

**DON TAPSCOTT  
și ALEX TAPSCOTT**

# REVOLUȚIA BLOCKCHAIN

*Despre felul în care tehnologia aflată  
la baza bitcoinului transformă banii,  
afacerile și lumea*

Traducere de Romică Lixandru

 ACT și Politon

2017

# Cuprins

Cuvânt-înainte	13
Mulțumiri	17

## **PARTEA I – SĂ ZICEM CĂ VREI O REVOLUȚIE**

<b>Capitolul 1</b>	
PROTOCOLUL ÎNCREDERII	29
<b>Capitolul 2</b>	
INIȚIALIZAREA VIITORULUI: ȘAPTE PRINCIPII DE PROIECTARE A ECONOMIEI BLOCKCHAINULUI	63

## **PARTEA A II-A – TRANSFORMĂRI**

<b>Capitolul 3</b>	
REINVENTAREA SERVICIILOR FINANCIARE	101
<b>Capitolul 4</b>	
REPROIECTAREA ARHITECTURII FIRMEI: CENTRUL ȘI MARGINILE	147
<b>Capitolul 5</b>	
NOI MODELE DE AFACERI: CUM SĂ FACI SĂ CURGĂ BANII ÎN BLOCKCHAIN	185
<b>Capitolul 6</b>	
REGISTRUL LUCRURILOR: ANIMAREA LUMII FIZICE	225
<b>Capitolul 7</b>	
REZOLVAREA PARADOXULUI PROSPERITĂȚII: INCLUZIUNEA ECONOMICĂ ȘI ANTREPRENORIATUL	259
<b>Capitolul 8</b>	
RECONSTRUCȚIA GUVERNULUI ȘI A DEMOCRAȚIEI	295

## **Capitolul 9**

ELIBERAREA CULTURII PE BLOCKCHAIN:  
O VESTE CARE NE BUCURĂ AUZUL

335

## **PARTEA A III-A – PERSPECTIVE PROMIȚĂTOARE ȘI PERICOLE**

### **Capitolul 10**

DEPĂȘIREA BLOCAJELOR:  
ZECE PROBLEME DE IMPLEMENTARE

371

### **Capitolul 11**

LEADERSHIP PENTRU URMĂTOAREA ERĂ

407

NOTE

452

PARTEA I



SĂ ZICEM CĂ VREI  
O REVOLUȚIE

## CAPITOLUL 1

---

# PROTOCOLUL ÎNCREDERII

Se pare că duhul tehnologic a evadat din nou din lampa sa. Invocat de o persoană sau de persoane necunoscute animate de motive tulburi, într-un moment istoric nesigur, duhul este acum la dispoziția noastră pentru o nouă tentativă – aceea de a transforma în bine rețeaua de distribuție a puterii economice și vechea ordine a afacerilor umane. Dacă ne vom dori asta.

Dă-ne voie să explicăm.

Primele patru decenii ale internetului ne-au adus e-mailul, World Wide Web, site-urile .com, rețelele de socializare, webul mobil, *big data*\*, *cloud computingul*\*\* și primele zile ale Internetului Lucrurilor. A fost extraordinar pentru reducerea costurilor căutării, pentru colaborare și pentru schimburile de informații. S-au diminuat barierele din calea intrării pe piață a noii media și a noului tip de divertisment, s-au creat noi forme de vânzare cu amănuntul și de organizare a muncii și s-a ajuns la o dezvoltare fără precedent a companiilor digitale. Grație tehnologiei

---

\*Este vorba de informații de volum mare, viteză mare și foarte diverse, care impun noi forme de procesare. Importanța lor este deosebită pentru firme, deoarece pe baza lor pot fi luate decizii strategice și de marketing, pot fi optimizate procesele de activitate și orientate în direcția spre care se îndreaptă piața și consumatorii. (n.tr.)

\*\* Se referă la servicii de calcul, aplicații, stocare și accesare a informațiilor și programelor direct de pe Internet. *Cloud*, care înseamnă „nor”, este de fapt internetul. Astfel de servicii sunt puse la dispoziție de diverse firme, de exemplu, Google, Apple, Amazon, dar și multe altele, cifra de afaceri anuală în acest sector depășind 100 de miliarde. (n.tr.)



senzorilor, s-a insuflat inteligență portofelelor, îmbrăcăminții, automobilelor, clădirilor și orașelor, inclusiv biologiei noastre. Toate acestea ne saturează mediul atât de complet, încât în curând nu ne vom mai „conecta”, ci ne vom vedea de treburi și de viață cufundați într-o tehnologie care a pătruns peste tot.

În ansamblu, internetul a făcut posibile o mulțime de schimbări pozitive – pentru cei care au acces la el –, dar are și câteva limitări serioase pentru afaceri și activitățile economice. *The New Yorker* ar putea să publice din nou, fără să modifice deloc, caricatura lui Peter Steiner din 1993, în care un câine îi spune altui câine: „Pe internet nu știe nimeni că ești câine”. În mediul online, nici acum nu putem să ne determinăm reciproc identitatea și nici să avem încredere unii în alții pentru a face tranzacții sau a schimba bani, fără să fim validați de un terț, cum ar fi o bancă sau un guvern. Tot acești intermediari ne colectează datele și ne invadează viața privată invocând profitul comercial și siguranța națională. Chiar și cu internetul, structura costurilor acestora lasă în afara sistemului financiar global aproximativ 2,5 miliarde de oameni. În ciuda promisiunii unei lumi împuternicite prin sistemul de la egal la egal, beneficiile economice și politice s-au dovedit a fi asimetrice – puterea și prosperitatea fiind canalizate spre cei care le dețineau deja, chiar dacă aceștia nu le mai obțin prin muncă. Banii produc mai mulți bani decât produc o mulțime de oameni.

Tehnologia nu mai creează prosperitate la fel cum nu distribuie nici viața privată. Dar, în această eră digitală, tehnologia poate fi întâlnită în miezul tuturor lucrurilor – bune și rele. Ea le oferă oamenilor posibilitatea să-și prețuiască și să-și încalce reciproc drepturile în feluri noi și profunde. Explozia comunicațiilor și a comerțului online creează un număr mai mare de oportunități pentru infracțiunile cibernetice. Legea lui Moore referitoare la dublarea anuală a puterii de procesare dublează și puterea escrocilor și hoților – „Nelegiuții lui Moore”<sup>1</sup> –, ca să nu mai vorbim de cei care trimit spamuri, de hoții de identitate, de cei care recurg la înșelăciune electronică pentru a obține date confidențiale, de



spioni, de cei care virusează computere pentru a le da diverse instrucțiuni, de hackeri, de cei care hărțuiesc și agresează online și de cei care sechestrează date informatice – infractori care utilizează softuri dăunătoare ce solicită răscumpărare pentru a returna datele sechestrate –, și lista continuă.

## ÎN CĂUTAREA PROTOCOLULUI DE ÎNCREDERE

Încă din 1981, inventatorii încercau să rezolve cu ajutorul criptografiei problemele de confidențialitate, securitate și incluziune ale internetului. Indiferent cum reprojectau procesul, existau întotdeauna breșe pentru că erau implicați diverși terți. Plățile cu carduri de credit prin Internet nu erau sigure, deoarece utilizatorii trebuiau să divulge prea multe date personale, iar comisioanele pentru tranzacții erau prea mari pentru plățile mici.

În 1993, un matematician strălucit pe nume David Chaum a inventat eCash, un sistem digital de plăți care reprezenta „un produs perfect din punct de vedere tehnic, ce făcea posibile plățile sigure și anonime pe internet... Era perfect adecvat pentru a trimite monede electronice de un cent, de cinci sau de zece cenți pe internet”<sup>2</sup>. Era atât de perfect, încât Microsoft și alții erau interesați să includă eCash ca opțiune în softul lor<sup>3</sup>. Problema era că, pe atunci, persoanele care cumpărau online nu se arătau interesate de confidențialitatea și securitatea online. DigiCash, compania olandeză a lui Chaum, a dat faliment în 1998.

În perioada aceea, unul dintre asociații lui Chaum, Nick Szabo, a scris un scurt articol intitulat “The God Protocol” („Protocolul lui Dumnezeu”), un joc de cuvinte pornind de la sintagma „particula lui Dumnezeu”, inventată de Leon Lederman, laureat al Premiului Nobel, prin care sublinia importanța bosonului lui Higgs pentru fizica modernă. În articolul său, Szabo se gândea la crearea unui protocol tehnologic alfa și omega, unul care să-l pună pe Dumnezeu în rolul de terț de încredere care intermediază toate tranzacțiile: „Toate părțile și-ar transmite



datele de intrare către Dumnezeu. Dumnezeu ar determina rezultatele corecte și apoi ar livra datele de ieșire. Cum Dumnezeu este manifestarea supremă a discreției în confesional, niciuna dintre părți nu va afla nimic în plus despre datele de intrare ale celorlalte părți, decât ce ar putea să afle din propriile date de intrare și de ieșire”<sup>4</sup>. Ideea lui era solidă: trebuia să accepți să ai o încredere oarbă ca să faci afaceri pe internet. Cum infrastructura nu are securitatea atât de necesară, deseori nu avem alte opțiuni și trebuie să tratăm intermediarii de parcă ar fi zei.

Un deceniu mai târziu, în 2008, industria financiară globală s-a prăbușit. Într-un moment probabil favorabil, una sau mai multe persoane ascunse sub pseudonimul Satoshi Nakamoto au schițat un protocol nou pentru un sistem monetar electronic *peer-to-peer*<sup>\*</sup>, care să utilizeze o criptomonedă numită bitcoin. Criptomonedele (monedele digitale) diferă de monedele tradiționale fiduciare<sup>\*\*</sup> prin faptul că nu sunt create sau controlate de stat. Acest protocol stabilea un set de reguli – sub forma unor calcule distribuite – care asigurau *integritatea* datelor schimbate între acele miliarde de dispozitive *fără să treacă printr-un terț de încredere*. Acest act aparent subtil a produs o scânteie care a încântat, a înspăimântat sau a captivat în vreun fel imaginația lumii informatice și s-a răspândit cu o viteză nemaipomenită la nivel de companii, guverne, printre apărătorii vieții private, printre activiștii din domeniul dezvoltării sociale, printre teoreticienii mass-media și jurnaliști, ca să menționăm doar câțiva, de pretutindeni.

„Ei au o reacție de genul «O, Doamne, asta e. Asta este marea descoperire. Asta așteptam noi»”, a declarat Marc Andreessen, cocreatorul primului browser Web comercial, Netscape, și unul

---

<sup>\*</sup>*Peer-to-peer* – în limbaj informatic, se referă la conexiunea directă dintre două computere din aceeași rețea, capabile să-și distribuie reciproc informații fără să fie necesară existența unui al treilea care să dețină rolul de server. (n.red.)

<sup>\*\*</sup> Monedă care a fost declarată mijloc legal de plată de către guvern, dar nu este susținută de o marfă fizică. Valoarea sa rezultă din raportul dintre cerere și ofertă și nu din valoarea materialului din care este făcută. Cea mai mare parte a monedelor naționale, inclusiv euro și dolarul american, sunt monede fiduciare. (n.tr.)





dintre marii investitori în companiile tehnologice. „El a rezolvat toate problemele. Indiferent cine este, ar trebui să primească Premiul Nobel – este un geniu.» Este exact ce trebuia! E rețeaua distribuită de încredere de care internetul a avut întotdeauna nevoie, dar pe care nu a avut-o niciodată.”<sup>5</sup>

În prezent, oameni inteligenți de pretutindeni încearcă să înțeleagă implicațiile unui protocol care le permite simplilor muritori să producă încredere printr-un cod inteligent. Lucrul acesta nu s-a mai întâmplat niciodată – tranzacții directe și de încredere între două sau mai multe părți, autentificate de colaborarea în masă și alimentate de interesele personale colective, nu de marile corporații motivate de profit.

Poate că nu este Atotputernicul, dar o platformă globală demnă de încredere pentru tranzacțiile noastre este ceva colosal. Noi o numim Protocolul Încrederii.

Acest protocol reprezintă baza pentru un număr din ce în ce mai mare de registre globale distribuite numite blockchainuri – cel mai mare dintre acestea fiind blockchainul bitcoin. Deși tehnologia este complicată și cuvântul *blockchain* nu este prea răsunător, ideea principală este simplă. Blockchainurile ne dau posibilitatea să trimitem bani direct și în siguranță de la unii la alții, fără să trecem printr-o bancă, o companie de carduri de credit sau PayPal.

În locul unui Internet al Informației, avem Internetul Valorii sau al Banilor. Este, de asemenea, și o platformă pe care toată lumea poate să determine ce este adevărat – cel puțin în ceea ce privește informația structurată înregistrată. La nivelul său fundamental, este un cod *open source*: oricine îl poate descărca gratuit, îl poate derula și îl poate utiliza pentru a elabora instrumente noi care să gestioneze tranzacțiile online. Astfel, are potențialul să dezlănțuie nenumărate aplicații noi și posibilități, care nu s-au materializat până acum, dar care au potențialul să transforme o mulțime de lucruri.



## CUM FUNCȚIONEAZĂ ACEST REGISTRU GLOBAL

Marile bănci și câteva guverne implementează blockchainurile ca registre distribuite care să revoluționeze felul în care este stocată informația și felul în care se desfășoară tranzacțiile. Obiectivele lor sunt laudabile – rapiditate, costuri mai mici, securitate, mai puține erori și eliminarea punctelor centrale de atac și de avarie. Aceste modele nu implică în mod necesar o criptomonedă pentru a face plăți.

Totuși, blockchainurile cele mai importante și cu acoperirea cea mai mare se bazează pe modelul de bitcoin al lui Satoshi. Iată cum funcționează.

Bitcoinul sau celelalte monede digitale nu sunt salvate în vre-un fișier aflat undeva; ele sunt reprezentate prin tranzacții înregistrate într-un blockchain – ca un fel de foaie de calcul sau un fel de registru contabil global, care se folosește de resursele unei mari rețele bitcoin *peer-to-peer*, pentru a verifica și aproba fiecare tranzacție cu bitcoini. La fel ca blockchainul care utilizează bitcoini, absolut toate blockchainurile sunt *distribuite*: ele funcționează pe computere, fiind puse la dispoziție de voluntari din întreaga lume; nu există nicio bază centrală de date care să fie spartă de hackeri. Blockchainul este *public*: poate fi văzut de oricine în orice moment, pentru că se găsește în rețea, nu într-o singură instituție însărcinată cu verificarea tranzacțiilor și cu înregistrările contabile. Iar blockchainul este *criptat*: utilizează o criptare complexă care lucrează atât cu chei publice, cât și cu chei private (oarecum similar cu sistemul de două chei necesare pentru deschiderea unei cutii de valori), pentru a se păstra securitatea virtuală. Nu trebuie să-ți faci griji din cauza slabelor paravane de protecție\* ale Target sau Home Depot sau din cauza funcționarului hoț de la Morgan Stanley ori din guvernul federal american.

La fiecare zece minute, la fel ca o bătaie a inimii rețelei bitcoin, toate tranzacțiile derulate sunt verificate, confirmate și

---

\* *Firewalls*, în original. (n.red.)



înregistrate într-un bloc care este legat de blocul anterior, alcătuind în felul acesta un lanț. Fiecare bloc trebuie să facă trimitere la blocul anterior pentru a fi valid. Această structură aplică o marcă temporală și stochează schimburile de valoare pentru totdeauna, împiedicând pe oricine să modifice registrul. Dacă ai vrea să furi un bitcoin, ar trebui să rescrii toată istoria respectivului bitcoin din blockchain ziua în amiaza mare. Lucrul acesta este practic imposibil. Astfel că blockchainul este un registru distribuit care reprezintă un consens în rețea pentru toate tranzacțiile care au existat vreodată. Asemenea World Wide Web-ului informației, aici avem Registrul Global al valorii – un registru distribuit pe care oricine îl poate descărca și utiliza pe computerul propriu.

Câțiva savanți au susținut că inventarea înregistrărilor contabile în partidă dublă a creat condițiile apariției capitalismului și statului național. Acest registru digital nou pentru tranzacții economice poate fi programat să înregistreze absolut orice informație valoroasă sau importantă pentru omenire: certificate de naștere și de deces, certificate de căsătorie, acte sau titluri de proprietate, diplome educaționale, conturi financiare, proceduri medicale, solicitări de plată a asigurării, voturi, proveniența alimentelor și orice lucru care poate fi exprimat printr-un cod.

Această platformă nouă permite o armonizare în timp real a înregistrărilor digitale despre aproape orice. De fapt, în scurt timp, miliarde de lucruri inteligente din lumea fizică vor detecta, răspunde, comunica, își vor cumpăra singure electricitatea și vor face schimburi de date importante, ocupându-se de toate, de la protecția mediului până la supravegherea sănătății noastre. Acest Internet al Tuturor Lucrurilor are nevoie de un Registru al Tuturor Lucrurilor. Lumea afacerilor, comerțul și economia au nevoie de Calculul Digital.

Atunci, de ce ți-ar păsa ție? Noi suntem convinși că adevărul ne *poate* elibera și că încrederea distribuită va afecta profund oamenii din toate clasele sociale. Poate că ești un meloman care vrea ca artiștii să poată trăi din arta lor. Sau un consumator care vrea să știe de unde provine de fapt carnea din hamburger. Poate



că ești un imigrant care s-a săturat să achite comisioane mari ca să trimită bani celor dragi, în țara natală. Sau o femeie saudită care vrea să editeze propria revistă de modă. Poate că ești un voluntar în scopuri caritabile care trebuie să identifice titlurile de proprietate ale terenurilor pentru proprietari, astfel încât să le poată reconstrui locuințele după un cutremur. Sau un cetățean care s-a săturat de lipsa de transparență și de responsabilitate a liderilor politici. Sau un utilizator al rețelelor de socializare care-și prețuiește viața privată și crede că toate datele pe care le generează ar trebui să aibă o oarecare valoare – pentru sine. Chiar în timp ce scriem, inovatorii dezvoltă aplicații bazate pe blockchain care să servească unor astfel de obiective. Și ele sunt doar începutul.

## O EXUBERANȚĂ RAȚIONALĂ PENTRU BLOCKCHAIN

Desigur, tehnologia blockchain are implicații profunde pentru numeroase instituții, lucru care ne ajută să explicăm entuziasmul multor persoane inteligente și influente. Ben Lawsky a renunțat la postul de comisar pentru servicii financiare al statului New York pentru a înființa o companie de consultanță în acest domeniu. El ne-a declarat: „În următorii cinci-zece ani, sistemul financiar ar putea să devină de nerecunoscut... și vreau să particip la schimbarea respectivă”<sup>6</sup>. Blythe Masters, fost director financiar și șef al Global Commodities în cadrul băncii de investiții JP Morgan, a pus bazele unei companii tehnologice axate pe blockchain, care să transforme domeniul. Coperta ediției din octombrie 2015 a revistei *Bloomberg Markets* o prezenta pe Masters sub titlul „Totul se reduce la blockchain”. Similar, în octombrie 2015, *The Economist* a publicat un articol pe prima pagină, „Mașina încrederei”, care susținea că „tehnologia aflată la baza bitcoinului ar putea să transforme felul în care funcționează economia”<sup>7</sup>. Pentru *The Economist*, tehnologia blockchain este „marele lanț al încrederei în lucruri”. Peste tot, băncile formează echipe de top care să