BlockChain ტექნოლოგიაზე დაფუძნებული ავტორიზაცია/ავთენტიფიკაციის მექანიზმი

ნათიგ კურბანოვი

სამაგისტრო ნაშრომი წარდგენილია ილიას სახელმწიფო უნივერსიტეტის ბიზნესის, ტექნოლოგიისა და განათლების ფაკულტეტზე მაგისტრის აკადემიური ხარისხის მინიჭების მოთხოვნების შესაბამისად

პროგრამული ინჟინერია

სამეცნიერო ხელმძღვანელი: **ერეკლე მაღრაძე**, ილიას სახელმწიფო უნივერსიტეტის ასოცირებული პროფესორი

პროექტის ხელმძღვანელი: ილიას სახელმწიფო უნივერსიტეტის, ბიზნესის ტექნოლოგიის და განათლების ფაკულტეტის, გამოთვლითი ცენტრის დირექტორი, ამავე უნივერსიტეტის ასოცირებული პროფესორი, **პაატა გოგიშვილი**

ილიას სახელმწიფო უნივერსიტეტი
თბილისი 2023

განაცხადი

როგორც წარდგენილი სამაგისტრო ნაშრომის ავტორი, ვაცხადებ, რომ ნაშრომი ჩემი ორიგინალური ნამუშევარია და არ შეიცავს სხვა ავტორების მიერ აქამდე გამოქვეყნებულ, გამოსაქვეყნებლად მიღებულ ან დასაცავად წარდგენილ მასალებს, რომლებიც არ არის მოხსენიებული ან ციტირებული სათანადო წესების შესაბამისად.

ნათიგ კურბანოვი

11 ივლისი 2023

მადლობა

მინდა მადლობა გადავუხადო ჩემს ხელმძღვანელს, ბატონ ერეკლე მაღრაძეს, მისი ხელმძღვანელობისა და მხარდაჭერისთვის. მისმა ღირებულმა ცოდნამ და გამოცდილებამ მნიშვნელოვანი როლი ითამაშა ამ ნაშრომის ჩამოყალიბებაში. და ბოლოს, მინდა გამოვხატო ჩემი გულწრფელი მადლიერება ჩემს ოჯახს ურყევი მხარდაჭერისა და გამხნევებისთვის. მათი სიყვარული და რწმენა ჩემს მიმართ იყო ჩემი მუდმივი მოტივაცია.

ნათიგ კურბანოვი

აბსტრაქტი

ბოლო ათწლეულის განმავლობაში მსოფლიოს მილიონობით მოსახლე ბლოკჩეინ ტექნოლოგიების [1] სწრაფი განვითარების მომსწრე და მონაწილე გახდა. იგი თავდაპირველად იყო შემოთავაზებული, როგორც ცენტრალიზებული ციფრული ფულადი ტრანზაქციების პრობლემის გადაჭრის დეცენტრალიზებული კონცეფცია, რომელიც სატოში ნაკამოტოს ფსევდონიმით 2008 წელს იყო წარმოდგენილი. კონცეფციის დოკუმენტში, რომელსაც ერქვა "Bitcoin: A Peer-to-Peer Electronic Cash System"[2], აღწერილი იყო ციფრული ვალუტა - ბიტკოინი და მისი დეცენტრალიზებული არქიტექტურა, ბლოკჩეინზე დაყრდნობით. მიუხედავად იმისა, რომ ეს დოკუმენტი კონკრეტულად ბიტკოინს აღწერდა, დროთა განმავლობაში გამოჩნდა ბევრი ფიზიკური/იურიდიული პირი თუ სახელმწიფო სტრუქტურა, რომლებმაც ციფრული ვალუტის მრავალი სახეობა შექმნეს.

სამაგისტრო ნაშრომი მიზნად ისახავს ბლოკჩეინ ტექნოლოგიაზე დაფუძნებული ავტორიზაცია/ავთენტიფიკაციის მექანიზმების შესწავლას და ამის საფუძველზე შემდგომ, კონცეპტუალური გადაწყვეტის მოძიების ოპტიმალური მიდგომების განხილვას. ეს თანამედროვე მიდგომები მათი უსაფრთხო და დეცენტრალიზებული არქიტექტურიდან გამომდინარე, დღითი დღე უფრო აქტუალური ხდება და დგება ბევრი საკითხი თუ როგორ უნდა განხორციელდეს ტრადიციული პროგრამული უზრუნველყოფების ტრანსფორმაცია ბლოკჩეინ ტექნოლოგიების გამოყენებით.

ნაშრომში არის წარმოდგენილი შედარებითი ანალიზი, რომელშიც განიხილება აღნიშნული პრობლემების გადაჭრის მეთოდები. თითოეული მეთოდისთვის გამოკვეთილია მათი უპირატესობები და ნაკლოვანებები. შემდგომ, არის წარმოდგენილი შერჩეული მიდგომები და დასაბუთებულია მათი შერჩევის მიზეზები. ასევე, წარმოდგენილი არის მიღებული პროგრამული უზრუნველყოფის UML [3] და Flowchart [4] დიაგრამები, მომხმარებლის ინტერფეისის (User Interface [5]) მაგალითები და მათთან ურთიერთქმედების გზები.

ძირითადი საძიებო სიტყვები: დეცენტრალიზებული სისტემები, ავტორიზაცია, ავთენტიფიკაცია, ბლოკჩეინ ტექნოლოგიები, ჭკვიანი კონტრაქტები;

Abstract

Over the last ten years, blockchain technology [1] has experienced exceptional growth and wide adoption globally. Initially introduced as a decentralized system by the pseudonymous Satoshi Nakamoto in 2008 through the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System,"[2] blockchain technology provided a novel solution to centralization issues in digital monetary transactions. Although the paper primarily focused on Bitcoin, various individuals, legal entities, and governmental structures have since utilized this technology to create numerous digital currencies.

The primary objective of this Master's thesis is to explore the authentication and authorization mechanisms based on blockchain technology, intending to discuss optimal methodologies for extending this concept further. The growing relevance of these state-of-the-art techniques, derived from their secure and decentralized design, raises multiple questions about transitioning conventional software architectures towards blockchain-enabled systems.

This research paper offers a comparative analysis where solutions to the issues mentioned earlier are debated. Each proposed methodology is examined with a spotlight on its merits and demerits. Following this, chosen processes are expounded, and the rationale behind their selection is elucidated. In addition, the thesis provides Unified Modeling Language (UML [3]) and Flowchart [4] diagrams of the developed software, examples of user interfaces [5], and their interaction mechanisms.

Keywords: decentralized systems, authorization, authentication, blockchain technology, smart contracts;