CZU 336.744

CRIPTOMONEDELE: EVOLUȚIE, PROVOCĂRI ȘI OPORTUNITĂȚI

Artiom BURLACA, *student, Facultatea de Științe Reale, Economice și ale Mediului, Universitatea de Stat „Alecu Russo" din Bălți*
Conducător științific: **Natalia BRANAȘCO,** *dr., conf. univ.*

Abstract: *This article describes the history of cryptocurrencies from their appearance in 2008 until now. It succinctly describes blockchain from a technical point of view and presents the fundamental problems of decentralized encryption technology and their solutions. It also talks about the legal provisions for the use of cryptocurrencies in the markets of countries that have accepted cryptocurrencies as a means of payment and the use of cryptocurrencies in the Republic of Moldova.*

Keywords: *cryptocurrencies, bitcoin, blockchain, decentralization, hash, volatility.*

Criptomonedele sunt monede digitale care utilizează criptografia – o tehnică pentru codificarea datelor pentru ca cei care nu dețin parola să nu le poată citi. Datorită criptografiei, criptomonedele sunt pur și simplu imposibil de falsificat, deși siguranța lor depinde, de asemenea, de câțiva alți factori. Deși în multe țări înalt dezvoltate criptomonedele sunt deja utilizate ca formă de plată pe o scară largă, ele încă provoacă multe confuzii, neînțelegeri și critică la adresa lor. Totuși, criptomonedele au o importanță destul de mare în economia mondială, doar Bitcoinul având o capitalizare de piață 500,144,303,882 € la data de 28.03.2023.

Criptomonedele moderne sunt sisteme decentralizate ce se bazează pe tehnologia blockchain. Blockchain–ul este o structură de baze de date distribuită care a fost descrisă pentru prima data de un criptograf care se numea David Chaum în dizertația sa din 1982. În lumea cripto, blockchain-ul este ca un registru public pentru tranzacțiile criptate ce este întreținut și actualizat de mii de oameni din jurul lumii. Tranzacțiile sunt anonime, însă sunt disponibile din punct de vedere public.

Bitcoin nu este prima monedă digitală. Nu este prima implementare a tehnologiei de blockchain. Nu este prima utilizare a criptografiei cu cheie publică pentru a păstra datele sigure. Însă pentru că toate aceste elemente sunt asamblate într-un singur sistem, este prima criptomonedă modernă. Înainte de crearea Bitcoin, existau mai multe exemple de monede digitale online, dar niciuna nu a reușit să atragă prea mult interes pentru a se stabili pe piețele financiare. Două exemple de astfel de monede sunt B-Money și Bit Gold.[1]

Lansarea bitcoinului

Domeniul de internet bitcoin.org a fost înregistrat în august 2008. Acesta rămâne pagina de home pentru cryptomonad, cea mai utilizată din lume. Pe 31 octombrie din același an, o persoană sau o organizație cu numele Satoshi Nakamoto a publicat o lucrare științifică numită: „Bitcoin: Un Sistem De Numerar Electronic Peer-to-Peer". Această lucrare este cunoscută în lume ca fiind „cartea albă a lui Satoshi". Lucrarea a prezentat conceptul tehnologiei de blockchain securizat criptografic. Bitcoin a fost descris ca o resursă digitală open-source teoretică. „Open source" însemna că nimeni nu o deținea și că toți puteau participa la utilizarea și dezvoltarea sa.

La începutul lui 2009, software-ul Bitcoin devine pentru prima dată disponibil publicului. Satoshi Nakamoto a minat primii 50 de Bitcoini, astfel lansând practica de minare cripto. La acea vreme, doar o echipă mică de programatori și entuziaști au participat la dezvoltarea sa, iar dintre aceștia doar puțini au anticipat că va fi văzut într-o zi ca o tehnologie revoluționară.

În primul an de existență al Bitcoin, nu a fost realist să i se atribuie o valoare reală. Dezvoltatorul Gavin Andersen a cumpărat 10.000 de Bitcoini cu 50$ și a creat un website numit Bitcoin Faucet unde a donat la propriu Bitcoin ca să se distreze.

Cea mai faimoasă poveste din această perioadă îl amintește pe Laszlo Hanycz, un dezvoltator de software care a cumpărat două pizza cu 10.000 de Bitcoini. Aceasta reprezintă și prima tranzacție cu Bitcoin în lumea reală. La prețul său maxim Bitcoin, acele două pizza ar fi valorat mult peste 600 milioane de dolari. Însă Laszlo nu și-a regretat niciodată decizia. El consideră că acesta a fost un pas crucial în consolidarea creșterii ecosistemul cripto.

În decembrie 2010, Satoshi Nakamote a postat ultimul său mesaj public în popularul forum online numit bitcointalk. A scris despre unele detalii minore referitoare la ultima versiune a software-ului. După aceasta, a ținut legătura cu unii programatori prin email, însă nici o urmă de el dupa aprilie 2011.

Pe aripile succesului, Bitcoin a început să se contureze ideea monedelor digitale descentralizate. În consecință, au început să apară primele criptomonede alternative. Pentru că aceste monede au fost alternative la cryptomonad stabilită, Bitcoin, acestea erau cunoscute ca altcoin-uri. Cele mai multe altcoin-uri oferă îmbunătățiri sporite față de protocolul original Bitcoin prin funcții precum vite-

ză mai mare, anonimat amplificat, și așa mai departe. Litecoin a fost printre primele altcoin-uri, și de aceea este uneori caracterizat ca argintul pentru aurul Bitcoin. Acum există mii de criptomonede [1].

Modelul de funcționare a criptomonedelor

Termenul „criptomonedă" nu este luat din cuvântul „cripto ca fiind „ascuns", ci din „Criptografie", o tehnică matematică de criptare a datelor. Datele din blockchain sunt criptate și fiecare adresă are o singură cheie privată care o poate descifra. Cheile private nu sunt stocate în blockchain, ele sunt doar secvențe necesare pentru a obține acces la blockchain. Știrile despre „Bitcoin a fost piratat" sau „Bitcoin furat" sunt situații în care cheile private, stocate pe schimburi, au fost furate atunci când un schimb este piratat. Deci, de fapt, nu bitcoinul este furat, ci doar cheia privată, ceea ce îi permite hoțului să transfere, de exemplu, bitcoini din portofelul „piratat" în al său. Cheia privată ar putea fi stocată chiar și pe o bucată de hârtie, fără nicio prezență pe un dispozitiv sau pe Internet pentru a o face în siguranță. De fapt, criptomonedele sunt primele programe care nu pot fi piratate direct, așa că orice știre despre pericolul unei scurgeri sau lipsa de transparență pur și simplu nu sunt adevărate și au întotdeauna un al doilea fundal tehnic.

Cuvântul „criptomonedă" este o combinație a celor două cuvinte „cripto" din criptografie și „monedă" care înseamnă o sursă de valoare. Criptomonedele sunt blockchain-uri care au un număr stabilit de monede care ar putea fi tranzacționate între adrese, dar întotdeauna în interiorul lor – în interiorul blockchain-ului. Nicio valoare nu poate fi luată sau adăugată la un blockchain prin omiterea algoritmului principal. Așa-numitele „criptomonede" sunt de fapt programe care se bazează în mare parte pe blockchain și sunt coduri open source care ar putea fi rulate pe fiecare computer cu acces la Internet.

Definim o monedă electronică ca un lanț de semnături digitale. Fiecare proprietar transferă moneda la următorul semnând digital un hash al tranzacției anterioare și cheia publică a următorului proprietar și adăugându-le la sfârșitul cozii. Un beneficiar poate verifica semnăturile pentru a verifica lanțul de proprietate (figura. 1) [6, pp. 1-3].

Problema este, desigur, că beneficiarul nu poate verifica dacă unul dintre proprietari nu a cheltuit dublu moneda. O soluție comună este introducerea unei autorități centrale de încredere, sau a unei monetări, care verifică fiecare tranzacție pentru cheltuieli duble. După fiecare tranzacție, moneda trebuie returnată la monetărie pentru a emite o nouă monedă, iar numai monedele emise direct de la monetărie sunt de încredere să nu fie cheltuite dublu. Problema cu această soluție este că soarta întregului sistem monetar depinde de compania care conduce monetăria, fiecare tranzacție trebuind să treacă prin ele, la fel ca o bancă. Avem nevoie de o modalitate prin care beneficiarul să știe că proprietarii anteriori nu au semnat tranzacții anterioare. Pentru scopurile noastre, cea mai de-

vreme tranzacție este cea care contează, așa că nu ne pasă de încercările ulterioare de a cheltui dublu. Singura modalitate de a confirma absența unei tranzacții este să fii la curent cu toate tranzacțiile. În modelul bazat pe monetărie, monetăria era la curent cu toate tranzacțiile și a decis care a sosit primul. Pentru a realiza acest lucru, tranzacțiile trebuie anunțate public și avem nevoie de un sistem pentru ca participanții să convină asupra unui istoric unic al ordinii în care au fost primite. Beneficiarul are nevoie de dovada că, la momentul fiecărei tranzacții, majoritatea nodurilor au fost de acord că este primul primit [1].

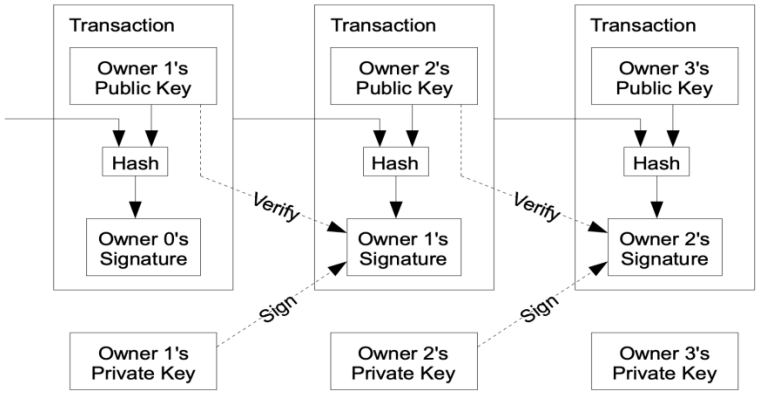

Figura 1. *Schema verificării lanțului de protecție a blockchain-ului*
Sursa: [6, p. 2]

Server de marcaj temporar

Soluția pe care este propusă începe cu un server de marcaj temporar. Un server de marcaj de timp funcționează prin preluarea unui hash dintr-un bloc de articole pentru a fi marcat temporar și publicarea pe scară largă a hash-ului, cum ar fi într-un ziar sau într-o postare use-net [3]. Marcajul temporal dovedește că datele trebuie să fi existat la momentul respectiv, evident, pentru a intra în hash. Fiecare marcaj temporal include marcajul de timp anterior în hash-ul său, formând un lanț, fiecare marca temporală suplimentară întărindu-i pe cele dinaintea sa (figura 2).

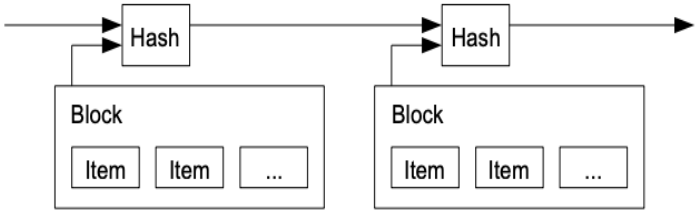

Figura 2. *Lanțul de întărire a block-ului*
Sursa: [6, p. 2]

Proof-of-Work

Pentru a implementa un server de marcaje temporare distribuite peer-to-peer, va trebui să fie folosit un sistem de proof-of-work similar cu Hashcash al lui Adam Back [6], mai degrabă decât postările din ziar sau Usenet. Dovada de lucru implică scanarea pentru o valoare care, atunci când este indexată, cum ar fi SHA-256, hash-ul începe cu un număr de zero biți. Munca medie necesară este exponențială în numărul de biți zero necesari și poate fi verificată prin executarea unui singur hash. Pentru rețeaua noastră de marcaj de timp, implementăm dovada de lucru prin incrementul unui nonce în bloc până când este găsită o valoare care oferă hash-ului blocului biții zero necesari. Odată ce efortul CPU a fost cheltuit pentru ca acesta să satisfacă dovezile de lucru, blocul nu poate fi schimbat fără a reface munca. Deoarece blocurile ulterioare sunt înlănțuite după el, munca de schimbare a blocului ar include refacerea tuturor blocurilor după el [6, p. 3-4].

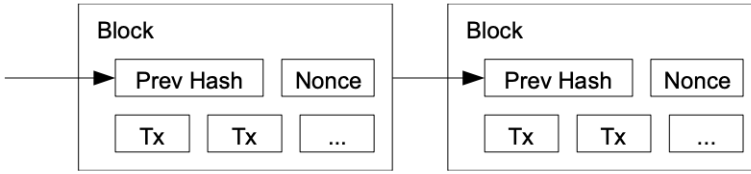

Figura 3. *Lanțul de întărire cu dovada lucrului efectuat a blockului*
Sursa: [6, p. 3]

Proba de lucru rezolvă și problema determinării reprezentării în luarea deciziilor majoritare. Dacă majoritatea s-ar baza pe o adresă-IP-un-vot, ar putea fi subminată de oricine poate să aloce mai multe IP-uri. Dovada muncii este, în esență, un CPU vot. Decizia majoritară este reprezentată de cel mai lung lanț, care are cel mai mare efort proof-of-work investit în el. Dacă majoritatea puterii procesorului este controlată de noduri oneste, lanțul cinstit va crește cel mai rapid și va depăși orice lanțuri concurente. Pentru a modifica un bloc trecut, un atacator ar trebui să refacă dovada de lucru a blocului și a tuturor blocurilor de după acesta și apoi să ajungă din urmă și să depășească munca nodurilor cinstite. Probabilitatea ca un atacator mai lent să ajungă din urmă scade exponențial pe măsură ce se adaugă blocurile ulterioare. Pentru a compensa creșterea vitezei hardware și interesul variabil pentru rularea nodurilor de-a lungul timpului, dificultatea dovezii de lucru este determinată de o medie mobilă care vizează un număr mediu de blocuri pe oră. Dacă sunt generate prea repede, dificultatea crește.

Reglementarea criptomonedelor

Criptomonedele sunt legale în majoritatea țărilor și sunt tratate ca bunuri normale. Taxele pot fi întotdeauna plătite pe baza istoricului tranzacțiilor, la schimbul de criptomonede, iar banii sub formă fizică ca USD sau EUR sunt retrași cu ușurință prin schimb în contul dumneavoastră bancar. În contextul utilizării tot mai frecvente a unor scheme de monedă virtuală (Bitcoin, Litecoin,

Ethereum, precum şi altele), atât pe piaţa internaţională, cât şi pe piaţa serviciilor de plată din Republica Moldova, Banca Naţională a Moldovei aduce unele precizări cu privire la riscurile asociate.

Moneda virtuală este o reprezentare digitală a valorii şi nu este emisă sau garantată de către o bancă centrală sau o autoritate publică. Nu este în mod obligatoriu ataşată unei monede naţionale, dar este utilizată de persoane fizice sau juridice ca alternativă a mijloacelor băneşti. Aceasta poate fi transferată, stocată sau tranzacţionată în mod electronic.

Utilizarea monedelor virtuale nu este reglementată în Republica Moldova. Acestea nu reprezintă o formă de monedă electronică în sensul Legii nr.114 din 18.05.2012 privind serviciile de plată şi moneda electronică, iar activitatea privind emiterea şi tranzacţionarea lor nu este supusă supravegherii de către organul abilitat. Din aceste considerente, utilizatorii monedelor virtuale sunt expuşi la o serie de riscuri, cum ar fi:

Riscuri asociate intereselor utilizatorilor:

Fraudarea operaţiunii de convertire, comisioane sau curs nefavorabile la efectuarea convertirii, spargerea portmoneelor, pierderea datelor personale, înghețarea sumei de către platforma de schimb la convertirea monedei virtuale în monedă simplă, pierderea sumei în cazul falimentării platformei de schimb, volatilitatea înaltă a cursului la care monedele virtuale ar putea fi schimbate etc.;

Nu este o garanţie că moneda virtuală va fi acceptată de comercianţi, suma poate fi debitată incorect, în unele cazuri utilizatorul nu poate converti moneda virtuală sau nu poate accesa portmoneul după pierderea cheii private etc.;

Riscuri pentru integritatea sistemului financiar:

Riscurile de spălare a banilor şi finanţare a terorismului; riscurile referitoare la crime financiare: utilizarea monedelor virtuale pentru vânzarea bunurilor interzise etc.

Banca Naţională a Moldovei atenţionează utilizatorii serviciilor de plată asupra faptului că monedele virtuale şi metodele de schimb aferente nu sunt supuse reglementării pe teritoriul Republica Moldova. Respectiv, fondurile utilizatorilor nu sunt protejate [8].

Volatilitatea criptomonedelor

Monedă cu volatilitate ridicată are o gamă de preţuri neregulate şi instabile, în timp ce o monedă mai puţin volatilă ar putea menţine o gamă de preţuri mai stabilă pe o perioadă de timp mult mai îndelungată (figura 4).

Volatilitatea criptomonedelor joacă un rol crucial în procesul decizional al investitorului. El foloseşte această caracteristică pentru a analiza riscurile şi pentru a determina câştigurile sau pierderile posibile care pot apărea la achiziţionarea unei monede.

Multe criptomonedelor existente sunt foarte volatile prin natura lor. Există mai multe motive pentru aceasta. Criptomonedelor sunt în mare parte neregle-

mentate, nu au nicio autoritate centrală și nu au niciun obstacol în calea intrării. Mai mult, piața criptomonedelor este încă relativ nouă și este în curs de dezvoltare zilnic.

Figura 4. *Graficul volatilității Bitcoin-ului*
Sursa: [7]

Rezumând cele spuse mai sus, concluzionăm că criptomonedele au avut un drum lung de la ideea de securizare a datelor până a una dintre cele mai sigure metode de transfer bănesc. Cu siguranță că tehnologia încă nu este perfectă și, în mâini greșite, poate aduce și daune considerabile cum ar fi fraude și spălare de bani. Este cunoscut faptul că criptomonedele sunt pe larg folosite în partea întunecată a internetului, cunoscută sub numele de „Darknet", pentru achitarea serviciilor și bunurilor de acolo, dar la fel ca multe alte inovații care au schimbat lumea în care trăim, trecerea la banii electronici va ridica la alt nivel relațiile economice.

Bibliografie:

1. *Prezentare Generală Preț Bitcoin*. [online] [citat 11.04.2023]. Disponibil: https://kriptomat.io/ro/criptomonede-pret/bitcoin-btc-valoare/
2. MASSIAS, H., AVILA, X.S., QUISQUATER, J.-J. *Design of a secure time-stamping service with minimal trust requirements.* In 20th Symposium on Information Theory in the Benelux, May 1999.
3. HABER, S., STORNETTA, W.S. *How to time-stamp a digital document*, In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
4. BAYER, D., HABER, S., STORNETTA, W.S. *Improving the efficiency and reliability of digital time-stamping*, In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
5. HABER, S., STORNETTA, W.S. *Secure names for bit-strings.* In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

6. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online] [citat 11.04.2023]. Disponibil: https://bitcoin.org/bitcoin.pdf
7. *TradingView* [online] citat 11.04.2023]. Disponibil: https://www.tradingview.com/chart/DGR92mZo/?symbol=CME%3ABTC1%21
8. *Moneda virtuală și riscuri asociate* [online] [citat 11.04.2023]. Disponibil: https://www.bnm.md/ro/content/moneda-virtuala-si-riscuri-asociate