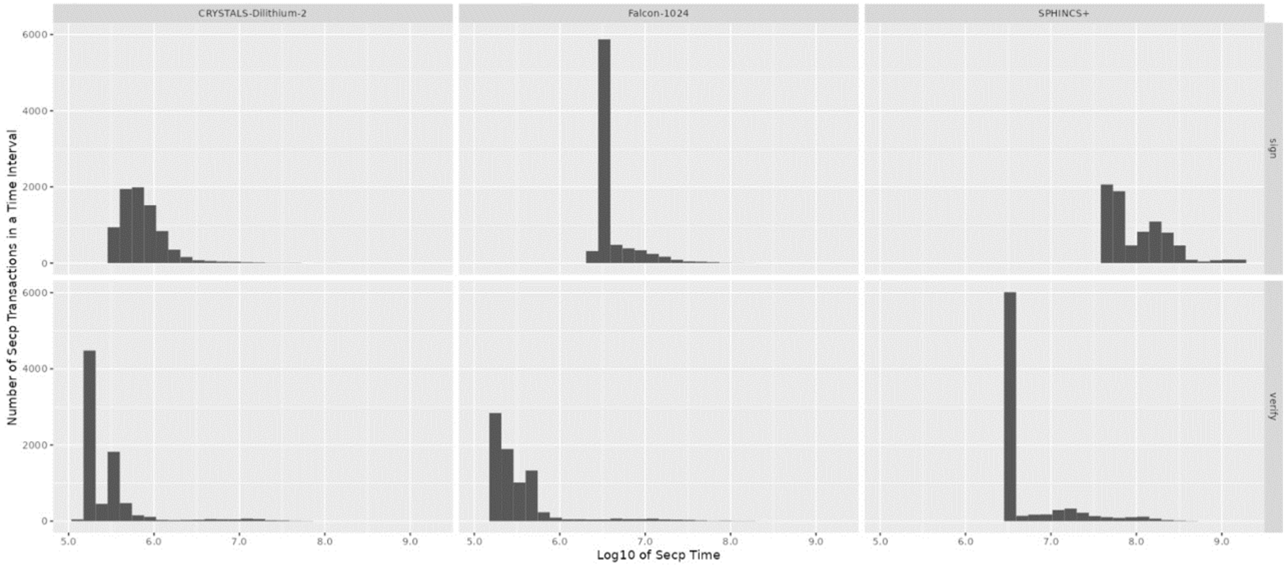


Figure 9 shows the log(time_secp)'s histogram for two kinds of transactions: ***sign*** and ***verify***, using three different PQC algorithms: CRYSTALS-Dilithium-2, Falcon-1024 and SPHINCS+. The X-axis represents log10(time_secp) and the Y-axis represents the number of secp transactions in a time interval. In all three cases, the the sign operation took more time to be executed than a verify. Of the three algorithms, CRYSTALS-Dilithium-2 had the best performance and the smallest difference in execution time between a sign and a verify operation. The histogram for the CRYSTALS-Dilithium-2 verify operation shows a log normal distribution for a sign operation and a bimodal distribution for a verify. A future work could try explaining the causes of this bimodality.

7.3 Security Analysis

Lattice-based post-quantum cryptographic algorithms like CRYSTALS-Dilithium and Falcon, are among the most promising candidates for securing digital communications against quantum attacks. Despite lattices being a well-established concept in mathematics, their application in cryptography is relatively novel and not as thoroughly tested as classical algorithms like RSA or ECC. One of the primary challenges with lattice-based PQC is the difficulty in rigorously proving their hardness. While these algorithms are built on mathematical problems that are conjectured to be hard, such as the Shortest Vector Problem (SVP) or the Learning With Errors (LWE) problem, definitive proofs of their security against all potential attack vectors remain elusive. This uncertainty arises because the cryptographic community has had less time to analyze and attempt to break these algorithms compared to more traditional cryptographic methods. As a result, while lattice-based PQC algorithms show great promise and offer strong resistance to both classical and quantum attacks, the cryptographic community continues to scrutinize and validate their robustness to ensure they can be reliably deployed in critical security applications.

Hash-based post-quantum cryptographic algorithms are grounded in the well-established and extensively studied principles of cryptographic hash functions. Unlike other newer PQC approaches, hash functions have been a fundamental component of cryptography for decades, underpinning widely used protocols and systems. This long history of usage means that the security properties of hash functions are well understood, and the potential threats against them have been thoroughly analyzed. Hash-based algorithms, such as SPHINCS+, leverage the robustness and simplicity of hash functions to create highly secure signature schemes. These schemes are inherently resistant to both classical and quantum attacks, as their security relies on the collision resistance and preimage resistance properties of the underlying hash functions [6]. Consequently, hash-based algorithms offer a high level of confidence in their security, benefiting from the extensive testing and scrutiny that hash functions have undergone over the years. This makes them a reliable choice for post-quantum security, particularly in applications where the utmost security is prioritized over performance.

To illustrate the differences in characteristics of the leading post-quantum algorithms, Table 2 highlights aspects such as the size of public and private keys, the size of the resulting signatures, and the achieved security level. The distinctive feature of SPHINCS+ becomes evident, showing relatively small public and private keys but generating significantly larger signatures compared to lattice-based algorithms like CRYSTALS-Dilithium-2 and Falcon-1024. This comparison is crucial for understanding the trade-offs involved in choosing each algorithm, especially when considering the specific requirements of different security applications.

7.4 Usability and Adoption Analysis

The integration of PQC into digital currency infrastructure represents a significant advancement in securing financial transactions against the potential threats posed by quantum computing. CRYSTALS-Dilithium-2, a lattice-based cryptographic algorithm, has emerged as a leading candidate for digital signatures in CBDCs due to its quantum resistance and efficiency. The adoption of CRYSTALS-Dilithium-2 within a CBDC platform based on DLT (Hyperledger Besu) underscores its practicality in a dual-capacity CBDC environment, catering to both wholesale and retail domains.

In terms of performance, CRYSTALS-Dilithium-2 has demonstrated superior time efficiency, with signature generation and verification processes completed in the realm of milliseconds. This is particularly crucial in the context of a CBDC, where the velocity of transactions directly impacts the fluidity of economic activity. The algorithm's swift execution time, coupled with its robust security profile, makes it an optimal choice for a Hyperledger Besu-based CBDC. Such a system not only ensures protection against quantum attacks but also facilitates a seamless and scalable transaction network, which is essential for the widespread usability and adoption of a digital currency in today's fast-paced financial landscape.

8 Feasibility Study

8.1 Implementation challenges

Integrating PQC operations, specifically sign and verify functions, from Bouncy Castle into Hyperledger Besu presented a unique set of challenges. The primary obstacle stemmed from Hyperledger Besu's architecture, which is predominantly tailored to support elliptic curve cryptography algorithms, particularly 'secp256k1'. This inherent limitation necessitated innovative approaches to accommodate alternative cryptographic frameworks, especially those required for post-quantum security.

One of the critical hurdles was the tight coupling of existing cryptographic operations with the secp256k1 algorithm within Besu's code base. This specificity meant that integrating PQC algorithms required not just the addition of new cryptographic routines but also a reevaluation and modification of the underlying infrastructure to support a broader range of cryptographic primitives. To address this challenge, we had to conduct simulations directly within Besu's source code. This approach allowed us to bypass the immediate constraints and test the feasibility of incorporating PQC operations. The simulations involved mock implementations of sign and verify functions that mimicked the behavior of post-quantum algorithms. Through this process, we could gather valuable metrics and insights into the performance implications, such as computational overhead and latency, introduced by PQC algorithms.

Furthermore, this experimental setup provided a sandbox for assessing the compatibility of PQC with Besu's existing components, such as transaction processing and block validation mechanisms. It highlighted the need for a more flexible cryptographic framework within Besu, capable of accommodating a diverse set of algorithms to future-proof the platform against quantum computing threats. Overall, the endeavor to integrate PQC operations from Bouncy Castle into Hyperledger Besu underscored the complexities of transitioning to post-quantum cryptography in established blockchain platforms. It also illuminated the path forward, emphasizing the necessity of adaptable and extensible cryptographic infrastructures to embrace the next generation of security algorithms.

8.2 Regulatory considerations and issues

With the imminent arrival of quantum computers, which have the potential to break traditional cryptographic systems, post-quantum cryptography becomes essential to ensure the security and privacy of digital financial transactions. This need is even more pressing when considering Brazilian legislation that regulates privacy, banking secrecy, and financial transactions: 1) **Security and Privacy**: The General Data Protection Law (LGPD), Law No. 13,709/2018 [19], establishes strict guidelines for the processing of personal data in Brazil, including financial data. Protecting this data is fundamental to preventing leaks that could compromise citizens' privacy. Post-quantum cryptography offers an advanced level of security capable of protecting data against quantum attacks, ensuring that sensitive information remains secure even with the advent of more advanced technologies. 2) **Banking Secrecy**: Banking secrecy in Brazil is regulated by Complementary Law No. 105/2001 [18], which protects the financial information of bank customers. The introduction of a CBDC, such as the Drex, increases the need for robust security measures to ensure that this information remains confidential. Post-quantum cryptography is a response to this need, providing a means to protect financial transactions and data against potential security breaches that could be exploited by quantum computers. 3) **Drex Regulation**: Drex [15], the Brazilian Central Bank's proposed CBDC, is governed by various circulars and norms that establish operational and security guidelines. Resolution such as No. 195/2022 [16], which address the regulation of technological innovations in the financial system, highlight the importance of cybersecurity and the need to adapt to new technologies to ensure the integrity of digital transactions.

In this way, PQC is vital for the secure implementation of a Brazilian CBDC, such as the Drex. It ensures compliance with privacy and banking secrecy laws while protecting financial transactions against future threats. The adoption of this technology not only ensures the protection of citizens' financial data but also strengthens confidence in Brazil's digital financial system, ensuring it is prepared for emerging technological innovations.

9 Conclusions

9.1 Contributions to the security of CBDC infrastructure

The adoption of PQC is essential for the successful implementation of the DREX CBDC in Brazil and is equally vital for the future of other Besu-based CBDC projects. As quantum computing advances, traditional cryptographic methods are becoming increasingly vulnerable. Post-quantum cryptography offers robust security solutions that are resistant to quantum attacks, ensuring the integrity, security, and privacy of digital currencies.

Quantum computers have the potential to solve complex mathematical problems much faster than classical computers. This capability poses a significant threat to current cryptographic algorithms, such as RSA and ECC, which are widely used in securing financial transactions and digital communications. In the context of CBDCs, where secure and reliable transactions are paramount, the vulnerability of these cryptographic methods could lead to severe breaches of security and loss of trust. Post-quantum cryptography provides cryptographic algorithms designed to be secure against quantum computing attacks. By implementing these algorithms, the DREX CBDC and other Besu CBDC projects can ensure that their cryptographic defenses remain robust even in the face of future technological advancements.

In Brazil, the implementation of a CBDC like DREX must comply with various regulatory standards related to data protection, privacy, and banking secrecy. The General Data Protection Law (LGPD) and Complementary Law No. 105/2001 emphasize the importance of safeguarding personal and financial data. Post-quantum cryptography ensures compliance with these laws by providing enhanced security measures that protect sensitive data from potential quantum threats. For any CBDC to be successful, it must gain the trust of its users. This trust is built on the assurance that their financial transactions are secure and their data is protected. Post-quantum cryptography plays a crucial role in enhancing transaction security by preventing unauthorized access and ensuring the confidentiality and integrity of financial data. As a result, users can confidently engage in digital transactions without fear of data breaches or financial losses.

9.2 Future-Proofing Besu CBDC Projects

The Besu platform, which supports the development of various CBDC projects, must integrate post-quantum cryptographic solutions to remain viable in the long term. By adopting PQC, Besu CBDC projects can future-proof their security infrastructure, making them resilient to the evolving landscape of cyber threats. This forward-thinking approach ensures that these projects are not only secure today but also prepared for the challenges of tomorrow.

The DREX CBDC is not just another digital currency; it is a cornerstone of the tokenized economy in Brazil. By facilitating secure and efficient digital transactions, DREX supports the broader adoption of tokenized assets, smart contracts, and decentralized finance (DeFi) applications. The integration of post-quantum cryptography into DREX's infrastructure ensures that these innovative economic activities can thrive in a secure and trusted environment. This makes DREX a critical component in the transition towards a more digital and tokenized economy.

9.3 Implications for the future of CBDC using Artificial Intelligence

Artificial Intelligence (AI) can significantly enhance cyber security measures for Central Bank Digital Currencies (CBDCs) in the context of post-quantum cryptography by addressing several key aspects:

- **Enhanced Threat Detection and Response:** Gen AI can process vast amounts of data more efficiently than traditional methods, enabling the detection of cyber threats in real time. This includes identifying patterns and anomalies that might indicate a cyber attack. Gen AI's ability to analyze and learn from large datasets helps in anticipating potential security breaches before they occur, making it a proactive tool in cyber security defenses.
- **Automation of Routine Tasks:** Gen AI can automate many routine cyber security tasks that are currently performed by human analysts. This includes monitoring network traffic, scanning for vulnerabilities, and applying security patches. Automation not only reduces the workload on cyber security teams but also minimizes the risk of human error, ensuring that security measures are consistently applied.
- **Mitigating Social Engineering and Data Disclosure Risks:** The sophistication of gen AI can be leveraged to combat AI-generated social engineering attacks and unauthorized data disclosures. By continuously learning from new threat vectors and patterns, gen AI can develop robust defense mechanisms against these types of attacks, ensuring the integrity and confidentiality of CBDC systems.
- **Human-AI Collaboration:** While gen AI can handle many aspects of cyber security autonomously, human oversight remains crucial. Gen AI systems will require continuous training and adaptation, which involves human cyber security experts to ensure ethical and accurate outcomes. This collaboration ensures that while gen AI enhances efficiency, human expertise is still pivotal in strategic decision-making and oversight.
- **Proactive Security Measures:** Gen AI can facilitate a shift from reactive to proactive cyber security strategies. By predicting and neutralizing threats before they manifest, gen AI helps in maintaining the resilience and robustness of CBDC systems. This proactive stance is crucial in the evolving landscape of cyber security threats, especially in the era of quantum computing.

In conclusion, integrating gen AI into the cyber security framework for CBDCs, particularly in a post-quantum cryptography context, can significantly enhance threat detection, automate routine security tasks, mitigate risks, and support human-AI collaboration for a proactive approach to cyber security. These points are derived from the report on "Generative artificial intelligence and cyber security in central banking" by the

Bank for International Settlements (BIS) [13], which outlines the opportunities and challenges of gen AI in enhancing cyber security for central banks.

9.4 Final Remarks

Post-quantum cryptography is fundamental to the full implementation of the DREX CBDC and the future of all Besu-based CBDC projects. By addressing the vulnerabilities posed by quantum computing, post-quantum cryptographic solutions provide the necessary security, compliance, and user trust required for the successful adoption and long-term sustainability of digital currencies. As the world moves towards a digital financial future, integrating post-quantum cryptography will be crucial in ensuring the security and resilience of CBDCs against emerging threats.

Both avenues for exploring quantum-safe user transaction signatures require a thorough evaluation of their feasibility and implications. Changing the signature scheme necessitates a deep understanding of the technical and operational challenges involved in transitioning to quantum-resistant algorithms. This includes assessing the computational efficiency, scalability, and security of the new methods, as well as their impact on user experience and system performance. On the other hand, developing Account Abstraction solutions involves investigating how to effectively decouple account logic from signature schemes. This requires innovative approaches to account management, ensuring that the abstraction layer can seamlessly integrate quantum-safe signatures while maintaining compatibility with existing addresses and protocols.

In this way, exploring quantum-safe user transaction signatures presents two potential avenues for future investigation. The first option involves evaluating the feasibility and implications of changing the signature scheme to ensure quantum resistance, albeit with the potential impact of losing the relation with existing addresses. Alternatively, further exploration into Account Abstraction solutions based on quantum-safe signatures could offer an innovative approach to addressing this critical aspect of quantum-resilient transaction security [14].

9.5 Future Work

In considering the future of research on the domain of Post-Quantum Cryptography (PQC) applied to Central Bank Digital Currencies (CBDCs), several promising directions emerge that warrant exploration. Building upon the insights gained from the current study, potential areas for further investigation include the application of PQC to user transaction signatures (quantum-proof wallets), Zero-Knowledge Proofs (ZKP), and self-sovereign identity, all designed to be quantum-proof:

- **Quantum-Proof Wallets** [1]: One of the most critical components of any digital currency system is the security of user transaction signatures. As quantum computers become more powerful, the cryptographic methods currently used to secure digital wallets will become increasingly vulnerable. Research into quantum-proof wallets aims to develop cryptographic algorithms that are resistant to quantum attacks, ensuring that user signatures cannot be forged or tampered with by quantum computers. Quantum-proof wallets would employ PQC algorithms to secure transaction signatures, providing a robust defense against quantum threats. This would involve investigating new signature schemes that can withstand the computational power of quantum computers while maintaining efficiency and user-friendliness. Ensuring the security of these wallets is paramount to maintaining user trust and the overall integrity of the CBDC system.
- **Zero-Knowledge Proofs (ZKP)** [40]: Zero-Knowledge Proofs (ZKP) are a method by which one party can prove to another that a statement is true without revealing any information beyond the validity of the statement itself. In the context of CBDCs, ZKP can enhance privacy and security by allowing transactions to be verified without disclosing the underlying data. Research into quantum-proof ZKP involves developing protocols that remain secure in the face of quantum computing capabilities. These quantum-resistant ZKP systems would enable private and secure transactions, preserving user confidentiality while ensuring regulatory compliance. This is particularly important for maintaining privacy in a digital financial ecosystem where data breaches and unauthorized disclosures are significant concerns.
- **Self-Sovereign Identity** [32]: Self-sovereign identity (SSI) refers to a digital identity model where individuals have control over their personal data and can manage their own identities without relying on a central authority. In the quantum future, ensuring the security of SSI systems is crucial to prevent identity theft and unauthorized access to personal information. Quantum-proof SSI would leverage PQC

to secure digital identities against quantum attacks. This involves creating cryptographic methods that protect identity data and authentication processes from being compromised by quantum computing. By developing quantum-resistant SSI systems, individuals can maintain control over their identities with enhanced security, thereby fostering greater trust in digital identity solutions integrated into CBDCs.

- **Changing the Signature Scheme** [59]: The first option involves evaluating the feasibility and implications of changing the signature scheme to ensure quantum resistance. This approach requires transitioning from current cryptographic methods, such as RSA or ECC, to quantum-resistant algorithms like lattice-based, hash-based, or multivariate polynomial-based schemes. These new algorithms are designed to withstand the computational power of quantum computers, thereby safeguarding transaction signatures. However, changing the signature scheme comes with significant challenges. One of the primary concerns is the potential impact on existing addresses. Current digital currency systems rely on established cryptographic methods for address generation and verification. Shifting to a quantum-resistant scheme could disrupt the relationship with existing addresses, necessitating a comprehensive overhaul of the address infrastructure. This transition would require careful planning and extensive testing to ensure compatibility and security across the entire system.
- **Account Abstraction Solutions** [65]: Alternatively, further exploration into Account Abstraction solutions based on quantum-safe signatures could offer an innovative approach to addressing this critical aspect of quantum-resilient transaction security. Account Abstraction is a concept that separates the logic of account management from the underlying signature scheme. By abstracting accounts, it becomes possible to implement quantum-safe signatures without disrupting the existing address infrastructure. Research into quantum-safe Account Abstraction solutions focuses on creating flexible and adaptable systems that can integrate new cryptographic methods as needed. This approach allows for a smoother transition to quantum-resistant signatures, minimizing the impact on users and existing infrastructure. Moreover, it provides a framework for future-proofing the system against emerging cryptographic threats, ensuring long-term security and resilience.

References

[1] Nabil Alkeilani Alkadri et al. *Deterministic Wallets in a Quantum World*. Cryptology ePrint Archive, Paper 2020/1149. https://eprint.iacr.org/2020/1149. 2020. URL: https://eprint.iacr.org/2020/1149.

[2] Ahmad J. Alkhodair, Saraju P. Mohanty, and Elias Kougianos. *Consensus Algorithms of Distributed Ledger Technology – A Comprehensive Analysis*. 2023. arXiv: 2309.13498 [cs.DC].

[3] Marcos Allende et al. “Quantum-resistance in blockchain networks”. In: (2023). DOI: 10.1038/s41598-023-32701-6. URL: https://doi.org/10.1038/s41598-023-32701-6.

[4] F. Arute, K. Arya, and R. et al. Babbush. “Quantum supremacy using a programmable superconducting processor.” In: *Nature* 574 (Oct. 2019), pp. 505–510. DOI: doi.org/10.1038/s41586-019-1666-5.

[5] Thomas Attema et al. *The PQC Migration Handbook. Guidelines For Migrating To Post-Quantum Cryptography*. Technical Report 040423. Netherlands: Netherlands National Communications Security Agency, Mar. 2023. 62 pp. URL: https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook (visited on 03/10/2024).

[6] Jean-Philippe Aumasson et al. “SPHINCS+”. In: *Submission to the NIST post-quantum project, v.3* (2020).

[7] Azure. https://learn.microsoft.com/en-us/azure/confidential-computing/quick-create-portal. Accessed: 2023-12-20. 2024.

[8] Henry Bambury and Phong Q. Nguyen. “Improved Provable Reduction of NTRU and Hypercubic Lattices”. In: *PQCrypto 2024* (2024).

[9] BIS. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm. Accessed: 2024-04-10. 2024.

[10] BIS. https://www.bis.org/publ/othp80.pdf. Accessed: 2024-04-10. 2024.

[11] BIS. *Blueprint for the future monetary system: improving the old, enabling the new*. https://www.bis.org/publ/arpdf/ar2023e3.pdf. Accessed: 2024-02-16. 2023.

[12] BIS. *Central Bank Digital Currencies*. Report 174. https://www.bis.org/cpmi/publ/d174.htm. Committee on Payments, Market Infrastructures, and Market Committee, Mar. 2018, p. 34.

[13] BIS. *Generative artificial intelligence and cyber security in central banking*. https://www.bis.org/publ/bppdf/bispap145.pdft. Accessed: 2024-06-04. 2024.

[14] Aditya Bisht. *Quantum-safe transactions on Ethereum*. https://medium.com/@adityabisht64/quantum-safe-transactions-on-ethereum-dd6f768c3bfe. Accessed: 2024-05-23. Dec. 2023.

[15] Banco Central do Brasil. *DREX*. https://www.bcb.gov.br/en/financialstability/drex_en. 2024.

[16] Banco Central do Brasil. *Lei do Sigilo Bancário*. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo. 2022.

[17] Banco Central do Brasil. *Post-Quantum Cryptography methods applied to the Brazilian instant payment system (Pix): A feasibility study*. https://news.microsoft.com/pt-br/com-apoio-da-fenasbac-banco-central-brazil-quantum-e-microsoft-exploram-o-uso-de-criptografia-pos-quantica-para-melhorar-seguranca-do-sistema-pix/. 2022.

[18] Governo Federal Brasileiro. *Lei do Sigilo Bancário*. https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm. 2001.

[19] Governo Federal Brasileiro. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. https://www.gov.br/inss/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais. 2021.

[20] Daniel R. L. Brown. "Elliptic Curve Cryptography". In: *Standards for Efficient Cryptography - Certicom* (2009).

[21] Donald E. Porter Chia-Che Tsai and Mona Vij. "Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX". In: *Proceeding of 2017 USENIX Conference on Usenix Annual Technical Conference* (2017).

[22] Atlantic Council. https://www.atlanticcouncil.org/cbdctracker. Accessed: 2024-03-24. 2024.

[23] Nathanaël Denis, Maryline Laurent, and Sophie Chabridon. "Integrating Usage Control Into Distributed Ledger Technology for Internet of Things Privacy". In: *IEEE Internet of Things Journal* 10.22 (Nov. 2023), pp. 20120–20133. ISSN: 2372-2541. DOI: 10.1109/jiot.2023.3283300. URL: http://dx.doi.org/10.1109/JIOT.2023.3283300.

[24] EIPS. May 2024. URL: https://eips.ethereum.org/EIPS/eip-7702 (visited on 05/28/2024).

[25] Ethereum. https://ethereum.org/en/what-is-ethereum/. Accessed: 2024-06-04. 2024.

[26] Aram W. Harrow and Ashley Montanaro. "Quantum computational supremacy". In: *Nature* 549.7671 (Sept. 2017), pp. 203–209. ISSN: 1476-4687. DOI: 10.1038/nature23458. URL: http://dx.doi.org/10.1038/nature23458.

[27] Khondokar Fida Hasan et al. "A Framework for Migrating to Post-Quantum Cryptography. Security Dependency Analysis and Case Studies". In: *IEEE Access* 12 (2024), pp. 23427–23450. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2024.3360412.

[28] Yining Hu et al. "Blockchain-based Smart Contracts - Applications and Challenges". In: *arXiv preprint arXiv:1810.04699* (2018).

[29] Lars Hupel and Makan Rafiee. "How Does Post-quantum Cryptography Affect Central Bank Digital Currency?" In: *Ubiquitous Security*. Springer Nature Singapore, 2024, pp. 45–62. ISBN: 9789819712748. DOI: 10.1007/978-981-97-1274-8_4. URL: http://dx.doi.org/10.1007/978-981-97-1274-8_4.

[30] Hyperledger. *Quorum Byzantine Fault Tolerance*. https://besu.hyperledger.org/private-networks/how-to/configure/consensus/qbftk. 2024.

[31] Hyperledger Foundation. *Hyperledger Besu*. https://www.hyperledger.org/projects/besu. Accessed: May 24, 2024.

[32] Identity. Apr. 2024. URL: https://www.identity.com/self-sovereign-identity/ (visited on 05/28/2024).

[33] Corporation Intel. Santa Clara, CA, 2016. URL: https://community.intel.com/legacyfs/online/drupal_files/managed/33/70/intel-sgx-developer-guide.pdf (visited on 05/22/2024).

[34] E. Kiktenko et al. "Quantum-secured blockchain". In: *Quantum Science and Technology* 3.3 (2018), p. 8.

[35] Andrew D. King et al. *Computational supremacy in quantum simulation*. 2024. arXiv: 2403.00910 [quant-ph].

[36] LACCHAIN. *TRANSACTIONS PER SECOND RATE TEST IN BESU NETWORK.* https://github.com/lacchain/Ethereum-Benchmark. 2024.

[37] John Lytle. *Performance of Hybrid Signatures for Public Key Infrastructure Certificates*. 2021.

[38] Evan R. MacQuarrie et al. "The emerging commercial landscape of quantum computing". In: *Nature Reviews Physics* 2.11 (Oct. 2020), pp. 596–598. ISSN: 2522-5820. DOI: 10.1038/s42254-020-00247-5.

[39] Artur Mariano et al. "A Practical View of the State-of-the-Art of Lattice-Based Cryptanalysis". In: *IEEE Access* 5 (Oct. 2017), pp. 24184–24202. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2017.2748179.

[40] Microsoft. https://github.com/microsoft/Nova. Accessed: 2024-01-10. 2024.

[41] Microsoft. https://learn.microsoft.com/en-us/azure/confidential-computing/trusted-execution-environment. Accessed: 2024-06-01. 2024.

[42] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. 2008.

[43] Nature. May 2024. URL: https://www.nature.com/subjects/information-technology/nature (visited on 05/28/2024).

[44] NIST. Gaithersburg, MD, Dec. 2016. URL: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information (visited on 03/17/2024).

[45] NIST. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022 (visited on 05/17/2024).

[46] NIST. *FIPS PUB 202 - SHA-3 standard: Permutation-based hash and extendable-output functions*. Tech. rep. National Institute of Standards and Technology, 2015. DOI: 10.6028/NIST.FIPS.202.

[47] NIST. *Migration to Post-Quantum Cryptography Quantum Readiness. Testing Draft Standards*. Technical Report SPECIAL PUBLICATION, 1800-38C. Gaithersburg, MD: NIST, Dec. 2023. 87 pp. URL: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms (visited on 03/10/2024).

[48] NIST. *Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography*. https://csrc.nist.gov/pubs/sp/1800/38/iprd-(1)y. Accessed: 2024-02-25. Jan. 2024.

[49] NIST. *NIST POST-QUANTUM CRYPTOGRAPHY UPDATE*. https://csrc.nist.gov/csrc/media/Presentations/2023/nist-post-quantum-cryptography-update/2a-Moody_NIST_PQC_2.pdf. 2023.

[50] NIST. *Post-Quantum Cryptography*. https://csrc.nist.gov/projects/post-quantum-cryptography. Accessed: 2024-01-12. Jan. 2024.

[51] NSA. *Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now*. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/. 2023.

[52] Anoop Kumar Pandey et al. "Cryptographic Challenges and Security in Post Quantum Cryptography Migration. A Prospective Approach". In: *proceedings [...]* 2023 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA). New York: IEEE, Sept. 2023, pp. 1–8. DOI: 10.1109/PKIA58446.2023.10262706. URL: https://ieeexplore.ieee.org/document/10262706 (visited on 03/29/2024).

[53] Ken Peffers et al. "A Design Science Research Methodology for Information Systems Research". In: *Journal of Management Information Systems* 24.3 (2007). Accessed: 2023-01-02, pp. 45–77. DOI: 10.2753/MIS0742-1222240302.

[54] A. Shamir R.L. Rivest and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* (1978).

[55] Manohar Raavi et al. "Security Comparisons and Performance Analyses of Post-quantum Signature Algorithms". en. In: *Applied Cryptography and Network Security*. Ed. by Kazue Sako and Nils Ole Tippenhauer. Cham: Springer International Publishing, 2021, pp. 424–447. ISBN: 9783030783754. DOI: 10.1007/978-3-030-78375-4_17.

[56] Oded Regev. "An Efficient Quantum Factoring Algorithm". In: arXiv:2308.06572 (Aug. 2023). DOI: 10.48550/arXiv.2308.06572. URL: http://arxiv.org/abs/2308.06572 (visited on 03/17/2024).

[57] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: `10.1109/SFCS.1994.365700`.

[58] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. ISSN: 0097-5397. DOI: `10.1137/S0097539795293172`.

[59] L. Soni, H. Chandra, and D.S. et al Gupta. "Quantum-resistant public-key encryption and signature schemes with smaller key sizes". In: *Cluster Computing* 27 (Dec. 2022), pp. 285–297. DOI: `https://doi.org/10.1007/s10586-022-03955-y`.

[60] The Legion of the Bouncy Castle. *Bouncy Castle Crypto APIs*. `https://www.bouncycastle.org/`. Accessed: 2024-04-11. 2023.

[61] Qiping Wang, Raymond Yiu Keung Lau, and Xudong Mao. "Blockchain-Enabled Smart Contracts for Enhancing Distributor-to-Consumer Transactions". In: *IEEE Consumer Electronics Magazine* 8.6 (2019), pp. 22–28. DOI: `10.1109/MCE.2019.2941346`.

[62] WEF. *Safeguarding central bank digital currency systems in the post-quantum computing age*. `https://www.weforum.org/agenda/2024/05/safeguarding-central-bank-digital-currency-systems-post-quantum-age/`. 2024.

[63] J R Wohlwend. "ELLIPTIC CURVE CRYPTOGRAPHY: PRE AND POST QUANTUM". In: 2016. URL: `https://api.semanticscholar.org/CorpusID:2182777`.

[64] World Economic Forum. *Modernizing Financial Markets with WCBDC*. Accessed on May 22, 2024. World Economic Forum. May 2024. URL: `https://www.weforum.org/publications/modernizing-financial-markets-with-wcbdc/`.

[65] Zeeve. 2023. URL: `https://www.zeeve.io/blog/exploring-the-benefits-of-account-abstraction-in-rollups/` (visited on 02/26/2024).