Criptografia din spatele comerțului electronic

Mazilu George-Viorel, grupa B3

Abstract

Datorită dezvoltării tot mai rapide a *Internetului* şi a dispozitivelor electronice mobile, cumpărăturile la distanţă devin preferinţa tot mai multor persoane. Comoditatea de a răsfoi magazinele de la distanţă a atras populaţia să aleagă **comerţul electronic**. Prin **comerţ electronic** se înţelege "activitatea de cumpărare sau vânzare prin intermediul transmiterii de date la distanţă, activitate specifică politicii expansive a marketingului companiilor comerciale" [wikipedia]. În plus, conform site-ului web "quora", doar 8.3% din banii existenţi sunt tipăriţi pe hârtie sau monezi, aproximativ $4,3 \cdot 10^{18}$ (triliarde) de dolari americani comparativ cu $51.5 \cdot 10^{18}$ dolari înregistraţi.

Cu toate acestea, puţini cunosc faptul că întregul comerţ electronic nu ar fi fost posibil fără numeroase principii matematice folosite în criptografia din spatele întregii activităţi. Atât siguranţa informaţiilor transmise de către vânzători cât şi a banilor tranzacţionaţi este asigurată de către algoritmi bine puşi la punct de către criptografi începând cu anul 1990. Primitivele criptografice precum semnăturile digitale, funcţiile hash şi tehnicile de securizare a canalelor de comunicare permit realizarea comerţului electronic în condiţii de maximă corectitudine. Deşi era considerat că plata în "bani gheaţă" este singurul mod prin care clientul îşi poate păstra anonimitatea cumpărăturilor,

au apărut protocoale electronice variate prin care se pot face tranzacţii fără ca identitatea cumpărătorului să poată fi asociată produsului. Cea mai revoluţionară metodă de comerţ electronic este tranzacţionarea criptomonedelor de tipul *Bitcoin*.

În începutul lucrării de faţă sunt amintite câteva din principalele primitive criptografice folosite de la apariţia conceptului de comerţ electronic până în prezent. În continuare, sunt descrise schemele "MicroMint" şi "Payword" care permit realizarea plăţilor de valori mici; după care sunt prezentate două scheme cu securitate suficient de ridicată pentru realizarea macroplăţilor: una care oferă anonimitate la alegere şi una care previne şantajul. În plus, se regăseşte o scurtă descriere a evoluţiei criptomonedelor "Bitcoin". În final, este descrisă sumar tehnologia *"JavaCard"* distribuită de compania Oracle şi implementarea unui protocol folosind această tehnologie.