THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Decentralized authentication of IoT devices based on blockchain technology**
Author's name:	**Viktoriia Chvykova**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of microelectronics
Thesis reviewer:	Ing. Ivo Veřtát, Ph.D.
Reviewer's department:	Faculty of electrical engineering, University of West Bohemia in Pilsen

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

How demanding was the assigned project?

The topic of the diploma thesis is selected from a relatively new and very rapidly developing area of secure authentication and verification of IoT devices even on microprocessors with limited computing power and power consumption.

Fulfilment of assignment **fulfilled with minor objections**

How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.

The basic theory of blockchain-based technologies, individual types, their advantages and disadvantages were described in the work, and a method for practical implementation on the development board was chosen. Experiments were performed to show the writing of commands to the IOTA Tangle and their back reading and processing using the development board for IoT with the STM32 microprocessor. I only slightly miss the attempt to perform a computational complexity analysis and data overhead compared to other authentication methods, but this alone would be a very complex topic. Perhaps at this point, there could be at least a search of current studies to see if and with what results someone had done this.

Methodology **correct**

Comment on the correctness of the approach and/or the solution methods.

The work first presents the basis of several alternative technologies (mainly Blockchain and DAG IOTA), compares their advantages and disadvantages, and then attempts at their practical implementation on development boards. However, conventional IoT authentication methods without the use of Blockchain or IOTA technologies may also have been described.

Technical level **C - good.**

Is the thesis technically sound? How well did the student employ expertise in the field of his/her field of study? Does the student explain clearly what he/she has done?

From a technical point of view, the work contains a large number of basic definitions of distributed ledger technologies and IoT networks and an explanation of their principle of operation. These areas could be more referred to the literature and the released space in the diploma thesis should be devoted to the field of device authentication in IoT networks in deeper technical details and how the distributed ledger technology can be used in this area and with what advantages.

Formal and language level, scope of thesis **C - good.**

Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?

The research part of the work with a theoretical introduction could be shorter, on the contrary, the practical part of the work would require a deeper description of the objectives and evaluation of the performed experiments (eg microcontroller load, memory occupancy, ...).

Selection of sources, citation correctness **B - very good.**

Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?
All references used are actual and closely related to the topic of the work. I only lack references to the statement from page 28 regarding the resistance of the compared methods to quantum computer attacks.

Additional commentary and evaluation (optional) *Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.*
Although the practical part of the work does not seem very extensive and complex, the implementation and modification of basic examples of technologies on the development boards of microcontrollers may not be straightforward and simple in this area of secured communication, encryption and authentication. I appreciate that the student managed to implement IOTA technology on a specific development board and verify it in a simple form, which can be useful for follow-up work that would further address the topic.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

In connection with my comments on the individual points of the review, I propose the final evaluation of the thesis in grade B and ask the following possible questions to defend the thesis:

1) *Can you clarify from which sources the information from page 28 on the resilience of methods to quantum computer attacks is taken and why is IOTA more resilient?*

2) *Have you found studies that address the computational complexity and growth of data overhead methods described for use in IoT networks? Alternatively, can any conclusions be drawn from these studies about the complexity of implementing decentralized or distributed authentication in simple hardware IoT?*

The grade that I award for the thesis is **B - very good.**

Date: **30.5.2022** Signature: