

CUPRINS

INTRODUCERE	9
1. BITCOIN: O PRIVIRE DE ANSAMBLU.....	11
1.1 Concepte de bază și definiții	11
1.1.1 Ce înseamnă de fapt Bitcoin?	11
1.1.2 Scurtă comparație între rolul Bitcoin, al băncilor și al altor sisteme de transfer de bani.....	17
1.1.3 Elementele defnitorii ale Bitcoin.....	20
2. ISTORIA LANȚULUI DE DATE (BLOCKCHAIN): DE LA MIȘCAREA CYPHERPUNK LA JP MORGAN CHASE	35
2.1 Fundamentele filozofice și ideologice ale Bitcoin.....	35
2.1.1 Ideologia libertariană și precursorii Bitcoin	35
2.2 Începuturile și dezvoltarea Bitcoin.....	38
2.2.1 Apariția Bitcoin	38
2.2.2 Atacuri și scandaluri legate de Bitcoin.....	40
2.2.3 Bula speculativă a criptomonedelor	41
3. CUM FUNCȚIONEAZĂ BITCOIN ȘI CUM POATE FI OPTIMIZAT	44
3.1 Funcțiile hash criptografice.....	44
3.2 O bază de date imutabilă (care nu poate fi modificată fără a se vedea acest lucru).....	48
3.2.1 Descompunerea unui bloc de date.....	48
3.2.2 Arborii Merkle	49
3.2.3 Nonce, sau manifestarea fizică a dovezii muncii	52
3.3 Semnături, ECDSA și adrese.....	56
3.4 Scriptul Bitcoin	64
4. BITCOIN ÎN VIAȚA REALĂ: PORTOFELE DIGITALE, ACTIVITATEA DE MINERIT ȘI ALTELE.....	74
4.1 Tipuri de utilizatori.....	74
4.2 Portofele digitale.....	75
4.3 Mecanisme de funcționare a portofelelor digitale.....	79
4.4 Activitatea de minerit	82
4.4.1 Bazinele miniere – mining pools	90
4.5 Evoluția Bitcoin	94
4.6 Utilizarea tehnologiei blockchain de către companii	96
4.6.1 Blockchain cu permisiune (permissioned blockchain) versus blockchain fără permisiune (permissionless blockchain).....	97
4.6.2 Potențiale utilizări ale tehnologiei blockchain	100
4.7 Situația criptomonedelor în România.....	109

5. STRATEGII DE ATAC ÎN REȚEAUA BITCOIN.....	114
5.1 Strategii de atac referitoare la bazine miniere.....	114
5.2 Atacul cu dublarea cheltuielilor	119
5.3 Atacuri prin cenzurarea tranzacțiilor	122
5.4 Mineritul egoist	124
5.5 Posibilități de apărare împotriva atacurilor	125
6. ETHEREUM ȘI CONTRACTELE SALE INTELIGENTE	139
6.1 Ethereum.....	143
6.2 Mașina Virtuală Ethereum (EVM).....	146
6.3 Exemple de utilizare a Ethereum.....	149
6.3.1 Utilizări de bază	149
6.3.2 Utilizări avansate.....	151
6.3.3 Utilizări amuzante.....	159
6.4 Situația actuală a tehnologiei blockchain și proiecte de viitor.....	160
6.5 Considerații finale despre tehnologia blockchain	180
7. CRIPTOMONEDELE ȘI LUMEA REALĂ – POT FI CRIPTOMONEDELE CONSIDERATE BANI?	184
7.1. Limbajul „criptic” al criptomonedelor	184
7.1.2 Monede „moderne”: monede electronice, monede digitale, monede virtuale și criptomonede	184
7.2. Conceptul de monedă – de la moneda marfă la inovațiile monetare și financiare moderne	194
7.2.1 Ce sunt banii? Evoluția conceptului de bani.....	194
7.2.2 Procesul de creare a banilor.....	200
7.2.3 Rolul băncii centrale și politica monetară.....	205
7.2.4 Alternative la banii emiși de statul național.....	212
7.2.5 Dimensiunea socială și politică a banilor.....	225
8. IMPLICAȚII DE SECURITATE ALE CRIPTOMOEDELOR.....	237
8.1 Utilizarea criptomonedelor pentru spălarea banilor și activități de crimă organizată.....	237
8.1.1 Criptomonede private și serviciile de mixer de criptomonede.....	238
8.1.2 Utilizarea criptomonedelor ca mijloc de spălare a banilor – cazul atacului malware Carbanak și Cobalt.....	247
8.2 Utilizarea criptomonedelor pentru alte activități ilegale	249
8.3 Corelarea utilizării criptomonedelor ca mijloace de plată alternative pentru evitarea impozitării.....	256
8.4 Utilizarea criptomonedelor pentru finanțarea terorismului.....	258
8.5 Criptomonedele ca armă utilizată la nivel de state.....	270
8.5.1 Finanțarea activităților de spionaj și război informațional prin utilizarea criptomonedelor	270
8.5.2 Utilizarea criptomonedelor pentru promovarea ideologiei extremiste.....	273
8.5.3 Utilizarea criptomonedelor pentru evitarea sancțiunilor economice.....	278

8.5.4 Utilizarea criptomonedelor pentru finanțarea sau manipularea alegerilor	285
8.6 Implicațiile extragerii criptomonedelor asupra securității energetice	291
8.7 Implicațiile criptomonedelor asupra stabilității financiare și a politicii monetare	295
8.7.1 Impactul asupra infrastructurii piețelor financiare	297
8.7.2 Impactul asupra altor intermediari și piețe financiare.....	298
8.7.3 Implicații asupra politicii monetare.....	298
8.7.4 Criptomonede emise de companii private – Studiu de caz Libra	302
8.8 Cum ar trebui să se implice autoritățile statului pentru a reduce riscurile aferente utilizării criptomonedelor?	321
 9. CONCLUZII	 326
 GLOSAR.....	 330
 BIBLIOGRAFIE.....	 340

INTRODUCERE

Tehnologia Blockchain are potențialul de a exercita o influență puternică asupra lumii moderne, în domeniul financiar, al energiei, în ceea ce privește identitatea online și industria IT, pentru a da doar câteva exemple. Cu toate acestea, tehnologia blockchain și criptomonedele sunt încă relativ puțin înțelese de către mulți oameni, fiind înconjurată de multe prejudecăți, mistere și mituri nefondate. Una dintre primele utilizări ale tehnologiei blockchain a reprezentat-o cea mai cunoscută criptomonedă, anume Bitcoin-ul, cea mai veche și cea mai răspândită aplicație de tip blockchain.

Scopul acestei cărți este acela de a prezenta o imagine de ansamblu asupra fenomenului criptomonedelor, cu accent pe cea mai cunoscută dintre acestea, Bitcoin. Vom analiza fenomenul atât din punct de vedere al aspectelor tehnice, dar și din punctul de vedere al interacțiunii dintre criptomonede și „lumea reală”. Fenomenul criptomonedelor este complex și într-o permanentă evoluție, astfel încât această carte nu își propune să fie un manual al investitorului în criptomonede, sau un tratat definitiv și exhaustiv privind acest subiect. Având în vedere viteza cu care se modifică ecosistemul crypto, avansurile tehnologice și modificările modului în care diverse state și autorități de reglementare reacționează la acest fenomen, subiectul este unul dinamic și fluid, prin urmare scopul cărții este de a prezenta câteva concepte de bază privind criptomonedele și a modului în care acestea influențează mediul de securitate, în diverse aspecte ale acestuia. Vom utiliza pe parcursul cărții o serie de termeni în limba engleză, deoarece aceștia sunt deja utilizați în limbajul din ecosistemul crypto și traducerea lor este fie imposibilă (datorită noutății conceptului nu există termeni echivalenți în limba română) sau ar face cartea dificil de citit de către cei familiarizați deja cu denumirile în limba engleză.

În prima parte a cărții ne vom concentra asupra aspectelor tehnice ale criptomonedelor, cu accent asupra primei și celei mai cunoscute criptomonedă, Bitcoin. Vom începe prin a prezenta această criptomonedă originară, motivele și contextul apariției acesteia, iar în capitolele următoare vom discuta despre celelalte criptomonede apărute ulterior (numite altcoins) și despre ecosistemul pe care acestea îl formează (ecosistemul crypto), pentru a înțelege modul în care acestea funcționează din punct de vedere tehnic.

Partea a doua a cărții va analiza rolul și locul criptomonedelor în cadrul sistemului economic și financiar, prin urmare vom intra în detaliile conceptului

de bani în sensul clasic al teoriei economice, pentru a încerca să clarificăm dacă criptomonedele pot fi considerate bani în sensul economic sau nu. Criptomonedele sunt uneori prezentate, în mod idealist, ca un panaceu al tuturor problemelor economiei și sistemului financiar actual, astfel că vom urmări să înțelegem care sunt avantajele și dezavantajele acestora și modul în care ele interacționează cu economia reală.

Secțiunea finală a cărții se va concentra asupra implicațiilor pe care criptomonedele și tehnologia blockchain le pot avea asupra securității naționale, în multiplele sale aspecte – de la siguranța utilizării lor în viața reală, de către oamenii obișnuiți, la utilizarea lor pentru a finanța crima organizată, terorismul, sau ca instrument de „soft power” pentru actori statali.

1. BITCOIN: O PRIVIRE DE ANSAMBLU

1.1 Concepte de bază și definiții

1.1.1 Ce înseamnă de fapt Bitcoin?

În funcție de persona căreia îi adresăm această întrebare, vom primi răspunsuri extrem de diferite: o inovație tehnică deosebită, un instrument de investiție, viitorul banilor, o modalitate de evita controlul statului asupra persoanei etc.. Definițiile diferă, în funcție de domeniul de specializare al celui care răspunde, de nivelul de cunoștințe de matematică, IT și economie ale acestuia, dar și în funcție de context.

În primul rând, **bitcoin este o criptomonedă**, mai precis prima apărută în ordine cronologică și cea mai cunoscută în cadrul publicului larg. Ce este însă o criptomonedă? *O criptomonedă reprezintă o monedă digitală sau virtuală care utilizează principiile informatice, economice și criptografia pentru asigurarea securității informațiilor, ceea ce o face mai dificil de contrafăcut.* O caracteristică principală a criptomonedelor și unul dintre principalele motive pentru care acestea sunt atât de atractive, o reprezintă natura lor organică: nu sunt emise de nici o autoritate centrală (de un stat anume), ceea ce le face în teorie imune la controlul sau interferența din partea unor actori externi (vom vedea pe parcursul cărții că în realitate lucrurile nu stau chiar așa).

Înainte de bitcoin au existat și alte criptomonede, însă bitcoin a reprezentat prima criptomonedă de succes, datorită naturii sale distribuite și descentralizate. Apariția bitcoin și succesul acestuia au încurajat ulterior apariția a numeroase alte monede și token-uri, care intră în categoria mare a criptomonedelor, chiar dacă majoritatea nu pot fi încadrate în conceptul economic de „monedă”.

Rațiunea care a dus la apariția criptomonedelor a derivat din filozofia libertariană, îmbrățișată de primii entuziaști ai conceptului, care au urmărit crearea unui instrument de plată care să permită anonimatul și care să nu fie influențat de politicile financiare duse de un stat. Valoarea monedelor clasice (monede fiat) derivă din voința unor autorități de reglementare la nivel centralizat, de stat, exprimată prin intermediul instrumentelor politicii monetare.

Să privim puțin în trecut, pentru a înțelege motivele apariției filozofiei libertariene. La încheierea celui de-al doilea război mondial, Statele Unite ale

Americii împreună cu țări din Europa de vest, Japonia, Canada și Australia au convenit implementarea sistemului monetar „Bretton Woods”, ce presupunea ca monedele emise de statele participante să aibă o valoare intrinsecă, raportată la un etalon comun, anume cantitatea de aur pe care Băncile Centrale o dețineau în rezerve. Nu era permis ca țările participante să emită cantități mai mari de monedă. Ulterior, la data de 15 August 1971¹, din rațiuni protecționiste, Statele Unite ale Americii au renunțat la acest sistem, instaurând regimul monedelor de tip „fiat”, a căror valoare este stabilită de guvernele naționale și de cererea existentă la nivel global. Ca exemplu, valoarea dolarului american nu este dată doar de economia americană, ci și de faptul că prețul barilului de petrol este fixat în dolari americani, astfel că guvernele fiecărui stat trebuie să-și formeze rezerve din această monedă. Prin urmare, aceasta generează o cerere mai mare de dolari pe piețele internaționale și implicit o creștere a valorii dolarului.

În România, politica B.N.R. de a crește sau scădea dobânda de referință, acționând asupra puterii de cumpărare a leului și cursului de schimb leu-euro, este cea care influențează valoarea monedei naționale. Politica monetară a guvernului poate influența în mod dramatic economia, cum a fost cazul Venezuelei sau Zimbabwe, când Banca Centrală duce o politică iresponsabilă și tipărește bani în exces, generând inflație galopantă. De asemenea, speculațiile asupra diverselor monede la bursă sau evenimente politice gen Brexit pot influența, uneori dramatic, valoarea unei monede naționale.

Acești factori, în combinație cu restricțiile și controalele din partea statelor în ceea ce privește modul de tranzacționare a monedelor clasice au generat pentru cetățenii obișnuiți un sentiment de nesiguranță referitoare la situația materială, care putea să se diminueze brusc ca urmare a unor influențe externe, pe care aceștia nu le puteau controla. De asemenea, mulți dintre entuziaștii tehnologiei IT nu priveau cu ochi buni faptul că autoritățile statului puteau avea controlul asupra informațiilor lor personale, privind sumele pe care le transferau prin intermediul sistemului bancar, a activității lor de investiții etc. Prin urmare, în lumea de nișă a pasionaților de IT a apărut ideea creării unui instrument de plată flexibil, care să nu fie supus controlului statelor în ceea ce privește emiterea, tranzacționarea și stabilirea valorii acestuia. Acest nou instrument de plată trebuia să fie democratic și flexibil, valoarea aceasta urmând a fi stabilită exclusiv pe bază de cerere și ofertă. Astfel a apărut conceptul de criptomonedă.

Din punct de vedere economic, criptomonedele nu îndeplinesc toate caracteristicile pentru a fi considerate monede (cum ar fi acceptarea generală în schimbul de bunuri și servicii), însă denumire este acceptată ca atare, prin urmare o vom folosi în continuare. Astfel, ele se situează într-o categorie aparte

¹ M. Bordo, *The operation and demise of the Bretton Woods system: 1958 to 1971*, VOX EU, 2017 <https://voxeu.org/article/operation-and-demise-bretton-woods-system>, accesat la 24.01.2017

din punct de vedere economic și generează controverse între promotorii lor, care le vad ca înlocuitori ai monedelor naționale și oponenții care văd în ele varianta modernă a bulei speculative a bulbilor de lalea din Olanda secolului 17.

Datorită noutății domeniului, conceptul de criptomonedă este fluid, fiind utilizat pentru a desemna concepte înrudite dar distincte. În acest context, este util să facem o scurtă paranteză pentru a clarifica diferența de terminologie. Astfel, termenul în limba engleză de **criptocurrency** a fost tradus ca și **criptomonedă** (termen pe care îl vom utiliza în cartea de față), dar și sub denumirea de **criptovalută**. Dacă pentru publicul larg termenul de criptomonedă (cryptocurrency) este mai des utilizat, în limbajul utilizat în ecosistemul crypto apare o diferențiere între termenii de **criptomonedă (cripto-coins)** și **tokenuri (tokens)**.

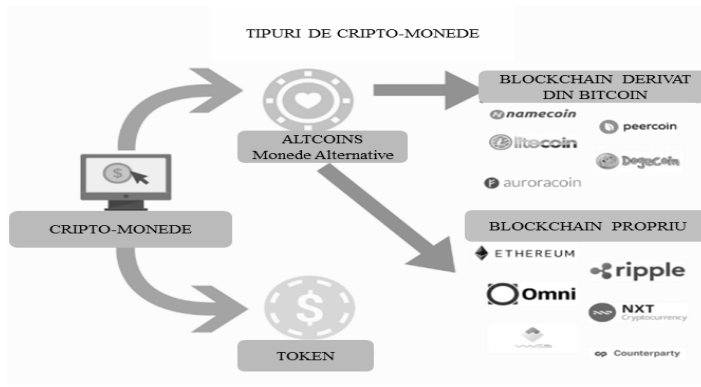


Figura 1 Tipuri de criptomonedă

Astfel, în categoria de **cripto-coins** găsim **bitcoin și altcoin** (alternative coin, adică monede alternative la bitcoin, care folosesc tot tehnologia blockchain). O parte din monedele alternative au fost construite pe baza unui cod sursă derivat din cel al Bitcoin, având caracteristici specifice. În cazul acestora, codul aflat la baza protocolului inițial al Bitcoin (care este open source) a fost modificat, rezultând o criptomonedă diferită (ex. Namecoin, Peercoin, Dogecoin, Litecoin etc). Alte criptomonedă s-au dezvoltat pe baza unei *tehnologii blockchain specifice, cu protocoale specifice și cod sursă diferit de cel al bitcoin*. Printre cele mai cunoscute sunt ethereum, despre care vom discuta într-un capitol ulterior, Ripple, Omni, next, Cardano etc.

Token-ul (cunoscut și sub denumirea de **utility token**) reprezintă o unitate digitală care se bazează pe un anumit activ, serviciu sau produs și care nu are propriul blockchain. Un token poate reprezenta practic orice activ care este fungibil și care poate fi tranzacționat, de la mărfuri de tot felul, la minereuri, la puncte de loialitate și chiar alte criptomonedă.

Putem compara un token cu jetoanele utilizate pentru a cumpăra cafea de la un automat. Întâi trebuie să achiziționezi jetonul cu o anumită sumă de

bani, apoi acesta poate fi utilizat pentru a avea acces la paharul cu cafea. În mod similar, token-urile dau acces la serviciile oferite de o platformă.

Un token se creează mult mai ușor decât o criptomonedă, pentru că nu este nevoie de modificarea codurilor unui anumit protocol existent sau de crearea de la zero a unui nou blockchain. Nu este necesar decât să se utilizeze un șablon deja existent pe un blockchain (cum ar fi platformele Ethereum sau Waves), care permit crearea de token. Funcționalitatea creării de token este posibilă datorită așa numitelor contracte inteligente (smart contracts), care reprezintă coduri de program auto-executabile și care nu au nevoie de o terță parte pentru a putea funcționa.

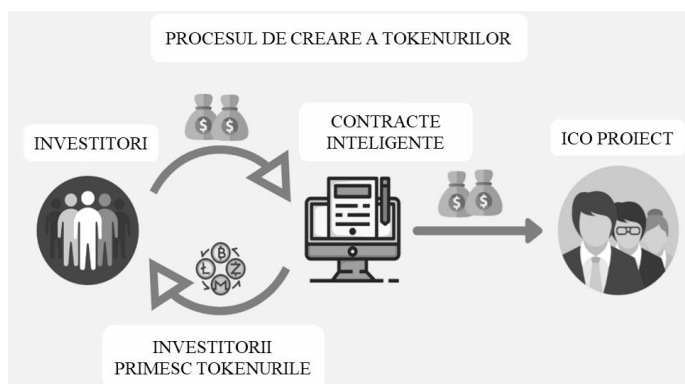


Figura 2 Procesul de creare a tokenurilor

Token-urile sunt create și distribuite publicului printr-un proces numit Ofertă Inițială de Monedă - Initial Coin Offering (ICO), care este practic o formă de crowd-funding (adunare de fonduri pentru un anumit proiect) în spațiul criptomonedelor. Dacă în lumea reală o companie care are nevoie de capital poate atrage investitori printr-o Ofertă Publică Inițială – Initial Public Offering (IPO) de acțiuni, în domeniul virtual se folosește ICO. Conceptul va fi descris în detaliu într-un capitol următor.

Pe scurt, principala *diferență dintre altcoin și token* este dată de structura lor: *altcoin sunt monede separate, care funcționează pe baza unui blockchain propriu, separat, pe când token-urile funcționează pe baza unui blockchain care facilitează crearea unor aplicații descentralizate.* Majoritatea criptomonedelor existente sunt tokenuri, datorită ușurinței cu care pot fi create.

Pentru a răspunde la întrebarea care apare în titlul acestui subcapitol, ***ce înseamnă de fapt bitcoin***, să clarificăm pentru început o diferență de semantică. Probabil cititorul a observat că până acum am utilizat termenul de bitcoin scris cu majuscule și minuscule. Nu este o greșeală de editare, deoarece „***bitcoin***” (***scris cu inițială minusculă***) este în general folosit de publicul larg și de mass media cu ***înțelesul de unitate monetară***. A poseda trei bitcoin înseamnă ca cineva este posesorul a trei unități monetare ce poartă denumirea

de bitcoin, așa cum altcineva poate spune ca are o sumă de bani exprimată în alte monede (naționale, de această dată) cunoscute sub numele de dolarul american, euro, lira turcească, yenul sau bolivarul.

Bitcoin (scris cu inițială majusculă) se referă la protocolul care guvernează această monedă, cu alte cuvinte la ansamblul de concepte tehnice, reguli și convenții care susțin generarea și funcționarea criptomonedei, cât și relațiile dintre utilizatori.

În al treilea rând, bitcoin, sau mai precis spus necesitatea dezvoltării unei alternative la monedele fiat care a generat criptomoneda, reprezintă **inspirația pentru tehnologia blockchain**, structura de date care stă la baza acestei cripto-monedede. O structură de date este un format virtual pentru organizarea, preluarea și stocarea informațiilor. Tehnologia blockchain specifică Bitcoin înregistrează pentru totdeauna istoricul tuturor tranzacțiilor care au avut loc vreodată în trecut și care au implicat Bitcoin. Asemenea unui registru contabil în care se pot doar introduce informații, fără să se poată modifica sau șterge informațiile din trecut, Bitcoin utilizează un registru în care se pot doar adăuga informații.

Nu în ultimul rând, **Bitcoin reprezintă o revoluție culturală**, materializarea dorinței de protejare a intimității identității și tranzacțiilor în sfera digitală și o mișcare spre descentralizare, de evitare a controlului unui stat sau al unei autorități centrale, percepute de inițiatorii mișcării ca fiind abuzive. În calitate de criptomonedă, Bitcoin-ul nu este susținut de nici un stat sau autoritate centrală, ideea din spatele conceptului fiind ca acesta să fie construit de către utilizatori, pentru utilizatori.

Bitcoin își găsește rădăcinile în **Mișcarea Cypherpunk**², apărută la sfârșitul anilor 80, care susținea necesitatea protecției vieții private prin criptografie. Membrii acestei mișcări (care continuă să fie activă și în prezent) nu au încredere că autoritățile statului sau marile corporații ar respecta intimitatea personală a oamenilor care le furnizează datele personale.

În 1992, Eric Hughes (matematician și programator), Timothy C. May (inginer electronist și cercetător științific principal la compania Intel, în primii ani de existență ai acesteia, autor de lucrări în domeniul politic și tehnic) și John Gilmore (programator și activist) au înființat un mic grup care se întâlnea săptămânal la compania celui din urmă, Cygnus Solutions, în San Francisco, denumit în mod ironic „cypherpunks” – termen combinat dintre cuvântul „cypher” (cifru) și cyberpunk (golan cibernetic)³.

Principalele idei ale mișcării pot fi regăsite în Manifestul Cypherpunk: „Confidențialitatea datelor este necesară unei societăți deschise în epoca cibernetică... Nu ne putem aștepta de la guverne, corporații sau alte organizații

² <https://www.activism.net/cypherpunk/>

³ R. Manne, *The Cypherpunk Revolutionary - Julian Assange. The Monthly March, 2011, No. 65*, <https://www.themonthly.com.au/issue/2011/february/1324596189/robert-manne/cypherpunk-revolutionary>, accesat la 05.07.2017