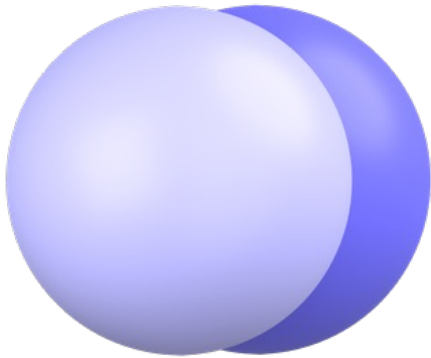# SPHINX

An open-source Post-Quantum blockchain layer 1

Open to anyone who want to join and contribute based on his/her passion in quantum-resistant blockchain ecosystem.

https://linktr.ee/sphinx.org

THE PROBLEM

Moore's Law: The number of transistors on microchips has doubled every two years

Our World in Data

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years.
This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.
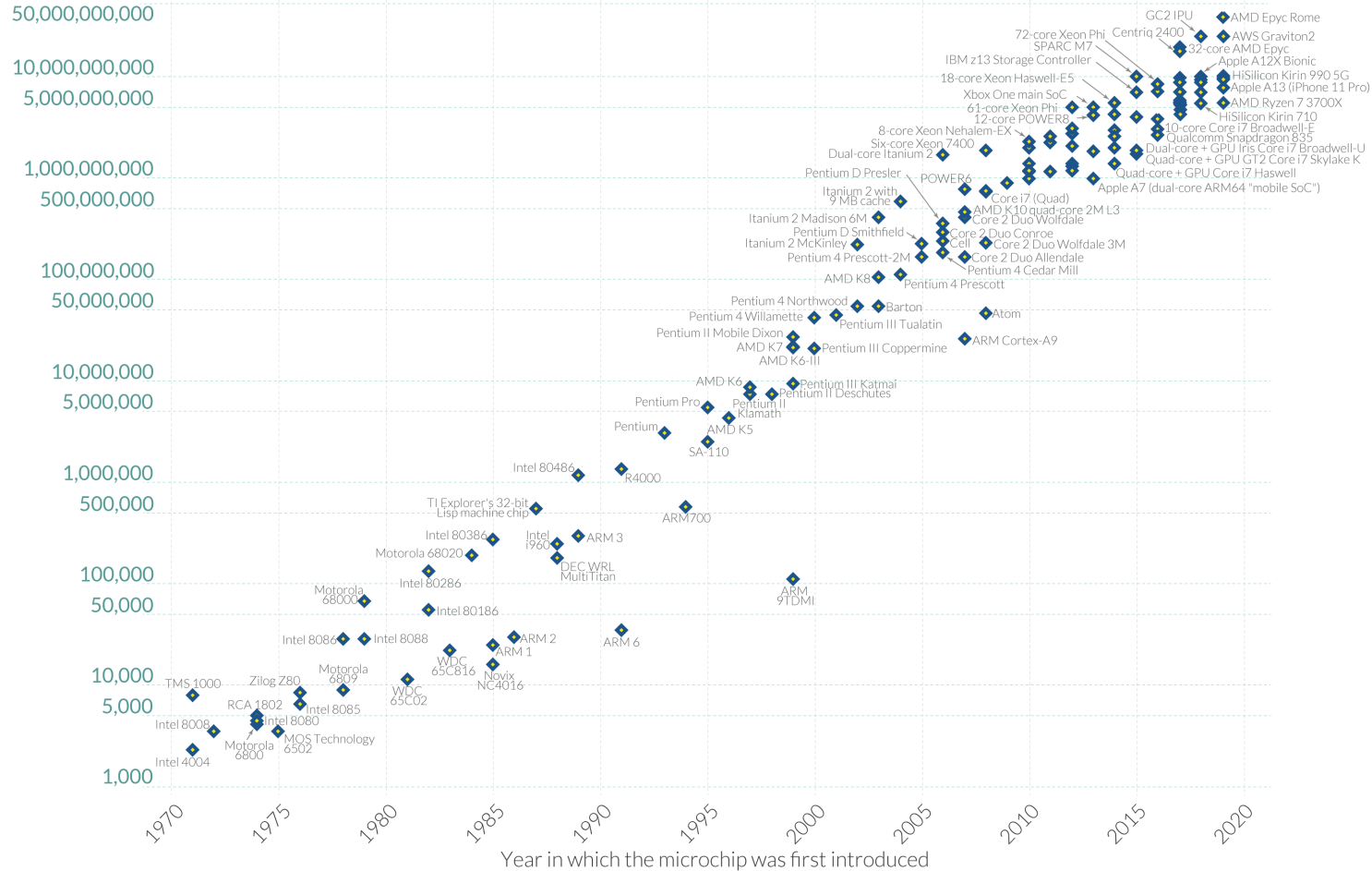
Moore's Law

IBM Roadmap to Scaling Quantum Technology

1. In 2023 IBM quantum scientists are building a quantum computer with a 1,121-qubit processor, called Condor.

2. Condor lays the groundwork for scaling to fully error-corrected, interconnected, 1-million-plus-qubit quantum computers.

3. In 2021, IBM will debut the 127-qubit "Eagle" chip

4. Eagle will be followed by the 433-qubit "Osprey" processor in 2022.

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor[†]

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates

Daniel Litinski @ PsiQuantum, Palo Alto

We use Shor's algorithm for the computation of elliptic curve private keys as a case study for resource estimates in the silicon-photonics-inspired active-volume architecture. Here, a fault-tolerant surface-code quantum computer consists of modules with a logarithmic number of non-local inter-module connections, modifying the algorithmic cost function compared to 2D-local architectures. We find that the non-local connections reduce the cost per key by a factor of 300-700 depending on the operating regime. At 10% threshold, assuming a 10-μs code cycle and non-local connections, one key can be generated every 10 minutes using 6000 modules with 1152 physical qubits each. By contrast, a device with strict 2D-local connectivity requires more qubits and produces one key every 38 hours. We also find simple architecture-independent algorithmic modifications that reduce the Toffoli count per key by up to a factor of 5. These modifications involve reusing the stored state for multiple keys and spreading the cost of the modular division operation over mul-

dreds or thousands of physical qubits. There exist two types of general-purpose architectures for surface codes: baseline architectures with nearest-neighbor logical two-qubit operations on a 2D grid [14–18], and the recently introduced active-volume architecture [19] utilizing a logarithmic number of non-local connections between patches. The latter leverages non-local connections to parallelize the execution of logical operations, resulting in a significant speedup compared to a fault-tolerant quantum computer with the same footprint, but strict 2D-local connectivity.

Different architectures. The existing literature on FTQC resource estimates primarily focuses on baseline architectures, relying on determining logical qubit counts (n_Q) and Toffoli gate counts (n_{Tof}) due to the relevance of the cost function $n_Q \cdot n_{\text{Tof}}$. Resource estimates for active-volume architectures are different, albeit not more complicated. Instead of counting qubits and gates, different fundamental subroutines are counted based on their specific costs, known as the active volume. This paper aims to guide the reader through a simplified active-volume resource estimation

Curve VS Shor's Algorithm

Efficiently solve for 'p'
computing on field 'F' using
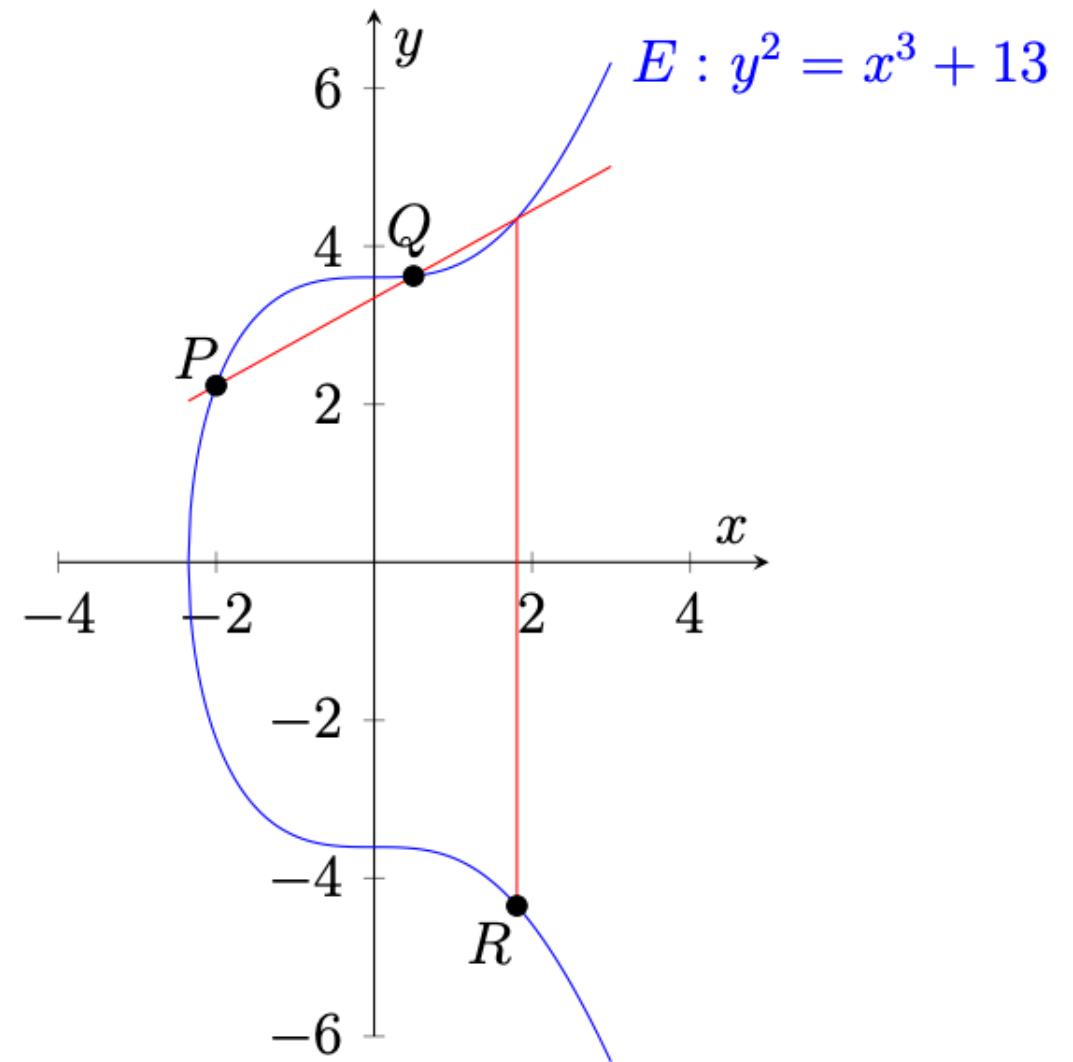coordinates 'a' and 'x'."

```
// Define the prime modulus p
const int p = 17;


// Perform addition in finite field
 int fieldAddition int a, int
        return (a + b) % p; }
}
```

$$E : y^2 = x^3 + 13$$

Grover's Algorithm can Reverse a black-box function (Hash Function) implemented as a quantum oracle in $O(\sqrt{N})$ iterations with $O(log2N)$ qubits, with N being the number of possible input combinations to the function.

NIST retires SHA 224 bit

Figure 1

Quantum computing's potential for significant speedup over classical computers, according to IBM internal analysis

Type of scaling	Time to solve problem				
Classical algorithm with exponential runtime	10 secs	2 mins	330 years	3300 years	Age of the universe
Quantum algorithm with polynomial runtime	1 min	2 mins	10 mins	11 mins	~24 mins

Quantum-computing landscape:

IBM Roadmap.

IBM quantum centric 100,000 qubits.

(EuroHPC JU) quantum-computers.

CISA & NSA was warn for global community

the deadline to we are migrate into post-

quantum era until 2035.

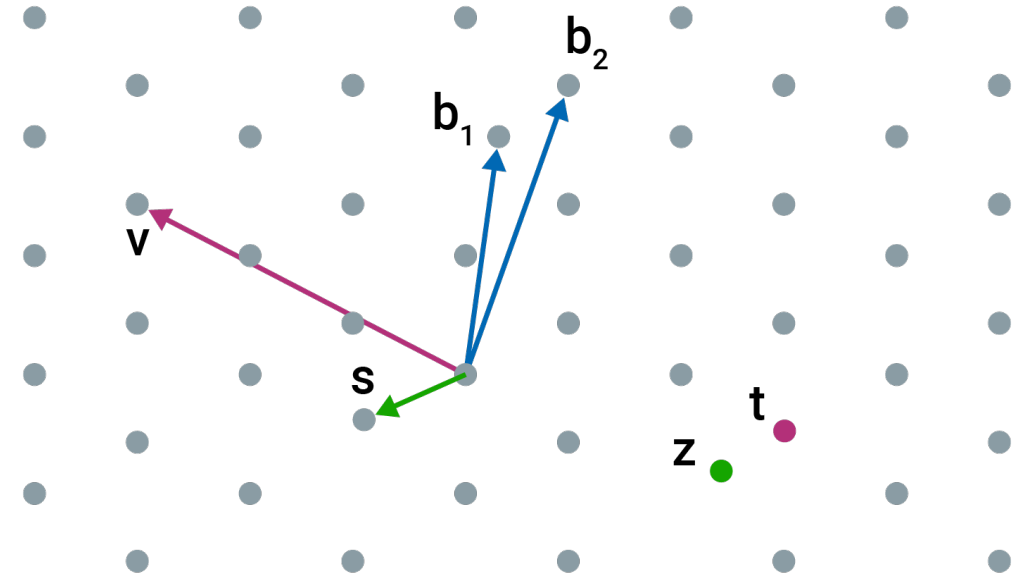# THE SOLUTION

N.I.S.T PQC 3rd winner (KEMs)

Lattice-based
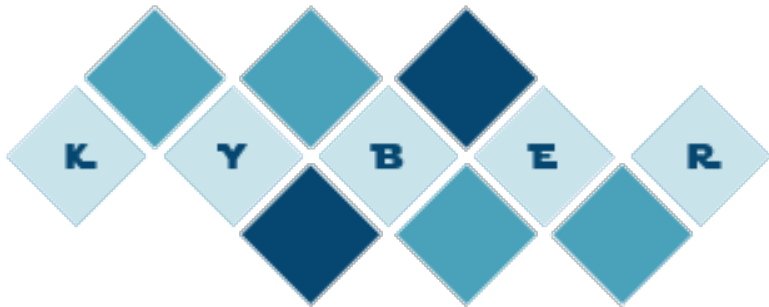
Crystals-kyber

(sk, pk, ct, hash)

Cloudflare Research: Post-Quantum Key Agreement

On essentially all domains served through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. Read our blog for the details.

You are using *X25519Kyber768Draft00* which is **post-quantum secure**.

Deployed key agreements

Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519Kyber512Draft00 `0xfe30`	
X25519Kyber768Draft00 `0x6399` (recommended) and `0xfe31` (obsolete)	

X25519Kyber*[x]*Draft00 is a hybrid of X25519 and Kyber*[x]*Draft00 (in that order).

Client support

- **Chrome** Canary (restricted to ≤HTTP/2) if you turn on *TLS 1.3 hybridized Kyber support* (`enable-tls13-kyber`) in `chrome://flags`. **[new!]**
- Our fork of **Go**.
- **BoringSSL** **[new!]**. Upstream only supports `0x6399`; for the others use our old fork.
- Our fork of **QUIC-go**.
- *Goutam Tamvada*'s fork of **Firefox**.
- Open Quantum Safe with the right setting. **[new!]**
- **Zig** nightly. **[new!]**

Contact

You can reach us directly at ask-research@cloudflare.com with questions and feedback.
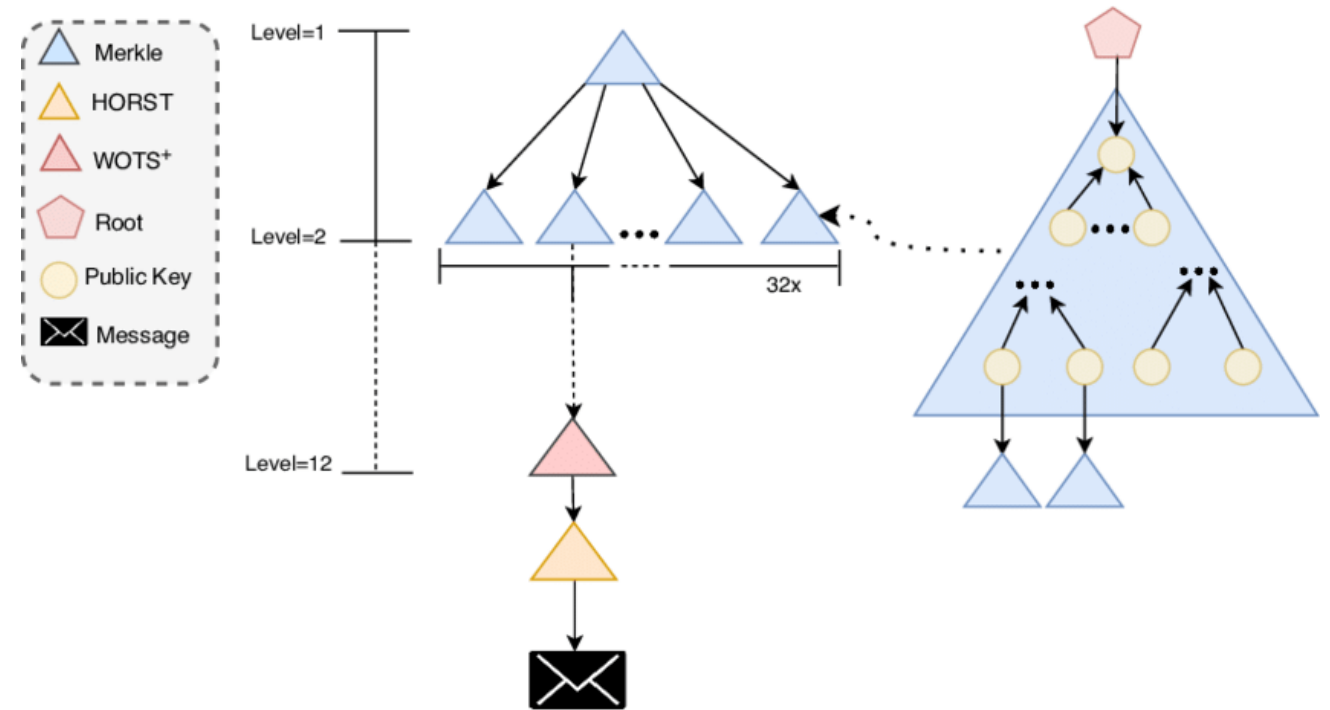
N.I.S.T PQC 4th winner

PQC (DSA)

"Stateless" hash-based

SPHINCS+
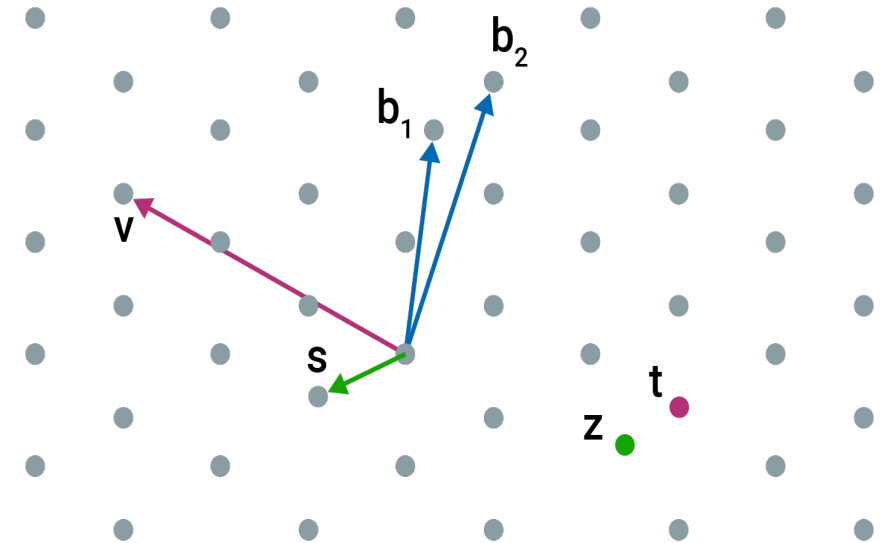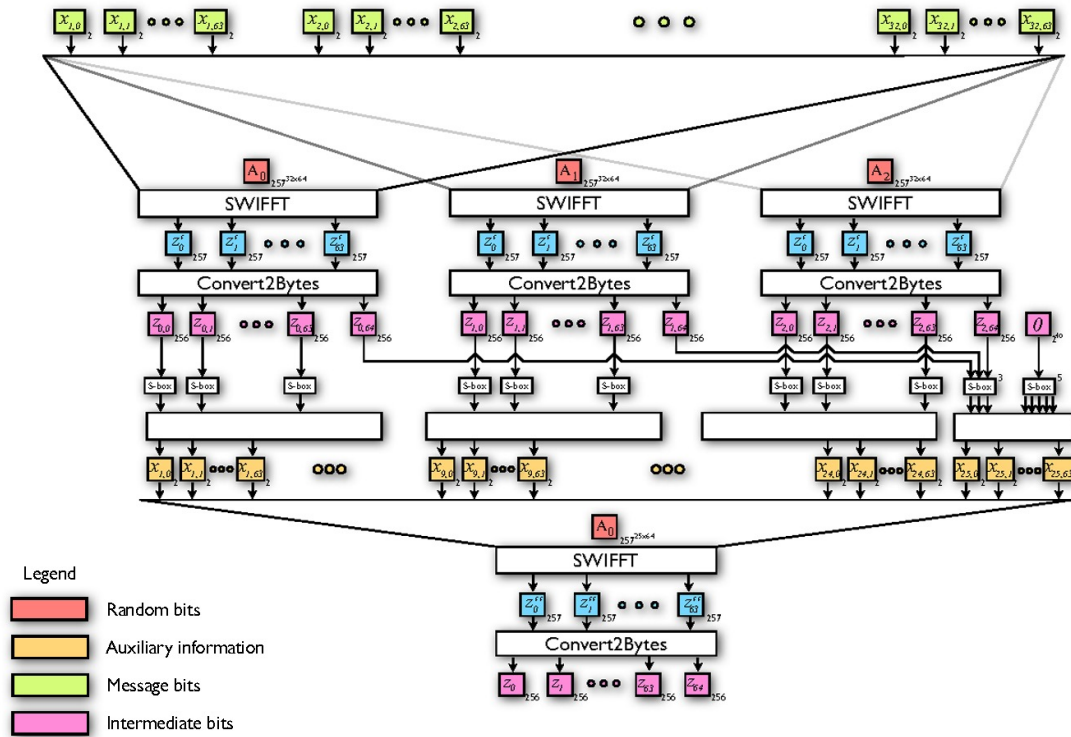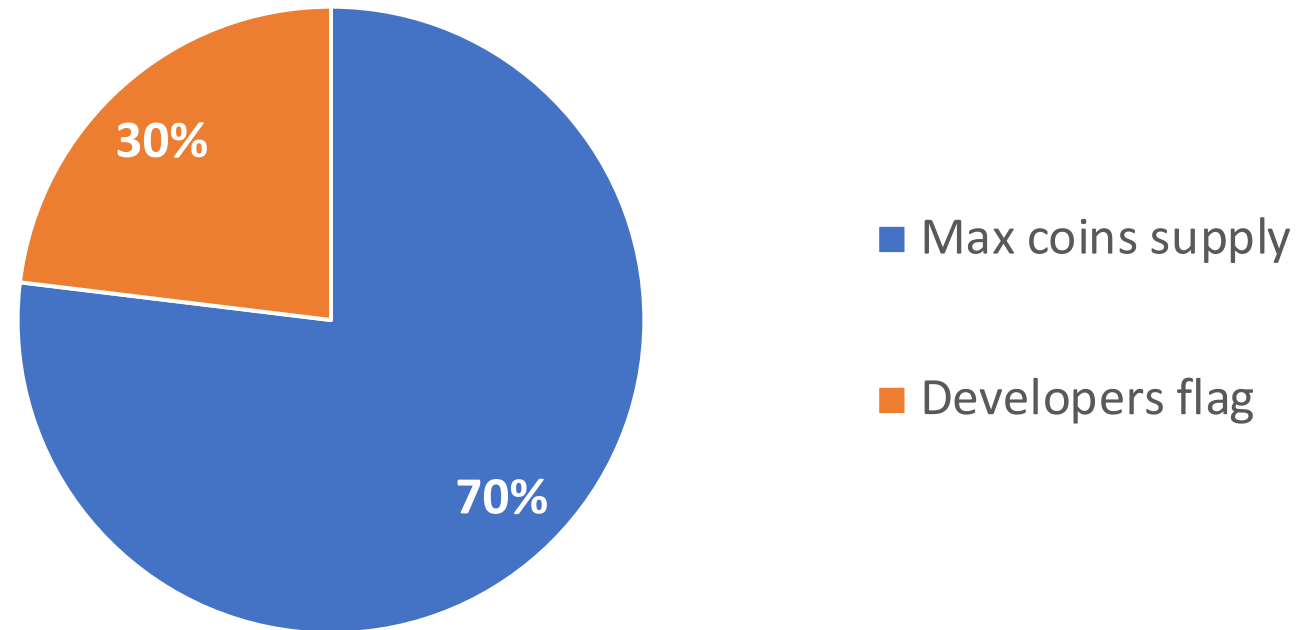
Sphincs+

(verify, sign, hash)

SWIFFTX Hash function

SWIFFT + SVP

TOKENOMIC

Max. supply 50 million "SPX" coins

- Max coins supply
- Developers flag

SPHINX

For more detil just visited our workspace;

https://github.com/SPHINX-HUB-ORG