



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 - 00000000000
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

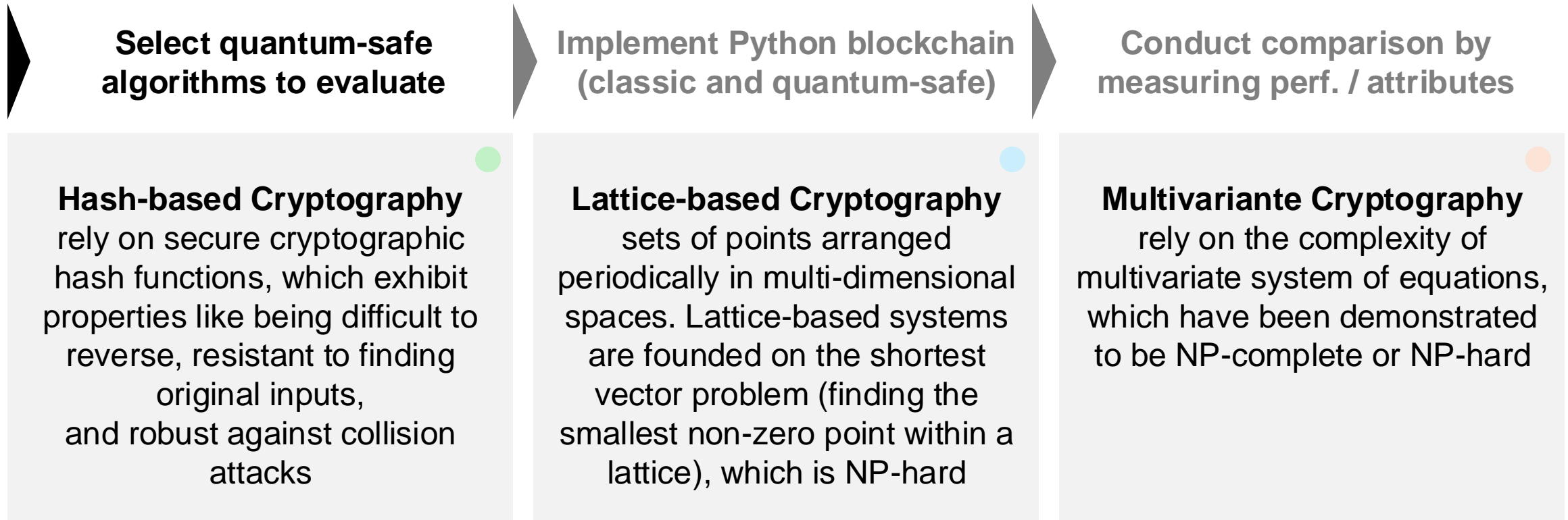
05 **Conclusion**

Discussion, Limitations and Further Research

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

- Dr. Lily Chen (mathematician and NIST fellow)

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



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

CRYSTALS-Dilithium, FALCON, SPHINCS+

Select quantum-safe algorithms to evaluate

Implement Python blockchain (classic and quantum-safe)

Conduct comparison by measuring perf. / attributes

The screenshot shows the GitHub repository page for 'post-quantum-blockchain' by user 'silas-pohl'. The repository is public and has 1 branch and 0 tags. The main branch is selected. The repository description is 'Evaluating the Feasibility of Introducing Quantum-Safe Digital Signatures For Blockchain Using the Example of a Minimal Python-based Blockchain'. The repository has 1 star, 1 watch, and 1 fork. The repository contains the following files and folders:

File/Folder	Description	Time
.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

The repository also has a 'Contributors' section with 2 contributors: silas-pohl (Silas Pohl).



**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