BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Bachelor's Thesis Assignment

155332

Institut:	Department of Intelligent Systems (DITS)
Student:	**Ľaš Michal**
Programme:	Information Technology
Title:	**Blockchain Resistant to Quantum Attack**
Category:	Security
Academic year:	2023/24

Assignment:

1. Learn about blockchain technology and the vulnerabilities a quantum attack can bring. Next, focus on existing blockchain implementations that claim to be resistant to quantum attack (e.g., Cardano, Ripple).
2. Learn about post-quantum cryptographic algorithms and discuss their suitability for use in blockchain.
3. Design your own quantum attack-resistant blockchain solution (with emphasis on ensuring integrity and security of transactions).
4. Implement the design. Existing libraries of post-quantum algorithms can be used. If too complex, some layers not related to security can be abstracted.
5. Test the functionality of the implementation, evaluate its performance and security parameters.
6. Compare the results with existing implementations and evaluate the effectiveness of the resulting solution.

Literature:

- NÚKIB: Útoky s využitím kvantového počítače mohou prolomit současné šifrování: řešením je včasná a efektivní implementace nových standardů. 5151/2023, E/630, Brno, strategická analýza, 2023
- NÚKIB: Kvantová hrozba a kvantově odolná kryptografie“, Příloha k dokumentu: Minimální požadavky na kryptografické algoritmy
- Brad Chase, & Ethan MacBrough. (2018). Analysis of the XRP Ledger Consensus Protocol. arXiv:1802.07242

Requirements for the semestral defence:
Items 1 to 3.

Detailed formal requirements can be found at https://www.fit.vut.cz/study/theses/

Supervisor:	**Malinka Kamil, Mgr., Ph.D.**
Head of Department:	Hanáček Petr, doc. Dr. Ing.
Beginning of work:	1.11.2023
Submission deadline:	9.5.2024
Approval date:	6.11.2023