



**Universitatea Tehnică a Moldovei**

**PLATFORMĂ DE VERIFICARE A  
TRANZACȚIILOR EFECTUATE ÎN  
CRIPTOVALUTĂ**

**Masterand:  
Guragata Sorin**

**Conducător:  
prof. univ., dr. hab. Guțuleac Emilian**

**Chișinău – 2017**

## **ADNOTAREA**

Teza este o cercetare a bazelor teoretice a criptografiei și aspectelor practice a tehnologiilor utilizate în sistemul de criptomonede care folosește algoritmul semnăturii digitale folosind curbe eliptice (ECDSA - Elliptic Curve Digital Signature Algorithm). S-a cercetat minuțios articolul fondatorului acestei sisteme Satoshi Nakamoto, unde s-a expus principiul de funcționare, elementele constituente și regulile de funcționare. Cu ajutorul clientului Bitcoin Core s-au efectuat teste experimentale în vederea specificului funcționării diferitelor elemente a sistemului peer-to-peer de verificare și validare a tranzacțiilor.

Practic a fost asamblat un calculator cu video card (AMD RX470 8Gb). S-a instalat clientul de minerit pe diferite criptomonede pentru testarea procesului de tranzacționare la nivelul verificării funcției hash cu primirea de sistem a recompensei în moneda respectivă și transferul prin intermediul Crypto Currency exchange <https://changelly.com/> în Bitcoin cu achiziționarea în portofelul privat .

## **ANNOTATION**

The thesis is a research theoretical basis and practical aspects of cryptography technologies used in crypto-currency system using digital signature algorithm with elliptic curves (ECDSA - Elliptic Curve Digital Signature Algorithm). It has been meticulously researched article founder Satoshi Nakamoto and this described system, where he exhibited operating principle, the constituent elements and rules of transactions and operations of encrypting decrypting. We use Bitcoin Core client from experimental tests performed to different elements of the system operation aspects of peer-to-peer verification of transactions.

It assembled a computer with video card (AMD RX470 8Gb). Installed client from mining crypto currency from test different trading process at the hash verification system for receiving a reward in that crypto currency and transfer via Crypto Currency Exchange [https://changelly.com](https://changelly.com/) in Bitcoin wallet to verify.

# CUPRINS

<b>INTRODUCERE .....</b>	<b>6</b>
<b>1. SISTEME FINANCIARE CENTRALIZATE ȘI DECENTRALIZATE.....</b>	<b>7</b>
1.1 Valuta, banii și monede.....	7
1.2 Sisteme financiare centralizate .....	10
1.3 Sisteme financiare decentralizate .....	12
<b>2. CRIPTOGRAFIA ȘI CRIPTOVALUTA .....</b>	<b>15</b>
2.1 Criptografia momente istorice .....	15
2.2 Algoritmi de criptare RSA, funcția hash, semnătura digitală, algoritmul semnăturii digitale folosind curbe eliptice .....	16
2.3 Aspectele practice de utilizare algoritmilor cu chei publice .....	25
<b>3 SISTEMUL DE VERIFICAREA TRANZACȚIILOR ÎN CRIPTOVALUTĂ.....</b>	<b>27</b>
3.1 Cripto-valuta principiul proiectării sistemice .....	27
3.2 Cripto-valută - elementul Portofele (Wallet).....	30
3.3 Crito-valuta – lanțurile tranzacțiilor Blockchain.....	32
<b>CONCLUZII GENERALE ȘI RECOMANDĂRI .....</b>	<b>38</b>
<b>BIBLIOGRAFE.....</b>	<b>39</b>