White Paper

—

Quantum-Resistant Blockchain Securing the Future of Digital Assets

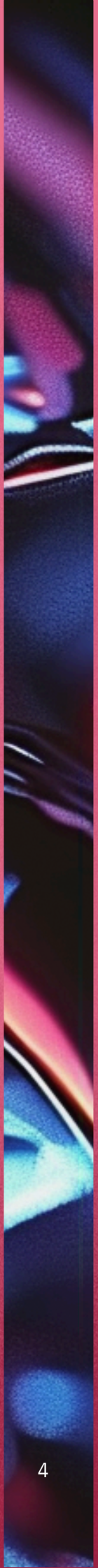
---- postquantum.network

Table of Contents

Contents List

1

Corporate Information and Bylaws



1.1 General Corporate Information

The company's business name is Post-Quantum Network. The company was registered in Dubai, United Arab Emirates, under a Limited Liability Company (LLC) license, and under the United Arab Emirates (UAE) laws, we have established and are currently operating the company as a limited liability company with an indefinite term.

Organizational Data

Post Quantum Network 0-25 Computer Plaza, Al Ain Centre, Al Fahidi Metro Station, Bur Dubai, UAE.

Registration date: November, 2018

Core team

Led by a team of cryptography experts, developers, specialists, and advisors.

Post-Quantum Network team has worked on projects like:

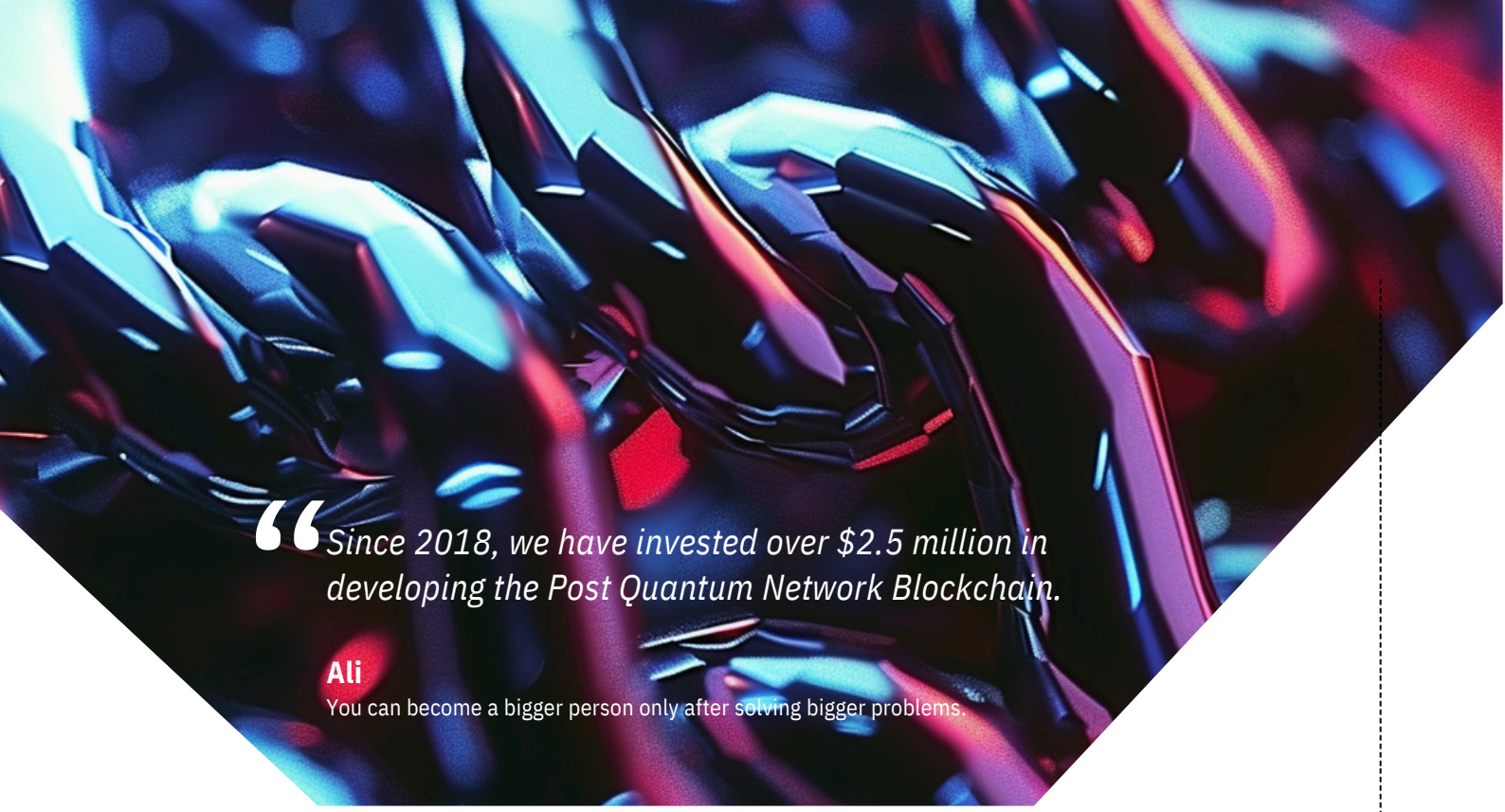
Decentraland, Opensea, McAfee, Tor Onion, Alethea AI, Brave Browser, CityDAO

Ali
Chief Technologist and Co-Founder

Roman Mykyta
Co-founder and Chief Cryptology Officer

2

Overview:
The Problem, Mission and Solution



> *Since 2018, we have invested over $2.5 million in developing the Post Quantum Network Blockchain.*
>
> **Ali**
> You can become a bigger person only after solving bigger problems.

2.1 Overview

In the ever-evolving landscape of technology, the advent of quantum computing poses a significant threat to traditional cryptographic systems. The Post Quantum Network (PQN) emerges as a purpose-built, industrial-grade, provably secure quantum computer-resistant blockchain conceived and being developed since 2018.

The emergence of quantum computing poses a significant threat to existing cryptographic protocols, including those underpinning blockchain technology. This white paper introduces the Post Quantum Network (PQN), a novel, provably quantum-resistant blockchain designed to secure digital assets and transactions in a post-quantum world.

The Post Quantum Network is built on quantum-resistant cryptography, approved by NIST, ensuring unparalleled security in the face of emerging quantum threats.

We prioritize energy efficiency and speed, delivering a platform that is both sustainable and responsive.

Post Quantum Network is pioneering a new generation of blockchain platforms designed to seamlessly integrate with business operations.

Our comprehensive framework offers the world's first fully quantum-resistant security stack, providing businesses with a robust and future-proof solution.

2.2 Mission

The Post Quantum Network is a Layer 1 hybrid blockchain platform designed to enable developers and businesses to create quantum-resistant solutions such as smart contracts, decentralized finance (DeFi), decentralized autonomous organizations (DAOs), decentralized applications (DApps), tokens, central bank digital currencies (CBDCs), non-fungible tokens (NFTs), metaverse solutions, and web3 applications using top programming language.

2.3 Solution

- **Security:** The first blockchain of its own kind, using two different schemes, Xtended Merkle Signature (XMSS) and Quantum Random Number Generation (QRNG), to secure its chain ecosystem against quantum computer attacks tested and approved by NIST.
- **Rapid Cloud Deployment:** Users can deploy the Post Quantum Network blockchain on major cloud platforms like Amazon AWS in under 5 minutes, with the speed of 1,900 TPS public chain and 97,000 TPS private blockchain, making the Post Quantum Network the fastest blockchain solution in the market.
- **Ethereum Compatibility:** Post Quantum Network is Ethereum EVM compatible, allowing for seamless migration of projects from the Ethereum network.
- **Staking:** PQCN token holders can earn an estimated 40% APY return on their staked tokens.
- **Web3 Domains:** the Post Quantum Network provides complete lifetime ownership of your Web3 domains without any renewal fees; you can register your domain for a lifetime with the Post Quantum Network without paying annual renewal costs.
- **Node Operators/Validators:** Node Operators are responsible for validating network transactions while operating either a full node or a basic node, thereby generating passive income for the duration of their contracts.
- **Real World Assets (RWA):** The Post Quantum Network is integrating real-world assets such as gold, silver, and diamonds into the blockchain in real-time, providing new investment opportunities while utilizing your cryptocurrency.

3

Competition

***2024**, after extensive research into different blockchain technologies, algorithms, and simulations, we couldn't find any truly quantum-resistant blockchains or existing networks utilizing more than one quantum-resistant technology. Post Quantum Network stands out as the only blockchain currently employing two NIST-approved quantum-resistant technologies: Merkle Signature Scheme (XMSS) and Quantum Random Number Generation (QRNG).*

The basic functionality of postquantum.network revolves around being a quantum-resistant blockchain. It is designed to protect against potential threats from quantum computing, using post-quantum cryptographic methods. The primary features include:

1. **Quantum Resistance:** It uses the Merkle Signature Scheme (XMSS) and Quantum Random Number Generation (QRNG), both of which are approved by NIST, to ensure the network's security remains intact even against quantum computing attacks.
2. **EVM Compatibility:** The network is compatible with the Ethereum Virtual Machine (EVM), meaning developers can easily build and run smart contracts and decentralized applications (dApps) on the blockchain using tools and coding languages familiar with Ethereum, such as Solidity.
3. **Quantum Secure Transactions:** The quantum-resistant cryptographic techniques enable secure, tamper-proof transactions even in a post-quantum world, where quantum computers could potentially break traditional cryptographic algorithms.

In 2018, we began working on the Post Quantum Network, recognizing that quantum computers were becoming more advanced and would fundamentally change the future of computing. Additionally, we understood the significant threat quantum computers posed to existing blockchains, as almost all were vulnerable to quantum attacks.

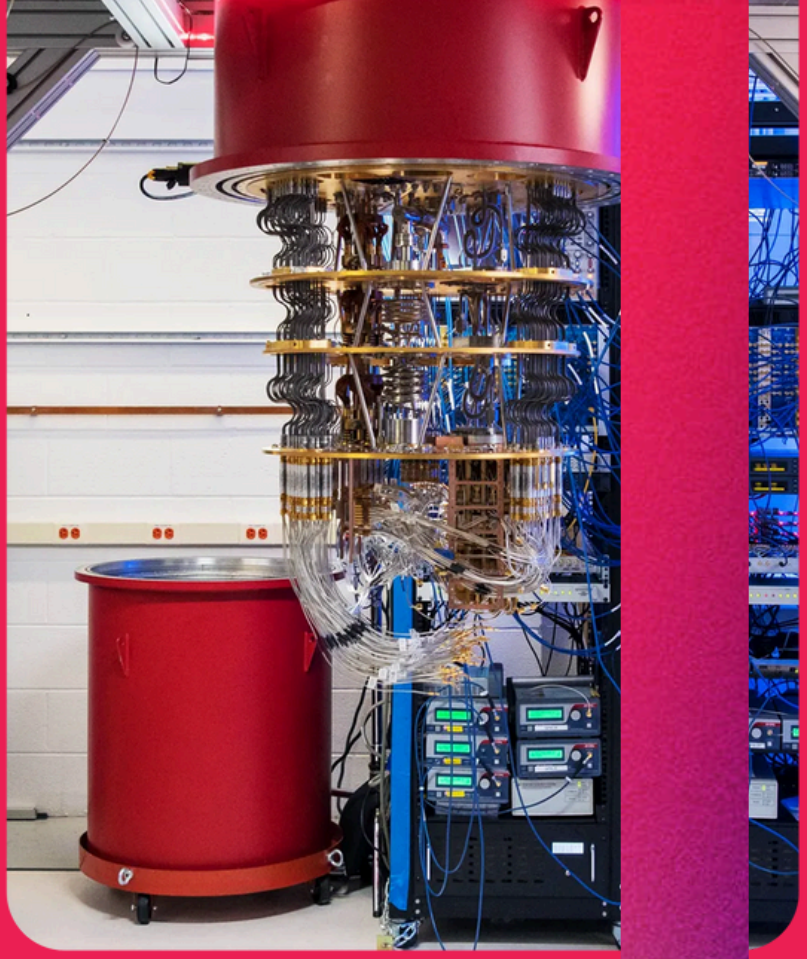
3.1 Limitations of Current Blockchain Technology

1. **Non-Intuitive Economic Models:** Existing blockchains, like Ethereum, use a volatile gas pricing system, placing fluctuating transaction costs on users. This creates unpredictability and biases the network towards miners, benefiting them at the expense of fairness and accessibility.
2. **Cryptographic Vulnerabilities:** Traditional blockchains rely on cryptographic methods that are not quantum-safe, leaving them vulnerable to quantum computing attacks. They also struggle with GDPR compliance and managing confidential data, limiting adaptability to modern privacy standards.
3. **Unpredictable Costs:** For businesses, transaction fees are hard to predict, making it difficult for finance directors to forecast operational costs.

PostQuantum.Network solves these issues by:

- Using a **FIAT-based pricing model** ensures predictable costs for businesses.
- Implementing **quantum-resistant cryptography** for future-proof security.
- Creating a **fair**, **unbiased** blockchain that eliminates miner favoritism and supports long-term sustainability.

4



Distinctiveness

Post Quantum Network vs. Ethereum and Solana

4.1 Concise comparison

Feature	PostQuantum.Network	Ethereum	Solana
Security	Uses Quantum-Resistant Cryptography (XMSS) and QRNG, protecting against quantum computing threats.	Relies on Elliptic Curve Cryptography (ECDSA), vulnerable to quantum computing attacks.	Uses ECDSA, not quantum-safe, vulnerable to quantum threats.
Transaction Fees	FIAT-based predictable pricing, stable and business-friendly.	Gas-based dynamic pricing, fluctuates with congestion, unpredictable costs.	Low, fixed fees, but can vary with extreme network demand.
Economic Model	Fairer, unbiased, no miner favoritism or excessive fees.	Miner-biased, miners prioritize higher-fee transactions.	Validator-based—can lead to concentration of wealth among large validators.
EVM Compatibility	EVM-compatible, supports Ethereum smart contracts and dApps.	Fully EVM-native, largest ecosystem for dApps.	Not EVM-compatible, uses its own programming model (Rust/C).
Quantum Resistance	Built-in quantum-safe encryption and security mechanisms.	Not quantum-safe, vulnerable to quantum computing.	Not quantum-safe, uses traditional cryptography.
Scalability	Designed for sustainability with minimal cost burden on users.	Layer 2 solutions improve scalability but come with complexity and high fees on Layer 1.	Highly scalable, uses Proof of History (PoH), achieving high throughput but faces centralization risks.
Transaction Speed	1,900 Transactions per Second (TPS) can achieve 155,200 (TPS) through a hybrid approach, which will make it the fastest and most secure blockchain platform.	15-30 transactions per second (TPS) on Layer 1, can increase with Layer 2.	65,000 TPS (theoretically), one of the fastest blockchain platforms.
Privacy & GDPR Compliance	Better suited for GDPR compliance and handling confidential data.	Challenged by privacy concerns and GDPR compliance issues.	Faces similar GDPR and privacy challenges as Ethereum.
Consensus Mechanism	Uses quantum-safe cryptographic schemes for long-term security.	Uses Proof of Stake (PoS) (Ethereum 2.0), but quantum-vulnerable.	Uses Proof of History (PoH) combined with Proof of Stake (PoS), but quantum-vulnerable.
Developer Ecosystem	Growing ecosystem, EVM-compatible, easy to transition from Ethereum.	Largest developer ecosystem, widely supported, many tools and integrations.	Smaller ecosystem, fewer developers, requires learning new tools (Rust/C).

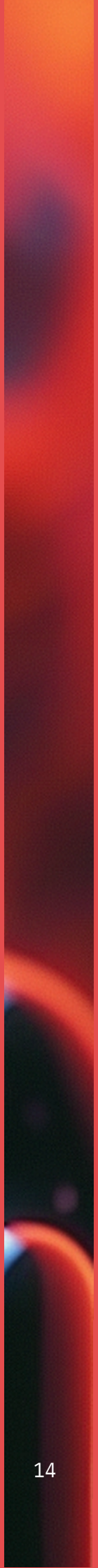
4.2 Other Advantages

- **Predictable pricing:** Uses FIAT-based pricing for transactions and deployment fees, providing businesses with greater cost certainty.
- **Quantum-safety:** Employs quantum-resistant cryptographic algorithms to protect against future quantum computing threats.
- **GDPR-friendliness:** Offers features for managing private data in compliance with GDPR regulations.
- **Energy efficiency:** Uses a Proof-of-Stake (PoS) consensus mechanism with (XMSS) and (QRNG), which is significantly less energy-intensive than Proof-of-Work.
- **Scalability:** Achieves high transaction throughput with relatively low computational requirements.
- **Data management:** Allows for private data storage between nodes, ensuring data privacy.
- **IoT-friendliness:** Supports communication and interoperability between IoT devices.
- **Multiple programming languages:** Enables developers to write smart contracts in popular programming languages, reducing the learning curve.
- **Developer-friendly pricing:** Offers a pricing model that incentivizes developers to write reusable code modules.

In summary, The Post Quantum Network aims to address several key limitations of current blockchains by providing a more predictable, secure, efficient, and developer-friendly platform.

5

Durability



5.1 Accountability of Post Quantum Network

- Open blockchain platform: PQN operates under permissive licensing, ensuring transparency and openness.
- Attribution and accountability: Responsibilities within the network can be properly attributed, ensuring accountability among all on-premise participants.
- Immutable and transparent ledger: Every transaction and data associated with it is registered and stored on an immutable blockchain, meaning it cannot be altered or erased, ensuring long-term transparency and trust.
- Traceability: Every transaction is traceable, and all data is searchable, making it simple to audit and verify activities within the network.
- High-level security: The platform provides advanced security by adhering to current cryptographic standards, thereby meeting the needs of third-party and network security.
- Full accountability: Given the transparency, immutability, and security features, the platform is fully accountable to its users.

5.2 Simplicity of Post Quantum Network

- **Low complexity code:** PQN runs on simpler code compared to other blockchain platforms, improving its performance and making it easier to maintain.
- **High adaptability:** The network's adaptability makes it well-suited for various industries, particularly for:
- Industry operations
- High-volume certified transactions
- Smart contracts
- **Connectivity:** It supports efficient data exchange in restricted computational environments, such as:
- **IoT networks**
- **Satellite node infrastructure networks**
- **Developer-friendly:** Popular, developer-friendly languages facilitate the writing of smart contracts, thereby simplifying the development process and promoting wider adoption.

5.3 Sustainable Solutions from the For-Profit Business Behind PQN

- Tailored solutions: The company behind PQN is ready to develop both standard and tailor-made solutions on the public PQN blockchain, targeting:
- Off-chain companies, including financial institutions, service providers, and other industries.
- Private blockchains for third parties needing special solutions.
- For-profit business model: This approach ensures that PQN can provide sustainable solutions by aligning its growth and development with the needs of traditional businesses.

5.4 Security of Post Quantum Network

- **Resistance to 51% attacks: The consensus protocol on PQN makes a 51% attack impossible to execute because:**
- Proof-of-Stake (PoS) and Quantum Random Number Generators (QRNGs) with XMSS (Extended Merkle Signature Scheme) Plus, attackers need to pay an upfront fee (instead of buying mining equipment) to participate in block validation, serving as a barrier.
- **Weight in selection:** In PQN, the weight in the validation process is based on the fee paid by the block proposer, not hash power as in traditional Proof of Work (PoW) systems.
- **Cost of attack deterrent:** While PoW-based systems may become more vulnerable due to falling GPU prices, PQN's Proof of Stake (PoS) model requires attackers to purchase a non-refundable license for block validation. If an attack fails, this investment is lost, making attacks less attractive.
- **Non-refundable license:** This economic model ensures that attackers face a significant financial loss if they attempt to compromise the network.

6

Background of the Platform

History

- How does blockchain work, and why is it used?

6.1 Blockchains: What Are They?

- Blockchain Definition: A decentralized, distributed, public digital ledger that records transactions across many computers.
- Data Resistance: Blockchain is resistant to data modification, recording transactions efficiently and verifiably.
- Block Structure: Each block contains:
- A cryptographic hash of the previous block,
- A timestamp,
- Transaction data.
- Security: Once recorded, a transaction cannot be altered without modifying all subsequent blocks.

6.2 A Design-Brought Security System

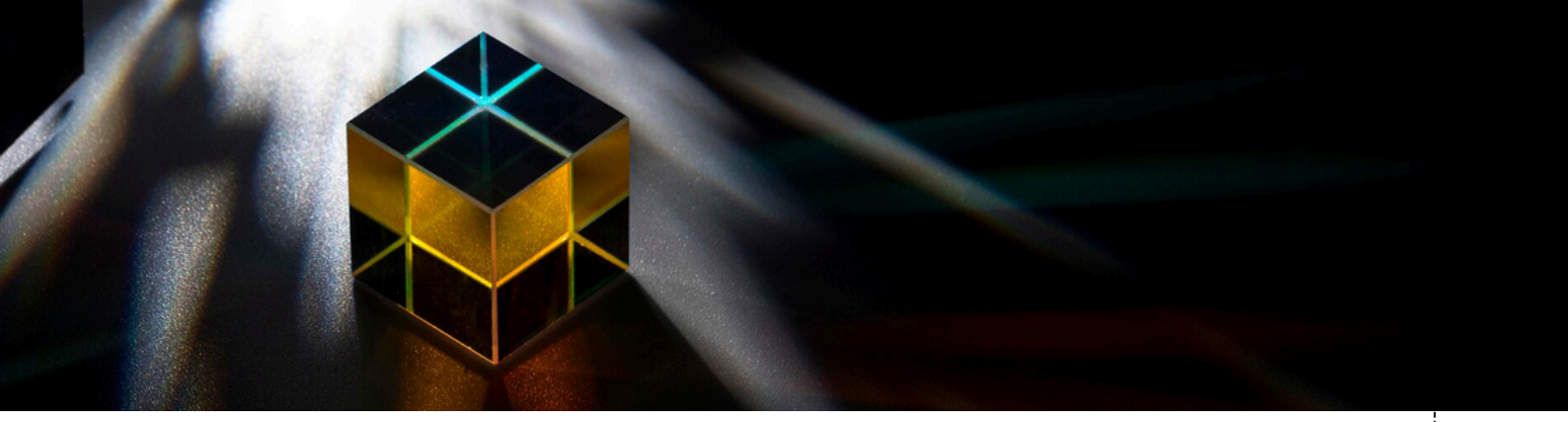
- P2P Network: Public blockchains are managed by a global peer-to-peer (P2P) network of computers, without a central authority.
- Validation Protocol: These computers adhere to blockchain protocols to validate new blocks.
- Consensus Mechanism: Modifying a block requires consensus from the majority of computers in the network.
- Security: Although blockchains are not completely unalterable, they are secure by design.

6.3 The First Practical Use of a Public Blockchain: Cryptocurrencies

- Bitcoin (BTC): First public blockchain used as the transaction ledger for Bitcoin, solving the double-spending problem without a trusted authority.
- Other Cryptocurrencies: Bitcoin inspired other cryptocurrencies like Ethereum (ETH), Ripple (XRP), and Litecoin (LTC), making blockchain a type of payment rail.

6.4 Public Blockchains

- Access: Public blockchains have no access restrictions; anyone can send transactions or become a validator.
- Economic Incentives: Validators usually use the Proof-of-Work (PoW) algorithm and are economically motivated.
- Limitations: Public blockchains (e.g., Bitcoin, Ethereum) cannot handle large-scale global trade or Internet of Things (IoT) due to scalability and performance issues.



6.5 Private Blockchains

- Permissioned Networks: Private blockchains restrict access to participants and validators invited by network administrators.
- Use Case: Companies use private blockchains for secure accounting, record-keeping, and payment procedures without sacrificing autonomy.

6.6 Hybrid Blockchains

- Hybrid blockchains combine elements of both public and private blockchains, aiming to strike a balance between security, accessibility, and performance. They offer a flexible approach that can be tailored to specific use cases.

6.7 Current Blockchain Challenges

- Challenges: Business blockchains before 2018 were too slow, energy-inefficient, non-scalable, and difficult to program.
- Post Quantum Network Solution: The network solves these issues by:
- Bypassing Ethereum's limitations,
- Providing fast, environment-friendly solutions,
- Supporting smart contracts in many programming language,
- Being quantum-proof and benefiting from Satellite Internet technology.

6.8 General Architecture of Post Quantum Network

6.8.1 Network Layer

- P2P Network: Independent nodes interconnect without centralized servers, following protocol rules.
- Epidemic Gossip Protocol: Similar to Bitcoin, where nodes only need knowledge about neighboring nodes, reducing network overhead.

6.8.2 Database Layer

- Database Contents: Stores blockchain data, including blocks, timestamps, metadata, and hashes.

6.8.3 Crypto (Security) Layer

- Cryptographic Security: Based on Kerckhoffs's principle, the system remains secure as long as the cryptographic key is kept secret.
- Quantum Resistance: The platform uses post-quantum cryptography and (XMSS)/(QRNG) with lattice-based problems, protecting against both classical and quantum attacks.

6.8.4 Satellite Nodes

- Overcomes limitations of existing blockchains, Post Quantum Network is using satellite nodes to make sure network remains operational even in the face of extreme conditions.

6.9 Quantum Hardness

- Quantum-Secure: The platform is resistant to all known quantum-breaking algorithms, protecting encrypted data even after quantum computers are built.
- Risk to Current Cryptography: Traditional algorithms like RSA and ECC are vulnerable to quantum attacks, but Post Quantum Network ensures future security.

6.10 Smart Contracts

Definition of Smart Contract

- Smart Contract: A self-executing piece of software that automates a transaction between parties when predefined conditions are met.
- Immutable: Once signed and recorded on a blockchain, smart contracts cannot be altered.

Solidity Language

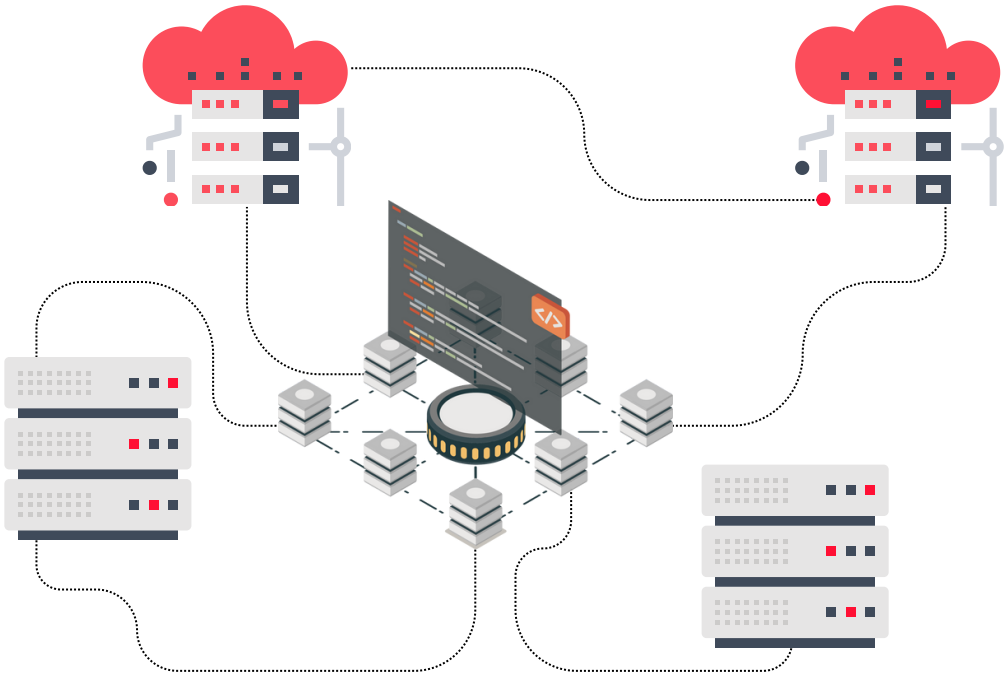
- Limitations of Solidity: Ethereum smart contracts require programming in Solidity, which is not widely used outside the platform and difficult for many developers.
- Post Quantum Network Advantage: Developers can write smart contracts in many language they already know, making development easier.

The Future of Smart Contracts According to Post Quantum Network

- Versatile Applications: Smart contracts can be applied to:
- Financial services (trade settlements, bond payments, insurance claims),
- Healthcare (data integrity in clinical trials),
- Intellectual property (royalty distribution).
- **Industry-Ready:** The Post Quantum Network platform provides a solution for industry-ready smart contracts, addressing speed, scalability, and ease of programming.

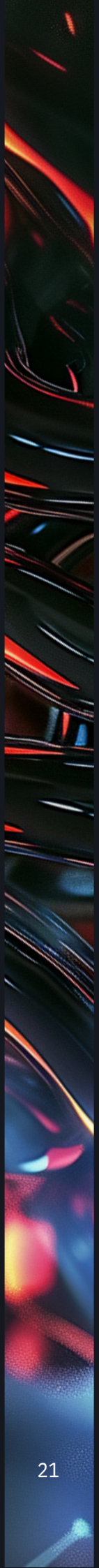
Developers of Smart Contracts

- Smart Contract Developer: A professional skilled in creating smart contracts over blockchain platforms, traditionally using Solidity on Ethereum but now supported in multiple languages on Post Quantum Network.



7

Block Functions



7.1 Block Generation

A Block generation refers to the creation of new blocks in the blockchain, carried out by mining nodes following specific protocols.

7.2 Mining

- Mining Process: In most blockchains, miners (individuals or entities) contribute computing power to verify transactions and add them to the blockchain.
- Rewards: Miners are compensated with the blockchain's cryptocurrency (e.g., Bitcoin) through the Proof-of-Work (PoW) process.
- Competitive Process: Mining is a competitive, randomness-based process. Miners pool their resources to improve chances of mining blocks, which generates transaction fees and rewards of newly created coins.

7.3 Proof-of-Work (PoW)

- PoW Mechanism: PoW is a resource-intensive process that requires miners to solve complex mathematical problems to generate a valid block.
- Energy Usage: PoW consumes a large amount of energy; for example, Bitcoin's network uses more power than many countries.
- First Consensus Algorithm: Bitcoin's PoW was the first distributed and trustless consensus mechanism. Many other blockchains, including Ethereum, initially adopted this model, but Ethereum plans to transition to a more efficient consensus system in the future.
- Key Feature: PoW does not require all network nodes to reach a consensus for every block, allowing for efficient block validation.

7.4 Consensus - Proof-of-Stake (PoS)

- PoS at Post Quantum Network: This system uses validators selected based on criteria like coin age and economic stake, significantly reducing energy consumption compared to PoW.
- Ownership and Validation: In PoS, the probability of validating transactions and creating new blocks depends on the amount of cryptocurrency held by the user (validator).
- Economic Incentives: PoS relies on economic game theory to secure the network, where validators have a financial incentive to maintain the network's integrity.
- Energy Efficiency: PoS consumes less electricity as validators (virtual miners) are selected through the protocol itself rather than competing with computational power.
- Challenges: PoS systems face certain challenges in providing the same guarantees as PoW, such as hidden security functions that PoW naturally offers.

7.5 Proof-of-Randomness (PoR)

- PoR Mechanism: Derived from Silvio Micali's verifiable randomness theory, PoR is an advancement of Algorand's randomness-driven consensus.
- Uniform Weighting: In PoR, nodes or users are weighted uniformly rather than variably, offering a solution to the scalability challenges Algorand faces.
- Neighbour-Only Randomness: PoR uses a neighbour-only randomness model where nodes only need knowledge of their direct peers (similar to a DHT-like structure).
- Bayesian Nash Equilibrium: PoR models its confidence values game-theoretically, adjusting the randomness through verifiable random sampling paths. This ensures that consensus is reached efficiently, even with limited network knowledge.

Block proposers at Post Quantum Network elect themselves in a transparently random way, devoid of the potential of manipulation or interference, based on the weight of their committed stakes.

8

Governance
(Token Model)

8.1 An Overview of Actors and Their Interests

PQCN is the Utility/Native token of Post Quantum Network Blockchain.

This section outlines the key actors in the Post Quantum Network ecosystem, detailing their efforts, resources, and economic benefits. It also highlights how value is captured through the use of the PQCN token, forming the core of the Token Architecture.

Actors	Benefits	Effort/Resources Provided	Comments
1. Generic Smart Contract Developers	Earn PQCN tokens when their code is reused by Specific Smart Contract Developers.	1) Write reusable generic code. 2) Pay for code deployment based on fixed FIAT rates.	This structure encourages enterprise adoption with predictable pricing and high-quality, reusable code. Code reuse is rewarded through token incentives.
2. Specific Smart Contract Developers	Enter the blockchain market without needing specialized blockchain skills.	1) Pay for code deployment and validator fees. 2) License fees go to Generic Smart Contract Developers.	Developers pay for their custom code and network fees, fostering collaboration between general and blockchain-specific developers.
3. Validators	Earn tokens from the Issuance Pool and transaction fees for validating blocks.	1) Pay deposit fees to enter validator pool. 2) Wait in a random queue to validate blocks.	Validator selection is random, and the deposit provides access but does not influence order. The process is designed to be inclusive and decentralized.
4. Full-Node Providers	Earn rewards based on the storage they provide for validated blocks.	Provide constant storage access for blockchain data on capable devices.	Full-Node Providers are rewarded in proportion to storage usage, creating a sustainable model. Validator and Full-Node Provider roles are interconnected.
5. Smart Contract Users (Transactors)	Interact with decentralized applications with trust and security.	Pay transaction fees for data-modifying operations.	Transaction fees are fixed in FIAT for predictability. Non-data-modifying actions are fee-free, while data addition requires a fee, ensuring platform sustainability.

9

Business Revenue Model

9.1 Token Description and Use of PQCN

PQCN is a utility token designed exclusively for the Post Quantum Network. It is not classified as a security and therefore offers no rights to dividend payments, interest payments, participation in liquidation procedures, or rights to liquidation proceeds. PQCN does not confer any governance rights, including participation, petitioning, or voting rights in shareholder meetings or other company gatherings. As a result, PQCN solely serves functional purposes, making it a utility token.

Token Utilities:

1. **Contract Deployment Fees:** Developers deploying new smart contracts on the platform must pay a fee in PQCN. The fee is proportional to the size and complexity of the contract being deployed.
2. **Execution of Deployed Contract Methods:** Application users are required to pay a fee for executing smart contract functions, especially when data is written to the blockchain. This fee is paid in PQCN and varies based on the data volume and the complexity of the smart contract function being executed.
3. **Token Transfer Fees:** Users transferring PQCN tokens to other addresses pay a flat transaction fee, independent of the amount being transferred.
4. **Web3 Fees:** Users who interact with Web3 platforms for buying or selling, such as decentralized domain names, NFTs, marketplaces, and RWAs, will pay with PQCN tokens.

9.2 Actors and Their Interests

The Post Quantum Network involves multiple actors, each with different roles and incentives within the ecosystem.

9.2.1 Generic Smart Contract Developers

Responsibilities:

- Develop reusable, generic smart contract code.
- Pay a deployment fee in PQCN to commit their code to the network.

Incentives:

- When their code is reused by Specific Smart Contract Developers, the network charges the latter and redistributes tokens to Generic Developers based on the proportion of reused code.
- These rewards can be sold on the open market, offering financial incentives for contributing reusable code.

9.2.2 Specific Smart Contract Developers

Responsibilities:

- Write specific code for decentralized applications (dApps), often by reusing generic code.
- Pay a usage fee for reused generic code and a deployment fee for their own specific code in PQCN.

Incentives:

- They can develop and deploy functional dApps on the Post Quantum Network by buying PQCN from the market to cover fees.

9.2.3 Users

Responsibilities:

- Interact with decentralized applications (dApps) built by Specific Smart Contract Developers.

Incentives:

- Users may need to pay transaction fees (in PQCN) for their interactions within the network. They purchase PQCN from the open market to cover these fees.

9.2.4 Validators

Responsibilities:

- Ensure the integrity of transactions by validating blocks using the Proof-of-Randomness consensus mechanism.
- Validators must stake a fixed amount of PQCN in a Deposit Pool to be eligible for validation.

Incentives:

- Validators that successfully validate blocks are rewarded with PQCN from the Issuance Pool. These rewards can be sold in the open market.

9.2.5 Full-Node Providers

Responsibilities:

- Run the Post Quantum Network software on capable devices, providing storage and computational power.

Incentives:

- Full-node providers must pay a registration fee in PQCN to join the network. In return, they receive PQCN rewards for validated blocks, which can be sold on the open market.

9.3 Functioning of Post Quantum Network

The Post Quantum Network functions through the collaborative work of two key players: Node Operators and Block Validators. Both actors are financially motivated by rewards to maintain the network's operation.

9.3.1 Issuance Pool

- Rewards for both Node Operators and Block Validators come from the Issuance Pool, which distributes a fixed number of tokens at regular intervals. This ensures a balance between supply and demand.

9.3.2 Revenues of the Network

The network's revenue sources feed into the Issuance Pool:

1. **Transaction Costs:** Paid by smart contract users.
2. **Code Deployment Costs:** Paid by Specific Smart Contract Developers.
3. **Code Deployment Costs:** Paid by Generic Smart Contract Developers.

9.3.3 Deposit Pool

- The Deposit Pool serves as a safeguard to prevent fraud during block validation. Block Validator candidates pay a license fee to participate, and upon successful selection, they receive a reward for verifying the transactions.

9.3.4 Minting

- When the combined rewards from the Issuance Pool and Deposit Pool are insufficient to cover transaction costs and rewards, the network may mint new tokens. If the network holds more tokens than required, it automatically burns the surplus to prevent inflation.

9.3.5 Network Operating Rules

- The network’s operation relies on established rules to ensure equilibrium between revenues (primarily fees) and costs (rewards). These rules also govern the distribution of rewards to Full Node Operators and Block Validators.

9.4 Revenue and Cost Plan Items

9.4.1 Revenues List

The Post Quantum Network generates revenue from the following sources:

- Sale of PQCN Tokens: Paid by token buyers.
- License Fees for Using Generic Smart Contracts: Paid by developers or users of smart contracts.
- Block Miners Fee: Paid by miners.
- Storage Fees: Paid by users who store data on the blockchain.

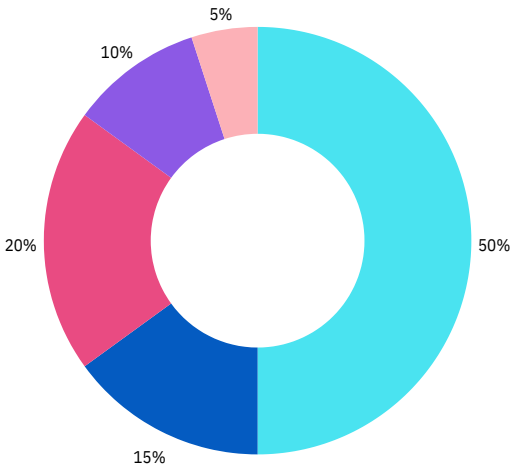
9.4.2 Cost Structure Plan

The cost structure for maintaining the Post Quantum Network includes the following breakdown:

- **Product Development (50%):** For platform improvements, upgrades, and overall development.
- **Marketing Costs (15%):** For branding, education, and community outreach.
- **Operations and Administration (20%):** To cover day-to-day network operations.
- **Legal Costs (5%):** For regulatory and compliance requirements.
- **Reserve (10%):** To ensure financial stability.

9.4.3 Cost Structure Plan

Funds raised from PQCN sales and other revenue streams will be used as follows:



- **Platform Development and Upgrades (50%):** Focused on enhancing the platform and recruiting talent.
- **Marketing (15%):** Targeting developers, investors, and spreading awareness about the network.
- **General Administration and Management (20%):** To ensure smooth operations.
- **Reserve (10%):** For future financial stability.
- **Legal and Regulatory (5%):** Covering legal and compliance needs.

10

Value Acquisition

10.1. Value Generation

The Post Quantum Network ecosystem generates and captures value through the use of its native coin, Post Quantum Coin (PQCN), in two distinct ways:

10.2 Real Value

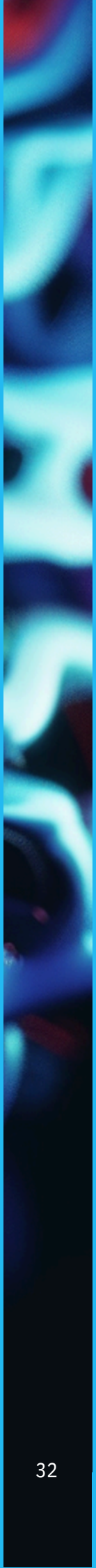
- Real value is derived from the actual cost of running decentralized applications (dApps) on the Post Quantum Network.
- This cost is paid directly by the users of these applications.
- The real value primarily reflects the costs of computing resources required to power the network.
- It serves as a baseline for developers building on the Post Quantum Network protocol.
- Developers can assess these baseline costs to understand the expenses associated with dApp development and maintenance on the network.

10.3 Added Value

- Added value comes from the utility provided by the dApps built on the Post Quantum Network.
- Post Quantum Network has pursued initial use cases to establish a foundation of high value-add applications.
- As the ecosystem grows, the ability to capture added value will increasingly be driven by the community of developers building on the platform.
- This added value will evolve through the creation of more diverse and innovative dApps that provide unique utility to users.
- The dynamics of this value-capture process inform the network's mathematical models, which help provide a systemic understanding of how the token value and price of PQCN are determined under various scenarios.

11

Tokenomics of Post Quantum Network, PQCN Token



11.1 Tokenomics

The table below breaks down the distribution of PQCN tokens across various phases, including sales, staking rewards, and community incentives. It ensures that the network has a balanced allocation for growth, rewards, and future liquidity.

Category	Percentage (%)	Number of Tokens	Price/Token
Seed Round	7%	28 million	$0.09
OTC Sale	15%	60 million	$0.11
Public ICO	25%	100 million	$0.14
Early Investor	5%	20 million	N/A
VC Reserve	20%	80 million	N/A
Liquidity Pool	8%	32 million	N/A
Future Liquidity	3%	12 million	N/A
Staking Rewards	27%	108 million	N/A
Community & Airdrop	2%	8 million	N/A
Ecosystem & Treasury	8%	32 million	N/A
Reserve	3%	12 million	N/A
Team & Advisors	3%	12 million	N/A

Total Tokens: 400 million PQCN

11.2 Vesting

Seed Round (7%, 28 million tokens, $0.09)

Vesting Schedule:

- Lock-up period: 6 months
- Vesting period: After the lock-up, tokens will vest over 12 months, linearly distributed monthly.

OTC Sale (15%, 60 million tokens, $0.11)

Vesting Schedule:

- Lock-up period: 3 months
- Vesting period: After the lock-up, vest over 9 months with linear monthly vesting.

Public ICO (25%, 100 million tokens, $0.14)

Vesting Schedule:

- Lock-up period: None
- Vesting period: Immediate access to 20% upon launch, with the remaining 80% vested over 6 months.

Early Investor (5%, 20 million tokens)

Vesting Schedule:

- Lock-up period: 6 months
- Vesting period: After lock-up, vest over 12 months.

VC Reserve (20%, 80 million tokens)

Vesting Schedule:

- Lock-up period: 12 months
- Vesting period: Vest linearly over 24 months.

Liquidity Pool (8%, 32 million tokens)

Vesting Schedule:

- No lock-up, as these tokens are immediately needed to provide liquidity for decentralized exchanges and other liquidity pools.

Future Liquidity (3%, 12 million tokens)

Vesting Schedule:

- Lock-up period: 12 months
- Vesting period: Vest over 24 months thereafter.

Staking Rewards (27%, 108 million tokens, 40% APY)

Vesting Schedule:

Tokens will be distributed through a staking rewards program at a rate of 40% APY. These tokens are dynamically released based on users staking their PQCN in the network.

Community & Airdrop (2%, 8 million tokens)

Vesting Schedule:

- Immediate release for airdrops.

Ecosystem & Treasury (8%, 32 million tokens)

Vesting Schedule:

- No lock-up, available for ecosystem grants and partnerships as needed.

Reserve (3%, 12 million tokens)

Vesting Schedule:

- Lock-up period: 6 months
- Vesting period: Vest over 18 months thereafter.

Team & Advisors (3%, 12 million tokens)

Vesting Schedule:

- Lock-up period: 12 months
- Vesting period: Vest over 24 months, monthly cliff.

12

Staking

12.1 Staking “PQCN” on Post Quantum Network

A key component of the Post Quantum Network is staking, which enables users to support network security while earning passive income. Users can earn a 40% Annual Percentage Yield (APY) for locking their $PQCN tokens on the Post Quantum Network platform by staking them. This is a highly competitive return for being an integral part of the ecosystem.

Staking Overview:

- **APY:** Users will earn a fixed 40% APY on their staked PQCN tokens.

For example, for every 100 PQCN staked, users can expect about 140 PQCN at the end of the staking period.

- **Staking Period:** To fully benefit from the 40% APY, users are required to lock their tokens for 1 year. Once tokens are locked in the staking contract, they cannot be withdrawn until the 12-month period is complete.

12.2 Flexible Reward Withdrawal:

While tokens must remain locked for the full year to secure the full APY, users have the flexibility to withdraw their staking rewards at any time. These rewards can be withdrawn right after staking begins, offering liquidity even within the lock-up period.

Users can withdraw their rewards more frequently by receiving them on an hourly, daily, weekly, or monthly basis. This feature provides users with continuous access to the yield generated by their staked tokens, ensuring both flexibility and earnings throughout the staking period.

12.3 Key Features of PQCN Staking:

1. **40% APY Yield:** Users earn a substantial annual return on their staked tokens.
2. **One-Year Lock-Up Period:** Tokens must remain locked for one year to receive the full staking yield.
3. **Instant Reward Withdrawal:** Users can withdraw staking rewards anytime after locking their tokens, without waiting for the staking period to end.
4. **Flexible Reward Distribution:** Rewards can be collected hourly, daily, weekly, or monthly, allowing users to access their earnings regularly.

13

Decentralized Domains

13.1 Web3/Domains

In the era of Web3, domain ownership is evolving beyond the limitations of traditional registrars. Post Quantum Network (PQN) introduces Decentralized Domains, a groundbreaking solution that gives users full, permanent ownership of their Web3 domains—without the need for renewal fees or annual payments.
With PQN's decentralized domains, once a domain is registered, it belongs to the user permanently. There are no ongoing fees or hidden costs. The ownership is recorded on the blockchain, ensuring it is censorship-resistant, transparent, and invulnerable to tampering or seizure.

The Traditional Problem

Conventional domain registration systems are centralized, with users renting domains through third-party registrars for a limited period. This system often requires yearly renewals and subjects users to price hikes, domain squatting risks, and potential censorship. Ownership is not truly in the hands of the users; instead, it is leased, and the domain can be revoked or suspended by the governing authority.

13.2 Key Benefits:

- **Lifetime Ownership:** No annual renewals or ongoing fees—once purchased, the domain is yours forever.
- **Censorship Resistance:** Your domain cannot be taken down or seized by any central authority.
- **Quantum-Resistant Security:** Domains are protected against both classical and quantum computing threats through cutting-edge cryptographic techniques.
- **True Decentralization:** Unlike traditional registrars, Post Quantum Network removes middlemen, placing full control of domain management into the hands of the owner.
- **Seamless Integration with Web3:** Decentralized Domains integrate directly with Web3 applications, allowing users to use their domain as an identity, wallet address, or access point for decentralized services.

13.3 How it Works:

- **Domain Registration:** Users register their domain on the PQN blockchain, paying a one-time fee.
- **Blockchain Recording:** The ownership details are permanently etched into the blockchain, providing an immutable and tamper-proof record.
- **Lifetime Ownership:** Once registered, the domain is yours for life, with no further payments required.

Post Quantum Network's Decentralized Domains empower users by giving them complete control over their digital identity in the Web3 ecosystem. No more intermediaries, no more renewals—just true ownership, secured by the most advanced quantum-resistant technology available.

14

Satellite Node

14.1 Satellite-node infrastructure

The Post Quantum Network's satellite-based infrastructure is a game-changer for blockchain technology. By utilizing satellite nodes, the network ensures rapid and secure global transactions, sidestepping the limitations of conventional internet infrastructure. Post Quantum Network's satellite-based network ensures uninterrupted operations even in the face of extreme conditions. Whether you're in a remote location or facing infrastructure challenges, the Post Quantum Network remains resilient and reliable because it does not rely on the Internet submarine cable.

How it works

The Post Quantum Network PQN consists of two types of nodes: Full Node and Light Node. Full-node operators require a **Starlink Internet Dish** and a dedicated **PC** or **server** to run the node 24/7. In contrast, Half Node operators can participate without a Starlink Dish by operating a dedicated PC only.

14.2 Key Benefits:

- Earn a Steady Income: Node operators can earn passive income by securing the network.
- Contribute to a revolutionary technology: By running a node, you become part of a groundbreaking blockchain network that is reshaping the blockchain industry.
- Enjoy Operational Continuity: The satellite-based infrastructure ensures that (PQN) transactions are always secure and accessible, even in challenging environments.

The Post Quantum Network's innovative approach has the potential to revolutionize various industries, from finance and supply chain management to decentralized applications. By combining the power of satellite technology with blockchain, Post Quantum Network is creating a more resilient, scalable, and secure blockchain for the future.

15

(XMSS) & (QRNGs)

15.1 XMSS & QRNG

The Post Quantum Network is the first Layer 1 blockchain that is truly a quantum-resistant blockchain because it’s built with the Extended Merkle Signature Scheme (XMSS) and Quantum Random Number Generation approved by the National Institute of Standards and Technology (NIST).

1. **eXtended Merkle Signature Scheme (XMSS)**
2. **Quantum Random Number Generators (QRNGs)**

eXtended Merkle Signature Scheme (XMSS):

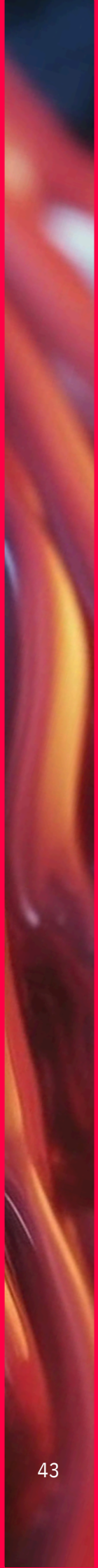
- Post-quantum security: XMSS is a post-quantum signature scheme, meaning it is resistant to attacks from quantum computers. This is crucial in the face of potential quantum threats to existing cryptographic algorithms.
- Reduced storage requirements: XMSS has smaller public key sizes than other post-quantum signature schemes, which can reduce storage requirements for nodes on the network.

Quantum Random Number Generators (QRNGs):

- Unpredictability: QRNGs generate truly random numbers, which can be used to introduce randomness into the consensus algorithm. This makes it more difficult for attackers to predict the outcome of the consensus process.
- Increased entropy: QRNGs can increase the entropy of the system, making it harder for attackers to manipulate the system's state.

16

Risk Factors



Risk of Foreign Currency: Foreign currency risk arises primarily from the acquisition of assets or liabilities denominated in foreign currencies. Fluctuations in exchange rates can be influenced by political and economic factors such as interest rate changes, trade policies, and the balance of payments between countries. Such fluctuations may negatively impact the value of the Company's foreign currency-denominated transactions, potentially affecting financial performance.

Risk in Operations: Operational risk encompasses potential losses caused by human error, process failures, or system malfunctions. This category also includes risks related to fraud or corporate misconduct. The Company monitors its internal processes and systems rigorously to mitigate operational risk. Despite these efforts, unforeseen operational issues could lead to financial losses, disruptions in service, or reputational damage.

Risk of Liquidity: Liquidity risk refers to the Company's ability to meet its financial obligations as they come due. It results from mismatches between the maturity profiles of assets and liabilities. While the Company's risk management strategies include internal procedures and liquidity limits, these measures may not always be sufficient. Any failure to manage liquidity risks could have significant negative effects on the Company's operations and financial stability.

Modifications to the Tax Environment: Changes in tax laws and regulations, or differing interpretations by tax authorities, may have adverse consequences for the Company's financial results. The tax treatment of cryptocurrencies is particularly uncertain and may be subject to future legal clarifications. Any unfavorable tax rulings could result in unexpected liabilities for the Company, affecting its business activities and profitability.

Management and Personnel Risks: The Company's success heavily depends on its management team and key personnel. Errors in judgment or the loss of skilled employees could lead to unforeseen costs or operational challenges, negatively impacting the Company. If key positions are left vacant or are filled with insufficiently qualified personnel, the Company's performance could suffer. The competitive market for experienced personnel may also drive up costs.

Risks of Licensing and Permits: The Company may need licenses and permits to operate legally in certain jurisdictions. Changes in regulatory requirements or delays in obtaining necessary licenses could hinder the Company's ability to conduct business, affecting its growth and financial performance.

Risk of Criminal Offenses: The digital asset sector, including token offerings, is vulnerable to fraud, money laundering, and terrorist financing. Regulatory authorities may take measures against the Company or third parties involved in illegal activities, leading to loss of investor capital and potential reputational harm.

Qualified Advice: The information provided in this document is not a substitute for professional financial or legal advice. Investment decisions should be based on an individual's own objectives, experience, and risk tolerance. Without seeking professional advice, investors may acquire unsuitable investments, increasing the risk of financial loss.

Contractual Risks: The Company's operations rely on the enforceability of its contracts, which may be subject to varying legal interpretations depending on jurisdiction. In certain instances, contractual terms could be found unenforceable, which may lead to material adverse effects on the Company's operations.

Potential Conflicts of Interest: The Company and its affiliates may engage in transactions with related parties, which could create conflicts of interest. Transactions driven by non-market forces may result in unfavorable terms for the Company or its stakeholders, potentially impacting its operations and financial results.

Risk of Civil Liability: The Company faces significant risk from potential legal claims, disputes, and regulatory actions. These proceedings may result in unpredictable costs and damages, negatively affecting the Company's financial condition and operational capabilities.

Risk of Theft and Loss: Despite adhering to the highest security standards, there is still the risk of theft or loss of tokens. The Company is not responsible for tokens stored on third-party platforms, or for investor negligence regarding best practices in virtual asset security. Any theft or loss could result in a complete loss of the investor's holdings.

Regulatory Framework Uncertainty: Cryptographic tokens, digital assets, and blockchain technologies exist within an evolving regulatory landscape. In some jurisdictions, regulations are still being formulated, while in others, existing laws may be amended. These regulatory uncertainties could negatively affect the Company's ability to operate and grow.

Hacker and Sabotage Attacks: The Company's IT infrastructure is at risk from cyberattacks and sabotage, which could lead to operational disruptions or financial losses. These risks include not only external threats from hackers but also internal risks such as employee misconduct or sabotage. Failure to prevent such attacks could negatively impact the Company's business activities.

Possible Attacks on Ethereum: Although Ethereum's transition to Proof-of-Stake (PoS) has reduced the risk of traditional mining attacks, new vulnerabilities could still arise. Any successful attacks on Ethereum's PoS system, such as targeting validators or exploiting bugs, could lead to transaction delays, double-spending, or faulty smart contract executions, thereby affecting the Company's operations.

Wallet and Private Key Risks: Investors must use Ethereum-compatible wallets to store their tokens. Failure to do so could result in the permanent loss of tokens. Additionally, the loss or theft of an investor's private key would result in the irreversible loss of all associated tokens. The Company bears no responsibility for the security of investors' private keys or wallets.

Highly Speculative Price Fluctuations: In secondary markets, token values are speculative and can experience rapid changes. The tokens are not backed by tangible assets, making their value highly unpredictable. Token holders risk losing their entire investment if market conditions deteriorate.

Liquidity and Token Value Risks: The tokens may lose their entire value. The Company does not guarantee token liquidity and is not responsible for token price fluctuations or the absence of a secondary market. Token prices can be highly speculative and subject to extreme volatility, with no direct link to Company assets.

No Refund of Tokens: There is no guarantee of refunds in the event of delays or failure in the development or completion of the platform. Token purchases are non-refundable, and the Company does not assume liability for potential non-completion of the project.

17

Legal Disclaimer

This White Paper has been prepared to provide information on the PQCN Token, its projected business model, and is for informational purposes only. It is expressly not an offering of a financial investment. The purchase of PQCN Tokens involves certain risks, including risks related to the acquisition of any tokens, financial, tax, and technical risks. Each reader of this documentation provided by Post Quantum Network should conduct an independent assessment of the potential value of the content to determine whether to participate in any token sale. The risks associated with new technologies and cryptocurrency tokens are relatively untested, and unforeseen technology-related events may occur at any time. Participants fully accept all associated risks. Additionally, as PQCN Tokens are issued on the Ethereum blockchain, Ethereum-related risks apply.

Modifications: Any information contained in this White Paper may be updated or modified at any time by Post Quantum Network. Therefore, its completeness and factual accuracy are not guaranteed, and this information may change without notice. Post Quantum Network is not obligated to provide notice of such changes to readers.

Limitation of Liability: While Post Quantum Network has taken steps to ensure the accuracy of the information contained in this White Paper at the time of publication, neither Post Quantum Network nor any of its officers, directors, employees, advisors, partners, or agents (the "Representatives") make any representation or warranty, express or implied, and will not accept any responsibility or liability in relation to the accuracy or completeness of the information in this White Paper or any other written or oral information made available to any party. Post Quantum Network and its Representatives expressly disclaim any and all responsibility for any direct or consequential loss or damage of any kind arising from: (i) reliance on any information contained in this White Paper; (ii) any error, omission, or inaccuracy in such information; or (iii) any action taken based on this information.

Risks, Representations, and Warranties: No representation or warranty is given as to the achievement or reasonableness of any future projections, estimates, prospects, or returns contained in this White Paper. Readers should not construe the content of this White Paper or any other communications by or on behalf of Post Quantum Network or its Representatives as advice. Accordingly, each reader should consult their own professional advisors regarding financial, legal, tax, and other matters before participating in any activity connected with the subject matter herein.
Crowdsales and cryptocurrencies are currently subject to limited regulation. Regulatory authorities around the world are scrutinizing businesses and operations associated with cryptocurrencies. Any person purchasing PQCN Tokens must be aware that the business model may change or need to be modified due to new regulatory requirements. Purchasers and other interested parties acknowledge that Post Quantum Network and its affiliates are not liable for any losses or damages resulting from changes in regulation. Post Quantum Network and its employees or collaborators assume no liability or responsibility for any losses or damages, except in cases of intentional misconduct or gross negligence.

Participation in the Token Sale: By participating in the token sale, purchasers represent and warrant that they:

- Are authorized and have the legal capacity to purchase PQCN Tokens under the laws applicable in their jurisdiction;
- Reside in a jurisdiction that permits participation in token sales, including ICOs, without requiring local authorization;
- Are not purchasing for speculative investment purposes;
- Will not use PQCN Tokens for illegal activities, including but not limited to money laundering or financing terrorism;
- Understand that Post Quantum Network is not responsible for any tax obligations arising from the acquisition of PQCN Tokens, and that the purchaser alone is responsible for determining what fiscal obligations apply;
- Understand that the purchase of PQCN Tokens is non-refundable; and
- Are solely responsible for determining whether the acquisition of PQCN Tokens is appropriate for them.

Investing in Tokens involves risks. While every effort has been made to ensure that this White Paper provides a complete overview of the risks related to Post Quantum Network and its Tokens, unforeseen circumstances may adversely affect the value of any investment.
This White Paper is prepared solely for the purpose of the Offering and may not be used for any other purpose. If a claim regarding this White Paper is brought before a court, the plaintiff may be required under Estonian law to bear the costs of translating the White Paper before legal proceedings can begin.