Universitatea Tehnică a Moldovei

PLATFORMĂ DE VERIFICARE A TRANZACȚIILOR EFECTUATE ÎN CRIPTOVALUTĂ

Masterand:

Guragata Sorin

Conducător:

prof. univ., dr. hab. Guţuleac Emilian

Chişinău – 2017

ADNOTAREA

Teza este o cercetare a bazelor teoretice a criptografiei și aspectelor practice a tehnologiilor utilizate în sistemul de criptovalută 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 principiu de funcționare, elementele constituente și regulile de funcționare. Cu ajutorul clientului Bitcoin Core s-au efectuat teste experimentale în vederea specificului funcționării diferitor elemente a sistemei peer-to-peer de verificare și validare a tranzacțiilor.

Practic a fost asamblat un calculator cu video cartelă (AMD RX470 8Gb). S-a instalat clientul de minerit pe diferite criptovalute pentru testarea procesului de tranzacționare la nivelul verificării funcției hash cu primirea de sistem a recompensei în criptovaluta 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 in Bitcoin wallet to verify.

CUPRINS