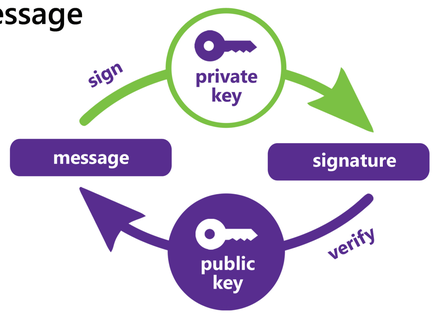
POST-QUANTUM BLOCKCHAIN

Securing the NEAR blockchain with the Falcon algorithm to resist quantum computer attacks

THE ROLE OF DIGITAL SIGNATURES IN CRYPTOGRAPHY

Digital signatures allow to sign and verify messages signatures to provide proof of authenticity of a message or a transaction. Digital signatures provide :

- **authentication** : the owner of the private key signed the message
- **integrity** : the message was not altered after the signing
- **non-repudiation** : the sender can't deny having sent and signed the message



Main digital signature algorithms:
- RSA digital signatures
- EcDSA
- EdDSA

QUANTUM COMPUTING IS COMING

A breakthrough : in 1994, Peter Shor formulates a quantum algorithm that can theoretically breaks all public key cryptographic system with a quantum computer.

In parallel, tech giants like Google and IBM, are taking up the race to build quantum computers and publicly announce having reached quantum supremacy.

Google / 2018 / 72 Qubits

IBM / 2022 / 433 Qubits*

* In quantum computing, a qubit or quantum bit is a basic unit of quantum information - the quantum version of the classic binary bit.

A MAJOR INNOVATION : THE BLOCKCHAIN

HISTORY
Bitcoin (2009)
Ethereum (2014)

KEY OBJECTIVES & PRINCIPLES
- Peer-to-peer transactions without central authority
- Decentralized servers
- The consensus mechanism
- A public ledger
- Smart contracts

A WIDE RANGE OF USE CASES
Financial transactions / Voting / Gaming / Decentralized file storage / DNS Servers / Traceability / etc

OUR CRITERIA TO CHOOSE A BLOCKCHAIN
Performance + Scalability + Security + Environmental impact

THE NEED FOR QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHMS

The need to design public-key algorithms that cannot be broken by quantum computer is urgent. In 2016, the NIST launched an international competition to find and standardize Post-Quantum algorithms.

In July 2022, among the 4 selected finalists, there was 1 for public key encryptions and 3 for digital signatures algorithms. The 3 finalists for digital signatures algorithms are :

CRYSTALS-DILITHIUM | **FALCON** | **SPHINCS+**

NEAR + Falcon = PQB

Why NEAR ?

- High level of security, compared to other blockchains that have been hit with attacks.
- A carbon-neutral proposal.
- Coded in RUST, a programming language praised for its safety.

Why Falcon ?

Among the NIST finalists, we decided to use the Falcon 512 algorithm. Falcon is a lattice-based signature scheme that offers compactness and security. One of our main goals is to keep the size of each block as small as possible. The decisive criteria for choosing Falcon 512 were :

Shorter public key size | **Shorter signature size**

PQB
POST-QUANTUM BLOCKCHAIN

Our final product

- A ready-to-use Kurtosis implementation that allows developers and users to test locally the NEAR Post-Quantum blockchain, and all the documentation to deploy it.

- A dedicated GitHub repo where our code is publicly available. We did not reimplement Falcon : we used "wrappers" to interface with the C implementation of Falcon which was coded by Thomas Pornin, one of Falcon co-author.

- On-going discussion with NEAR developers about the best way to transition to a post-quantum NEAR protocol.

- An informative website explaining our project and showing a roadmap for the deployment of our product.

Our approach : gaining knowledge from Falcon authors

We had the opportunity to discuss with 3 co-authors of Falcon.

Thomas PORNIN : He is currently working for the NCC group in Montreal. He is the developer of the only production implementation of the Falcon algorithm. He told us that Falcon was the most complex cryptography algorithm he had to implement.

Zhenfei ZHANG : He is currently working for the Ethereum Foundation. His mission is to integrate post-quantum cryptography securely and efficiently within the Ethereum blockchain. We were therefore able to discuss with him and obtain his opinion on the choice of the cryptographic algorithm within the framework of a blockchain.

Pierre-Alain FOUQUE : He is a teacher and researcher in mathematics applied to cryptography at the University of Rennes 1. We had the opportunity to meet with him at his lab at IRISA. He gave us some leads to improve our performance in terms of signature size for the Falcon algorithm.

More info at : post-quantum-team.github.io

Teacher : Elian PRIVAT
5A Students : Maximilien CHAUX - Alizée HAMON - Madigan LEBRETON - Bertrand MARTIN

École d'ingénieurs ensibs Université Bretagne Sud