CUPRINS

INTRODUCERE

Tehnologia Blockchain are potenţialul de a exercita o influenţă puternică asupra lumii moderne, în domeniul financiar, al energiei, în ceea ce priveşte identitatea online şi industria IT, pentru a da doar câteva exemple. Cu toate acestea, tehnologia blockchain şi criptomonedele sunt încă relativ puţin înţelese de către mulţi oameni, fiind înconjurate de multe prejudecăţi, mister şi mituri nefondate. Una dintre primele utilizări ale tehnologiei blockchain a reprezentat-o cea mai cunoscută criptomonedă, anume Bitcoin-ul, cea mai veche şi cea mai răspândită aplicaţie de tip blockchain.

Scopul acestei cărţi 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 şi din punctul de vedere al interacţiunii dintre criptomonede şi „lumea reală". Fenomenul criptomonedelor este complex şi într-o permanentă evoluţie, astfel încât această carte nu îşi propune să fie un manual al investitorului în criptomonede, sau un tratat definitiv şi exhaustiv privind acest subiect. Având în vedere viteza cu care se modifică ecosistemul cripto, avansurile tehnologice şi modificările modului în care diverse state şi autorităţi de reglementare reacţionează la acest fenomen, subiectul este unul dinamic şi fluid, prin urmare scopul cărţii este de a prezenta câteva concepte de bază privind criptomonedele şi a modului în care acestea influenţează mediul de securitate, în diverse aspecte ale acestuia. Vom utiliza pe parcursul cărţii o serie de termeni în limba engleză, deoarece aceştia sunt deja utilizaţi în limbajul din ecosistemul cripto şi traducerea lor este fie imposibilă (datorită noutăţii conceptului nu există termeni echivalenţi în limba română) sau ar face cartea dificil de citit de către cei familiarizaţi deja cu denumirile în limba engleză.

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

Partea a doua a cărţii va analiza rolul şi locul criptomonedelor în cadrul sistemului economic şi 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 şi sistemului financiar actual, astfel că vom urmări să înţelegem care sunt avantajele şi dezavantajele acestora şi modul în care ele interacţionează cu economia reală.

Secţiunea finală a cărţii se va concentra asupra implicaţiilor pe care criptomonedele şi tehnologia blockchain le pot avea asupra securităţii naţionale, în multiplele sale aspecte – de la siguranţa utilizării lor în viaţa reală, de către oamenii obişnuiţi, la utilizarea lor pentru a finanţa crima organizată, terorismul, sau ca instrument de „soft power" pentru actori statali.

1. BITCOIN: O PRIVIRE DE ANSAMBLU

1.1 Concepte de bază şi definiţii

1.1.1 Ce înseamnă de fapt Bitcoin?

În funcţie de persona căreia îi adresăm această întrebare, vom primi răspunsuri extrem de diferite: o inovaţie tehnică deosebită, un instrument de investiţie, viitorul banilor, o modalitate de evita controlul statului asupra persoanei etc.. Definiţiile diferă, în funcţie de domeniul de specializare al celui care răspunde, de nivelul de cunoştinţe de matematică, IT şi economie ale acestuia, dar şi în funcţie de context.

În primul rând, ***bitcoin este o criptomonedă***, mai precis prima apărută în ordine cronologică şi 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 şi criptografia pentru asigurarea securităţii informaţiilor, ceea ce o face mai dificil de contrafăcut*. O caracteristică principală a criptomonedelor şi 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 interferenţa din partea unor actori externi (vom vedea pe parcursul cărţii că în realitate lucrurile nu stau chiar aşa).

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

Raţiunea care a dus la apariţia criptomonedelor a derivat din filozofia libertariană, îmbrăţişată de primii entuziaşti ai conceptului, care au urmărit crearea unui instrument de plată care să permită anonimatul şi care să nu fie influenţat de politicile financiare duse de un stat. Valoarea monedelor clasice (monede fiat) derivă din voinţa unor autorităţi de reglementare la nivel centralizat, de stat, exprimată prin intermediul instrumentelor politicii monetare.

Să privim puţin în trecut, pentru a înţelege motivele apariţiei filozofiei libertariene. La încheierea celui de-al doilea război mondial, Statele Unite ale

Americii împreună cu ţări din Europa de vest, Japonia, Canada şi 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 deţineau în rezerve. Nu era permis ca ţările participante să emită cantităţi mai mari de monedă. Ulterior, la data de 15 August 1971[1], din raţiuni protecţioniste, Statele Unite ale Americii au renunţat la acest sistem, instaurând regimul monedelor de tip „fiat", a căror valoare este stabilită de guvernele naţionale şi de cererea existentă la nivel global. Ca exemplu, valoarea dolarului american nu este dată doar de economia americană, ci şi de faptul că preţul barilului de petrol este fixat în dolari americani, astfel că guvernele fiecărui stat trebuie să-şi formeze rezerve din această monedă. Prin urmare, aceasta generează o cerere mai mare de dolari pe pieţele internaţionale şi implicit o creştere a valorii dolarului.

În România, politica B.N.R. de a creşte sau scădea dobânda de referinţă, acţionând asupra puterii de cumpărare a leului şi cursului de schimb leu-euro, este cea care influenţează valoarea monedei naţionale. Politica monetară a guvernului poate influenţa în mod dramatic economia, cum a fost cazul Venezuelei sau Zimbabwe, când Banca Centrală duce o politică iresponsabilă şi tipăreşte bani în exces, generând inflaţie galopantă. De asemenea, speculaţiile asupra diverselor monede la bursă sau evenimente politice gen Brexit pot influenţa, uneori dramatic, valoarea unei monede naţionale.

Aceşti factori, în combinaţie cu restricţiile şi controalele din partea statelor în ceea ce priveşte modul de tranzacţionare a monedelor clasice au generat pentru cetăţenii obişnuiţi un sentiment de nesiguranţă referitoare la situaţia materială, care putea să se diminueze brusc ca urmare a unor influenţe externe, pe care aceştia nu le puteau controla. De asemenea, mulţi dintre entuziaştii tehnologiei IT nu priveau cu ochi buni faptul că autorităţile statului puteau avea controlul asupra informaţiilor lor personale, privind sumele pe care le transferau prin intermediul sistemului bancar, a activităţii lor de investiţii etc. Prin urmare, în lumea de nişă a pasionaţilor de IT a apărut ideea creării unui instrument de plată flexibil, care sa nu fie supus controlului statelor în ceea ce priveşte emiterea, tranzacţionarea şi stabilirea valorii acestuia. Acest nou instrument de plată trebuia să fie democratic şi flexibil, valoarea aceasta urmând a fi stabilită exclusiv pe bază de cerere şi 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 şi 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 şi generează controverse între promotorii lor, care le vad ca înlocuitori ai monedelor naţionale şi oponenţii care văd în ele varianta modernă a bulei speculative a bulbilor de lalea din Olanda secolului 17.

Datorită noutăţii 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 diferenţa de terminologie. Astfel, termenul în limba engleză de ***criptocurrency*** a fost tradus ca şi ***criptomonedă*** (termen pe care îl vom utiliza în cartea de faţă), dar şi sub denumirea de ***criptovalută***. Dacă pentru publicul larg termenul de criptomonedă (cryptocurrency) este mai des utilizat, în limbajul utilizat în ecosistemul cripto apare o diferenţiere între termenii de ***criptomonedă (cripto-coins)*** şi ***tokenuri (tokens)***.

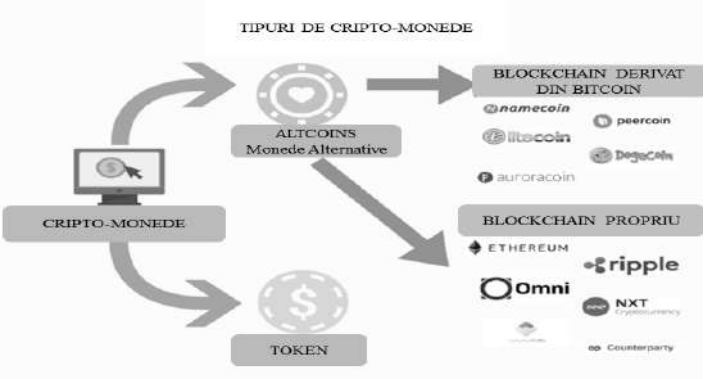

Figura 1 Tipuri de criptomonede

Astfel, în categoria de ***cripto-coins*** găsim ***bitcoin şi 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 iniţial al Bitcoin (care este open source) a fost modificat, rezultând o criptomonedă diferită (ex. Namecoin, Peercoin, Dogecoin, Litecoin etc). Alte criptomonede s-au dezvoltat pe baza unei *tehnologii blockchain specifice, cu protocoale specifice şi 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 şi sub denumirea de ***utility token***) reprezintă o unitate digitală care se bazează pe un anumit activ, serviciu sau produs şi care nu are propriul blockchain. Un token poate reprezenta practic orice activ care este fungibil şi care poate fi tranzacţionat, de la mărfuri de tot felul, la minereuri, la puncte de loialitate şi chiar alte criptomonede.

Putem compara un token cu jetoanele utilizate pentru a cumpăra cafea de la un automat. Întâi trebuie să achiziţionezi 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 uşor 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 şablon deja existent pe un blockchain (cum ar fi platformele Ethereum sau Waves), care permit crearea de token. Funcţionalitatea creării de token este posibilă datorită aşa numitelor contracte inteligente (smart contracts), care reprezintă coduri de program auto-executabile şi care nu au nevoie de o terţă parte pentru a putea funcţiona.

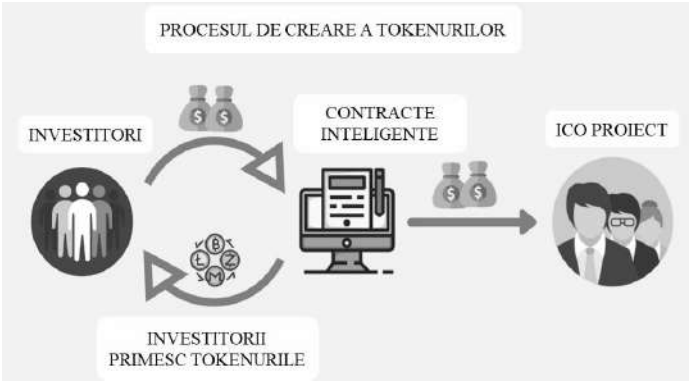

Figura 2 Procesul de creare a tokenurilor

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

Pe scurt, principala *diferenţă dintre altcoin şi token* este dată de structura lor: *altcoin sunt monede separate, care funcţionează pe baza unui blockchain propriu, separat, pe când token-urile funcţionează pe baza unui blockchain care facilitează crearea unor aplicaţii descentralizate*. Majoritatea criptomonedelor existente sunt tokenuri, datorită uşurinţei 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 diferenţă de semantică. Probabil cititorul a observat că până acum am utilizat termenul de bitcoin scris cu majuscule şi minuscule. Nu este o greşeală de editare, deoarece „***bitcoin" (scris cu iniţială minusculă)*** este în general folosit de publicul larg şi de mass media cu ***înţelesul de unitate monetară***. A poseda trei bitcoin înseamnă ca cineva este posesorul a trei unităţi monetare ce poartă denumirea

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

Bitcoin (scris cu iniţială majusculă) se referă la protocolul care guvernează această monedă, cu alte cuvinte la ansamblul de concepte tehnice, reguli şi convenţii care susţin generarea şi funcţionarea criptomonedei, cât şi relaţiile dintre utilizatori.

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

Nu în ultimul rând, ***Bitcoin reprezintă o revoluţie culturală***, materializarea dorinţei de protejare a intimităţii identităţi şi tranzacţiilor în sfera digitală şi o mişcare spre descentralizare, de evitare a controlului unui stat sau al unei autorităţi centrale, percepute de iniţiatorii mişcării ca fiind abuzive. În calitate de criptomonedă, Bitcoin-ul nu este susţinut de nici un stat sau autoritate centrală, ideea din spatele conceptului fiind ca acesta să fie construit de către utilizatori, pentru utilizatori.

Bitcoin îşi găseşte rădăcinile în ***Mişcarea Cypherpunk***[2], apărută la sfârşitul anilor 80, care susţinea necesitatea protecţiei vieţii private prin criptografie. Membrii acestei mişcări (care continuă să fie activă şi în prezent) nu au încredere că autorităţile statului sau marile corporaţii ar respecta intimitatea personală a oamenilor care le furnizează datele personale.

În 1992, Eric Hughes (matematician şi programator), Timothy C. May (inginer electronist şi cercetător ştiinţific principal la compania Intel, în primii ani de existenţă ai acesteia, autor de lucrări în domenii politic şi tehnic) şi John Gilmore (programator şi activist) au înfiinţat 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) şi cyberpunk (golan cibernetic)[3].

Principalele idei ale mişcării pot fi regăsite în Manifestul Cypherpunk: „Confidenţialitatea datelor este necesară unei societăţi deschise în epoca cibernetică… Nu ne putem aştepta de la guverne, corporaţii sau alte organizaţii

[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