Slovak University of Technology in Bratislava
Faculty of informatics and information technologies

Reg. No.: FIIT-16768-116160

Lukáš Častven

Practical usage of Zero-knowledge in different use-cases in blockchains

Bachelor’s thesis

Thesis supervisor: Ing. Kristián Košťál PhD.

December 2023

Slovak University of Technology in Bratislava
Faculty of informatics and information technologies

Reg. No.: FIIT-16768-116160

Lukáš Častven

Practical usage of Zero-knowledge in different use-cases in blockchains

Bachelor’s thesis

Study programme: Informatics

Study field: Computer Science

Training workplace: Institute of Computer Engineering and Applied Informatics

Thesis supervisor: Ing. Kristián Košťál PhD.

December 2023

Slovenská technická univerzita v Bratislave
Ústav počítačového inžinierstva a aplikovanej informatiky

Fakulta informatiky a informačných technológií
2023/2024

ZADANIE BAKALÁRSKEJ PRÁCE

Autor práce:	Lukáš Častven
Študijný program:	informatika
Študijný odbor:	informatika
Evidenčné číslo:	FIIT-16768-116160
ID študenta:	116160
Vedúci práce:	Ing. Kristián Košťál, PhD.
Vedúci pracoviska:	Ing. Katarína Jelemenská, PhD.
Názov práce:	**Practical usage of Zero-knowledge in different use-cases in blockchains**
Jazyk, v ktorom sa práca vypracuje:	slovenský jazyk
Špecifikácia zadania:	Zero-knowledge proofs (ZKPs) are an exciting breakthrough in applied cryptography that will unlock new use cases across an array of industries, from Web3 to supply chains to the Internet of Things. By verifying the authenticity of information without revealing it, ZKPs can help enhance digital systems' privacy, security, and efficiency. Current use cases are decentralized identity, private transactions, secure and scalable Layer-2s, voting systems, IoT, supply chains, etc. Examine existing solutions and proposals in this domain by conducting state-of-the-art analysis. Propose a system that will utilize Zero-knowledge techniques in some of the existing blockchain networks to enhance its functionality by one of the picked goals. Implement such a solution, which can be done in a smart contract way or as a core network plugin. Potential blockchain networks to use are Polkadot, Kusama, Near, Tezos, Algorand, Moonbeam, Ethereum, etc. Evaluate the implemented solution and compare it with existing ones. Discuss the results and conclude with new findings.
Rozsah práce:	40
Termín odovzdania práce:	21. 05. 2024
Dátum schválenia zadania práce:	
Zadanie práce schválil:	

Anotácia

Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Študijný program: Informačná bezpečnosť

Autor: Lukáš Častven

Bakalárska práca: Velmi dolezity projekt

Vedúci projektu: Ing. Kristián Košťál PhD.

December 2023

Bakalárska práca skúma aplikáciu dôkazov s nulovým vedomím (ZKPs) v blockchaine. Dôkazy s nulovým vedomím sú kryptografická metóda, ktorá umožňuje overenie dát bez odhalenia samotných dát, čo je ideálne pre bezpečné a súkromné aplikácie v blockchainoch. Táto práca je zameraná na návrh a implementáciu konceptu schémy tajne adresy s použitím ZKPs. Táto schéma umožňuje odosielateľom odvodiť tajnú adresu z verejných údajov príjemcu. Iba príjemca má kontrolu nad touto adresou, a zaroveň neodhaľuje žiadne informácie o tom, kto príjemca je.

Výskum zahŕňa analýzu kryptografických princípov za ZKPs, nasledovanú vysvetlením návrhu schémy tajne adresy a jej integráciou do blockchainu Ethereum.

Táto práca prispieva do oblasti ukázaním, ako možno využiť ZKPs v blockchaine na riešenie problémov súkromia, ponúkajúc riešenie vo forme konceptuálnej implementácie schémy tajne adresy s použitím ZKPs.

Annotation

Slovak University of Technology in Bratislava

Faculty of informatics and information technologies

Degree Course: Informatics

Author: Lukáš Častven

Bachelor’s thesis: Practical usage of Zero-knowledge in different use-cases in blockchains

Supervisor: Ing. Kristián Košťál PhD.

December 2023

This bachelor’s thesis investigates the application of Zero Knowledge Proofs (ZKPs) in blockchains. Zero Knowledge Proofs are a cryptographic method which enables the validation of data without revealing the data itself, making it ideal for secure and private applications in blockchain networks. The focus of this thesis is the design and implementation of a proof of concept Stealth Address scheme using ZKPs. This scheme allows any sender to derive a stealth address from recipients public data. Only the recipient has control over this address, yet it does not leak any information about who the recipient is.

The research includes an analysis of the cryptographic principles behind ZKPs, followed by a explanation of the Stealth Address scheme’s design and its integration into a an Ethereum blockchain.

This thesis contributes to the field by showcasing how ZKPs can be utilized in blockchain to address privacy concerns, offering a solution in the form of a proof of concept implementation of Stealth Address scheme using ZKPs.

Table of contents

List of Figures

List of abbreviations used

EVM	Ethereum Virtual Machine
ZK	Zero Knowledge
ZKP	Zero Knowledge Proof

Chapter 1

Introduction

Zero Knowledge Proofs (ZKPs) are a powerful cryptography primitive. They allow for the verification of a statement's truth without disclosing or in any way revealing the actual content of the statement. This characteristic is crucial for maintaining trust between parties while also preserving privacy.

The concept of ZKPs was first introduced in a 1989 research paper, "The Knowledge Complexity of Interactive Proof Systems."[1]. This work describes how in traditional proofs, such as demonstrating a graph is Hamiltonian, more information is typically revealed than just the truth of the theorem. This paper develops a computational complexity theory focusing on the knowledge part within a proof. It introduces zero knowledge proofs, a novel concept where proofs only confirm the correctness of a proposition without exposing any extra knowledge. The paper focuses on interactive proofs, where a dialogue between a prover and a verifier occurs. In these interactive proofs, the prover aims to convince the verifier about the truth of a private statement, with a very small probability of error. This interaction is pivotal in ZKPs, as it allows for the verification of a statement's truth without revealing the actual information or knowledge behind the statement, maintaining the principle of conveying no knowledge beyond the proposition's correctness.

This thesis extends the application of ZKPs to the concept of stealth addresses in blockchain, as outlined in Vitalik Buterin's article "An Incomplete Guide to Stealth Addresses."[2]. Stealth addresses are critical for privacy on blockchains, allowing assets to be transferred without revealing the recipient's identity and making it difficult to link transactions to specific individuals.

Stealth addresses allow a sender (Alice) to transfer assets to a receiver (Bob) without publicly revealing the Bob's identity. To achieve this, Bob must first provide a public meta stealth address generation data. This data has different structure based on the underlying stealth address generation schema. From this data Alice computes a new stealth address that only Bob can control, and sends the assets to that newly generated address. Bob can then access these assets from another address, only by providing a ZKP of given address ownership.

Chapter 2

Analysis

The analysis section of the thesis starts with demonstration of interactive proofs with goal to build up intuition behind interactive proofs [1, 3]. This section explains how Alice attempts to prove to Bob that she knows an algorithm, with which she computes some pair (N, y), such that this pair is part of the quadratic residue language QR. Specifically, Alice needs to convince Bob that there exists an x such that y equals x squared modulo N, effectively placing the pair (N, y) within the QR language, which includes all pairs where y is a quadratic residue of N.

The analysis section continues by highlighting a practical limitation of interactive proofs in real world cryptography. It notes that for Alice to prove something to multiple parties, she would need to engage in separate interactions with each one. This approach is not scalable and becomes impractical for widespread verification needs. However, the thesis introduces the Fiat-Shamir transform [4], a significant breakthrough that addresses this issue. This transform allows for converting the interactive proof into a non-interactive format by processing the interaction transcript, making the proof more practical and scalable for real-world cryptographic applications.

While in theory any NP statement [1] can be proven using interactive proofs, practical implementation requires specific definition and encoding of the statement. There are two main models of general computation, those are circuits and turing machines. To trace the computation of a turing machine, the representation needs to somehow handle memory and thus would accrue more complexity than if a circuit is used. To represent a statement as a circuit, an arithmetic circuit, a computation model composed of addition and multiplication operations, is used. This circuit encodes the statement into a form suitable for "zk-ifying", enabling the application of interactive proofs to a broader range of practical scenarios.

The analysis section then explores various ZKP systems, each with unique properties and proof constructions. The most renowned among these are SNARKs (Succinct Non-interactive ARguments of Knowledge), Bulletproofs, and STARKs (Scalable Transparent ARguments of Knowledge). These systems differ in aspects such as computational efficiency, size of proofs, and the need (or lack thereof) for a trusted setup. Each system offers advantages and challenges, making them suitable for different applications.

The final part of the analysis examines how ZKP systems such as SNARKs enable the creation of a stealth address scheme that upholds privacy and security. This section assesses how these systems fulfill the necessary properties for a stealth address scheme, focusing on their ability to ensure transaction confidentiality while maintaining the anonymity of the recipient's identity.

2.1 Proof of quadratic residuosity

$$QR = \{(N, y) : \exists x, y \equiv x^2 \pmod{N}\}$$

2.2 Arithmetic circuit

in a finite field $\mathbb{F}_p$

the interaction part is non-practical => Fiat Shamir

R1Cs

SNARKs - from Dan Boneh MOOC commitments SZDL lemma = a polynomial is zero-polynomial with dp probability = zero - test

Chapter 3

Návrh riešenia

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Chapter 4

Implementácia

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Chapter 5

Testovanie

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Chapter 6

Záver

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

6.1 Zhodnotenie projektu

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

6.2 Možné vylepšenia

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Resumé

References

[1] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof Systems". In: *SIAM Journal on Computing* 18.1 (Feb. 1989), pp. 186–208. ISSN: 1095-7111. DOI: 10.1137/0218012. URL: http://dx.doi.org/10.1137/0218012.

[2] *An incomplete guide to stealth addresses — vitalik.eth.limo*. https://vitalik.eth.limo/general/2023/01/20/stealth.html. [Accessed 12-12-2023].

[3] *ZKP MOOC Lecture 1: Introduction and History of ZKP — youtube.com*. https://www.youtube.com/watch?v=uchjTIlPzFo&list=PLS01nW3Rtgor_yJmQsGBZAg5XM4TSGpPs. [Accessed 16-12-2023].

[4] Amos Fiat and Adi Shamir. "How To Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, pp. 186–194. ISBN: 9783540180470. DOI: 10.1007/3-540-47721-7_12. URL: http://dx.doi.org/10.1007/3-540-47721-7_12.

Appendix A

Špecifikácia API rozhrania

This is the application programming interface

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.10

A.1 Endpointy

- v1 - API version 1
- v2 - API version 2
- test - API placeholder

A.2 Cesty

- A.2.1 Auth
- A.2.2 Music
- A.2.3 Pictures
- A.2.4 Video
- A.2.5 Mail

A.2.1 Auth

A.2.2 Music

A.2.3 Pictures

A.2.4 Video

A.2.5 Mail

Appendix B

Project task schedule

B.1 Zimný semester

1st-4th week	Consultations & finding related research
5th-6th week	Working on the Introduction and Analysis chapters
7th week	Consultations
8th-10th week	Working on the Analysis chapters
11th-12th week	Working on the Solution proposal chapter

B.2 Letný semester

1st-2nd week	Consultations & designing API specification
3rd-6th week	Consultations & implementation of back-end
7th-9th week	Implementation of server
10th week	Consultations & implementation of front-end
11th-12th week	Finishing documentation & solution testing

Appendix C

Contents of the digital medium

Registration number of the thesis in the information system: FIIT-16768-116160

Contents of the digital medium (ZIP archive):

Name of the submitted archive: BP_LukasCastven.zip.