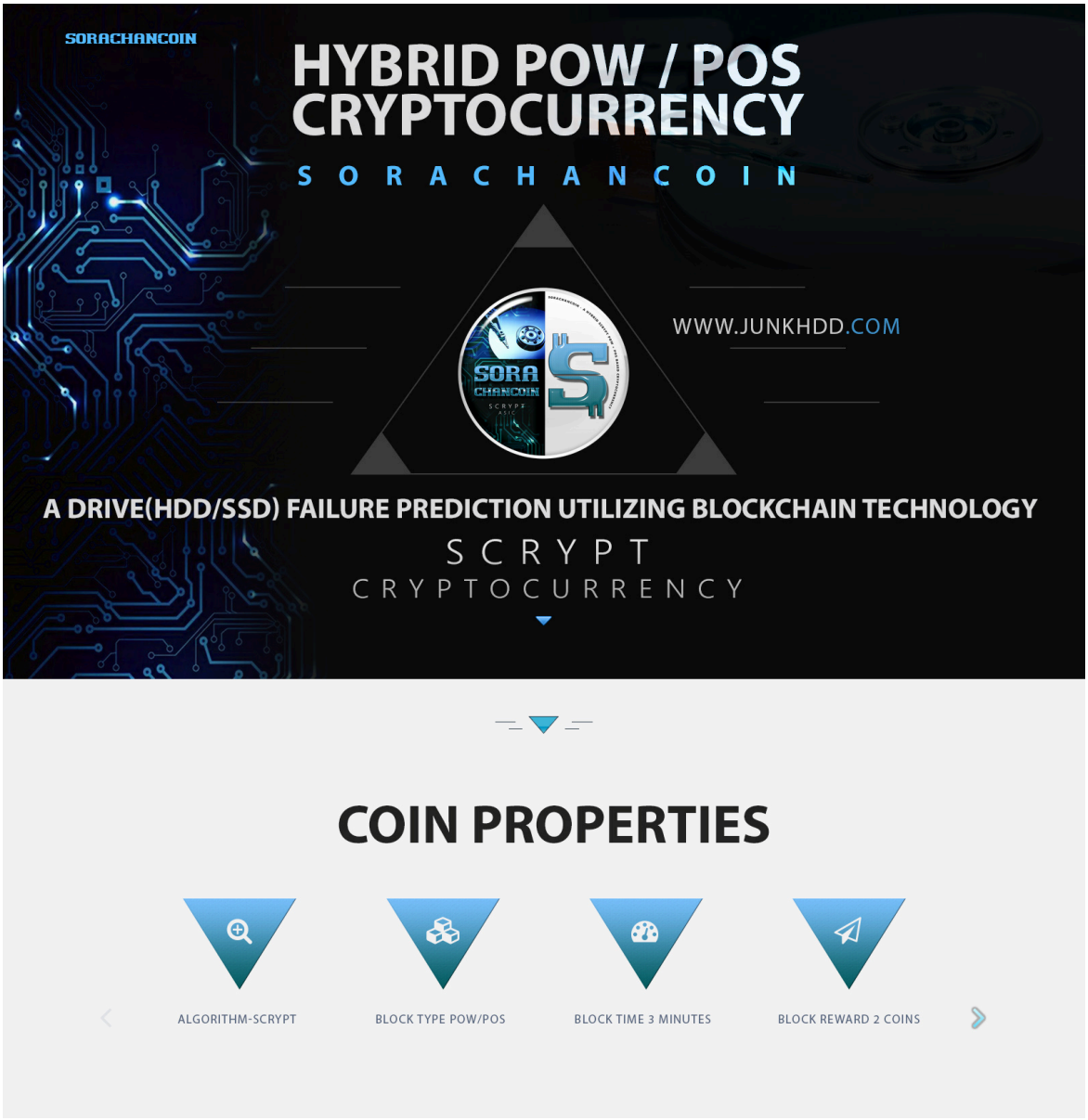


When executing PoW mining with a quantum computer, it involves searching for the hash value specified by PoW, which is assumed to utilize Grover's algorithm.

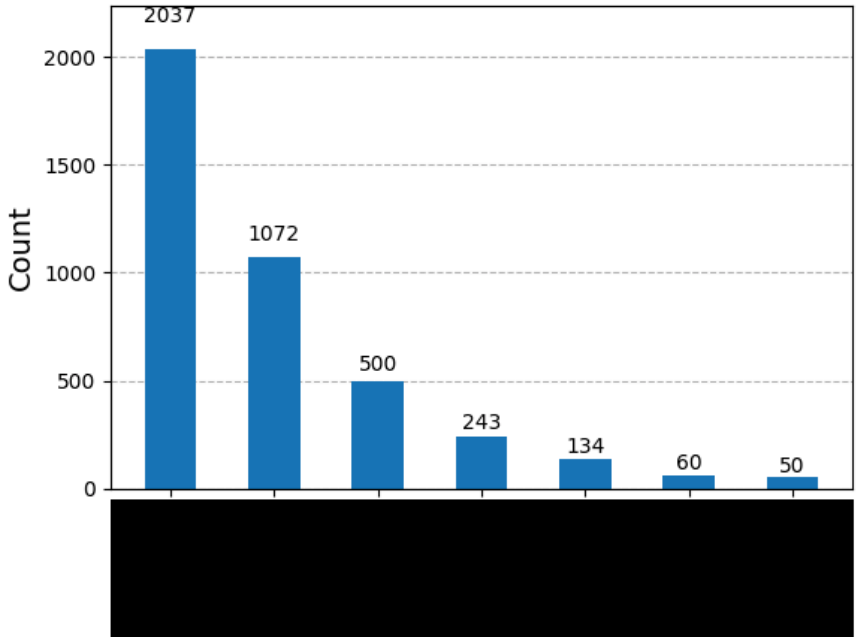
However, Grover's algorithm requires an interference process of probability amplitudes caused by rotation along the z-axis. To find the target Nonce, this interference process must be executed approximately 2^128 times (in the case of SHA-256, the standard is 2^256, and its square root results in 2^128 times).

Because this interference process takes a considerable amount of time, it has been a prevailing theory that, even with quantum computation, a significant speed improvement cannot be expected.

Computer	SHA-256 Preimage Attack
Classical	$O(2^{256})$
Quantum	$O(2^{128})$ Grover's algorithm

What? In that case, considering the time aspect, it would only be slightly faster than an ASIC, so it could be interpreted that quantum computers do not pose a threat to PoW mining. That was the conventional way of thinking.

However, when we reproduced this PoW logic in a simplified form using a quantum circuit and applied a certain effect, we encountered an unexpected phenomenon. The following is the simulation result (IBM Qiskit Aer).



Since this matter involves security concerns, the bit pattern at the bottom of the graph has been blacked out.

The number of measurements is 4096. When observing the graph, the distinctive shape immediately stands out. In other words, the probability amplitude takes on the shape of a "half-life" curve. This means that, specifically for PoW logic, we have discovered an algorithm that can efficiently transform the probability amplitude into a half-life-like shape by applying a certain effect.

The efficiency of this method is far beyond what Grover's algorithm can achieve. Below is the computational complexity if this quantum computation were applied to SHA256D.

algorithm	SHA-256D PoW
Grover's algorithm	$O(2^{128})$
This discovered approach	An exponentially efficient search is possible.

By passing through this shape, it ultimately reaches the target Nonce efficiently.

That is the core aspect of this discovered algorithm. However, it has also been found that this alone is not sufficient to reach the Nonce.

There is one more absolutely essential element for reaching the Nonce, and surprisingly, it is the "avalanche effect," which is directly related to the security of the hash.

Therefore, even if the hash function is replaced with a post-quantum cryptographic hash function, it is meaningless. For this reason, the top priority is to incorporate quantum resistance into PoW through an alternative approach that does not rely on the hash function.

This is because, compared to ECDSA, the structure of SHA-256 is simpler and easier to implement in a quantum circuit. Furthermore, due to this impact, we will begin the SORA White Paper based on these observations.

A PoW quantum mining algorithm that does not use Grover's algorithm has been discovered. The real problem is its speed.

Computer	Mining speed (SHA-256D)
S19 pro: 4.5 million units	10 minutes / 1 block
Just one Quantum computer is enough	a few seconds / 1 block

This isn't just a 51% attack - **it's a complete 100% takeover.**

Furthermore, the hash functions proposed for post-quantum cryptography have all been rendered "invalid" due to a certain mathematical property.

Since this can be mathematically proven, the possibility of transitioning from PoW to an alternative consensus mechanism has now come into consideration. **However, we also understand that PoW is extremely important. This is because PoS has a high degree of centralization.For this reason, SORA has adopted a hybrid approach from the very beginning.** Thus, we will seriously consider and implement quantum resistance for PoW. However, this is a more difficult challenge than dealing with keys and signatures. The reason is that there are many conditions to consider. It is necessary to ensure compatibility with ASICs as usual while maintaining the avalanche effect and designing a resistance mechanism that excludes quantum computing.

1. Introduction

1.1 Background

The advancement of quantum computers has begun to take steps toward practical implementation. As a result, there is a growing risk that current asymmetric cryptographic algorithms, such as RSA and ECC, may be broken. Furthermore, an even more serious issue has been pointed out: Proof-of-Work (PoW) mining itself may become vulnerable to quantum computing attacks.

1.2 Problem Awareness

The current security foundation of blockchain is primarily based on asymmetric cryptography, which is vulnerable to quantum computer attacks. However, beyond that, PoW mining itself poses an even greater risk if quantum computers leverage their computational power, mining could become automated, potentially leading to large-scale, organized attacks, including monopolization and resale of mining operations. For this reason, the implementation of a quantum-resistant cryptographic foundation has become an urgent necessity.

1.3 Objective

We have implemented the cryptocurrency SORA, which incorporates a new cryptographic foundation with quantum resistance. This project has undergone extensive verification using actual quantum computers to confirm its resilience. This is not only a first step in addressing immediate concerns but also a crucial alternative to prepare for the quantum-native generation of the future.

2. Overview of SORA

2.1 Quantum-Resistant Cryptographic Structure

SORA adopts a hash-based cryptographic algorithm combined with deep learning to achieve high resistance against quantum computing attacks. This approach ensures both ease of implementation and high-speed performance.

2.2 Quantum-Resistant ECDSA Structure

The quantum-resistant system of SORA is designed with a structure that allows future expansion to up to 128 different algorithms. It utilizes reserved areas and multi-signature mechanisms, providing a highly adaptable and interoperable framework.

2.3 Quantum Resistance in L2

SORA's Layer 2 (L2) also incorporates quantum resistance. It primarily employs a hash-based state chain to facilitate accounting proofs and contract management.

2.4 Verification Using Actual Quantum Computers

SORA is rigorously verifying the practicality of post-quantum cryptography through real quantum computers. Special attention is given to re-examining Grover’s algorithm to ensure the core verification of quantum resistance.

3. Details of Quantum Resistance

3.1 Quantum Resistance in ECDSA and PoW Mining

To address the threats posed by quantum computing, SORA enhances ECDSA resistance while also introducing new methods to mitigate vulnerabilities in PoW mining.

Quantum-Resistant ECDSA

- Adopts an extended structure of ECDSA with quantum resistance, capable of supporting up to 128 different resistance mechanisms.
- Utilizes reserved areas and multi-signature techniques to establish a more robust signature algorithm.

Quantum Resistance in PoW Mining

- Introduces a quantum-resistant PoW algorithm designed to suppress quantum acceleration of hash calculations.
- Implements adaptive difficulty adjustment and quantum-resistant protocols to prevent quantum computers from gaining an unfair advantage in hash computations.
- Designs a flexible mining process to minimize the impact of quantum attacks.

By integrating these technologies, SORA aims to maintain security in the quantum era and establish itself as a practical and resilient cryptocurrency.

3.2 Verification Using Actual Quantum Computers

The quantum resistance of SORA has been rigorously tested through both simulations and real-world quantum computer experiments. Urgent attention is required to ensure the resilience of PoW mining algorithms against quantum-based attacks.

Urgency of Quantum Resistance in PoW Mining

- Quantum computers pose a significant threat by potentially monopolizing mining operations.
- Simulations and real-world quantum experiments have observed state vectors, confirming the possibility of quantum mining attacks achieving not just 51% dominance but full (100%) control.
- Strengthening PoW resistance to quantum attacks is an urgent challenge that must be addressed immediately.

Verification Methods and Results

- A thorough evaluation was conducted by comparing actual quantum computer experiments with simulation results to determine the effectiveness of existing quantum-resistant PoW methods.
- The influence of Grover's algorithm was scrutinized to verify whether theoretically secure methods hold up in practical quantum implementations.
- The analysis of state vectors was carried out to measure the extent to which quantum hash computation surpasses traditional PoW mechanisms.

Based on these results, SORA will continue improving its PoW algorithm to establish itself as a robust cryptocurrency for the quantum era.

3.3 Over-Reliance on Grover's Algorithm and Its Limitations

In recent years, many studies have focused on Grover's algorithm as the primary example of quantum search. However, the assumption that "search = Grover's algorithm" is a flawed oversimplification, and quantum resistance must be evaluated from multiple perspectives.

Lack of Comprehensive Verification

- Many studies proceed under the assumption that Grover's algorithm is the dominant quantum threat, while actual quantum-based verification remains insufficient.
- The influence of other quantum algorithms and the possibility of combined attack scenarios are not fully considered.

Risk of Complacency

- The belief that "as long as a system resists Grover's algorithm, it is secure" leads to complacency.
- Overlooking alternative quantum threats can delay fundamental countermeasures needed for practical deployment.

SORA avoids restricting its analysis to Grover's algorithm alone and evaluates quantum resistance from multiple angles to implement more comprehensive defense strategies.

3.4 The PoW Quantum Mining Algorithm Discovered by SORA

SORA has identified a PoW quantum mining algorithm that, despite targeting hash functions, exploits a shortcut to reach the desired Nonce without using Grover's algorithm.

Critical Risk Factors

- It bypasses Grover's algorithm, which is typically the most time-consuming quantum operation.
- It effectively nullifies PoW's difficulty adjustment, potentially rendering the traditional PoW model obsolete.
- As a result, a complete (100%) mining attack could be executed, leading to mining monopolization by quantum computers.

Given the confirmation of this emerging threat, the urgent development of a new PoW system adapted to the quantum computing era is necessary. SORA is actively working on addressing this challenge and developing the most optimal solutions to defend against quantum attacks.

3.5 The Nature and Risks of Cryptocurrencies

Cryptocurrencies differ fundamentally from conventional cryptographic applications in that their value is directly tied to cryptographic security. As a result, the risks they face are significantly different from those affecting authentication or data protection.

Direct Dependence on Cryptographic Security

- The value of a cryptocurrency is inherently linked to the security of its cryptographic foundation.
- If the cryptographic system is compromised, the asset value will be immediately lost, and trust will be irreversibly damaged.

The Critical Consequence of Neglecting Quantum Resistance

- Many authentication cryptosystems can afford alternative recovery measures if compromised, but cryptocurrencies face systemic collapse if their cryptographic foundation fails.
- In the quantum era, failing to prioritize security could lead to catastrophic consequences.

SORA fully acknowledges these inherent risks and implements quantum resistance as a top priority.

4. Building Quantum Resistance

4.1 Fundamental Issues in Post-Quantum Cryptography

Is post-quantum cryptography truly quantum-resistant? This question arises from how post-quantum cryptography is defined.

Reliance on Grover's Algorithm

- Many post-quantum cryptographic techniques are designed based on the assumption that Grover's algorithm shortens search time to $\sqrt{N}$.
- To counteract this, increasing the address space is a common strategy, but this does not guarantee fundamental security.

Is That Really Sufficient?

- Simply expanding the address space is not enough to ensure genuine quantum resistance.
- There is a risk of overlooking new quantum algorithms or yet-to-be-discovered methods of attack.

SORA critically reassesses what "quantum resistance" truly means and strives to build a more comprehensive approach beyond just increasing address space.

4.2 The Challenges of Hash-Based Post-Quantum Cryptography

Current post-quantum hash functions are primarily designed to counteract Grover's algorithm by increasing address space. However, the mathematical properties of hash functions themselves remain unchanged.

Contradictions in Hash Functions and Post-Quantum Cryptography

- If an attack does not exploit weaknesses in the hash function itself but instead uses it as a stepping stone for another attack, the issue no longer pertains to hash security.
- Consequently, replacing a hash function with a post-quantum certified hash function does not necessarily improve quantum resistance.

Discovery of the PoW Quantum Mining Algorithm

- SORA's newly discovered attack vector does not target hash function weaknesses directly but rather exploits vulnerabilities in the overarching PoW process.
- Thus, switching to a post-quantum-certified hash function does not provide quantum resistance.

SORA emphasizes the need for careful evaluation of post-quantum cryptography and continues its research to develop truly effective quantum resistance.

5. Conclusion

This whitepaper has analyzed the impact of quantum computing advancements on cryptocurrencies and demonstrated the importance of the quantum-resistant technology built into SORA.

- The development of quantum computers threatens the security of existing cryptographic algorithms, such as RSA and ECDSA.
- The security of PoW mining is significantly undermined, making the risk of 100% dominance far beyond a 51% attack a reality.
- Relying solely on post-quantum cryptography based on Grover's algorithm is a limited approach and does not provide a fundamental solution.
- SORA continues research to address vulnerabilities in traditional PoW mining by countering quantum algorithms, ensuring true quantum resistance.

As we move into the quantum era, urgent action is required to protect the future of cryptocurrencies. SORA is committed to securing quantum resistance and realizing a safe, decentralized network.