ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Quantum-Safe Blockchain

Evaluating the Feasibility of Introducing Quantum-Safe Digital Signatures For Blockchain Using the Example of a Minimal Python-based Blockchain

Kimika Uehara - 0000000000
Silas Pohl - 1900124387

01 **Introduction**

Motivation and Research Question

02 **Method**

Approach to Answer Our Research Question

03 **Implementation**

Practical Showcase of the Project

04 **Results**

Measurements, Metrics and Graphs

05 **Conclusion**

Discussion, Limitations and Further Research

“It’s time to prepare for quantum threats.”

- Dr. Lily Chen (mathematician and NIST fellow)

https://www.theverge.com/22523067/nist-challenge-quantum-safe-cryptography-computer-lattice

How feasible is the integration of quantum-safe signature algorithms into blockchains?

Select quantum-safe algorithms to evaluate

Implement Python blockchain (classic and quantum-safe)

Conduct comparison by measuring perf. / attributes

Hash-based Cryptography
rely on secure cryptographic hash functions, which exhibit properties like being difficult to reverse, resistant to finding original inputs,
and robust against collision attacks

Lattice-based Cryptography
sets of points arranged periodically in multi-dimensional spaces. Lattice-based systems are founded on the shortest vector problem (finding the smallest non-zero point within a lattice), which is NP-hard

Multivariante Cryptography
rely on the complexity of multivariate system of equations, which have been demonstrated to be NP-complete or NP-hard

First group of winners from NIST’s six-year competition

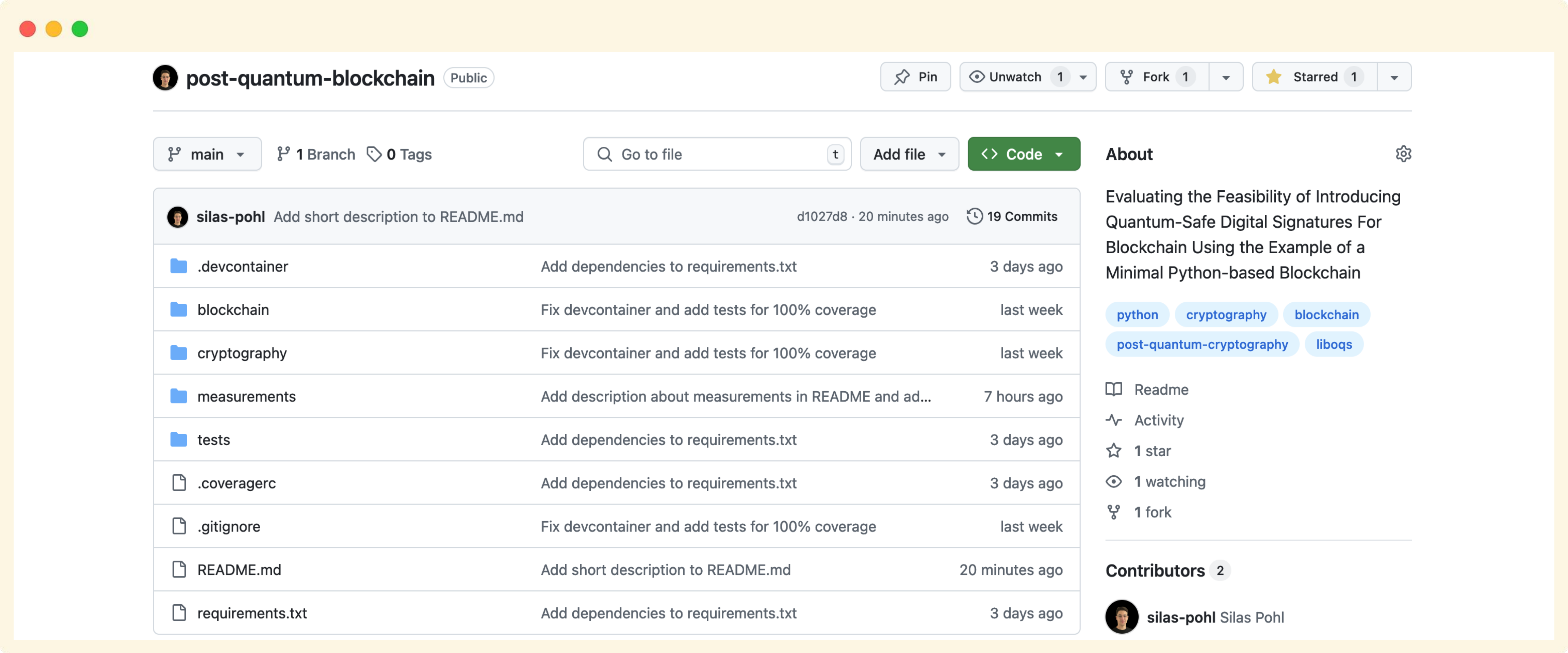
CYSTALS-Dilithium, FALCON, SPHINCS+

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Select quantum-safe algorithms to evaluate

Implement Python blockchain (classic and quantum-safe)

Conduct comparison by measuring perf. / attributes



silas-pohl Add short description to README.md d1027d8 · 20 minutes ago 19 Commits

.devcontainer	Add dependencies to requirements.txt	3 days ago
blockchain	Fix devcontainer and add tests for 100% coverage	last week
cryptography	Fix devcontainer and add tests for 100% coverage	last week
measurements	Add description about measurements in README and ad...	7 hours ago
tests	Add dependencies to requirements.txt	3 days ago
.coveragerc	Add dependencies to requirements.txt	3 days ago
.gitignore	Fix devcontainer and add tests for 100% coverage	last week
README.md	Add short description to README.md	20 minutes ago
requirements.txt	Add dependencies to requirements.txt	3 days ago

About

Evaluating the Feasibility of Introducing Quantum-Safe Digital Signatures For Blockchain Using the Example of a Minimal Python-based Blockchain

silas-pohl Silas Pohl

https://github.com/silas-pohl/post-quantum-blockchain

- Select quantum-safe algorithms to evaluate
- Implement Python blockchain (classic and quantum-safe)
- **Conduct comparison by measuring perf. / attributes**

Public & Secret Key Sizes	**Signature Size**	**Blockchain Storage**
Transaction Time	**Verification Time**	**Mining Time**

SHOWCASE