Universitatea Tehnică a Moldovei

# ELABORAREA ALGORITMULUI CRIPTOREZISTENT DE TRANSFER A DATELOR ÎN REȚEAUA BLOCKCHAIN ETHEREUM PENTRU SMART CONTRACTS

**Student :** **Leanca Andrei**

**Conducător :** **Ganea Victoria**

**conf. univ.,dr**

**Chișinău, 2023**

# REZUMAT

**Autor: Andrei Leancă**, gr. SISRC-211M

**Tema:** ”Elaborarea algoritmului criptorezistent de transfer a datelor in retaua Blockchain Ethereum pentru Smart Contracte „

**Structura lucrării:** Teza constă dintr-o notă explicativă de 48 de pagini, inclusiv o introducere de 1 pagină, 3 tabele, 19 figuri, o listă de 20 de surse, dintre care 5 surse în limba străină.

**Cuvintele cheie:** Smart contract, criptare, blockchain, ethereum.

**Problematica studiului:** Problema cheie a tezei este securitatea transmiterii datelor pe internet între utilizatori.

**Scopul lucrării:** Elaborarea algoritmului criptorezistent de transfer a datelor în rețeaua Blockchain Ethereum pentru Smart Contracte.

**Obiectivele:**

1. Compara sistemele de mesagerie instantanee existente;
2. Analiza și comparare algoritmilor și sistemele de criptare a datelor existente;
3. Explorarea platformei blockchain Ethereum și contractele inteligente;
4. Dezvoltarea unui algoritm descentralizat de transmisie și stocare a datelor bazat pe platforma Ethereum;

**Metodele aplicate**: Metodele aplicate sunt standarde pentru crearea unui algoritm a Smart contractelor si anume: crearea unui identificator, semnarea cu o cheie privată, crearea unui lanț local de testare, transmiterea unei tranzacții.

**Rezultatele obținute:**

Această teză se prezintă studiul de dezvoltarea unui algoritm automatizat pentru transmiterea securizată a datelor între utilizatori într-o rețea folosind semnături criptografice cu cheie publică și privată.

Problema cheie a tezei este securitatea transmiterii datelor pe internet între utilizatori. O atenție deosebită este acordată sistemului de criptare criptografică RSA și unei platforme pentru crearea de servicii online descentralizate bazate pe blockchain - Ethereum. Codul este scris folosind limbajele de programare JavaScript și Solidity și platforma de programare Node.js. Teza poate fi împărțită în următoarele părți logice: criptare, tipuri de criptare și blockchain.

Această teză descrie în detaliu criptarea. În primul rând, vom studia rolul său în criptografie și securitate pe internet. Examinăm tipurile de criptare, cum ar fi criptarea simetrică și asimetrică. O parte separată a tezei detaliază modul în care funcționează tehnologia blockchain Ethereum, de ce a fost aleasă și cum funcționează contractul inteligent. Câteva messenger concurente - WhatsApp, Telegram, Viber - care folosesc criptarea end-to-end au fost comparate cu soluția finală.

Metodologia utilizată confirmă faptul că utilizarea stocării publice (descentralizate) a datelor este sigură, deoarece este practic imposibil de compromis cheia privată a Ethereum.

## SUMMARY

**Author: Andrei Leancă**, gr. SISRC-211M

**Topic:** "Elaboration of crypto-resistant data transfer algorithm in Ethereum Blockchain network for Smart Contracts"

**Structure of the thesis:** The thesis consists of a explanatory note of 48 pages, including a 1 page introduction, 3 tables, 19 figures, a list of 20 sources, including 5 foreign language sources.

**Key words:** Smart contract, encryption, blockchain, ethereum.

**Research area:** The key issue of the presented thesis is the security of data transmission over the Internet between multiple users.

**Thesis purpose:** Development of crypto-resilient data transfer algorithm in the Ethereum Blockchain of Smart Contracts.

**Objectives:**

1. Compare existing instant messaging systems;
2. Analysis and comparison of existing data encryption algorithms and systems;
3. Exploring the Ethereum blockchain platform and smart contracts;
4. Development of a decentralised data transmission and storage algorithm based on the Ethereum platform;

**Applied methods**: The implemented methods are standards for creating a Smart Contract algorithm to be more specific: creation of an identified, signing up with a private key, creation of a local test chain, transmission of a transaction.

**The obtained results:**

This thesis presents the study of the development of an automated algorithm for the secure transmission of data between users in a network, using cryptographic signatures with public and private key

The main issues of the presented thesis is the security of data transmission over the internet between users. Particular attention is paid to the RSA cryptographic encryption system and to a platform for creating decentralized online services based on the blockchain - Ethereum. The code is written using the following programming languages: JavaScript and Solidity, and also the programming platform Node.js. The thesis can be structured in the following logical divisions: encryption, types of encryption and blockchain.

This thesis describes encryptions in detail. Firstly, we study the role of encryption in cryptography and internet security. We examine the types of encryption, such as symmetrical and asymmetrical encryption. Secondly, a section of the thesis details the way in which the Ethereum blockchain technology works, why it was the chosen technology and how the Smart Contract works. Several competing messengers - Whatsapp, Telegram, Viber- which use end-to-end encryption are compared with the ultimate solution.

The methodology used confirms the fact that the use of public (decentralized) data storage is secure, due to the fact that it is virtually impossible to compromise Ethereum's private key.

**CUPRINS**

# INTRODUCERE

Lucrarea va avea în vedere rezolvarea problemelor de transmitere securizată a datelor între utilizatorii din rețea folosind o semnătură criptografică cu chei publice și private.

Relevanța acestei lucrări se datorează faptului că există o tendință de creștere a numărului de atacuri și de hacking a corespondenței secrete. Metodele și tehnologiile atacurilor la rețele de la distanță sunt îmbunătățite în mod regulat, iar algoritmii și sistemele de criptare existente nu protejează întotdeauna pe deplin informațiile confidențiale. Dar dezvoltarea tehnologiilor blockchain, care au o putere criptografică ridicată, nu stă, de asemenea, pe loc. Aceste circumstanțe fac ca dezvoltarea și implementarea unui sistem securizat de transmisie a datelor folosind o semnătură criptografică cu chei publice și private să fie foarte relevantă.

**Scopul** lucrării este elaborarea algoritmului criptorezistent de transfer a datelor in rețeaua Blockchain Ethereum pentru Smart Contracte.

În acest caz, este necesar să se rezolve următoarele **obiective**:

1. Compara sistemele de mesagerie instantanee existente;
2. Analiza și comparare algoritmilor și sistemele de criptare a datelor existente;
3. Explorarea platformei blockchain Ethereum și contractele inteligente;
4. Dezvoltarea unui sistem descentralizat de transmisie și stocare a datelor bazat pe platforma Ethereum.

# CONCLUZII

În timpul elaborării acestei lucrări au fost puși la discutați diverși algoritmi de criptare și aspectele teoretice ale acestora. O atenție deosebită a fost acordată criptosistemului RSA, bazelor sale matematice și a fost demonstrat un mic exemplu. Acest algoritm a fost ales pentru a implementa un sistem de transmitere securizată a datelor între utilizatori într-o rețea. În urma muncii depuse, se pot trage următoarele concluzii:

1. RSA este unul dintre cei mai puternici algoritmi de criptare cu cheie publică și privată și de semnătură electronică. Criptosistemul este utilizat în cele mai populare produse și protocoale de securitate sporită utilizate în prezent și poate fi considerat ca fiind unul dintre fundamentele comunicării securizate pe Internet.

2. De asemenea, a fost studiată platforma Ethereum pentru crearea de aplicații decentralizate, contractele sale inteligente și modul în care acestea funcționează. Această tehnologie blockchain este cât se poate de sigură pentru stocarea datelor, deoarece ar fi nevoie de secole pentru a sparge cheia secretă Ethereum. Datorită acestui fapt, un mesager bazat pe această tehnologie va elimina necesitatea de a implementa două tipuri de camere de chat - secret și cloud. În plus, este garantată neinterferența terților și a intrușilor în conversațiile secrete. Utilizatorii pot accesa în timp real, de pe orice dispozitiv, fișierele și mesajele trimise și primite anterior. Această funcție este extrem de utilă în cazul pierderii sau schimbării smartphone-ului sau în cazul utilizării aceluiași cont pe dispozitive diferite.

3. În urma explorarii platformei Blcokchain Ethereun sa studiat modul de creare a Smart contractrelor pe platforma data, a fost stabilit ca orice bloc are nevoie de o confiramare a unicității si care sunt in blockchain POW (Prowe of work) și in Ethereum POS (Prowe of stake) in urma constarilor data s-a constatat că stocarea blockchain este neprofitabilă din cauza costului destul de ridicat al tranzacțiilor, dar cât se poate de fiabilă și sigură.

4. În urma efetcuiuiarii lucrării date sau stabili pașii pentru crearea unui algoritm deccentralizat de transfer si storcare a dateleor bazat pe platforma Etherreum și anume Smart Contract pașii sunt : Elaborarea Cheilor ( crearea unui identificator care este compus din cheia privată, cheia publica si adresa, efectutarea unei tranzacții, cirptarea infromației cu o semnatură creată cu cheia privata, crearea unui lant (blockchain) trimiterea unuei tranzacții) , Semnarea și verificarea datelor cu Solidity (compilarea la nivel de bytecode, trimiterea unuei tranzactii pentru a crea o instanată nou), criptarea și semnarea mesajelor.

**BIBLIOGRAFIE**


1. Интуит – Institutul national deschis. [Curs online].- Calea de accesare: https://www.intuit.ru/studies/courses/691/547/lecture/12377

2. Ишмухаметов, Ш.Т. Математические основы защиты информации: учеб. пособие / Ш.Т. Ишмухаметов, Р.Г. Рубцов — Казань: Казанский федер. Ун- т, 2012. — 138 с

3. Как устроен AES [Curs online]// Хабрахабр – Calea de accesare URL: https://habr.com/post/112733/

4. Bazele criptării (PARTE 1) - ALGORITMUL DIFI-CELLMAN [Curs online] / Securitylab - 25.01.2016 - Calea de accesare URL: https://www.securitylab.ru/analytics/478912.php

5. Scriem Smart contract pe solidity. [Curs online] / Хабрахабр – 07.10.2016 - Calea de accesare URL: https://habr.com/post/312008/

6. De ce in mesageria Telegram nu este pornita End-to-end cripatrea instant [Curs online]// Medium - Calea de accesare URL: https://medium.com/@tglive/telegram-end-to-end-e93554cb9e46

7. Exemplu algorimului de criptare RSA [Curs online] // Infoprotect.net - Calea de accesare URL: http://infoprotect.net/varia/algoritm_shifrovaniya_rsa_primer

8. Романьков, В.А. Введение в криптографию. Курс лекций / В.А. Романьков. — М.: ФОРУМ, 2012. — 240 с.

9. Îndrumar pentru limbajul Solidity [Curs online] / James Ray // GitHub - Calea de accesare URL: https://github.com/ethereum/wiki/wiki/%D0%A0%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE-%D0%BF%D0%BE-Solidity

10. Салий, В.Н. Криптографические методы и средства защиты информации: учеб. пособие / В.Н. Салий; Саратов: Саратовский гос. ун-т имени Н.Г. Чернышевского, 2012. — 41 с

11. Ященко, В.В. Введение в криптографию. / В.В. Ященко — 4-е изд., [доп.]. — М.: МЦНМО, 2012. — 348 с.

12. Asymmetric cryptography (public key cryptographt). [Curs online] /Margaret Rouse // SearchSecurity – 05.06.2015 - Calea de accesare: https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

13. Ethereum Yellow Paper [Curs online] / ethereum.github.io // Dr. Gavin Wood – 28.05.2018 - Calea de accesare URL: https://ethereum.github.io/yellowpaper/paper.pdf

14. Everything you wanted to know about the next generation of public key crypto.[ Resursa online] / Nick Sullivan // Ars Technica – 25.10.2013 – Calea de accesare: https://arstechnica.com/information-technology/2013/10/a- relatively-easy-to-understand-primer-

on-elliptic-curve-cryptography/2/

15. RSA algorithm (Rivest-Shamir-Adleman). [Resursa online] /Margaret Rouse // SearchSecurity – 15.05.2014 - Calea de accesare URL: https://searchsecurity.techtarget.com/definition/RSA

16. Spy-funded privacy tools (like Signal and Tor) are not going to protect us from President Trump [Resursa online] // Yasha Levine / Surveillance Valley 09.12.2016 - Calea de accesare URL: https://surveillancevalley.com/blog/government-backed-privacy-tools-are-not-going-to-protect-us-from-president-trump

17. Technology Box — pagina predestinata intrebarilor legata de securitatea informațională [Curs online]. – Calea de accesare: http://teh-box.ru/informationsecurity/algoritm-shifrovaniya-rsa-na-palcax.html

18. Ţurcanu Dinu, Spinu Natalia, Popovici Serghei, Țurcanu Tatiana. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences Vol. IV, no. 1 (2021), pp. 74 – 83. Calea de accesare URL: https://jss.utm.md/wp-content/uploads/sites/21/2021/03/JSS-1-2021_74-83.pdf

19. What is Ethereum? [Curs online] / Alyssa Hertig // CoinDesk – Calea de accesare URL: https://www.coindesk.com/information/what-is-ethereum/

20. What is symmetric encryption.[ Curs online] / David Bisson // Venafi Blog – 09.11.2017 – Calea de accesare: https://www.venafi.com/blog/what- symmetric-encryption

21. White Paper [Curs online] / GitHub - Calea de accesare URL: https://github.com/ethereum/wiki/wiki/White-Paper

22. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. Chișinău, Publisher ,,Tehnica-UTM", 2022. - Calea de accesare URL: http://www.repository.utm.md/bitstream/handle/5014/20549/Computer-networks-Practical-examples-DS.pdf?sequence=1&isAllowed=y

23. Hashcash Curs online] / Calea de accesrre Wikipedia https://en.wikipedia.org/wiki/Hashcash#:~:text=Hashcash%20is%20a%20proof%2Dof,part%20of%20the%20mining%20algorithm

24. ASIC [Curs online] / Calea de accesare URL: https://www.investopedia.com/terms/a/asic.asp

25. Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities / Calea de accesare URL: https://www.sciencedirect.com/science/article/abs/pii/S2214212620307808?via%3Dihub

26. Proof of stake / Calea de accesare URL: https://en.wikipedia.org/wiki/Proof_of_stake

Proof of stake FAQ / Calea de accesare URL: https://vitalik.ca/general/2017/12/31/pos_faq.html