IT UNIVERSITY OF COPENHAGEN

Computer Science Department
Direct phone: +45 2988 3541
E-mail: beda@itu.dk
Journal no.: 09-2024

September 16, 2024

Report on the PhD Thesis of Tomasz Lizurej

To Whom It May Concern,

I am writing to report on the thesis submitted by Tomasz Lizurej as part of the requirements to obtain a PhD degree. The thesis presents novel research results on the theory and practice of blockchain systems security. It includes three main results, namely on manipulating algorithms used in reputation systems, verifying that trusted hardware behaves as expected and the new paradigm of individual cryptography.

In Chapter 2, the thesis investigates how easy it is to manipulate FGA, a weight prediction method for signed weighted networks. This method has been used to estimate trust as part of reputation systems with data derived from blockchain-based decentralized finance platforms. Surprisingly, the results presented in the thesis are that it is not only theoretically hard to manipulate FGA but also hard to do so in practice.

In Chapter 3, the thesis introduces the new paradigm of Individual Cryptography, which ensures that a single entity controls an important cryptographic secret (*e.g.*, a signature key for a cryptocurrency scheme) instead of sharing this secret among a set of parties in such a way that no single party controls it. The main solution presented towards this goal is to allow a party to prove to any verifier that they know the entire secret, *i.e.*, a proof of individual knowledge. Besides finding applications in preventing "renting" of cryptographic secrets in blockchain systems, the proof of individual knowledge construction proposed as a solution is based on Proof-of-Work puzzles usually employed for blockchain consensus.

In Chapter 4, the thesis proposes new methods for efficiently testing whether a Boolean circuit implements a given function by means of a small set of test inputs. Such methods allow for checking if trusted hardware implements the functions it is supposed to. As such trusted hardware modules underpin the security of several prominent blockchain protocols and applications, it is important to verify their correctness.

All results in the thesis represent important novel scientific contributions and have been published in top conferences, which shows their recognition by the broader scientific community. Hence, the thesis meets the highest international standards of scientific research and is deemed sufficient to grant a PhD degree.

Yours sincerely,

Bernardo David
Associate Professor