**Blokų grandinių ir kvantiniais skaičiavimais grįstų sprendimų kūrimas ir tyrimai**

Dr. Ernestas Filatovas, prof. dr. Saulius Masteika, prof. dr. Remigijus Paulavičius, doc. dr. Linas Petkevičius

Blokų grandinių technologijos esama technologinė būklė bei jos pritaikomumas įvairiose srityse reikalauja nuolatinio tobulinimo, nes egzistuoja daug mokslinių iššūkių, kaip pavyzdžiui, ribotas masteliavimas, didelis energijos suvartojimas, decentralizacijos lygio problemos ir saugumo klausimai. Reikalingi moksliniai tyrimai skirtinguose blokų grandinių lygmenyse (0, 1 ir 2 lygmenyje). Taip pat yra būtina tirti įvairius konsensuso protokolus bei masteliavimo sprendimus - pačioje blokų grandinėje, už grandinės ribų ir šoninėje grandinėje, taip siekiant padidinti blokų grandinių funkcionalumą ir našumą. Sparčiai vystantis ir augant įvairioms blokų grandinėms, jų integracija tampa vis aktualesnė, todėl interoperabilumo sprendimai šiuo metu yra kaip niekad aktualūs. Be to, reikia įvertinti įvairių blokų grandinių decentralizacijos lygį, ypač atsižvelgiant į masteliavimo ir saugumo sprendimus. Pastarojo meto DeFi ir NFT tendencijos parodė ne tik šių technologijų potencialą, tačiau ir iškėlė daug saugumo ir privatumo iššūkių, kuriuos būtina kuo greičiau spręsti. Sparti kvantinių kompiuterių pažanga pasaulyje įgalina išspręsti uždavinius, kurie klasikiniams kompiuteriams yra sunkiai arba iš viso neįveikiami, o taip pat leidžia pasiekti žymiai didesnę spartą. Todėl labai svarbu Lietuvai neatsilikti šiame kontekste ir skirti tam reikiamą dėmesį. Iš vyraujančių temų matyti, kad labai svarbu tirti ir kurti kvantinių kompiuterių algoritmus įvairiems mašininio mokymosi ir optimizavimo uždaviniams spręsti. Be to, kvantiniai kompiuteriai, lyginant su klasikiniais, pasižymi papildomu saugumu ir efektyvumu. Todėl dabartinių blokų grandinių saugumo ir atsparumo atakų uždaviniai turėtų būti sprendžiami ir panaudojant kvantinius kompiuterius. Galiausiai turėtų būti tiriami unikalūs iššūkiai ir galimybės derinant šias dvi inovatyvias technologijas ir tai, kaip jas galima panaudoti sprendžiant realius uždavinius įvairiose pramonės šakose.

**Development of blockchain and quantum computing techniques**

Blockchain technology's actual theoretical status and applicability in various domains need to be improved, as many research challenges exist, such as limited scalability, high energy consumption, decentralization concerns, and security issues. Research impact is required at different layers (Layer 0, Layer 1, and Layer 2) of blockchains. The investigation of different consensus protocols as well as various types of scaling solutions – on-chain, off-chain, and side-chain – to increase the functionality and performance of blockchains is demanding. With the rapid development and growth of various blockchains, their integration becomes increasingly relevant; therefore, interoperability solutions should also be investigated. Moreover, the decentralization level of various blockchains, also considering scaling solutions, must be assessed. Also, the recent trend in DeFi and NFT raised many security and privacy challenges, which need to be addressed. Rapid progress in quantum computing makes it possible to solve problems that are virtually impossible for classical computers to solve or to offer significantly faster speeds. Therefore, it is very important for Lithuania to keep up in this field and give it the attention it needs. Among the prevailing themes, developing quantum computing algorithms for various machine learning and optimization problems is essential. Moreover, quantum

computing offers extra security and effectiveness over its classical counterpart. Therefore, the security of the current blockchains and problems of resisting attacks should be carried out by exploiting the quantum computers. Finally, the unique challenges and opportunities in combining these two innovative technologies and how they can be leveraged to solve real-world problems in various industries should be investigated.