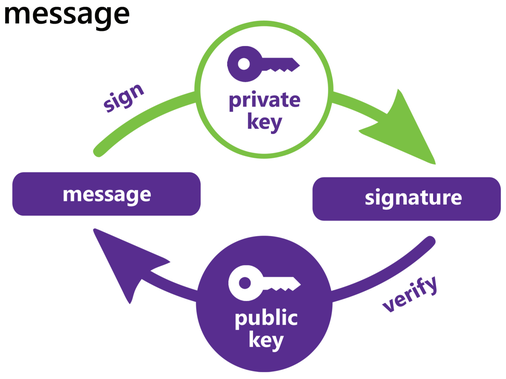
POST-QUANTUM BLOCKCHAIN

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 / 2018 / 50 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 / 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 ?

	Decentralization	Security	Scalability	Consensus
Avalanche	+++	+++	4 500 tps	Proof of Stake DAG
Bitcoin	+	+++	7 tps	Proof of Work
Elrond	+++	+++	15 000 tps	Proof of Stake
Ethereum	+	+++	15 tps	Proof of Stake
Fantom	++	+++	Theory: 300 000 tps Practice: 4 500 tps	Proof of Stake DAG
Near	+++	++++	~ 1600 and 8000 tps	Proof of Stake
Solana	+++	+	~2 000 and 3 000 tps	Proof of Stake Proof of History

We decided to use the NEAR blockchain because of the high security level it offers compared to other blockchains that have been hit with attacks, as well as its carbon-neutral proposal and the RUST language it is using.

Implementation language

The NEAR blockchain is coded in RUST. We used “wrappers” to interface with the C code of Falcon. Our development is available on the GitHub repo of our project.

Why Falcon ?

	Dilithium2	Dilithium3	Dilithium5	Falcon-512	Falcon-1024	Ed25519
Public key size	+++	++	+	++++	++	++++
Signature size	++	+	+	++++	+++	++++
Signature verification performance	++++	+++	++	+++	+	+
Quantum Core-SVP Hardness	+	+++	++++	+	++++	N/A
Secure implementation	++++	++++	++++	++	++	++++
Total	14	13	12	14	12	13

Among the NIST finalists, we decided to use the Falcon 512 algorithm. The decisive criteria for the crypto algorithm to be implemented in a blockchain in order to reduce the quantity of data saved within each block were :
- Shorter public key size
- Shorter signature size

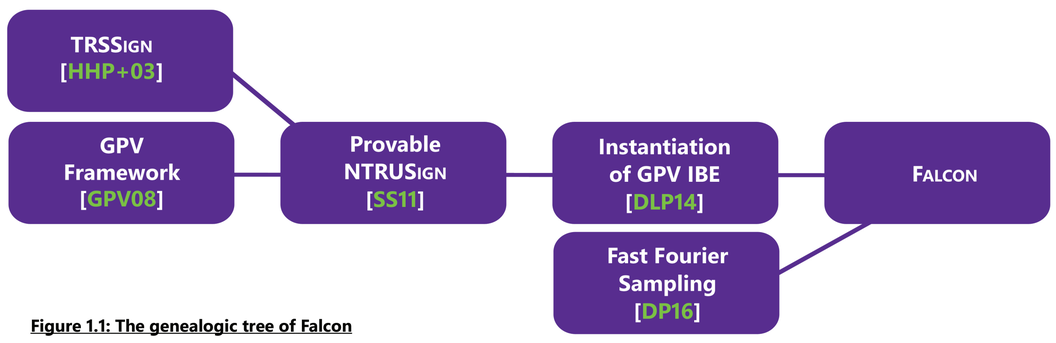


Figure 1.1: The genealogic tree of Falcon

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

École d'ingénieurs ensibs Université Bretagne Sud