

REVOLUȚIA BLOCKCHAIN

Alte cărți de **Don Tapscott**

Paradigm Shift:

The New Promise of Information Technology (1993)

Coautor, Art Caston

The Digital Economy:

Promise and Peril in the Age of Networked Intelligence (1995)

Growing Up Digital:

The Rise of the Net Generation (1997)

Who Knows:

Safeguarding Your Privacy in a Networked World (1997)

Coautor, Ann Cavoukian

Digital Capital:

Harnessing the Power of Business Webs (2000)

Coautori, David Ticoll și Alex Lowy

The Naked Corporation:

How the Age of Transparency Will Revolutionize Business (2003)

Coautor, David Ticoll

Wikinomics:

How Mass Collaboration Changes Everything (2006)

(*Wikinomics. Cultura colaborării în masă*) (2010)

Coautor, Anthony D. Williams

Grown Up Digital:

How the Net Generation Is Changing the World (2008)

(*Crescuți digital. Generația Net îți schimbă lumea*) (2011)

Macrowikinomics:

New Solutions for a Connected Planet (2010)

Coautor, Anthony D. Williams

**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

All rights reserved including the right of reproduction in whole or in part in any form.
Această ediție este publicată prin acordul cu Portfolio, membră a grupului
Penguin Publishing Group, o companie Penguin Random House LLC.

Blockchain Revolution

Copyright © 2016 by Don Tapscott and Alex Tapscott
Originally published by Portfolio/Penguin, an imprint of Penguin Random
House LLC.

© 2017 Editura ACT și Politon pentru prezenta ediție românească

Editura ACT și Politon
Str. Înclinată, nr. 129, Sector 5, București, România, C.P. 050202.
tel: 0723 150 590, e-mail: office@actsipoliton.ro
www.actsipoliton.ro/blog

Traducător: **Romică Lixandru**
Redactor: **Ines Simionescu**
Editor: **Maria Nicula**
Tehnoredactor: **Teodora Vlădescu**
Coperta: **Mădălina Ioniță**
Copyright Manager: **Andrei Popa**

Descrierea CIP a Bibliotecii Naționale a României

TAPSCOTT, DON

**Revoluția blockchain: despre felul în care tehnologia aflată la baza
bitcoinului transformă banii, afacerile și lumea/ Don & Alex Tapscott; trad.:**
Romică Lixandru. - București: ACT și Politon, 2017

ISBN 978-606-913-258-6

I. Tapscott, Alex

II. Lixandru, Romică (trad.)

33

62

AVERTISMENT: Distribuirea, copierea sau piratarea în orice fel a acestei cărți nu este pedepsită numai prin lege, dar contravine și tuturor normelor și principiilor etice și sănătoase pe care un astfel de titlu le promovează. Ce fel de efect va avea energia pe care vreți să o transmiteți mai departe, dacă aceasta vine prin furt, ilegalitate și lipsă de respect față de autor și față de toți cei care au contribuit la crearea acestei cărți, astfel ca ea să ajungă la dumneavoastră? Împărtășiți cu ceilalți informațiile importante, valorile și lecțiile pe care le-ați aflat din acest material, într-un mod corect și responsabil.

*Anei Lopes și lui Amy Welsman, pentru că au făcut
posibilă această carte și au înțeles
că „blockchainul este tot ceea ce contează”.*

„O capodoperă. Analizează elegant potențialul tehnologiei blockchain de a se ocupa de cele mai presante provocări globale contemporane.”

– **Hernando de Soto**, economist, președinte al Institutului pentru Libertate și Democrație, Peru

„Blockchainul reprezintă pentru creditare ceea ce reprezintă internetul pentru informație. Asemenea internetului de la început, blockchainul are potențialul de a transforma totul. Citește această carte și vei înțelege.”

– **Joichi Ito**, director al Laboratorului Media din cadrul MIT

„În această călătorie extraordinară spre frontierele finanțelor, cei doi Tapscott pun într-o lumină nouă fenomenul blockchain și ne explică într-o pledoarie convingătoare de ce trebuie să-i înțelegem cu toții mai bine puterea și potențialul.”

– **Dave McKay**, președinte și director general al Royal Bank of Canada

„Demontează promisiunea și pericolul reprezentate de blockchain într-un stil totodată accesibil și erudit. *Revoluția blockchain* le oferă cititorilor o avanpremieră privilegiată a viitorului.”

– **Alec Ross**, autor, *The Industries of the Future*

„Dacă există vreun subiect care ar trebui demistificat, acela ar fi blockchainul. Împreună, cei doi Tapscott au reușit pe deplin și astfel au surprins entuziasmul, potențialul și importanța acestui subiect pentru toată lumea.”

– **Blythe Masters**, director general al Digital Asset Holdings

„Această carte are calitatea predictivă a romanului *1984* al lui George Orwell și viziunea lui Elon Musk. Citește-o sau ești mort.”

– **Tim Draper**, fondator al Draper Associates, DFJ și Draper University

„Blockchainul este un val tehnologic radical și, așa cum a făcut de atâtea ori, Tapscott se află chiar pe val, de data aceasta însoțit de fiul său Alex, făcând surfing în zori. E o cursă pe cinste.”

– **Yochai Benkler**, șeful Catedrei Berkman de studii juridice antreprenoriale, Harvard Law School

„Dacă lucrezi în afaceri sau în cadrul guvernului, ești obligat să înțelegi revoluția blockchain. Nimeni nu a mai scris vreodată o carte mai antrenantă sau mai sistematic documentată pe acest subiect decât cei doi Tapscott.”

– **Erik Brynjolfsson**, profesor la MIT;
coautor al *The Second Machine Age*

„O relatare indispensabilă și actualizată a felului în care tehnologia aflată la baza bitcoinului ar putea – și ar trebui – să descătușeze potențialul real al unei economii digitale de a distribui prosperitatea.”

– **Douglas Rushkoff**, autor al volumelor *Present Shock*
și *Throwing Rocks at the Google Bus*
(*Aruncând cu pietre în autobuzul Google*)

„Schimbările tehnologice care înainte se derulau în decursul unei generații ne lovesc acum aproape într-o clipă și nimeni nu spune această poveste mai bine decât cei doi Tapscott.”

– **Eric Spiegel**, președinte și director general
al Siemens SUA

„Sunt puțini liderii care ne fac să privim în viitorul apropiat așa cum face Don Tapscott. Prin *Revoluția blockchain*, el și fiul său Alex ne învață, ne provoacă și ne prezintă un mod cu totul nou de a ne gândi la viitor.”

– **Bill McDermott**, director general al SAP SE

„*Revoluția blockchain* este un amestec strălucit de istorie, tehnologie și sociologie care abordează toate aspectele protocolului blockchain – o invenție care, în timp, se poate dovedi la fel de memorabilă precum inventarea tiparului.”

– **James Rickards**, autor al volumelor
Currency Wars și *The Death of Money*

„*Revoluția blockchain* funcționează pe post de atlas pentru lumea banilor digitali, explicând cu măiestrie peisajul actual și iluminând în același timp un drum care merge tot înainte către un sistem financiar global mai echitabil, mai eficient și mai conectat.”

– **Jim Breyer**, director general al Breyer Capital

„*Revoluția blockchain* este un ghid absolut necesar și hotărâtor al acestei tehnologii care schimbă lumea.”

– **Jerry Brito**, director executiv al Coin Center

„Incredibil. Cu adevărat incredibil. Felul în care cei doi Tapscott examinează blockchainul ca model de includere într-o lume din ce în ce mai centralizată este în același timp nuanțat și extraordinar.”

– **Steve Luczo**, președinte și director general al Seagate Technology

„Construiește o pledoarie solidă atât în favoarea capacității blockchainului de a mări transparența, cât și în favoarea capacității acestuia de a asigura confidențialitatea. După cum spun chiar autorii, «Internetul Lucrurilor are nevoie de un Registrul al Lucrurilor».”

– **Chandra Chandrasekaran**, director general al Tata Consultancy Services

„Epicentrul încrederii este pe cale să se disperseze! Narațiunea definitivă a posibilităților revoluționare oferite de un sistem descentralizat de încredere.”

– **Frank D'Souza**, director general al Cognizant

„Identifică o mișcare tehnologică profundă și nouă și o conectează la cea mai profundă dintre nevoile umane: încrederea. Este documentată cu meticulozitate și scrisă provocator. Absolut toți oamenii de afaceri și toți decidenții politici trebuie să citească *Revoluția blockchain*.”

– **Brian Fetherstonhaugh**, președinte și director general al OgilvyOne Worldwide

„*Revoluția blockchain* pregătește terenul pentru un val de progres tehnologic aflat abia la început.”

– **Frank Brown**, director general și director operațional al General Atlantic

„O lectură obligatorie. Vei înțelege cu adevărat motivul pentru care blockchainul devine cu repeziune una dintre cele mai importante tehnologii emergente de la internet încoace.”

– **Brian Forde**, director al Digital Currency Initiative, Laboratorul Media din cadrul MIT

„Tehnologia blockchain are potențialul de a revoluționa industria, finanțele și guvernarea – o lectură obligatorie pentru oricine este interesat de viitorul banilor și al umanității.”

– **Perianne Boring**, fondatoare și președinte
al Camerei de Comerț Digital

„Când tehnologia caracteristică unei generații transformă lumea în care trăim, suntem cu adevărat norocoși să avem cartografi precum Don Tapscott, iar acum și pe fiul său Alex, care ne explică încotro ne îndreptăm.”

– **Ray Lane**, proprietar și director general al GreatPoint Ventures;
partener emerit la Kleiner Perkins

„Don și Alex au scris manualul hotărâtor pentru cei care încearcă să treacă de această nouă și promițătoare frontieră.”

– **Benjamin Lawsky**, fost comisar pentru servicii financiare, statul
New York; director general al The Lawsky Group

„*Revoluția blockchain* este un manifest edificator și are o importanță deosebită pentru următoarea eră digitală.”

– **Dan Pontefract**, autor al *The Purpose Effect*;
director de concepție al TELUS

„Cea mai bine documentată, mai sistematică și mai pătrunzătoare carte despre cea mai interesantă tehnologie nouă de la internet încoace. O lucrare de o claritate excepțională și cu o perspectivă uimitor de amplă și de profundă.”

– **Andreas Antonopoulos**, autorul volumului
Mastering Bitcoin (Gestionarea bitcoinului)

„*Revoluția blockchain* surprinde și clarifică superb minunata lume nouă a banilor descentralizați, iluzorii.”

– **Tyler Winklevoss**, cofondator
al Gemini and Winklevoss Capital

„O perspectivă fascinantă – și relaxantă – asupra tehnologiei care are puterea să redeseneze economia globală. Ce premiu! Ce carte!”

– **Paul Polman**, director general al Unilever

Cuprins

Cuvânt-înainte	13
Mulțumiri	17

PARTEA I – SĂ ZICEM CĂ VREI O REVOLUȚIE

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

PARTEA A II-A – TRANSFORMĂRI

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

Cuvânt-înainte

Cartea celor doi Tappscot, tată și fiu, vine să facă lumină în lumea blockchainului și a beneficiilor pe care această tânără tehnologie le va aduce viitorului nostru. Cartea este extrem de bine documentată, având la bază peste doi ani de cercetări și mai bine de o sută de interviuri cu pionierii tehnologiei blockchain.

Dincolo de binecunoscuta monedă virtuală bitcoin, tehnologia blockchain a devenit „pariul deceniului” pentru toată industria financiară, de la bănci la companii de asigurări sau trading. În contextul democratizării internetului și al facilităților de comunicare aparent fără limite, apare o nouă clasă de active: datele. Actorii îndrăgiți ai internetului, de la Facebook la Google și Amazon, au în spate colecții uluitoare de informații despre fiecare dintre noi ca utilizatori. Cu ajutorul blockchain și *peer-to-peer* acest trend se inversează. Ne putem proteja identitatea și apăra valoarea proprietății generate la nivel individual.

Deși trăim într-o lume tot mai digitalizată și avem deja acces la „case inteligente” și comunicare instantanee cu orice colț al lumii, industria financiară poartă încă în spate sechelele erei pre-industriale. Tranzacțiile pe bursă se fac în nanosecunde, dar decontarea efectivă a banilor durează trei zile. Cumpărarea unui hamburger la McDonald’s durează cu tot cu servire câteva minute, dar banii de pe cardul tău vor intra în contul vânzătorului tot peste trei zile. Riscurile care îngreunează acum decontările în sistemul financiar global promet să fie rezolvate prin tehnologia blockchain, care ar accelera decontările până la ordinul secundelor.



De curând, Estonia a anunțat oficial că va fi prima țară care va emite monedă virtuală. Numele acesteia va fi „estcoin”, iar consilierul lor pentru această – să-i spunem nouă ispravă digitală – este nimeni altul decât Vitalik Buterin, fondatorul Ethereum, a doua criptovalută după capitalizarea de piață.

Nenumărate par a fi aplicațiile blockchain pentru viața noastră de zi cu zi, de la identificarea reputației pentru acordarea de credite, la urmărirea provenienței reale a unui produs de pe raftul supermarketului și de la contabilitatea în partidă triplă la emiterea de obligațiuni și acțiuni în criptovalută – și am enunțat doar câteva dintre aplicațiile posibile ale blockchainului.

Într-un moment al istoriei în care „poți fi oricine pe internet” se pare că omenirea are nevoie de o porție zdravănă de integritate, atât din partea oamenilor, cât și a companiilor. Așa cum spune economistul Michael Jensen, integritatea devine realmente un factor de producție alături de capital, muncă și tehnologie.

În mod cert tehnologia ne revoluționează prezentul și modelează viitorul, iar blockchainul folosește puterea rețelei descentralizate pentru a valida o mare varietate de tranzacții într-un timp extrem de rapid și care, mai înainte de toate, sunt arhivate astfel încât să nu mai poată fi șterse sau modificate. Mai în glumă, mai în serios, am putea afirma că această tehnologie poate fi comparată cu un adevărat „ser al adevărului” pentru reputația indivizilor și a relațiilor în care aceștia sunt implicați, protejându-le în același timp identitatea.

Chiar dacă nu ești pasionat de finanțe sau tehnologie, cartea de față reprezintă o necesară lectură pentru înțelegerea lumii în care vom trăi, iar blockchainul își va pune accentul asupra vieții noastre cotidiene, a călătoriilor, vacanțelor, educației, cumpărăturilor, asupra muncii, a relațiilor și, de ce nu, chiar asupra fericirii.

Am convingerea că timpul alocat lecturii acestei cărți îți va fi răsplătit cu informații valoroase care te vor ajuta să te orientezi prin jungla de informații care se năpustesc zi de zi asupra ta prin



toate mijloacele și îți vor oferi un punct de plecare solid în înțelegerea acestei tehnologii noi și revoluționare.

Lectură plăcută și mulțumiri autorilor pentru acest veritabil manual de blockchain.

EUSEBIU BURCAȘ, fondator Burcash™

MULȚUMIRI

Această carte a rezultat din confluența a două minți și a două traiectorii de viață. Don conducea un program sindicalizat de cercetare în valoare de 4 milioane de dolari, numit Global Solutions Networks (GSN), la Rotman School of Management din cadrul Universității din Toronto. Inițiativa investiga modele noi, de tip rețea, pentru soluționarea problemelor globale și de guvernare globală. El a studiat felul în care internetul este guvernat de un ecosistem format din multiple părți interesate și a început să fie atras de monedele digitale și de guvernanța* lor. În acest timp, Alex era unul dintre directorii executivi ai băncii de investiții Canaccord Genuity. El a observat entuziasmul crescând pentru companiile bazate pe bitcoin** și blockchain*** aflate în fazele de

* *Guvernanță* - Termenul nu este prezent în dicționarul limbii române; însă este utilizat din ce în ce mai frecvent în vorbirea curentă fiind un echivalent pentru englezescul *governance* - conducere, administrație, cărmuire, stăpânire, guvernare. Nevoia de a crea un termen nou în limba română probabil a survenit pentru a face o distincție cât mai clară între actul de conducere exercitat de un guvern și conducerea exercitată în cazul unor structuri economice, sociale sau de altă natură. (n.red.)

** *Bitcoin* - rețea consensuală ce oferă un nou sistem de plată și bani complet digitali. Este primul sistem de plată *peer-to-peer* descentralizat susținut de utilizatorii săi fără o autoritate centrală sau intermediari. Din perspectiva unui utilizator, bitcoin reprezintă în mare bani cash pentru internet. Bitcoin poate fi văzut și ca cel mai proeminent sistem de contabilitate în partidă triplă existent. (n.red.)

*** *Blockchain* - este pentru lumea finanțelor comparabil cu ce era acum douăzeci de ani internetul pentru lumea informației: o tehnologie care permite tranzacții rapide, securizate și descentralizate. Tehnologia blockchain este folosită mai ales în contextul monedelor virtuale ca bitcoinul, dar are un potențial mult mai mare de



Început în anul 2013 și a început să îndrepte eforturile firmei sale în acest spațiu. La începutul lui 2014, în timpul unei excursii tată-fiu la schi, în Mont-Tremblant, am dezbătut la o cină mai multe idei despre colaborarea pe acest subiect, iar Alex a fost de acord să conducă un proiect de cercetare despre guvernanta monedelor digitale, care a culminat cu raportul său intitulat *A Bitcoin Governance Network (O rețea de guvernanta a bitcoinului)*. Cu cât am intrat mai adânc în subiect, cu atât am ajuns să fim mai convinși că avea să devină următorul domeniu revoluționar.

În acest timp, agentul nostru, Wes Neff de la Leigh Bureau, împreună cu editorul lui Don, Adrian Zackheim de la Portfolio/Penguin (*Wikinomics, Macrowikinomics*), îl încurajau pe Don să formuleze conceptul unei cărți noi. Când raportul lui Alex a ajuns să fie recunoscut la scară largă drept paradigmă dominantă de gândire în acest domeniu, Don l-a abordat pe Alex, cerându-i să-i fie coautor. Spre meritul său, Adrian ne-a făcut o ofertă pe care nu o puteam refuza și cartea nu a ajuns niciodată la licitație, așa cum se întâmplă în mod normal.

Apoi am luat o decizie care acum, privind retrospectiv, ni se pare o decizie inteligentă. L-am abordat pe cel mai bun editor pe care îl cunoșteam, Kirsten Sandberg, care lucrase anterior la Harvard Business School Press, și am rugat-o să ne editeze viitoarea carte. A lucrat spectaculos, iar colaborarea noastră s-a desfășurat atât de ușor încât i-am cerut să devină membră cu normă întreagă a echipei care se ocupa de cercetarea pentru carte. Împreună cu noi, Kirsten a luat parte la peste o sută de interviuri, colaborând în timp real, în vreme ce încercam să înțelegem multitudinea de aspecte puse în discuție și să elaborăm formulări utile care să explice acest set de evoluții extraordinare unui public nespecializat din punct de vedere tehnic. Ea ne-a ajutat să dăm viață poveștii. În sensul acesta, a fost coautoarea noastră, iar

a inova, aplicabil în numeroase domenii. Avantajul ei este că poate stoca o bază publică de date, protejate de criptografie, fără să aibă nevoie de reglementare din partea unei autorități centrale. Adoptată pe scară largă, ar aduce un nivel de transparență fără precedent, fie în zona privată, fie în administrația publică. (n.red.)



cartea nu ar fi apărut fără ea, cel puțin nu în actuala sa formă inteligibilă. Îi suntem foarte recunoscători pentru acest lucru, precum și pentru toate îndemnurile și replicile amuzante.

Le mulțumim din inimă celor de mai jos, care ne-au oferit cu generozitate timpul și ideile lor și fără de care această carte nu ar fi fost posibilă. În ordine alfabetică:

Jeremy Allaire, fondator, președinte și director general, Circle
Marc Andreessen, cofondator, Andreessen Horowitz
Gavin Andresen, director științific, Bitcoin Foundation
Dino Angaritis, director general, Smartwallet
Andreas Antonopoulos, autorul volumului *Mastering Bitcoin*
(*Gestionarea bitcoinului*)
Federico Ast, CrowdJury
Susan Athey, profesor de economie tehnologică, Stanford
Graduate School of Business
Adam Back, cofondator și președinte, Blockstream
Bill Barhydt, director general, Abra
Christopher Bavitz, director general, Cyberlaw Clinic, Harvard
Law School
Geoff Beattie, președinte al consiliului de administrație, Relay
Ventures
Steve Beauregard, director general și fondator, GoCoin
Mariano Belinky, partener comandat, Santander InnoVentures
Yochai Benkler, șeful Catedrei Berkman de studii juridice
antreprenoriale, Harvard Law School
Jake Benson, director general și fondator, LibraTax
Tim Berners-Lee, inventator, World Wide Web
Doug Black, senator, Senatul Canadei, Guvernul Canadei
Perriane Boring, fondator și președinte, Camera de Comerț
Digital
David Bray, bursier Eisenhower în 2015 și director executiv
invitat rezident la Universitatea Harvard
Jerry Brito, director executiv, Coin Center



Paul Brody, lider strategic pentru cele două Americi, Grupul tehnologic al EY (anterior IoT la IBM)

Richard G. Brown, director tehnic, R3 CEV (fost arhitect executiv pentru inovarea industriei și dezvoltarea afacerilor, IBM)

Vitalik Buterin, fondator, Ethereum

Patrick Byrne, director general, Overstock

Bruce Cahan, cercetător invitat, Stanford Engineering; Stanford Sustainable Banking Initiative

James Carlyle, inginer-șef, MD, R3 CEV

Nicolas Cary, cofondator, Blockchain Ltd.

Toni Lane Casserly, director general, CoinTelegraph

Christian Catalini, lector universitar, MIT Sloan School of Management

Ann Cavoukian, director executiv, Privacy and Big Data Institute, Ryerson University

Vint Cerf, cocreator al internetului și director responsabil de sectorul online, Google

Ben Chan, inginer de software, BitGo

Robin Chase, cofondator și fost director general, Zipcar

Fadi Chehadi, director general, ICANN

Constance Choi, director, Seven Advisory

John H. Clippinger, director general, ID3, cercetător, Laboratorul Media din cadrul MIT

Bram Cohen, creator, BitTorrent

Amy Cortese, jurnalist, fondator al Locavest

J.-F. Courville, director operațional, RBC Wealth Management

Patrick Deegan, director tehnic, Personal BlackBox

Primavera De Filippi, cercetător permanent la CNRS și conferențiar universitar la Berkman Center for Internet and Society, Harvard Law School

Hernando de Soto, președinte, Institutul pentru Libertate și Democrație

Peronet Despeignes, operațiuni speciale, Augur

Jacob Dienelt, arhitect și director economic al Blockchain, itBit și Factom

Joel Dietz, Swarm Corp



Helen Disney, (anterior) Bitcoin Foundation

Adam Draper, director general și fondator, Boost VC

Timothy Cook Draper, investitor de capital de risc; fondator,
Draper Fisher Jurvetson

Andrew Dudley, fondator și director general, Earth Observation

Joshua Fairfield, profesor de drept, Washington and Lee
University

Grant Fondo, partener, Securities Litigation and White Collar
Defense Group, Privacy and Data Security Practice, Goodwin
Procter LLP

Brian Forde, fost consilier, Casa Albă; director, Digital Currency,
Laboratorul Media din cadrul MIT

Mike Gault, director general, Guardtime

George Gilder, fondator și partener, Gilder Technology Fund

Geoff Gordon, director general, Vogogo

Vinay Gupta, coordonator de proiect, Ethereum

James Hazard, fondator, Common Accord

Imogen Heap, muzician și compozitor, câștigătoare a Premiului
Grammy

Mike Hearn, fost inginer Google, Vinumeris/Lighthouse

Austin Hill, cofondator și principalul inițiator, Blockstream

Toomas Hendrik Ilves, președintele Estoniei

Joichi Ito, director, Laboratorul Media din cadrul MIT

Eric Jennings, cofondator și director general, Filament

Izabella Kaminska, reporter financiar, *Financial Times*

Paul Kemp-Robertson, cofondator și director editorial, Contagious
Communications

Andrew Keys, Consensus Systems

Joyce Kim, director executiv, Stellar Development Foundation

Peter Kirby, director general și cofondator, Factom

Joey Krug, dezvoltator, Augur

Haluk Kulin, director general, Personal BlackBox

Chris Larsen, director general, Ripple Labs

Benjamin Lawsky, fostul comisar pentru servicii financiare al
statului New York; director general, The Lawsky Group



Charlie Lee, creator, director tehnic; fost director responsabil pentru partea de inginerie, Litecoin
Matthew Leibowitz, partener, Plaza Ventures
Vinny Lingham, director general, Gyft
Juan Llanos, vicepreședinte executiv pentru parteneriate strategice și director responsabil cu transparența, Bitreserve.org
Joseph Lubin, director general, Consensus Systems
Adam Ludwin, fondator, Chain.com
Christian Lundkvist, Balanc3
David McKay, președinte și director general, RBC
Janna McManus, director de relații cu publicul la nivel global, BitFury
Mickey McManus, Maya Institute
Jesse McWaters, specialist în inovații financiare, Forumul Economic Mondial
Blythe Masters, director general, Digital Asset Holdings
Alistair Mitchell, partener comandat, Generation Ventures
Carlos Moreira, fondator, președinte al consiliului de administrație și director general, WISEKey
Tom Mornini, fondator și promotor al clientului, Subledger
Ethan Nadelmann, director executiv, Drug Policy Alliance
Adam Nanjee, șeful Fintech Cluster, MaRS
Daniel Neis, director general și cofondator, KOINA
Kelly Olson, New Business Initiative, Intel
Steve Omohundro, președinte, Self-Aware Systems
Jim Orlando, director general, OMERS Ventures
Lawrence Orsini, cofondator și director, LO3 Energy
Paul Pacifico, director general, Featured Artists Coalition
Jose Pagliery, reporter, CNNMoney
Stephen Pair, cofondator și director general, BitPay Inc.
Vikram Pandit, fost director general, Citigroup; investitor la Coinbase, Portland Square Capital
Jack Peterson, dezvoltator, Augur
Eric Piscini, director, servicii bancare/tehnologie, Deloitte Consulting



Kausik Rajgopal, șeful biroului din Silicon Valley, McKinsey and Company
 Suresh Ramamurthi, președintele consiliului de administrație și director tehnic, CBW Bank
 Sunny Ray, director general, Unocoin.com
 Caterina Rindi, director responsabil de comunicarea cu comunitățile online pe rețelele de socializare, Swarm Corp
 Eduardo Robles Elvira, director tehnic, Agora Voting
 Keonne Rodriguez, director de produs, Blockchain Ltd.
 Matthew Roszak, fondator și director general, Tally Capital
 Colin Rule, președintele consiliului de administrație și director general, Modria.com
 Marco Santori, consilier, Pillsbury Winthrop Shaw Pittman LLP
 Frank Schuil, director general, Safello
 Barry Silbert, fondator și director general, Digital Currency Group
 Thomas Spaas, director, Belgium Bitcoin Association
 Balaji Srinivasan, director general, 21; partener, Andreessen Horowitz
 Lynn St. Amour, fost președinte, The Internet Society
 Brett Stapper, fondator și director general, Falcon Global Capital LLC
 Elizabeth Stark, profesor invitat, Yale Law School
 Jutta Steiner, Ethereum/Provenance
 Melanie Swan, fondator, Institute for Blockchain Studies
 Nick Szabo, GWU Law
 Ashley Taylor, Conensys Systems
 Simon Taylor, vicepreședinte pentru parteneriate antreprenoriale, Barclays
 David Thomson, fondator, Artlery
 Michelle Tinsley, director, Mobility and Payment Security, Intel
 Peter Todd, responsabil de calitate, CoinKite
 Jason Tyra, CoinDesk
 Valery Vavilov, director general, BitFury
 Ann Louise Vehovec, vicepreședinte, proiecte strategice, RBC Financial Group
 Roger Ver, “The Bitcoin Jesus”, Memorydealers KK



Akseli Virtanen, manager de fond speculativ, Robin Hood Asset Management

Erik Voorhees, director general și fondator, ShapeShift

Joe Weinberg, cofondator și director general, Paycase

Derek White, director de creație și director responsabil de informațiile digitale, Barclays Bank

Ted Whitehead, director general, Manulife Asset Management

Zooko Wilcox-O'Hearn, director general, Least Authority Enterprises

Carolyn Wilkins, prim-viceguvernator, Bank of Canada

Robert Wilkins, director general, myVBO

Cameron Winklevoss, fondator, Winklevoss Capital

Tyler Winklevoss, fondator, Winklevoss Capital

Pindar Wong, pionier al internetului, președintele consiliului de administrație al VeriFi

Gabriel Woo, vicepreședinte pentru inovație, RBC Financial Group

Gavin Wood, director tehnic, Ethereum Foundation

Aaron Wright, profesor, Cardozo Law School, Yeshiva University

Jonathan Zittrain, Harvard Law School

Adresăm mulțumiri speciale și câtorva persoane care au pus umărul efectiv la treabă. Anthony Williams și John Bigham din cadrul proiectului GSN au colaborat strâns cu Alex la raportul inițial despre guvernarea monedelor digitale. Joan McCalla, fost director executiv al Cisco, a făcut o cercetare amănunțită pentru capitolele despre Internetul Lucrurilor (Internet of Things, IoT) și de asemenea despre guvernare și democrație. Am avut parte și de mult sprijin familial, directorul de IT Bob Tapscott petrecându-și mai multe zile descărcând și intrând în detaliile blockchainului bitcoin pentru a ne oferi informații direct de la sursă despre problemele tehnice. Antreprenorul tehnologic Bill Tapscott a avut ideea revoluționară a unui sistem personal de tranzacționare a creditelor pentru emisiile de carbon bazat pe blockchain, iar directorul tehnic Niki Tapscott și soțul său, analistul financiar James Leo, s-au dovedit a fi adevărate cutii de rezonanță în tot



acest timp. Katherine Mac-Lellan din cadrul Grupului Tapscott (un avocat la îndemână) s-a ocupat de o parte dintre problemele mai dificile legate de contractele inteligente, precum și de gestionarea procesului de interviuare. Phil Courneyeur a căutat cu atenție în fiecare zi materiale interesante, iar David Ticoll a oferit informații foarte utile despre evoluțiile erei digitale de până acum. Wes Neff și Bill Leigh din cadrul Leigh Bureau ne-au ajutat să cizelăm conceptul cărții (a câta carte ar fi asta, băieți?). Ca întotdeauna (de mai bine de douăzeci de ani), Jody Stevens a dirijat perfect administrarea întregului proiect, care include atât bazele de date, finanțele și gestionarea documentelor, cât și procesul de corectură și de producție – un job cu normă întreagă, pe lângă celelalte joburi cu normă întreagă de care se achită în cadrul Grupului Tapscott.

Mulțumiri speciale lui Dino Mark Angaritis, directorul general al companiei blockchain Smartwallet; lui Joseph Lubin, director general al studioului de dezvoltare Ethereum, Consensus Systems; și lui Carlos Moreira din cadrul companiei de securitate cu expansiune rapidă WISeKey – fiecare dintre ei petrecându-și foarte mult timp cu noi făcând brainstorming. Sunt cu toții străluciți și au fost foarte amabili că ne-au ajutat. Acum avem ocazia să ne bucurăm de faptul că asistăm la succesul fiecăreia dintre companiile lor în acest domeniu. De asemenea, adresăm multe mulțumiri și echipei noastre extraordinare de la Penguin Random House, condusă de editorul nostru Jesse Maeshiro și supervizată de Adrian Zackheim.

Cel mai important lucru, am vrea să le mulțumim din suflet soțiilor noastre, Ana Lopes (Don) și Amy Welsman (Alex), care s-au dovedit mai mult decât tolerante față de obsesia noastră de a descifra această enigmă complexă timp de aproape un an. Suntem amândoi foarte norocoși să avem niște parteneri de viață atât de minunate.

Scrierea acestei cărți a fost o experiență plăcută pentru amândoi și trebuie să spunem că ne-am bucurat de fiecare clipă. Așa cum a spus cândva o persoană celebră: „Dacă doi oameni



sunt de acord în orice privință, unul dintre ei este inutil”. Ne-am provocat reciproc zilnic, punându-ne la încercare convingerile și presupunerile, iar prezenta carte este dovada vie a acestei colaborări sănătoase și viguroase. Nu uita, colaborarea chiar pare floare la ureche când ai atât de mult ADN în comun și o istorie comună de explorare a lumii întinsă pe parcursul a treizeci de ani. Sperăm să descoperi că produsul acestei colaborări este important și util.

Don Tapscott și Alex Tapscott, ianuarie 2016

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”¹ –, 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”². Era atât de perfect, încât Microsoft și alții erau interesați să includă eCash ca opțiune în softul lor³. 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”⁴. 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*^{*}, care să utilizeze o criptomonedă numită bitcoin. Criptomonedele (monedele digitale) diferă de monedele tradiționale fiduciare^{**} 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

^{*}*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.)

^{**} 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.”⁵

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”⁶. 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”⁷. Pentru *The Economist*, tehnologia blockchain este „marele lanț al încrederei în lucruri”. Peste tot, băncile formează echipe de top care să



investigheze oportunitățile, câteva dintre ele incluzând zeci de experți reductabili în domeniul tehnologiei. Bancherii iubesc ideea de tranzacții sigure, instantanee și lipsite de fricțiuni, dar există câțiva care se tem de ideile de deschidere, descentralizare și de noi forme de monedă. Industria serviciilor financiare a reetichetat și privatizat deja tehnologia blockchain, referindu-se la ea prin sintagma *tehnologia registrelor distribuite*, ca o încercare de a împăca cele mai bune aspecte ale bitcoinului – securitatea, viteza și costul – cu un sistem complet închis a cărui utilizare depinde de permisiunea unei bănci sau a unei instituții financiare. Pentru ele, blockchainurile sunt baze de date mai trainice decât cele pe care le au deja, baze de date care le permit părților interesate – cumpărători, vânzători, custozi și autorități de reglementare – să păstreze înregistrări comune, imposibil de șters, reducând astfel costul, reducând riscul de decontare și eliminând punctele centrale de prăbușire.

Investițiile în companiile *start-up** axate pe blockchain încep să ia avânt, la fel ca investițiile în companiile .com din anii 1990. Cei care investesc capital de risc afișează un entuziasm de o asemenea anvergură, încât ar face să roșească și un investitor în companii .com din anii 1990. Numai în 2014 și în 2015, în ecosistemul emergent al blockchainului a pătruns un capital de risc în valoare de peste un miliard de dolari, iar rata investițiilor aproape că se dublează anual.⁸ „Suntem foarte încrezători”, spunea Marc Andreessen într-un interviu acordat cotidianului *The Washington Post*, că, „atunci când ne vom regăsi aici peste douăzeci de ani, vom vorbi despre ea [tehnologia blockchain] la fel cum vorbim azi despre internet.”⁹

Organele de reglementare au devenit și ele atente, înființând echipe speciale care să analizeze ce tip de legislație ar avea sens, în caz că ar fi necesară. Guvernele autoritare, cum este cel al Rusiei, au interzis ori au limitat sever utilizarea bitcoinului, așa

*Firmă de obicei nou-înființată, cu o dezvoltare foarte rapidă, care vine în întâmpinarea unei cerințe a pieței prin crearea sau oferirea unui produs, proces sau serviciu inovator. (n.tr.)



cum au procedat și statele democratice care știu că ar fi mai bine să se abțină, cum ar fi Argentina, dată fiind istoria sa marcată de crize monetare. Guvernele mai chibzuite din Vest depun eforturi considerabile pentru înțelegerea modului în care noua tehnologie ar putea să transforme nu doar sistemul bancar centralizat și natura banilor, ci și operațiunile guvernului și natura democrației. Carolyn Wilkins, prim-viceguvernator al Bank of Canada, crede că a venit momentul ca băncile centrale din toată lumea să studieze serios implicațiile transformării integrale a sistemelor monetare naționale în monede digitale. Principalul economist al Băncii Angliei, Andrew Haldane, a propus o monedă națională digitală pentru Marea Britanie.¹⁰

Sunt vremuri tulburi. Desigur, mulțimea din ce în ce mai mare de entuziaști include și un număr de oportuniști, de speculanți și de infractori. Prima poveste pe care o aud oamenii despre monedele digitale este cea a falimentului platformei de tranzacționare Mt. Gox sau a condamnării lui Ross William Ulbricht, fondatorul pieței negre virtuale Silk Road*, care a fost arestat de Biroul Federal de Investigații pentru trafic de droguri, de arme și pornografie infantilă și care utiliza blockchainul bitcoin ca sistem de plăți. Prețul bitcoinilor a fluctuat dramatic, iar deținerea acestora încă rămâne concentrată. Un studiu din 2013 a demonstrat că 937 de persoane dețineau jumătate din totalul de bitcoini, deși lucrul acesta se schimbă în prezent.¹¹

Cum să ajungem de la pornografie și jocuri piramidale la prosperitate? Pentru început, cu excepția cazului în care ești agent de bursă, nu ar trebui să te intereseze bitcoinul, care continuă să rămână un activ speculativ. Subiectul acestei cărți este mai amplu decât activul. Ea discută despre puterea și potențialul platformei tehnologice de bază.

Asta nu înseamnă că bitcoinul sau criptomonedele ar fi lipsite de importanță, așa cum au lăsat să se înțeleagă câteva persoane care se luptă să-și disocieze proiectele de activitățile scandaloase

* În traducere, „Drumul Mătăsi”, dar această piață neagră era o platformă pentru vânzarea de droguri. (n.tr.)



ale trecutului. Aceste monede sunt esențiale pentru revoluția blockchain, care se referă înainte de toate la schimburile de valori *peer-to-peer*, în special de bani.

OBȚINEREA ÎNCREDERII ÎN ERA DIGITALĂ

În afaceri, încrederea înseamnă perspectiva ca partenerul să se comporte conform celor patru principii ale integrității: onestitatea, considerația, responsabilitatea și transparența.¹²

Oonestitatea nu mai este doar o problemă de etică; ea a devenit și o problemă economică. Dacă vor să se bucure de relații bazate pe încredere cu angajații, partenerii, clienții, acționarii și publicul, organizațiile trebuie să comunice adevărul, exact și complet. Fără minciuni prin omisiune, fără confuzii datorate complexității.

În afaceri, **considerația** înseamnă frecvent un schimb echitabil de beneficii sau dezavantaje pe care părțile îl vor realiza cu bună-credință. Dar încrederea presupune un respect autentic pentru interesele, dorințele sau sentimentele celorlalți și posibilitatea ca părțile să poată opera manifestând o bunăvoință reciprocă.

Responsabilitatea înseamnă asumarea unor angajamente clare față de părțile interesate și respectarea acestora. Atât indivizii, cât și instituțiile trebuie să demonstreze că și-au onorat angajamentele și că și-au recunoscut promisiunile încălcate, fiind preferabil ca verificarea lor să fie efectuată chiar de părțile interesate sau de experți independenți din afară. Fără să arunce responsabilitatea pe umerii altora și fără să se joace de-a învinuirea reciprocă.

Transparența înseamnă acțiune la vedere, la lumina zilei. „Oare ce ascund?” este semnul unei transparențe scăzute care conduce la neîncredere. Bineînțeles, companiile sunt perfect îndreptățite să aibă secrete comerciale și alte tipuri de informații asupra cărora există drepturi de proprietate. Dar, când se pune problema informației pertinente pentru clienți, acționari,



angajați și alte părți interesate, deschiderea activă este esențială în vederea câștigării încrederii. În loc să se „îmbrace” ca să atragă succesul, corporațiile pot mai degrabă să se „dezbrace” pentru a avea succes.

În linii mari, încrederea în companii și în alte instituții se află la un minim istoric. „Barometrul încrederii” realizat de compania de relații cu publicul Edelman pe anul 2015 arată că încrederea în instituții, mai ales în corporații, a scăzut până la valorile deplorabile din perioada mării recesiuni din 2008. Edelman observa că până și industria tehnologică, odată impenetrabilă, care s-a menținut ca sectorul cu cea mai ridicată cotă de încredere, a înregistrat, pentru prima dată, scăderi în majoritatea țărilor. La nivel global, directorii generali și oficialii guvernamentali continuă să fie sursele de informație cel mai puțin credibile, clasându-se după experții din mediul academic sau din domeniu.¹³ În mod similar, în sondajul său din 2015, care măsura încrederea americanilor în instituții, Gallup raporta că „afacerile” erau pe penultimul loc între cele cincisprezece instituții măsurate; mai puțin de 20% dintre respondenți indicau că au un nivel considerabil sau ridicat de încredere. Doar Congresul SUA înregistra un scor mai mic.¹⁴

În lumea de dinaintea blockchainului, încrederea în tranzacții decurgea din faptul că persoanele, intermediarii sau alte organizații acționau cu integritate. Cum de cele mai multe ori nu ne putem cunoaște partenerii, ca să nu mai vorbim că nu știm dacă sunt integri sau nu, am ajuns să ne bazăm pe terți care nu doar garantează pentru necunoscuți, ci păstrează înregistrări ale tranzacțiilor și prezintă logica afacerilor și logica tranzacțiilor care alimentează comerțul online. Acești intermediari puternici – băncile, guvernele, PayPal, Visa, Uber, Apple, Google și alte conglomerate digitale – recoltează cea mai mare parte a valorii.

În lumea emergentă a blockchainului, încrederea derivă din rețea, ba chiar și din obiectele din rețea. Carlos Moreira, angajat al companiei de securitate criptografică WISeKey, spunea că noile tehnologii delegă efectiv încrederea – chiar și lucrurilor fizice.



„Dacă un obiect, indiferent dacă este un senzor dintr-un turn de telecomunicații, un bec sau un monitor cardiac, nu prezintă încredere că va funcționa bine sau că se va achita de servicii, va fi respins automat de celelalte obiecte.”¹⁵ Registrul însuși constituie baza încrederii.¹⁶

Pentru a evita confuziile, „încrederea” se referă la cumpărarea și vânzarea de bunuri și servicii și la integritatea și protejarea informațiilor, nu la încrederea în toate demersurile de afaceri. Totuși, în această carte vei citi despre felul în care un registru global ce conține informații adevărate poate să contribuie la încorporarea integrității în toate instituțiile noastre și poate să creze o lume mai sigură și mai demnă de încredere. După părerea noastră, companiile care își derulează o parte sau chiar toate tranzacțiile pe blockchain vor beneficia de o creștere a prețului acțiunilor de pe urma încrederii. Acționarii și cetățenii vor ajunge să pretindă ca toate firmele tranzacționate la bursă și toate organizațiile finanțate din banii contribuabilului să-și administreze cel puțin trezoreriile prin blockchain. Datorită transparenței crescute, investitorii vor putea să determine dacă directorul general chiar a meritat bonusul acela umflat. Contractele inteligente care vor deveni posibile prin blockchainuri le vor cere partenerilor să-și respecte angajamentele, iar alegătorii vor putea să vadă dacă reprezentanții lor spun adevărul sau dacă acționează respectând integritatea fiscală.

ÎNTOARCEREA INTERNETULUI

Prima eră a internetului a început odată cu energia și cu spiritul unui Luke Skywalker tânăr – cu convingerea că orice puști care locuiește pe o planetă dură și deșertică poate să distrugă un imperiu al răului și să pună bazele unei civilizații noi prin lansarea unui .com. Desigur, o idee naivă, dar numeroase persoane, inclusiv autorii, au nutrit speranța că internetul, întruchipat de World Wide Web, avea să revoluționeze lumea industrială, în care puterea era deținută de câțiva, iar structurile de putere erau greu de



escaladat și încă mai greu de răsturnat. Spre deosebire de vechile mijloace de comunicare în masă, care erau centralizate și controlate de forțe puternice și în care utilizatorii erau inerti, noile mijloace erau distribuite și neutre, toți fiind participanți activi, nu receptori pasivi. Costurile scăzute și comunicarea masivă *peer-to-peer* de pe internet aveau să contribuie la subminarea ierarhiilor tradiționale și să ajute la includerea cetățenilor din statele în curs de dezvoltare în economia globală. Valoarea și reputația aveau să fie rezultatul calității contribuției, nu al statutului. Dacă erai inteligent și harnic în India, meritele tale aveau să-ți aducă o reputație. Lumea avea să fie mai uniformă, mai meritocratică, mai flexibilă și mai fluidă. Lucrul cel mai important, tehnologia avea să contribuie la prosperitatea tuturor, nu doar la averea celor puțini.

Câteva dintre aceste lucruri s-au materializat. Au existat colaborări în masă precum Wikipedia, Linux și Galaxy Zoo. Externalizarea și modelele de afaceri de tip rețea le-au oferit oamenilor din țările în curs de dezvoltare șansa de a se integra mai bine în economia globală. În prezent, două miliarde de persoane colaborează social ca egali. Avem cu toții acces la informație în feluri fără precedent.

Cu toate acestea, Imperiul a ripostat. Acum ne este limpede că puterile concentrate din domeniul afacerilor și din guvern și-au subordonat arhitectura democratică originală a internetului după propria lor voință.

În prezent, există instituții uriașe care controlează și dețin aceste noi mijloace de producție și de interacțiune socială – infrastructura care constituie baza acestora; colecții valoroase gigantice și din ce în ce mai mari de date; algoritmi care controlează tot mai mult afacerile și viața de zi cu zi; lumea aplicațiilor; și capacitățile emergente extraordinare, învățarea automată și automobilele autonome. Din Silicon Valley și de pe Wall Street până în Shanghai și Seul, această nouă aristocrație profită de avantajele sale de membru al grupului pentru a exploata cea mai extraordinară tehnologie inventată vreodată, în ideea de a le oferi



oamenilor putere în rolul de actori economici, astfel încât să acumuleze averi spectaculoase și să-și consolideze puterea și influența asupra economiilor și societăților.

Multe dintre temerile legate de latura întunecată exprimate de primii pionieri digitali s-au materializat în cea mai mare parte.¹⁷ Avem creșteri ale produsului intern brut, dar niciun fel de creștere proporțională a numărului de locuri de muncă din majoritatea statelor dezvoltate. Înregistrăm creșteri în crearea bunăstării, dar și inegalități sociale din ce în ce mai mari. Companiile tehnologice puternice și-au mutat o mare parte din activitate de pe Webul deschis, distribuit, egalitarist și aducător de putere în grădini online închise, împrejmuite de ziduri sau în aplicații asupra cărora au drept de proprietate, cu un acces limitat doar la vizualizare* pentru cei din afară, și care, pe lângă alte efecte, reușesc să suprimă dialogul. Forțele corporatiste au capturat multe dintre aceste minunate tehnologii *peer-to-peer*, democratice și deschise și le utilizează pentru a extrage un procent nemăsurat de valoare.

Urmarea este că puterea economică a devenit și mai de neatinș, mai concentrată și mai fermă pe poziții. În loc să fie distribuite mai larg și mai democratic, datele sunt strânse grămadă și utilizate de un număr și mai mic de entități, care le utilizează frecvent pentru a controla și mai multe lucruri și pentru a dobândi și mai multă putere. Dacă acumulezi date și puterea care le însoțește, îți poți consolida în continuare poziția, generând o cunoaștere asupra căreia există drepturi de proprietate. Privilegiul acesta surclasează meritul, indiferent de originile sale.

Mai mult, puternicele „conglomerate digitale”, cum ar fi Amazon, Google, Apple și Facebook – fiecare dintre ele fiind la un moment dat o companie de tip *start-up* în domeniul internetului –, capturează colecțiile valoroase de date generate frecvent de cetățeni și de instituții în silozuri private de date, nu pe Web. Deși

*Este vorba despre *read-only access*, în care utilizatorului i se permite să acceseze anumite fișiere și directoare pe care le poate vizualiza, dar nu le poate aduce modificări și nici șterge. (n.tr.)



crează foarte multă valoare pentru consumatori, una dintre urmări ar fi aceea că datele devin o clasă nouă de active – una care ar putea să eclipseze clasele anterioare de active. O altă consecință este subminarea conceptelor noastre tradiționale despre viața privată și autonomia individuală.

Guvernele de toate tipurile utilizează internetul pentru a-și îmbunătăți operațiunile și serviciile, dar acum au început să utilizeze și tehnologie care să monitorizeze și chiar să manipuleze cetățenii. În multe state democratice, guvernele utilizează tehnologii informaționale și de comunicații pentru a-și spiona cetățenii, a controla opinia publică, a-și promova interesele înguste, a șubrezi drepturile și libertățile și, în general, pentru a se menține la putere. Guvernele represive, cum sunt cel al Chinei și cel al Iranului, îngrădesc internetul, exploatăndu-l pentru a suprima disidența și pentru a-și mobiliza cetățenii în jurul propriilor obiective.

Aceasta nu înseamnă că Webul a murit, cum au sugerat câțiva. Webul este esențial pentru viitorul lumii digitale și ar trebui să susținem cu toții eforturile care se desfășoară deja pentru apărarea lui, cum ar fi cele ale World Wide Web Foundation (Fundația World Wide Web), care luptă să-l mențină deschis, neutru și evoluând constant.

Acum, odată cu apariția tehnologiei blockchain, s-a deschis o întreagă lume de noi posibilități care să inverseze toate aceste tendințe. Acum avem o adevărată platformă *peer-to-peer*, care permite numeroase lucruri interesante pe care le-am discutat în carte. Fiecare dintre noi vom putea să devenim stăpânii propriilor identități și propriilor date personale. Putem să facem tranzacții, să creăm valoare și să o tranzacționăm fără intermediari puternici care să funcționeze ca arbitri ai banilor și ai informației. Miliarde de oameni excluși vor putea să pătrundă în curând în economia globală. Ne putem proteja viața privată și putem exploata financiar propriile informații. Ne putem asigura că cei care creează vor fi plătiți pentru proprietatea lor intelectuală. În loc să încercăm să soluționăm problema inegalității sociale



tot mai mari doar prin redistribuirea bogăției, putem să începem să schimbăm felul în care este *distribuită* bogăția – felul în care este creată din start, în timp ce oamenii de pretutindeni, de la fermieri și până la muzicieni, pot să se bucure mai deplin, a priori, de bogăția pe care o creează. Nu par să existe niciun fel de limite.

Aici vorbim mai degrabă despre Yoda, nu despre Dumnezeu. Dar, chiar dacă nu este divin, acest protocol nou creează condițiile pentru desfășurarea unor colaborări bazate pe încredere, într-o lume în care sunt necesare, și asta înseamnă foarte mult. Încântați? Noi suntem.

AVATARUL TĂU PERSONAL ȘI CUTIA NEAGRĂ A IDENTITĂȚII

De-a lungul istoriei, fiecare formă nouă de media a permis omului să transcendă timpul, spațiul și mortalitatea. Această capacitate – pe care îndrăznim să o numim – divină readuce inevitabil în discuție întrebarea existențială a identității: Cine suntem? Ce înseamnă să fii om? Cum ne conceptualizăm pe noi înșine? Așa cum remarca Marshall McLuhan, în timp, mediul devine mesajul. Oamenii modelează și sunt modelați de media. Creierile noastre se adaptează. Instituțiile noastre se adaptează. Societatea se adaptează.

„În ziua de azi ai nevoie de o organizație care a fost înzestrată cu dreptul de a-ți furniza o identitate, cum ar fi un card bancar, un card pentru clienții fideli ai companiilor aeriene sau un card de credit”¹⁸, ne-a spus Carlos Moreira de la WISeKey. Părinții tăi ți-au dat un nume, obstetricianul sau moașa acreditați de stat care te-au adus pe lume au luat amprenta piciorului tău și au garantat pentru greutatea și înălțimea ta, iar ambele părți au confirmat ora, data și locul venirii tale pe lume, semnându-ți certificatul de naștere. Acum, ei pot înregistra certificatul acesta în blockchain și pot conecta la el atât înștiințările tradiționale legate de naștere, cât și un fond pentru facultate. Prietenii și familia pot să



contribuie cu bitcoini la educația ta superioară. Iată, așa începe fluxul datelor tale.

În primele zile ale internetului, Tom Peters scria: „Tu ești proiectele tale”¹⁹. Voia să spună că afilierea noastră corporatistă și titlaturile posturilor noastre nu ne mai definesc. Ideea echivalentă și tot atât de adevărată din prezent este: „Tu ești datele tale”. „Necazul este că”, după cum ne spune Moreira, „identitatea respectivă este a ta acum, dar datele generate de interacțiunile tale din lume sunt deținute de altcineva”²⁰. Astfel te percep majoritatea corporațiilor și instituțiilor, prin dărele condensate de date de pe internet. Ele îți colectează laolaltă datele într-o reprezentare virtuală a ta și oferă acestui „eu virtual” noi beneficii extraordinare dincolo de cele mai frumoase vise ale părinților tăi.²¹ Dar comoditatea are un preț: viața privată. Cei care spun că „viața privată a murit, las-o baltă” se înșală.²² Viața privată este temelia societăților libere.

„Oamenii au o reprezentare foarte simplistă a identității”²³, ne-a declarat teoreticianul blockchainului Andreas Antonopoulos. Utilizăm cuvântul *identitate* pentru a descrie sinele, proiecția aceluși sine în lume și toate caracteristicile pe care le asociem cu respectivul sine sau cu una dintre proiecțiile sale. Acestea pot să vină de la natură, de la stat, de la organizații private. S-ar putea să avem unul sau mai multe roluri și o serie de parametri atașați acestor roluri, iar rolurile se pot schimba. Să ne gândim la ultimul tău loc de muncă. Rolul tău s-a schimbat organic din cauza schimbărilor din munca propriu-zisă care trebuia făcută sau din cauza revizuirilor prin care a trecut descrierea postului?

Dar dacă „eul tău virtual” ar fi deținut efectiv de tine – ar fi avatarul tău personal – și „ar locui” în cutia neagră a identității tale, astfel încât să-ți poți transforma în bani propriul flux de date și să dezvălui doar ce trebuie atunci când îți exerciți un anumit drept? De ce conține permisul tău de conducere mai multe informații decât faptul că ai trecut de examenul de conducere și ai demonstrat că ai capacitatea de a conduce? Imaginează-ți o nouă eră a Internetului în care avatarul tău personal gestionează și



protejează conținutul cutiei tale negre. Acest soft de încredere care te slujește ar putea să elibereze doar detaliul sau cantitatea de informații solicitată în fiecare situație și, în același timp, să șteargă firimiturile de date care rămân în urma ta în timp ce navighezi prin lumea digitală.

Lucrurile acestea s-ar putea să pară științifico-fantastice, asemenea celor prezentate în filme ca *Matrix* sau *Avatar*. Dar tehnologiile blockchain din ziua de azi le fac posibile. Joe Lubin, directorul general al Consensus Systems, se referă la acest concept prin sintagma „un act de identitate și o imagine publică digitale și persistente” într-un blockchain. „Colegilor mei din facultate le prezint o latură a personalității diferite de cea pe care o afișez atunci când iau cuvântul la Chicago Fed”, a spus el. „În economia digitală online voi reprezenta diferitele mele aspecte și voi interacționa în respectiva lume de pe platforma unor personalități diferite.” Lubin se așteaptă să aibă o „personalitate standard”, o versiune a sa care își plătește impozitele, obține împrumuturi și își face asigurare. „Probabil că voi avea o personalitate în afaceri și o altă personalitate în familie, pentru a separa preocupările pe care aleg să le conectez la personalitatea mea standard. S-ar putea să am o personalitate de jucător pe care să nu o vreau conectată la personalitatea afișată în afaceri. Ba chiar s-ar putea să am o personalitate pentru webul întunecat care nu poate fi niciodată conectată la celelalte.”²⁴

Cutia ta neagră ar putea să includă informații cum ar fi actele de identitate emise de guvern, numărul de la Asigurările Sociale, informațiile medicale, conturile pentru servicii, conturile financiare, diplomele, drepturile de practică, certificatul de naștere, diferite alte acreditări și informații atât de personale încât nu vrei să le dezvălui, dar cărora vrei să le determini valoarea monetară, cum ar fi preferințele sexuale sau starea de sănătate, pentru un sondaj sau pentru o cercetare. Ai putea să cedezi dreptul de folosire a acestor date pentru anumite obiective unor entități specifice pentru perioade determinate de timp. Ai putea să trimiți un

* Federal Reserve Bank of Chicago (Banca Rezervelor Federale din Chicago). (n.tr.)



subset al caracteristicilor tale oftalmologului și un subset diferit fondului speculativ, în care ai vrea să investești. Avatarul tău ar putea să răspundă la întrebări prin „da” sau „nu”, fără să dezvăluie cine ești: „Ai douăzeci și unu de ani sau peste? Ai câștigat peste 100.000 de dolari anual în ultimii trei ani? Ai un indice de masă corporală cuprins între limite normale?”²⁵.

În lumea fizică, reputația ta este locală – proprietarul magazinului local, angajatorul tău, prietenii de la o petrecere, toți au o anumită părere despre tine. În economia digitală, reputațiile diferitelor personalități ale avatarului tău vor fi portabile. Portabilitatea va contribui la introducerea oamenilor din întreaga lume în economia digitală. Oamenii cu un portofel și un avatar digital care locuiesc în Africa și-ar putea demonstra reputația necesară, spre exemplu, pentru a împrumuta bani să demareze o afacere. „Vezi, toți oamenii aceștia mă cunosc și garantează pentru mine. Sunt demn de încredere din punct de vedere financiar. Sunt un cetățean emancipat al economiei digitale globale.”

Identitatea reprezintă doar o parte mică din asta. Restul este o nebuloasă – o nebuloasă a identității – formată din microparticule legate mai puternic sau mai slab de identitatea ta. Dacă încercăm să le înregistrăm pe toate în blockchain, un registru imuabil, nu vom pierde doar nuanțele interacțiunii sociale, ci vom pierde și darul uitării. Oamenii nu ar trebui să fie definiți niciodată după cea mai proastă zi a lor.

UN PLAN PENTRU PROSPERITATE

În această carte vei citi zeci de povești despre inițiative care au devenit posibile datorită acestui protocol al încrederii care creează oportunități noi pentru o lume mai prosperă. Mai întâi de toate, prosperitatea se referă la nivelul de trai. Pentru a-l putea atinge, oamenii trebuie să aibă mijloacele, instrumentele și oportunitățile cu care să creeze bogăție materială și să beneficieze de condiții economice prielnice. Dar pentru noi implică mai mult de-atât – siguranța persoanei, securitate, sănătate, educație,



dezvoltarea durabilă a mediului, șansa de a-ți modela și controla propriul destin și de a participa în economie și în societate. Pentru a se putea bucura de prosperitate, oamenii trebuie să aibă un minim acces la o formă de servicii financiare de bază, pentru a putea înmagazina și transfera valoarea în mod fiabil, la comunicații, la instrumente de tranzacționare prin care să se conecteze la economia globală și la securitatea, protecția și garantarea titlurilor de proprietate pentru pământ și pentru alte active pe care le dețin legal.²⁶ Aceasta și altele sunt promisiunea blockchainului. Relatările pe care le vei citi ar trebui să-ți contureze imaginea unui viitor în care va exista prosperitate pentru toată lumea, nu doar mai multă bogăție și mai multă putere pentru cei bogați și puternici. Poate chiar imaginea unei lumi în care suntem stăpâni pe datele noastre și ne putem apăra viața privată și securitatea personală. O lume deschisă în care să putem contribui cu toții la infrastructura noastră tehnologică, nu o lume cu grădini împrejmuite de ziduri, în care companiile mari oferă aplicații pentru care au drepturi de proprietate. O lume în care miliarde de oameni excluși pot să ia parte acum la economia globală și să se bucure de generozitatea ei. Iată o avanpremieră.

Crearea unei adevărate economii de partajare *peer-to-peer*

Experții vorbesc adeseori despre Airbnb, Uber, Lyft, TaskRabbit și altele ca despre platforme pentru „economia de partajare”. Este o noțiune elegantă – persoane egale creează valoare și participă la repartizarea ei. Dar aceste companii au foarte puțin de-a face cu partajarea. În realitate, ele au succes tocmai pentru că nu împart nimic – strâng totul la un loc. Avem de-a face cu o economie de agregare. Uber este o corporație de 65 de miliarde de dolari ce reunește servicii de taximetrie. Airbnb, site-ul preferat în valoare de 25 de miliarde de dolari al celor din Silicon Valley, adună la un loc locurile libere de cazare. Altele colectează echipamente sau meseriași prin platformele lor centralizate, asupra cărora au drepturi de autor, și apoi le vând mai departe. Pe parcursul



desfășurării procesului, ele colectează date pe care le vor exploata comercial. Niciuna dintre companiile acestea nu exista cu un deceniu în urmă, pentru că nu fuseseră create precondițiile tehnologice: telefoane inteligente prezente pretutindeni, GPS și sisteme sofisticate de plată. Acum, odată cu blockchainurile, există tehnologia necesară pentru reinventarea acestor domenii. Marii revoluționari ai zilei urmează să fie victimele unei revoluții.

În locul companiei centralizate Airbnb, imaginează-ți o aplicație distribuită – să o numim Airbnb blockchain sau bAirbnb –, în principiu, o cooperativă deținută de membrii săi. Atunci când cineva care caută să închirieze vrea să găsească o listă cu locuințe, softul bAirbnb scanează blockchainul căutând toate intrările, le filtrează și le afișează pe cele care satisfac criteriile. Cum rețeaua creează o înregistrare a tranzacției în blockchain, o recenzie pozitivă din partea utilizatorului le mărește reputațiile și le consacără identitățile – de data aceasta fără niciun intermediar. Vitalik Buterin, fondatorul blockchainului Ethereum, spune următoarele: „În timp ce majoritatea tehnologiilor au tendința să automatizeze, împingând muncitorii la periferie unde execută munci mărunte, blockchainurile automatizează și dizolvă centrul. În loc să lase taximetriștii fără loc de muncă, blockchainul lasă Uber-ul șomer și le permite taximetriștilor să lucreze direct cu consumatorul”²⁷.

Restructurarea sistemului financiar urmărind viteza și incluziunea

Industria serviciilor financiare ajută actuala economie globală să meargă ca pe roate, dar, în prezent, sistemul este plin de probleme. Spre exemplu, este fără îndoială cel mai centralizat sector din lume și ultimul domeniu în care se face simțit efectul transformățional al revoluției tehnologice. Bastioanele vechii ordini financiare, cum ar fi băncile, încearcă din răspuțeri să apere monopolurile și blochează adeseori inovațiile revoluționare. În plus, sistemul financiar funcționează pe o tehnologie învechită și este guvernat



prin reglementări care datează de la jumătatea secolului al XIX-lea. Este plin de contradicții și de progrese inegale care îl fac ocazional lent, de multe ori nesigur și în mare parte obscur pentru părțile interesate.

Tehnologia registrului distribuit poate să elibereze o mulțime de servicii financiare din chingile vechilor instituții, încurajând competiția și inovația. Lucrul acesta este bun pentru utilizatorul final. Chiar și atunci când au acces la vechiul internet, miliarde de oameni sunt excluși din economie din simplul motiv că instituțiile financiare nu le oferă servicii de genul bankingului, deoarece ar fi clienți neprofitabili și riscanți. După apariția blockchainului, nu doar că acești oameni vor ajunge să se conecteze, ci, și mai important, vor fi incluși în activitatea financiară, putând să cumpere, să împrumute, să vândă și să aibă în general posibilitatea de a-și crea o viață prosperă.

Instituțiile care ocupă poziții dominante similare se pot transforma în jurul tehnologiei blockchainului, dacă vor găsi leadershipul care să reușească aceasta. Tehnologia are un potențial foarte mare pentru a revoluționa domeniul în bine – de la bănci la burse de valori, de la companii de asigurări la firme de contabilitate, firme de brokeraj, microcreditori, rețele de carduri de credit, agenți imobiliari și tot ce este cuprins între ele. Când toată lumea utilizează același registru distribuit, decontările nu durează zile întregi, ele se produc imediat, în văzul tuturor. Miliarde de oameni vor avea de câștigat, iar această transformare ar putea să-i elibereze și să confere putere antreprenorilor din întreaga lume.

Protejarea globală a drepturilor economice

Drepturile de proprietate sunt atât de inexorabil legate de sistemul democrației noastre capitaliste încât prima versiune preliminară a Declarației de Independență elaborată de Jefferson enumera viața, libertatea și căutarea *proprietății*, nu a fericirii, ca drepturi inalienabile ale omului.²⁸ În timp ce aceste crezuri pline



de aspirații puneau bazele societății și economiei moderne de care ne bucurăm în cea mai mare parte a lumii dezvoltate, nici până în ziua de azi o mare parte din populația lumii nu se bucură de beneficiile acestora. Chiar dacă s-au înregistrat câteva progrese la capitolele viață și libertate, majoritatea proprietarilor din lume își pot vedea căminul sau bucățița de pământ confiscate arbitrar de funcționari guvernamentali corupți, prin simpla apăsare a unui buton în programul bazei guvernamentale centralizate cu datele despre proprietate. În absența unui act care să dovedească deținerea proprietății, proprietarii de terenuri nu pot să obțină un credit, un permis de construcție și nici să-și vândă proprietatea, dar pot fi expropriați – toate acestea constituind impedimente serioase în calea prosperității.

Hernando de Soto, economist peruan și președinte al Institutului pentru Libertate și Democrație, una dintre cele mai strălucite minți economice ale lumii, sugerează că aproape cinci miliarde de persoane din întreaga lume sunt împiedicate să participe integral la valoarea creată prin globalizare, din cauza fragilității drepturilor lor de proprietate asupra propriilor terenuri. El susține că blockchainul ar putea să schimbe situația. „Idea centrală a blockchainului este că drepturile asupra bunurilor pot fi tranzacționate, indiferent dacă sunt financiare, active fizice sau idei. Obiectivul nu este doar acela de a înregistra parcela de teren, ci de a înregistra drepturile implicate, astfel încât deținătorul lor să nu poată fi deposedat.”²⁹ Drepturile universale de proprietate ar putea să pună bazele unei agende noi pentru dreptate globală, creștere economică, prosperitate și pace. În această paradigmă nouă, drepturile sunt protejate de tehnologie, nu de miliții sau de soldați gata să intervină în orice moment. „Blockchainul este adecvat pentru o lume guvernată de lucruri reale, nu de lucruri fictive. Și cred că lucrul acesta este bun”³⁰, recunoaște de Soto. Și este descentralizat. Nu e controlat de vreo autoritate centrală, toată lumea știe ce se întâmplă și ține minte pentru totdeauna.



Sfârșitul jafului din transferurile de bani în străinătate

Aproape toate rapoartele, articolele sau cărțile care trec în revistă beneficiile criptomonedelor discută oportunitatea transferurilor de bani în străinătate. Și pe bună dreptate. Cel mai mare flux de fonduri către statele în curs de dezvoltare nu este reprezentat nici de ajutorul extern, nici de investițiile externe directe. În realitate, este vorba de fluxul banilor transferați, repatriați în statele sărace de diasporele acestora stabilite în străinătate. Procesul presupune timp, răbdare și uneori curaj pentru a merge în fiecare săptămână în același cartier sărăcăcios, unde se află biroul prin care se derulează trimiterea banilor, pentru a completa aceleași formulare de fiecare dată și pentru a plăti același comision de 7%. Există o modalitate mai bună.

Abra și alte companii dezvoltă rețele de plăți care utilizează blockchainul. Obiectivul Abra este acela de a-și transforma absolut toți utilizatorii în casieri. Întregul proces – de la plecarea fondurilor dintr-o țară și până la sosirea lor în alta – durează o oră, nu o săptămână, și costă 2% în loc de 7% sau mai mult. Abra își dorește ca rețeaua sa de plăți să depășească numeric toate bancomatele fizice din lume. Western Union a avut nevoie de 150 de ani pentru a ajunge la 500.000 de agenți în întreaga lume. Abra va atinge numărul acesta de casieri în primul său an.

Eliminarea birocrăției și corupției ce caracterizează ajutoarele externe

Oare ar putea blockchainul să soluționeze problemele ajutorului extern? Cutremurul din 2010 din Haiti a fost unul dintre cele mai ucigătoare dezastre naturale din istoria scrisă. Au pierit între 100.000 și 300.000 de oameni. În perioada imediat următoare, guvernul din Haiti s-a dovedit a fi el însuși o responsabilitate. Comunitatea globală a donat peste 500 de milioane de dolari Crucii Roșii, o instituție cunoscută. O investigație ulterioară a



dezvăluit faptul că fondurile au fost cheltuite prost sau au dispărut complet.

Blockchainul poate să amelioreze distribuirea ajutorului extern prin eliminarea intermediarilor care iau ajutorul înainte să ajungă la destinație. În al doilea rând, ca registru permanent al circulației fondurilor, blockchainul determină instituțiile să devină mai responsabile pentru acțiunile lor. Imaginează-ți ce s-ar întâmpla dacă ai putea să urmărești fiecare dolar pe care l-ai donat Crucii Roșii din punctul de plecare de pe telefonul tău mobil până la persoana pe care a ajutat-o. Ai putea să-ți plasezi banii într-un cont escrow*, eliberând diverse sume după ce Crucea Roșie mai îndeplinește câte o condiție.

Recompensarea prioritară a creatorilor de valoare

În timpul primei generații a internetului, numeroși creatori de proprietate intelectuală nu au fost recompensați în mod adecvat. Prima probă este reprezentată de muzicienii și compozitorii care au semnat cu case de discuri ai căror șefi nu au reușit să-și imagineze felul în care internetul avea să le influențeze domeniul. Ei nu au reușit să se adapteze erei digitale și să-și reinventeze modelele de afaceri, cedând lent puterea distribuitorilor inovatori din mediul online.

Gândește-te cum au reacționat principalele case de discuri față de Napster, platforma de distribuire *peer-to-peer* a fișierelor din domeniul muzicii, lansată în 1999. Liderii de atunci ai industriei muzicale au făcut front comun pentru a da în judecată compania, fondatorii acesteia și un număr de *optsprezece mii de utilizatori ai ei*, dezintegrând platforma până în iulie 2001. Alex Winter, regizorul unui documentar despre Napster, a declarat

* Cont *escrow* - depozit colateral care are ca scop principal protejarea participanților la tranzacții comerciale; principala lui caracteristică este că permite depunerea sumelor în favoarea beneficiarului, însă ridicarea acestora este condiționată de îndeplinirea unor condiții contractuale. (n.red.)



pentru *The Guardian*: „Eu am o problemă cu gândirea în alb și negru aplicată marilor schimbări culturale... În cazul platformei Napster exista o porțiune enormă de gri cuprinsă între poziția «Pot să distribui tot ce am cumpărat» și punctul de vedere «Ești un infractor chiar și atunci când distribui un singur fișier dintre cele pe care le-ai cumpărat»³¹.

Noi suntem de acord. De obicei, cocreația împreună cu consumatorii este un model de afacere mai sustenabil decât darea lor în judecată. Tot acest incident a pus industria muzicală în lumina fierbinte a reflectoarelor, dezvăluind toate tacticile sale depășite de marketing, ineficiențele sale masive de distribuție și ceea ce unii au numit politici antimuzicieni.

De atunci s-au schimbat foarte puține lucruri. Până acum. Vom arunca o privire la noul ecosistem al muzicii care se naște pe blockchain, sub conducerea cântăreței și compozitoarei britanice Imogen Heap, a violoncelistei Zoë Keating și a dezvoltatorilor și antreprenorilor blockchainului. Toate industriile culturale sunt pregătite pentru transformări revoluționare, iar promisiunea pe care o fac este că vor recompensa complet creatorii pentru valoarea pe care o creează.

Reconfigurarea corporației ca motor al capitalismului

Odată cu creșterea unei platforme globale *peer-to-peer* pentru identitate, încredere, reputație și tranzacții, vom putea în cele din urmă să reelaborăm structurile profunde ale firmei în vederea inovației, creării de valoare distribuită și poate chiar a prosperității celor mulți, nu a bogăției celor puțini. Lucrul acesta nu înseamnă firme mai mici în termenii impactului sau veniturilor. Dimpotrivă, discutăm despre construirea companiilor secolului XXI, câteva dintre ele putând să devină creatori masivi de bogăție și lideri pe propriile piețe. Noi credem că întreprinderile vor semăna mai mult cu rețelele decât cu ierarhiile verticale integrate



ale erei industriale. Ca atare, există posibilitatea unei distribuirii (nu redistribuirii) mai democratice a bogăției.

Vom face o scurtă incursiune și prin lumea absolut amețitoare a contractelor inteligente, a noilor agenți economici autonomi și a ceea ce a primit numele de întreprinderi autonome distribuite, în care softul inteligent preia controlul asupra conducerii și organizării a numeroase resurse și capacități, înlăturând poate corporațiile. Contractele inteligente permit înființarea a ceea ce numim întreprinderi deschise de tip rețea care se bazează pe un set nou de modele de afaceri sau pe modele vechi care utilizează blockchainul.

Animarea obiectelor și punerea lor la muncă

Specialiștii în tehnologie și scriitorii de literatură științifico-fantastică și-au imaginat multă vreme o lume în care o rețea globală unitară de senzori conectați la internet ar putea să capteze fiecare eveniment, acțiune sau schimbare de pe pământ. Tehnologia blockchain va permite lucrurilor să colaboreze, să facă schimb de unități de valoare – energie, timp și bani – și să reconfigureze lanțurile de aprovizionare și procesele de producție, în funcție de informația distribuită despre cerere și capacitate. Putem să atașăm metadatele* la dispozitive inteligente, să le programăm să recunoască alte obiecte după metadatele acestora și să acționeze sau să reacționeze la anumite circumstanțe fără pericolul erorii sau al vicierii.

În timp ce lumea fizică se trezește la viață, toată lumea poate să prospere – de la micii fermieri din brusa australiană, care au nevoie de energie electrică pentru afacerile lor, și până la proprietarii de locuințe din întreaga lume, care pot să devină membri ai unei rețele electrice distribuite prin blockchain.

* *Meta* - element de compunere în cadrul unor substantive sau adjective însemnând „după” sau exprimând noțiunea de transformare, de schimbare. (n.red.)



Cultivarea antreprenorului de blockchain

Antreprenoriatul este esențial pentru o economie înfloritoare și o societate prosperă. Internetul trebuia să elibereze antreprenorii, oferindu-le instrumentele și capacitățile marilor companii, lăsând la o parte numeroase obligații, cum ar fi cultura moștenită, procesele osificate și balastul inutil. Cu toate acestea, succesul fulminant al miliardarilor .com împinge într-un con de umbră un adevăr neliniștitor: antreprenoriatul și deschiderea de noi afaceri au înregistrat un declin constant pe parcursul ultimilor treizeci de ani în numeroase economii dezvoltate.³² În statele în curs de dezvoltare, internetul a făcut prea puțin pentru a coborî barierele pentru viitorii antreprenori, care trebuie să îndure birocrații guvernamentale deconcertante. Internetul nu a deblocat nici instrumentele financiare esențiale pentru înființarea unei afaceri și nici nu le-a pus la dispoziția miliardelor de oameni. Bineînțeles, nu suntem toți meniți să devenim antreprenori, dar absența instrumentelor financiare și răspândirea procedurilor birocratice îngreunează chiar și eforturile omului de rând, care încearcă doar să câștige un salariu decent.

Problema este complexă, dar blockchainurile pot să contribuie la supraalimentarea antreprenoriatului și, prin urmare, la prosperitate, în multe feluri importante. Pentru a obține acces la un loc în care să poată depozita fără grijă valoarea și la o modalitate de a face afaceri în afara propriei comunități, omul de rând care trăiește în statele în curs de dezvoltare nu are nevoie decât de un dispozitiv conectat la internet. Accesul la economia globală înseamnă un acces mai mare la noi surse de credit, de finanțare, la noi furnizori, parteneri și oportunități de investiții. Niciun talent sau resursă nu sunt prea mici pentru a nu putea primi o valoare monetară în blockchain.



Formarea unor guverne de către popor pentru popor

Pregătește-te pentru schimbări mari atât în sfera guvernului, cât și în cea a guvernării. Tehnologia blockchain revoluționează deja mașinăria guvernamentală și modul în care o putem face să obțină performanțe ridicate – mai bine și mai ieftin. Aceasta creează, de asemenea, noi oportunități de schimbare a democrației înseși – prin felul în care guvernele pot să devină mai deschise și mai independente față de controlul grupurilor de interese și să aibă un comportament în acord cu cele patru valori ale integrității. Examinăm felul în care tehnologiile blockchain pot să transforme semnificația calității de cetățean și a participării la procesul politic, de la vot la accesarea serviciilor sociale, și de la rezolvarea unora dintre problemele mari și dificile ale societății până la tragerea la răspundere a reprezentanților aleși pentru neîndeplinirea promisiunilor care i-au ajutat să câștige alegerile.

PROMISIUNEA ȘI PERICOLUL NOII PLATFORME

Dacă există șase milioane de oameni în *The Naked City*³³, avem șase milioane de obstacole peste care trebuie să treacă această tehnologie pentru a-și îndeplini potențialul. În plus, există câteva dezavantaje îngrijorătoare. Unii spun că tehnologia nu este pregătită pentru o audiență maximă; utilizarea ei este în continuare dificilă, iar aplicațiile extraordinare abia se nasc. Alți critici ne semnaleză cantitatea uriașă de energie consumată doar în rețeaua bitcoin pentru a se ajunge la consens: Ce se va întâmpla atunci când mii sau milioane de blockchainuri interconectate vor procesa fiecare miliarde de tranzacții în fiecare zi? Sunt stimulentele suficient de mari pentru ca oamenii să participe și să se comporte prudent de-a lungul timpului și să nu încerce să domine rețeaua? Tehnologia blockchain este oare cel mai periculos distrugător de joburi?

Acestea nu sunt întrebări legate de tehnologie, ci de leadership și guvernare. Prima perioadă a Internetului s-a lansat datorită viziunii și intereselor comune ale principalelor părți



interesate – guverne, organizații ale societății civile, dezvoltatori și oameni obișnuiți ca tine. Blockchainul are nevoie de un leadership similar. Vom discuta pe larg în carte de ce liderii noii paradigme distribuite vor trebui să-și confirme rolul și să dea drumul unui val de inovație economică și instituțională, pentru a garanta că de data aceasta promisiunea va fi respectată. Te invităm să intri în rândurile lor.

Această carte a apărut ca urmare a programului Global Solution Networks – în valoare de 4 milioane de dolari – din cadrul Rotman School of Management, Universitatea din Toronto. Finanțat în principal de marile corporații specializate în tehnologie și de fundațiile Rockefeller și Skoll, de Departamentul de Stat al SUA și de agenția guvernamentală Industry Canada, inițiativa a explorat noi abordări în materie de rezolvare a problemelor globale și de guvernare. Am fost amândoi implicați în desfășurarea programului. (Don l-a înființat; Alex a condus proiectul despre criptomonede.) În 2014, am lansat o întreprindere de cercetare cu durata de un an pe tema revoluției declanșate de blockchain și a implicațiilor sale pentru afaceri și societate, culminând cu această carte. În cadrul ei am încercat să privim dintr-o perspectivă adecvată promisiunea și pericolele noii platforme.

Dacă inovatorii din afaceri, din guvern și din societatea civilă acționează cum trebuie, vom trece de la un internet animat în principal de costurile în scădere ale căutării, coordonării, colectării de date și luării de decizii – în care obiectivul consta în monitorizarea, medierea și stabilirea unei valori monetare a informației și a tranzacțiilor de pe Web – la unul animat de costurile în scădere ale negocierii, reglementării și respectării acordurilor sociale și comerciale, în care obiectivul va fi reprezentat de integritate, securitate, colaborare, confidențialitatea tuturor tranzacțiilor și crearea și distribuirea valorii. Este vorba de o reorientare la 180 de grade a strategiei. Rezultatul poate fi o economie a egalilor cu instituții care sunt cu adevărat distribuite, globale și aducătoare de putere – și, prin urmare, legitime. Schimbând fundamental ceea ce putem să facem online, felul în



care o facem și cine poate participa, noua platformă ar putea chiar să creeze condițiile tehnologice pentru aplanarea unora dintre cele mai exasperante probleme economice și sociale.

Dacă nu facem ce trebuie, tehnologia blockchain, care promite atât de mult, va fi îngrădită sau chiar zdrobită. Și mai grav, ar putea să devină un instrument pe care instituțiile puternice să îl utilizeze pentru a-și consolida bogăția sau, dacă este deturnată de guverne, o platformă pentru un nou tip de societate a supravegherii. Tehnologiile strâns înrudite ale softului distribuit, criptografiei, agenților autonomi și chiar ale inteligenței artificiale ar putea să scape de sub control și să se întoarcă împotriva ființelor umane care le-au creat.

Există posibilitatea ca această tehnologie nouă să fie întârziată, blocată, subutilizată sau mai rău. Blockchainul și criptomonedele, în special bitcoinul, au luat deja un avânt uriaș, dar nu putem prezice dacă vor reuși sau nu și, în cazul în care reușesc, cât de repede se va întâmpla asta.³⁴ Predicțiile sunt întotdeauna demersuri riscante. Teoreticianul tehnologiei David Ticoll recunoaște: „Mulți dintre noi nu am făcut o treabă bună atunci când am prezis impactul integral al Internetului. Printre lucrurile care ne-au scăpat se numără fenomenele dăunătoare de tipul ISIS-ului, iar câteva predicții mari și optimiste s-au dovedit eronate”. El continuă: „Dacă blockchainul este la fel de mare și de universal ca Netul, avem șanse mari să facem o treabă la fel de proastă prezicând atât avantajele, cât și dezavantajele acestuia”³⁵.

Așa că, în loc să prezicem un viitor al blockchainului, noi pleddăm în favoarea sa. Susținem că ar trebui să reușească, deoarece ne-ar putea ajuta să intrăm într-o nouă eră a prosperității. Noi credem că economia funcționează cel mai bine atunci când funcționează pentru toți, iar această nouă platformă este un motor de incluziune. Diminuează drastic costul transmiterii unor fonduri precum transferurile de bani în străinătate. Reduce semnificativ bariera din calea deținerii unui cont bancar, obținerii unui credit și investirii. Și sprijină antreprenoriatul și participarea la



comerțul global. Catalizează capitalismul distribuit, nu doar un capitalism redistribuit.

Toată lumea ar trebui să înceteze să i se opună și să facă pașii potriviți pentru a i se alătura. Hai să nu punem această forță la treabă în folosul imediat al celor puțini, ci în folosul durabil al celor mulți.

Azi suntem amândoi încântați de potențialul acestei reprize secunde a internetului. Suntem entuziasmați de noul val masiv de inovație care se dezlănțuie, de potențialul său de prosperitate și de crearea unei lumi mai bune. Cartea aceasta este pledoaria noastră pentru a-ți stârni interesul, pentru a înțelege acest viitor val și pentru a-ți lua măsuri de asigurare că promisiunea este respectată.

Așa că ține-te bine și citește mai departe! Ne aflăm într-unul dintre acele momente esențiale ale istoriei umane.

CAPITOLUL 2

INIȚIALIZAREA* VIITORULUI: ȘAPTE PRINCIPII DE PROIECTARE A ECONOMIEI BLOCKCHAINULUI

„Libertatea depinde de viața privată”, a declarat Ann Cavoukian, director executiv al Privacy and Big Data Institute din cadrul Universității Ryerson. „Am aflat asta pentru prima dată acum treizeci de ani, când am început să merg la conferințe în Germania. Nu e deloc întâmplător că Germania este țara care ocupă locul întâi la nivel mondial în domeniul confidențialității și protecției datelor. Locuitorii ei au trebuit să îndure abuzurile celui de-al Treilea Reich și anularea completă a tuturor libertăților lor, lucruri care au început cu eliminarea totală a dreptului la viață privată. Când s-a terminat cu asta, au zis: «Nu se va mai întâmpla niciodată»”¹.

Astfel că este ironic – sau perfect potrivit – ca una dintre primele platforme informatice descentralizate *peer-to-peer* care garantează confidențialitatea utilizatorului să se numească Enigma, care este și numele pe care l-a primit aparatul inventat de inginerul german Arthur Scherbius, pentru transcrierea informațiilor criptate. Scherbius a proiectat Enigma pentru utilizări comerciale: prin intermediul aparatului său, companiile globale puteau

* *Bootstrapping*, în original – termen folosit în informatică și care se referă la procesul de pornire a unei secvențe de inițializare sau la cel de încărcare a unui sistem de operare. (n.red.)



să-și transmită rapid și în siguranță secretele comerciale, ponturile bursiere și alte informații cu acces privilegiat. În decurs de câțiva ani, forțele armate germane produceau primele versiuni ale Enigmei pentru a transmite prin radio mesaje cifrate pentru trupe. În timpul războiului, naziștii au utilizat Enigma pentru a difuza planurile strategice, detaliile obiectivelor și sincronizarea atacurilor. Era un instrument al suferinței și al oprimării.

Enigma noastră contemporană este un instrument al libertății și al prosperității. Proiectat în Laboratorul Media din cadrul MIT de Guy Zyskind și de Oz Nathan, noua Enigmă îmbină virtuțile registrului public al blockchainului, a cărui transparentă „oferă stimulente puternice pentru un comportament onest”, cu ceva cunoscut sub numele de *criptare homomorfică** și *calcule securizate între mai multe părți*². Spus mai simplu, „Enigma ia informația – orice informație –, o sparge în bucăți și o criptează în fragmente de date care sunt distribuite aleatoriu spre noduri din cadrul rețelei. Nu se află într-un singur loc”, a zis Cavoukian. „Enigma utilizează tehnologia de tip blockchain pentru a integra datele și pentru a urmări toate fragmentele de informație.”³ O poți pune la dispoziția unor terți și acești terți o pot utiliza în calcule fără ca măcar să o decripteze vreodată.⁴ Dacă funcționează, ar putea să reconfigureze felul în care ne abordăm propria identitate online. Imaginează-ți că ai o cutie neagră care conține informațiile tale personale și tu ești singurul care o poate controla și accesa.

Indiferent cât de grozav ar putea să pară, există motive întemeiate pentru a pași cu multă grijă peste granița criptografică. În primul rând, trebuie să formeze cumva o rețea largă de participanți. În al doilea rând, „criptografia este un domeniu în care nu vrei niciodată să utilizezi cele mai noi și mai grozave instrumente, pentru că avem o istorie întreagă de algoritmi pe care toată lumea îi credea siguri, erau utilizați timp de patru sau cinci ani, apoi apărea un om de știință foarte inspirat care ieșea la rampă și

* *Homomorphic* - în matematică reprezintă transformarea unui set în altul capabil să păstreze operațiile dintre membrii celui dintâi. (n.red.)



declara că există o breșă, astfel că se alegea praful de toată treaba”, a declarat Austin Hill de la Blockstream. „Acesta este motivul pentru care noi preferăm în general algoritmi foarte conservatori, foarte bine consacrați, cu un trecut îndelungat. Lucrurile acestea sunt gândite luând foarte mult în calcul evoluțiile viitoare, iar bitcoinul a fost proiectat având în minte acest obiectiv.”⁵

Totuși, din moment ce are implicații profunde în domeniile confidențialității, securității și sustenabilității, conceptul merită luat foarte în serios. „Ei susțin că Enigma ne oferă ceva care garantează confidențialitatea”, ne-a spus Cavoukian. „Afirmția lor nu este deloc modestă, dar exact de genul acesta de lucruri avem din ce în ce mai multă nevoie în actuala lume conectată și interconectată.”⁶

În cercetarea noastră ne-am intersectat cu câteva proiecte inițiate în domeniul tehnologiilor blockchain, ai căror dezvoltatori aveau aspirații similare de a face posibile drepturile fundamentale ale omului – nu doar dreptul la viață privată și la securitate, ci și drepturile de proprietate, de recunoaștere a calității de persoană în baza legii și de participare la guvernare, la cultură și economie. Imaginează-ți o tehnologie care ar putea să ne păstreze libertatea de a alege pentru noi înșine și pentru familiile noastre, de a ne exprima aceste alegeri în lume și de a ne controla propriul destin, indiferent unde am locuit sau unde ne-am născut. Ce noi instrumente și ce locuri noi de muncă am putea să creăm cu aceste capacități? Ce noi afaceri și servicii? Cum ar trebui să ne gândim la oportunități? Răspunsurile se aflau chiar sub ochii noștri, fiind dăruite de Satoshi Nakamoto.

CELE ȘAPTE PRINCIPII DE PROIECTARE

Noi credem că această nouă eră ar putea fi inspirată de viziunea lui Satoshi Nakamoto, proiectată în jurul unui set de principii implicite și realizată de spiritul colaborator al numeroșilor lideri pasionați și la fel de talentați din cadrul comunității.



Măreța sa viziune s-a limitat la bani, nu la obiectivul mai amplu al creării celei de-a doua generații a internetului. Nu exista nicio discuție despre reinventarea firmei, despre schimbarea instituțiilor noastre sau despre transformarea civilizației în bine. Chiar și așa, viziunea lui Satoshi a fost uluitoare în simplitatea, originalitatea și perspectiva pe care o avea asupra omenirii. Celor care au citit articolul din 2008 le-a fost limpede că urma să înceapă o nouă eră a economiei digitale. În timp ce prima eră a economiei digitale a fost declanșată de convergența tehnologiilor de calcul și de comunicații, această a doua eră va fi alimentată de o combinație inteligentă între ingineria informatică, matematică, criptografie și economia comportamentală.

Interpretul de muzică folk Gordon Lightfoot cânta emoționant: „Dacă ai putea citi în mintea mea, iubire, ce poveste ți-ar spune gândurile mele”. Satoshi s-a retras, refuzând orice fel de comunicare din 2011 (deși numele lui mai apare pe forumurile de discuții din când în când), dar noi credem că protocolul încrederii pe care l-a inițiat poate fi utilizat la reconfigurarea instituțiilor și economiei noastre.

Toți cei cu care am stat de vorbă au fost nerăbdători să ne împărtășească idei despre tehnologia blockchain. Fiecare conversație, fiecare raport oficial, fiecare subiect de pe forum a scos la suprafață un număr de teme pe care le-am transformat prin inginerie inversă în principii de proiectare – principii pentru crearea de soft, servicii, modele de afaceri, piețe, organizații și chiar guverne pe baza blockchainului. Satoshi nu a scris niciodată despre aceste principii, dar ele sunt implicite în platforma tehnologică pe care a eliberat-o. Noi le vedem ca pe niște principii care vor contura următoarea eră a economiei digitale și o eră a încrederii reînnoite.

Dacă ești nou în acest spațiu, noi sperăm că principiile te vor ajuta să înțelegi elementele de bază ale revoluției blockchain. Chiar dacă ești un sceptic de neclintit față de blockchainul bitcoin, ele tot îți vor fi de folos în timp ce îți contempli viitorul ca antreprenor, inventator, inginer sau artist care caută colaborări



active cu oameni ce au viziuni similare, ca proprietar sau investitor în active de tot felul; sau ca manager care vrea să-și reimagineze rolul în această economie a blockchainului pe cale să se nască.

1. Integritatea în rețea

Principiu: Încrederea este intrinsecă, nu extrinsecă. Integritatea este codificată în fiecare etapă a procesului și este distribuită, nu este investită într-un singur membru. Participanții pot să facă schimb direct de valori, așteptându-se ca partea cealaltă să acționeze cu integritate. Asta înseamnă că valorile integrității – onestitatea propriilor vorbe și fapte, considerația pentru interesele celorlalți, responsabilitatea față de consecințele propriilor decizii și acțiuni și transparența în luarea deciziilor și în executarea acțiunilor – sunt codificate în drepturile de decizie, în structurile de stimulente și în operațiuni, astfel încât acțiunea lipsită de integritate este fie imposibilă, fie costă mult mai mult timp, bani, energie și reputație.

Problemă de rezolvat: Oamenii nu au putut să tranzacționeze sau să facă afaceri direct pe internet din simplul motiv că banii nu seamănă cu celelalte bunuri informaționale și cu proprietatea intelectuală în sine. Poți să trimiți același selfie tuturor prietenilor tăi, dar nu ar trebui să-i dai prietenului tău un dolar pe care l-ai dat deja altcuiva. Banii trebuie să iasă din contul tău și să intre în cel al prietenului. Nu pot să existe în ambele locuri și cu atât mai puțin în mai multe locuri. Astfel că există riscul să cheltui o unitate de monedă digitală în două locuri, iar unul dintre ele va refuza să onoreze tranzacția, la fel ca în cazul unui cec fără acoperire. Aceasta poartă numele de *problema dublei cheltuiiri*. Este bună pentru escrocii care vor să-și cheltuiască banii de două ori. Este rea pentru cel care primește suma neonorată și rea pentru reputația ta online. În mod tradițional, atunci când efectuăm plăți online, rezolvăm problema dublei cheltuiiri prin trecerea fiecărei tranzacții prin bazele de date centrale ale unuia sau mai multor terți, cum ar fi un serviciu de transfer de bani (precum



Western Union), o bancă comercială (Citicorp), un organism guvernamental (Commonwealth Bank of Australia), o companie de carduri de credit (Visa) sau o platformă de plăți online (PayPal). În unele zone ale lumii, decontarea poate să dureze zile sau chiar săptămâni întregi.

Progres remarcabil: Satoshi s-a folosit de o rețea distribuită *peer-to-peer* deja existentă și de un pic de criptografie inteligentă pentru a crea un *mecanism de consens* care să poată soluționa problema dublei cheltuiuri la fel de bine, dacă nu chiar mai bine, decât un terț de încredere. În blockchainul bitcoin, rețeaua marchează temporal prima tranzacție în care utilizatorul cheltuiește o anumită monedă și refuză cheltuirile ulterioare ale monedei, eliminând astfel dubla cheltuire. Participanții la rețea care conduc noduri bitcoin complet operaționale – și care poartă numele de *mineri* – strâng la un loc tranzacțiile recente, le organizează sub forma unui bloc de date și repetă procesul la fiecare zece minute. Fiecare bloc trebuie să facă trimitere la blocul anterior pentru a fi valid. Protocoalele includ și o metodă pentru revendicarea spațiului de pe hard, astfel încât toate nodurile să poată înmagazina în mod eficient tot blockchainul. În ultimul rând, blockchainul este public. Oricine poate să vadă efectuarea tranzacțiilor. Nimeni nu poate să ascundă o tranzacție și aceasta face bitcoinul mai ușor de urmărit decât banii.

Satoshi nu a încercat doar să dizolve intermedierea puterii băncilor centrale, ci a încercat și să elimine ambiguitatea și interpretările conflictuale privitoare la ceea ce s-a întâmplat. Să lase codul să vorbească de la sine. Să lase rețeaua să ajungă algoritmic la un consens referitor la ce s-a întâmplat și să-l înregistreze criptografic în blockchain. Mecanismul pentru atingerea consensului este decisiv. „Consensul este un proces social”, scria într-o postare pe blog Vitalik Buterin, pionier al blockchainului Ethereum. „Ființele umane reușesc foarte bine să ajungă la un consens... fără niciun ajutor din partea algoritmilor.” El a explicat că, atunci când un sistem crește dincolo de capacitatea unei persoane de a rezolva partea de matematică, oamenii apelează la agenți



software. În rețelele *peer-to-peer*, algoritmul pentru consens divizează dreptul de a actualiza starea rețelei, adică de a vota care este adevărul. Algoritmul distribuie acest drept unui grup de membri care constituie un grup economic, un grup care și-a pus banii la bătaie, ca să zicem așa. Din spusele lui Buterin, lucrul important la acest grup economic este că membrii săi sunt distribuiți în siguranță: niciun membru singur și niciun cartel nu ar trebui să poată să învingă o majoritate, chiar dacă au mijloacele și stimulentele necesare pentru a face aceasta.⁷

Pentru a obține consensul, rețeaua bitcoin utilizează ceea ce poartă numele de mecanismul de *confirmare a muncii*. Ar putea să pară complicat, dar ideea este simplă. Din moment ce nu ne putem baza pe identitatea minerilor pentru a selecta persoana care creează următorul bloc, vom crea un puzzle care este dificil de rezolvat (adică, necesită foarte multă *muncă*), dar este ușor de verificat (adică, toți ceilalți pot să verifice răspunsul foarte repede). Participanții sunt de acord că oricine soluționează primul problema va crea următorul bloc. Minerii trebuie să cheltuiască resurse (hardware care să execute calculele și electricitate), pentru a soluționa puzzle-ul identificând hash*-ul corect, un fel de amprentă unică pentru un fișier text sau de date. Pentru fiecare bloc pe care îl găsim, minerii sunt recompensați cu bitcoini. Puzzle-ul este configurat matematic astfel încât este imposibil să găsești o scurtătură pentru a-l rezolva. Acesta este motivul pentru care, atunci când restul rețelei vede răspunsul, toată lumea e convinsă că a fost depusă foarte multă muncă pentru determinarea lui. În plus, rezolvarea puzzle-ului este continuă, „ajungând la valori apropiate de 500.000 de trilioane de hash-uri pe secundă”, după spusele lui Dino Mark Angaritis. Minerii „caută un hash care să respecte specificațiile. Statistic, ar trebui să apară unul la fiecare zece minute. Este un proces Poisson, astfel că durează uneori un minut, iar alteori o oră, dar, în medie, durează zece minute”.

* Este vorba despre valoarea unei funcții hash (funcție de dispersie sau de rezumat). Funcțiile hash sunt folosite în informatică pentru a accelera căutările în bazele mari de date sau pentru comparări de date, precum și în criptografie. (n.tr.)



Angaritis ne explică felul în care funcționează: „Minerii colectează toate tranzacțiile în așteptare pe care le găsesc în rețea și trec datele printr-o funcție hash criptografică numită algoritmul de securitate hash (SHA-256), care produce o *valoare hash* de 32 biți. Dacă valoarea hash este sub un anumit prag (stabilit de rețea și corectat la fiecare 2.016 blocuri), minerul a găsit răspunsul la puzzle și a «rezolvat» blocul. Din păcate pentru miner, găsirea valorii hash corecte este foarte dificilă. Dacă valoarea hash este incorectă, minerul ajustează ușor datele de intrare și încearcă din nou. Fiecare încercare are ca rezultat o *valoare hash complet diferită*. Minerii trebuie să încerce de mai multe ori până găsesc răspunsul corect. Începând din noiembrie 2015, numărul de încercări de găsire a valorii hash este, în medie, de 350 de milioane de trilioane. Ceea ce înseamnă foarte multă muncă!”⁸

Este posibil să auzi și de alte mecanisme de consens. Prima versiune a blockchainului Ethereum – Frontier – utilizează tot confirmarea muncii, dar dezvoltatorii Ethereum 1.1 speră că o vor putea înlocui cu un mecanism de *confirmare a mizei*. Confirmarea mizei le cere minerilor să investească în și să păstreze un stoc de valoare (adică, alte monede digitale care s-au născut în blockchain, cum ar fi Peercoin, NXT etc.). Nu trebuie să depună efort ca să voteze. Alte blockchainuri, cum ar fi Ripple și Stellar, se bazează pe rețele de socializare pentru a obține consensul și pot să recomande ca participanții noi (adică, nodurile noi) să genereze o *listă cu noduri unice* de cel puțin o sută de noduri în care au încredere să voteze în situația respectivă. Genul acesta de confirmare este lipsit de neutralitate: nou-veniții au nevoie de inteligență socială și de reputație pentru a participa. *Confirmarea activității* este un alt mecanism; acesta îmbină confirmarea muncii și confirmarea mizei, unde un număr aleatoriu de mineri trebuie să aprobe un bloc utilizând o criptocheie înainte ca blocul să devină oficial.⁹ *Confirmarea capacității* le cere minerilor să aloce pentru minerit un volum considerabil din hard drive-ul lor. Un concept similar, *confirmarea stocării*, le cere



minerilor să aloce și să pună la dispoziție spațiu de stocare într-un *cloud* distribuit.

Stocarea este importantă. Datele din blockchainuri sunt diferite de datele de pe internet într-un aspect important. Pe internet, cea mai mare parte a informației este maleabilă și trecătoare, iar data și momentul exact al publicării ei nu sunt esențiale pentru informațiile trecute sau viitoare. În blockchain, mișcarea bitcoinilor prin rețea este marcată de fiecare dată, începând cu momentul emiterii monedei. Pentru a fi valid, un bitcoin trebuie să facă trimitere atât la propria istorie, cât și la istoria blockchainului. Prin urmare, blockchainul trebuie păstrat în întregime.

Importanța proceselor de minerit – asamblarea unui bloc de tranzacții, cheltuirea de resurse, rezolvarea problemei, atingerea consensului, păstrarea unei copii a întregului registru – este atât de mare, încât au existat câteva voci care au spus că blockchainul bitcoin este un serviciu public asemănător internetului, un serviciu care are nevoie de sprijinul publicului. Paul Brody de la Ernst & Young crede că toate aparatele noastre electronice ar trebui să-și doneze puterea de procesare pentru întreținerea unui blockchain: „Mașina ta de tuns iarba sau mașina de spălat vase va avea un CPU* care va fi probabil de o mie de ori mai puternic decât ar fi necesar, așa că de ce nu l-ai pune să se ocupe de minerit? Nu cu scopul de a-ți aduce bani, ci pentru întreținerea părții din blockchain care îți revine ție”¹⁰, spune el. Indiferent de mecanismul de consens, blockchainul asigură integritatea prin codul inteligent, nu prin ființele umane care aleg să facă ce trebuie.

Implicații pentru economia blockchainului: În loc să lăsam marile companii și guvernele să verifice identitățile oamenilor și să garanteze pentru reputațiile lor, putem să ne punem încrederea în rețea. *Pentru prima dată în istorie, avem o platformă care asigură încrederea în tranzacții și o mulțime de informații înregistrate, indiferent de felul în care se va comporta cealaltă parte.*

* *Central Processing Unit* - unitate centrală de prelucrare sau unitate centrală de procesare. (n.tr.)



Implicațiile pentru majoritatea activităților sociale, politice și economice sunt incredibile. Nu este vorba doar despre cine cu cine s-a căsătorit, despre cine pe cine a votat, cine pe cine a plătit, este vorba despre toate activitățile care necesită înregistrări de încredere și tranzacții sigure. Cine și ce deține? Cine și ce drepturi are asupra acestei proprietăți intelectuale? Cine a absolvit facultatea de medicină? Cine a cumpărat arme? Cine a făcut acești pantofi Nike, acest dispozitiv Apple sau acest lapte praf pentru sugari? De unde provin aceste diamante? Încrederea este elementul indispensabil al economiei digitale, iar o platformă pentru o colaborare în masă sigură și de încredere conține o mulțime de posibilități pentru un nou tip de organizare și de societate.

2. Puterea distribuită

Principiu: Sistemul distribuie puterea într-o rețea *peer-to-peer* fără niciun punct unic de control. Nicio tabără nu poate să închidă sistemul. Dacă o autoritate centrală reușește să cenzureze sau să blocheze o persoană sau un grup, sistemul va supraviețui în continuare. Dacă mai mult de jumătate din rețea încearcă să ia cu asalt întregul, toată lumea va vedea ce se petrece.

Problema de rezolvat: În prima eră a internetului, orice instituție mare cu o bază robustă și amplă de utilizatori, indiferent dacă erau angajați, cetățeni, clienți sau alte organizații, nu se deranja prea tare cu propriul contract social. Puterile centrale au dovedit în repetate rânduri că sunt dispuse și capabile să acționeze sfidând utilizatorii, înmagazinând și analizând datele utilizatorilor, dând curs solicitărilor de date ale guvernelor fără ca utilizatorii să știe și implementând schimbări la scară largă fără acordul utilizatorilor.

Progres remarcabil: Costurile de energie pe care le presupune dominarea blockchainului bitcoin ar depăși beneficiile financiare. Satoshi a implementat o metodă de confirmare a muncii care le cere utilizatorilor să folosească foarte multă putere de calcul (lucru care consumă extrem de multă electricitate) pentru apărarea rețelei și emiterea de monede noi. El a fost inspirat de



soluția criptografului Adam Back, Hashcash, care reduce spamul și atacurile de blocare a serviciului. Metoda lui Back le cerea utilizatorilor e-mailului să ofere o confirmare a muncii atunci când trimit mesajul. De fapt, acesta marca un e-mail drept „corespondență urgentă” pentru a semnala importanța mesajului pentru expeditor. „Mesajul este atât de important, încât am depus toată această energie atunci când ți l-am expedit.” Crește costurile expedierii de spamuri, de *malware** sau de *ransomware***.

Oricine poate să descarce protocolul bitcoin gratuit și poate să păstreze o copie a blockchainului. Aceasta mobilizează *bootstrappingul*, o tehnică de încărcare a programului pe computerul sau pe dispozitivul mobil al unui voluntar prin câteva instrucțiuni simple care pun în mișcare restul programului. Este complet distribuit într-o rețea pe bază de voluntariat, cum ar fi BitTorrent, o bază de date partajată de proprietate intelectuală care se află pe zeci de mii de computere din toată lumea.

Bineînțeles, aceasta apără rețeaua de mâna statului, ceea ce poate fi bine sau rău, în funcție de situație – cum ar fi cazul unui disident dintr-un stat totalitar care luptă pentru drepturile femeilor *versus* cazul unui infractor dintr-un stat democratic care șantajează. Regimurile totalitare nu ar putea să blocheze conturile bancare sau să confiște fondurile activiștilor politici. Statele nu ar putea să-și însușească în mod arbitrar activele din blockchain, așa cum a făcut administrația lui Franklin Delano Roosevelt prin Ordinul Executiv 6102 al lui Roosevelt, care îi obliga pe cetățeni să predea guvernului „monedele de aur, lingourile de aur și certificatele ce atestă deținerea de aur”, în caz contrar riscând să fie amendați sau arestați.¹¹ Josh Fairfield de la Universitatea Washington and Lee a pus punctul pe i: „Nu mai există un intermediar pe care să-l vânezei”¹². Blockchainul se află peste tot. Voluntarii îl mențin actualizându-și propria copie a blockchainului și punându-și unitățile de procesare disponibile ale computerului la lucru pentru minerit. Nu există nicio înțelegere

* *Malware* - softuri dăunătoare. (n. red.)

** *Ransomware* - softuri dăunătoare ce solicită răscumpărare. (n.red.)



secretă. Toate acțiunile sau tranzacțiile sunt difuzate în rețea, în vederea verificării și validării ulterioare. Nu trece nimic printr-un terț cu rol central; nu se stochează nimic pe un server central.

Satoshi a distribuit și *monetăria* legând emiterea de bitcoini de crearea unui bloc nou în registru, plasând puterea emiterii de monedă în mâinile tuturor celor din rețeaua de membri. Indiferent cine ar fi minerul care rezolvă puzzle-ul și prezintă prima confirmare a muncii, el poate primi câțiva bitcoini noi. Nu există nicio Rezervă Federală, nicio bancă centrală sau trezorerie care să aibă controlul asupra rezervei de bani. Mai mult, fiecare bitcoin conține linkuri directe cu blocul care l-a generat și cu toate tranzacțiile ulterioare.

Astfel că nu este nevoie de niciun fel de intermediar. Funcționarea blockchainului reprezintă o colaborare de masă de cea mai bună calitate. Ai putere asupra datelor tale, asupra proprietății tale și asupra nivelului tău de participare. Puterea de calcul distribuită este cea care face posibilă puterea umană colectivă și distribuită.

Implicații pentru economia blockchainului: Poate că o platformă de felul acesta ar putea să facă posibile noi modele distribuite de creare a bogăției. Poate că noile tipuri de colaborări *peer-to-peer* vor putea să-și fixeze ca obiectiv cele mai frustrante probleme sociale ale omenirii. Poate că vom reuși să rezolvăm criza de încredere și chiar de legitimitate a instituțiilor din ziua de azi, transferând cetățenilor o parte din puterea reală, punându-le la dispoziție oportunități reale de prosperitate și de participare în cadrul societății, în loc să încercăm să-i păcălim cu manevre de relații publice.

3. Valoarea ca stimulent

Principiu: Sistemul armonizează stimulentele tuturor părților interesate. Bitcoinul sau vreun alt simbol valoric sunt esențiale pentru această armonizare și corelate cu reputația. Satoshi a programat softul pentru a-i recompensa pe cei care lucrează la el și aparține celor care dețin și utilizează unitățile sale de valoare, astfel încât să aibă cu toții grijă de el. Ca un fel de Tamagotchi suprem, blockchainul este o agoniseală de zile negre distribuită global.¹³



Problemă de rezolvat: În prima eră a internetului, concentrarea puterii în corporații, în combinație cu dimensiunile gigantice, complexitatea și opacitatea lor, le-a permis acestora să extragă disproporționat de multă valoare tocmai din rețelele care le înzestraseră cu drepturi. Marile bănci au exploatat sistemul financiar până în punctul de colaps, deoarece „structurile de stimulente pentru majoritatea directorilor de la vârf și pentru mulți dintre ofițerii de credit din aceste bănci [erau] gândite să încurajeze comportamentele mioape și asumarea unor riscuri excesiv de mari”, susține economistul Joseph Stiglitz. Aceasta cuprindea și „exploatarea celor mai săraci americani”. El a rezumat problema astfel: „Dacă le oferi oamenilor stimulente rele, ei se vor comporta rău și s-au comportat exact cum ne-am fi așteptat”¹⁴.

Companiile .com mari au atras lumea cu servicii gratuite în comerțul cu amănuntul, în căutări și în rețelele de socializare în schimbul datelor utilizatorilor. Conform unei cercetări Ernst & Young, aproape două treimi dintre managerii chestionați au declarat că au colectat date despre consumatori pentru a-și impulsiona afacerile și aproape 80% au susținut că veniturile lor au crescut ca urmare a acestei extracții de date. Dar atunci când astfel de firme sunt atacate de hackeri, consumatorii sunt cei care trebuie să sufere costurile furtului de informații referitoare la cardurile de credit și conturile bancare. Nu este deloc surprinzător că, în cadrul aceluiași studiu, aproape jumătate dintre consumatori au spus că vor bloca accesul la datele lor în următorii cinci ani și mai bine de jumătate au spus că deja furnizează mai puține date decât în ultimii cinci ani, inclusiv faptul că se autocenzurează pe rețelele de socializare.¹⁵

Progres remarcabil: Satoshi s-a așteptat ca participanții să acționeze urmărindu-și propriul interes. El înțelegea teoria jocurilor. Știa că rețelele lipsite de gardieni au fost vulnerabile la atacurile Sybil, când nodurile creează identități multiple, diluează drepturile și depreciază valoarea reputației.¹⁶ Atât integritatea rețelei *peer-to-peer*, cât și reputația membrilor săi se reduc atunci când nu știi dacă ai de-a face cu trei persoane sau cu o persoană



care utilizează trei identități. Ca urmare, Satoshi a programat codul sursă astfel încât, indiferent cât de egoist vor acționa oamenii, acțiunile lor să fie în beneficiul sistemului în ansamblu și să sporească reputațiile proprii, indiferent de felul în care aleg să se identifice. Resursele necesare pentru mecanismul de consens combinate cu recompensele în bitcoini îi puteau forța pe participanți să procedeze cum trebuie, făcându-i demni de încredere în sensul că erau previzibili. Atacurile de tip Sybil nu ar fi fost viabile economic.

Satoshi scria că, „prin convenție, prima tranzacție dintr-un bloc este o tranzacție specială care lansează o monedă nouă deținută de creatorul blocului. Aceasta adaugă un stimulent care determină nodurile să sprijine rețeaua”¹⁷. Bitcoinul este un stimulent care îi face pe mineri să participe la crearea unui bloc și la legarea lui de blocul anterior. Cei care termină primii un bloc primesc un număr de bitcoini pentru eforturile lor. Protocolul lui Satoshi i-a recompensat generos cu bitcoini pe cei care au adoptat de la început sistemul: în primii patru ani, minerii primeau 50 de bitcoini (BTC) pentru un bloc. La intervale de patru ani, recompensa pentru fiecare bloc avea să se înjumătățească: 25 BTC, 12,5 BTC etc. Din moment ce au devenit proprietari de bitcoini, sunt interesați să asigure succesul pe termen lung al platformei, cumpărând cel mai bun echipament pentru derularea operațiunilor de minerit, cheltuind energie cât mai eficient cu putință și întreținând registrul. Bitcoinul reprezintă, de asemenea, și un drept de proprietate asupra blockchainului, nu doar un stimulent pentru participarea la minerit sau la tranzacțiile cu ceilalți, ci prin deținerea platformei înseși. Conturile distribuite ale utilizatorilor sunt cel mai simplu element al infrastructurii rețelei criptografice. Deținând și utilizând bitcoini, finanțăm dezvoltarea blockchainului.

În rolul grupului economic, Satoshi i-a distribuit pe *proprietarii puterii de calcul*. Aceasta îi obligă pe mineri să consume o resursă exterioară rețelei, și anume electricitatea, dacă vor să participe la sistemul de recompense. Din când în când, diferiți mineri găsesc două blocuri la fel de valide, cu înălțimi egale, iar



restul minerilor trebuie să aleagă blocul pe care vor construi mai departe. În general, ei îl aleg pe acela care cred că va câștiga, în loc să construiască pe amândouă, pentru că altminteri ar fi obligați să-și scindeze puterea de procesare între bifurcații, iar prin această strategie nu ar reuși decât să piardă valoare. Cel mai lung lanț reprezintă cea mai mare cantitate de muncă și, de aceea, participanții îl aleg ca versiune standard a blockchainului. Pe de altă parte, Ethereum a ales *deținătorii de monedă* pe post de grup economic. Ripple și Stellar au ales rețeaua socială.

Paradoxul acestor strategii de obținere a consensului este că, atunci când cineva acționează urmărindu-și propriile interese, persoana servește rețeaua *peer-to-peer* și, la rândul său, lucrul acesta afectează reputația persoanei respective ca membru al grupului economic. Înainte de apariția tehnologiilor blockchain, oamenii nu puteau să exploateze prea ușor valoarea propriilor reputații online. Asta nu era doar din cauza atacurilor de tip Sybil, unde un computer putea să joace mai multe roluri. Identitatea are fațete multiple, este nuanțată și efemeră. Sunt puțini cei care văd toate laturile, ca să nu mai vorbim de subtilitățile sau de arcul identității noastre. În contexte diferite, trebuie să prezentăm un document sau altul care să confirme vreun aspect al identității noastre. Oamenii „fără acte” sunt forțați să colaboreze doar cu cercul lor social. În blockchainurile de tipul Stellar, lucrul acesta reprezintă un start excelent, un mijloc prin care să creezi o prezență digitală persistentă și să pui bazele unei reputații care să fie portabilă mult în afara propriei comunități geografice.

Un alt progres remarcabil pentru păstrarea valorii este *politică monetară* programată în software. „Toate tipurile de bani pe care omenirea le-a utilizat vreodată au fost nesigure într-un fel sau altul”, a spus Nick Szabo. „Această lipsă de siguranță s-a manifestat într-o mare diversitate de modalități, de la falsificare la furt, dar cea mai nocivă dintre ele a fost probabil inflația.”¹⁸ Satoshi a plafonat rezerva de bitcoini la 21 de milioane care să fie emiși de-a lungul timpului pentru a preveni inflația arbitrară. Dată fiind înjumătățirea la fiecare patru ani a bitcoinilor extrași



de pe urma unui bloc și actuala rată a mineritului – șase blocuri pe oră –, acele 21 de milioane de BTC ar trebui să fie în circulație în jurul anului 2140. Niciun fel de hiperinflație sau de devalorizare a monedei care să fie provocată de birocrății incompetente sau corupte.

Monedele nu sunt singurele active pe care le putem tranzacționa în blockchain. „Abia am început să intrăm timid în domeniul posibilităților”, declară Hill de la Blockstream. „Încă ne găsim în punctul acela din 1994 în ceea ce privește aplicațiile și protocoalele care profită efectiv de rețea și arată lumii: «Iată ce lucruri complet revoluționare puteți face.»”¹⁹ Hill se așteaptă să vadă diferite instrumente financiare, de la autenticitatea confirmării activului la calitatea de proprietar pe baza confirmării proprietății. El se așteaptă, de asemenea, să vadă aplicații bitcoin în Metavers (o lume virtuală), în care poți să schimbi bitcoini în dolari Kong și îl poți angaja pe Hiro Protagonist să-ți obțină informații ilegal.²⁰ Sau să intri în OASIS (o lume cu mai multe utopii virtuale) în care ajungi efectiv să descoperi oul de Paște, să câștigi averea lui Halliday, să le dai celor de la Google permisiunea de a utiliza drepturile de poziționare virtuală ale OASIS și să cumperi o mașină care se conduce singură pentru a merge prin Toronto.²¹

Și, bineînțeles, există și Internetul Lucrurilor, unde ne înregistrăm dispozitivele, le alocăm o identitate (Intel face deja asta) și coordonăm plăți între ele utilizând bitcoini, nu multiplele monede fiduciare. „Poți să definești toate aceste cazuri noi de afaceri pe care vrei să le realizezi, apoi le poți programa să funcționeze interacționând în cadrul rețelei și să utilizezi infrastructura rețelei fără să fie nevoie să construiești un blockchain nou de la zero, doar pentru tine”, a spus Hill.²²

Spre deosebire de monedele fiduciare, fiecare bitcoin poate fi divizat până la a opta zecimală. Aceasta le permite utilizatorilor să combine și să împartă valoarea de-a lungul timpului într-o singură tranzacție, însemnând că un input poate avea mai multe outputuri de-a lungul mai multor perioade de timp, ceea ce este mult mai eficient decât o serie de tranzacții. Utilizatorii pot să



elaboreze contracte inteligente care să contorizeze utilizarea unui serviciu și să efectueze fracțiuni minuscule de plăți la intervale regulate.

Implicații pentru economia blockchainului: Prima eră a internetului a ratat toate acestea. Acum avem o platformă pe care oamenii și chiar lucrurile au stimulente financiare adecvate pentru a colabora eficient și a crea aproape orice. Imaginează-ți grupuri de discuții online în care participanții au reputații care să merite a fi amplificate, în parte deoarece un comportament rău îi va costa din punct de vedere financiar. Trolii ar putea să se abțină. Imaginează-ți o rețea de panouri solare *peer-to-peer* în care proprietarii de locuințe sunt recompensați în timp real în blockchain pentru generarea de energie regenerabilă. Imaginează-ți un proiect de software cu *open source*, în care o comunitate de dezvoltatori îi plătește pe supercontributori pentru codul acceptabil. Să ne imaginăm că nu există țări. Nu e greu.²³

4. Securitatea

Principiu: Măsurile de siguranță sunt încorporate în rețeaua care nu are niciun punct de avarie și ne asigură nu numai confidențialitate, ci și autenticitate și nerefuzarea întregii activități. Oricine vrea să participe trebuie să utilizeze criptografia – nu există opțiunea refuzului –, iar consecințele unui comportament nechibzuit rămân izolate la persoana care s-a comportat nechibzuit.

Problemă de rezolvat: Atacul cibernetic, furtul de identitate, fraudă, agresiunea online, virusarea computerelor pentru a le da diverse instrucțiuni, spamul, *malware*-urile, *ransomware*-urile – toate acestea subminează siguranța persoanei în societate. În loc să aducă transparență și o reducere a încălcărilor, prima eră a internetului pare să nu fi făcut mare lucru pentru a spori siguranța persoanelor, instituțiilor și activității economice. Utilizatorul obișnuit al internetului trebuie să se bazeze de multe ori pe parole slăbuțe pentru a-și proteja e-mailul și restul conturilor online, pentru că nici furnizorii de servicii, nici angajatorii nu insistă pentru ceva mai puternic. Să luăm exemplul intermediarului



financiar obișnuit: nu se specializează pe dezvoltarea unei tehnologii sigure; se specializează pe inovația financiară. În același an în care Satoshi își publica raportul, violările securității datelor de la firme financiare precum BNY Mellon, Countrywide și GE Money reprezentau peste 50% din totalul furturilor de identitate raportate în acel an, conform Identity Theft Resource Center.²⁴ Până în 2014, cifra respectivă a scăzut la 5,5% pentru sectorul financiar, dar violările securității datelor medicale și a celor din sectorul serviciilor de sănătate au urcat până la 42% din totalul anului respectiv. IBM a declarat că, în medie, costul unei violări a securității datelor este de 3,8 milioane de dolari, ceea ce înseamnă că încălcările securității datelor au costat cel puțin 1,5 miliarde de dolari pe parcursul ultimilor doi ani.²⁵ Costul mediu al fraudării identității medicale pentru o persoană se apropie de 13.500 de dolari, iar infracțiunile sunt în creștere. Consumatorii nu mai știu ce aspect al vieții lor va cădea pradă hackerilor.²⁶ Dacă următoarea etapă a revoluției digitale se referă la transferul direct al banilor între părți, atunci transferul trebuie să devină impene-trabil pentru hackeri.

Progres remarcabil: Satoshi le-a cerut participanților să utilizeze infrastructura cu chei publice (ICP) pentru a crea o platformă sigură. ICP este o formă avansată de criptografie „asimetrică”, în care utilizatorii primesc două chei care au funcții diferite: una este pentru criptare și alta pentru decriptare. Prin urmare, ele sunt asimetrice. Blockchainul bitcoin este în prezent cea mai mare implementare civilă a ICP din lume și ocupă locul doi în clasamentul general, pe locul întâi fiind sistemul de acces comun al Departamentului de Apărare al SUA.²⁷

Apărută pentru prima dată în anii 1970²⁸, criptografia asimetrică a câștigat ceva influență în anii 1990 sub forma programelor gratuite de criptare a e-mailului, cum ar fi Pretty Good Privacy. PGP este destul de sigur și, în linii mari, o bătaie de cap în ceea ce privește utilizarea, pentru că trebuie să fie folosit de toți membrii rețelei tale și trebuie să ții evidența celor două chei proprii și a cheilor publice ale tuturor. Nu există nicio opțiune de resetare a



parolei. Dacă ți-ai uitat parola, trebuie să o iei de la capăt. Conform corporației Virtru, „utilizarea criptării e-mailurilor este în creștere. Chiar și așa, doar 50% dintre e-mailuri sunt criptate în tranzit, iar criptarea de la un capăt la altul a e-mailurilor este încă și mai rară”²⁹. Câțiva oameni utilizează *certificate digitale*, fragmente de cod care protejează mesajele fără operațiunile de criptare-decriptare, dar utilizatorii trebuie să facă o cerere (și să plătească o taxă anuală) pentru certificatul personal, iar cele mai răspândite servicii de e-mail – Google, Outlook și Yahoo! – nu sunt compatibile cu ele.

„Sistemele anterioare au eșuat pentru că le lipseau stimulentele, iar oamenii nu au perceput niciodată confidențialitatea ca pe un stimulent suficient de important încât să securizeze sistemele respective”³⁰, a declarat Andreas Antonopoulos. Blockchainul bitcoin rezolvă aproape toate aceste probleme furnizând un motiv temeinic pentru adoptarea la scară mare a ICP pentru toate tranzacțiile valoroase, nu doar prin utilizarea bitcoinului, ci și prin protocoalele comune ale bitcoinului. Nu trebuie să ne facem griji din cauza programelor de protecție slabe, a angajaților hoți sau hackerilor de asigurări. Dacă utilizăm amândoi bitcoini, dacă putem stoca și tranzacționa bitcoini în siguranță, atunci putem stoca și face schimb de informații foarte confidențiale și de active digitale în siguranță în blockchain.

Iată cum funcționează. Moneda digitală nu este stocată într-un fișier în sine. Ea este reprezentată de tranzacțiile indicate de un *hash* criptografic. Utilizatorii păstrează criptocheile de la banii lor și tranzacționează direct unii cu alții. Această securitate este însoțită de responsabilitatea de a-ți păstra cheile private secrete.

Standardele de securitate contează. Blockchainul bitcoin funcționează pe bine cunoscutul și consacratul SHA-256 publicat de U.S. National Institute of Standards and Technology (Institutul Național de Standarde și Tehnologie al SUA), acceptat ca standardul federal de procesare a informațiilor în SUA. Dificultatea numărului mare de repetiții ale acestui calcul matematic necesar pentru găsirea soluției unui bloc forțează dispozitivul de calcul să



consume o cantitate substanțială de electricitate pentru a rezolva puzzle-ul și a câștiga un nou bitcoin. Alți algoritmi, cum ar fi confirmarea mizei, consumă mult mai puțină energie.

Amintește-ți ce ne spunea Austin Hill la începutul acestui capitol despre faptul că nu trebuie să utilizăm niciodată cel mai nou și mai grozav algoritm. Hill, care lucrează cu criptograful Adam Back la Blockstream, și-a exprimat îngrijorarea față de criptomonedele care nu utilizează confirmarea muncii. „Eu nu cred că această confirmare a mizei funcționează până la urmă. Pentru mine, este un sistem în care bogații devin mai bogați, în care oamenii care au monede decid care va fi consensul, pe când confirmarea muncii este până la urmă un sistem înrădăcinat în fizică. Îmi place mult, deoarece este foarte similar cu sistemul pentru aur.”³¹

În ultimul rând, lanțul cu cea mai mare lungime este și cel mai sigur. Securitatea blockchainului lui Satoshi are beneficii mari de pe urma relativei sale maturități și a bazei sale stabile de utilizatori de bitcoini și mineri. Atacarea lui cibernetică ar avea nevoie de mai multă putere de calcul decât atacarea unor lanțuri scurte. Hill a spus: „De fiecare dată când una dintre rețelele acestea noi începe cu un lanț complet nou, se găsesc o grămadă de oameni care-și direcționează puterea latentă a computerelor, toate computerele și toate unitățile centrale de procesare pe care le-au închis pentru minerit, și le asmut împotriva acelor rețele noi pentru a le manipula și pentru a ataca de fapt rețelele”³².

Implicații pentru economia blockchainului: În era digitală, este evident că securitatea tehnologică este precondiția securității persoanei în societate. În ziua de azi, biții pot să treacă de programele noastre de protecție și prin portofelele noastre. Hoții pot să fure din buzunare sau să ne deturneze mașinile din celălalt capăt al lumii. Pe măsură ce fiecare dintre noi se bazează din ce în ce mai mult pe instrumente și platforme digitale, astfel de amenințări s-au înmulțit în feluri pe care majoritatea celor dintre noi nici nu le înțelegem. Având blockchainul bitcoin, cu designul său mai sigur și cu transparența sa, putem să facem tranzacții de valoare și să protejăm ce se petrece cu datele noastre.



5. Confidențialitatea

Principiu: Oamenii ar trebui să dețină controlul asupra propriilor date. Punct. Oamenii ar trebui să aibă dreptul să decidă ce, când, cum și cât de mult din identitățile lor vor să aducă la cunoștința cuiva. Respectarea dreptului la viața privată pe care îl are cineva nu este același lucru cu respectarea vieții private. Trebuie să le facem pe amândouă. Eliminând nevoia de a avea încredere în alții, Satoshi a eliminat necesitatea cunoașterii identităților reale ale celorlalți pentru a putea interacționa cu ei. „Am stat de vorbă cu numeroși ingineri și informaticieni și mi-au spus cu toții – fiecare în parte: – «Bineînțeles că putem încorpora confidențialitatea în arhitectura datelor, în designul programelor. Sigur că putem»”³³, a spus Ann Cavoukian.

Problemă de rezolvat: Confidențialitatea este un drept fundamental al omului și temelia societăților libere. În ultimii douăzeci de ani ai internetului, bazele centrale de date, atât din sectorul public, cât și din cel privat, au acumulat informații confidențiale de toate felurile despre persoane și instituții, uneori fără ca acestea să știe. Oamenii de pretutindeni sunt îngrijorați de faptul că marile corporații creează ceva ce am putea numi *clonele lor cibernetice*, extrăgând prin fracturare datele lor din lumea digitală. Până și guvernele democratice creează state de supraveghere, lucru confirmat de felul în care Agenția Națională de Securitate a SUA și-a extins excesiv drepturile de monitorizare de curând, spionând fără niciun mandat pe internet. Aceasta reprezintă o dublă încălcare a vieții private, prima constând în colectarea și utilizarea datelor noastre, fără ca noi să înțelegem sau să fi fost de acord, și cealaltă în neprotejarea acestora împotriva hackerilor. „Totul se rezumă la abandonarea demersurilor cu sumă zero, a propunerilor ori-ori, câștig-pierdere, poți să ai un interes sau pe celălalt. Lucrul acesta mi se pare depășit, aparținând trecutului și foarte contraproductiv”, a spus Cavoukian. „În locul lui, noi venim cu un model cu sumă pozitivă care, în principiu, spune că te poți bucura și de confidențialitate și de _____ completează spațiul liber.”³⁴



Progres remarcabil: Satoshi nu a instalat nicio condiție de identitate la nivelul rețelei înseși, ceea ce înseamnă că nimeni nu trebuia să furnizeze vreun nume, o adresă de e-mail sau alte date personale pentru a descărca și a utiliza softul bitcoin. Blockchainul nu are de ce să știe cine este fiecare dintre noi. (Iar Satoshi nu era interesat să captureze datele cuiva pentru a vinde și alte produse. Softul său *open source* era cel mai bun în marketingul bazat pe leadership intelectual.) Așa funcționează Society for Worldwide Interbank Financial Telecommunication (Societatea pentru Telecomunicații Financiare Interbancare Mondiale) – dacă plătești cu numerar, SWIFT nu îți cere de regulă să te identifiți –, dar presupunem că o mulțime de birouri ale SWIFT au camere de luat vederi, iar instituțiile financiare trebuie să respecte condițiile antisplărare de bani/cunoaște-ți clientul pentru a adera la SWIFT și a-l putea utiliza.

În plus, palierele de identificare și verificare sunt separate de cel de tranzacție, ceea ce înseamnă că Partea A difuzează transferul de bitcoini de la adresa Părții A la adresa Părții B. Nu se face nicio referire la identitatea cuiva în acea tranzacție. Apoi, rețeaua confirmă nu doar că Partea A controla cantitatea de bitcoini specificată, dar și faptul că a autorizat tranzacția înainte de a recunoaște mesajul Părții A ca fiind „outputul necheltuit al tranzacției” asociat cu adresa Părții B. Rețeaua se va asigura că Partea B controlează acum bitcoini respectivi doar atunci când Partea B va pleca să cheltuiască suma respectivă.

Să comparăm aceasta cu utilizarea cardurilor de credit, un model centrat pe identitate. Acesta este motivul pentru care sunt furate adresele și numerele de telefon ale câtorva milioane de oameni de fiecare dată când este spartă o bază de date. Să ne gândim la numărul de înregistrări atașate la câteva dintre cele mai recente cazuri de încălcare a securității datelor: T-Mobile, 15 milioane de înregistrări; JPMorgan Chase, 76 de milioane; Anthem Blue Cross Blue Shield, 80 de milioane; eBay, 145 de milioane; Office of Personnel Management, 37 de milioane; Home Depot, 56 de milioane; Target, 70 de milioane și Sony, 77 de milioane; și au



existat spargeri mai mici la companii de transporturi aeriene, universități, companii de gaz și electricitate, unități spitalicești, câteva dintre cele mai prețioase elemente de infrastructură.³⁵

În cadrul blockchainului, participanții pot opta să mențină un grad de anonim personal, în sensul că nu trebuie nici să atașeze vreun alt detaliu al identității lor și nici să stocheze detaliile respective în vreo bază de date centrală. Nu putem să subliniem cât de colosal este lucrul acesta. *Nu există nicio aglomerare tentantă de date personale în blockchain.* Protocoalele blockchainului ne permit să alegem nivelul de confidențialitate pe care îl considerăm acceptabil în orice tranzacție sau în orice mediu. Ne ajută să ne gestionăm mai bine identitățile și interacțiunile cu lumea.

Un *start-up* numit Personal BlackBox Company, LLC, urmărește să ajute corporațiile mari să-și transforme relația cu datele consumatorilor. Directorul de marketing al PBB, Haluk Kulin, ne-a declarat: „Companii precum Unilever sau Prudential ne abordează și ne spun: «Suntem foarte interesați să construim relații de date mai bune. Ne putem folosi de platforma voastră? Suntem foarte interesați să ne reducem responsabilitatea în domeniul datelor». Ele înțeleg că datele devin un activ din ce în ce mai toxic în cadrul corporațiilor”³⁶. Platforma sa le oferă clienților acces la date anonime – foarte similar cu un studiu clinic, unde companiile farmaceutice nu cunosc decât aspectele relevante ale sănătății pacienților – fără să-și asume vreun risc de securitate. Câțiva consumatori pot să cedeze mai multe informații în schimbul bitcoinilor sau al altor beneficii din partea corporațiilor. În fundal, platforma companiei PBB utilizează ICP, astfel încât doar consumatorii să poată avea acces la propriile date prin cheile lor private. Nici măcar PBB nu are acces la datele consumatorilor.

Blockchainul oferă o platformă pentru realizarea unor forme foarte flexibile de atestare selectivă și anonimă. Austin Hill a comparat-o cu internetul. „O adresă TCP/IP* nu este identificată cu un act public de identitate. Nu există identificare nici măcar la

* Protocol de control al transmisiei/Protocol Internet. (n.tr.)



nivelul rețelei. Oricine se poate conecta la internet, poate să obțină o adresă IP și poate începe să trimită și să primească nestingerit pachete de oriunde din lume. Noi, ca societate, am avut beneficii incredibile permițând acest grad de utilizare a pseudonimelor... Bitcoin funcționează aproape identic. Rețeaua în sine nu impune identitatea. Este un lucru bun pentru societate și pentru designul adecvat al rețelei.”³⁷

Ca urmare, deși blockchainul este public – oricine îl poate vedea în orice moment pentru că se află în rețea, nu în cadrul vreunei instituții centralizate însărcinate cu verificarea contabilă a tranzacțiilor și cu efectuarea de înregistrări –, identitățile utilizatorilor sunt pseudonime. Aceasta înseamnă că trebuie să faci foarte multă triangulare a datelor pentru a descoperi cine sau ce deține o anumită cheie publică. Expeditorul poate să furnizeze doar metadatele pe care trebuie să le cunoască destinatarul. Mai mult, oricine poate să dețină mai multe seturi de chei publice/private, la fel cum oricine poate să aibă mai multe dispozitive sau puncte de acces la internet și mai multe adrese de e-mail sub pseudonime diferite.

Acestea fiind spuse, furnizorii de servicii de internet ca Time Warner, care distribuie adrese IP, păstrează înregistrări care leagă identitățile de conturi. În mod similar, dacă vei cumpăra un portofel bitcoin de pe o piață online autorizată cum ar fi Coinbase, respectiva piață este obligată să facă toate demersurile necesare pentru respectarea condițiilor antispălare de bani/cunoaște-ți clientul. Spre exemplu, iată politica de confidențialitate a Coinbase: „Colectăm informațiile care ne sunt trimise prin computerul tău, telefonul mobil sau alte dispozitive de acces. Informațiile acestea ar putea să includă adresa ta IP, informații despre dispozitiv care includ, dar nu se limitează numai la identificator, numele și tipul dispozitivului, sistemul de operare, locația, informațiile despre rețeaua mobilă și informațiile standard despre conectare, cum ar fi tipul de *browser*, traficul spre și dinspre site-ul nostru, precum și paginile pe care le-ai accesat pe site-ul nostru web”³⁸. Așadar, guvernele pot să cheme în instanță furnizorii



de internet și platformele de schimburi pentru acest tip de date ale utilizatorilor. Dar nu pot să cheme în instanță blockchainul.

Este de asemenea important să știm că putem proiecta niveluri mai mari de transparență în orice set de tranzacții, în orice aplicație sau model de afaceri, în cazul în care toate părțile interesate sunt de acord să se procedeze astfel. Vom vedea capacități noi în diferite situații în care transparența radicală are sens. Companiile creează încredere atunci când le spun adevărul clienților, acționarilor sau partenerilor de afaceri.³⁹ Mai precis, confidențialitate pentru persoane, transparență pentru organizații, instituții și oficialități publice.

Implicații pentru economia blockchainului: Cu siguranță, blockchainul ne oferă oportunități pentru a opri goana dementă spre o societate a supravegherii. Să ne gândim acum la problema colecțiilor corporatiste de tip *big data* pentru fiecare dintre noi. Ce înseamnă pentru o corporație faptul că deține informații perfecte despre tine? Au trecut mai bine de douăzeci de ani de când am intrat în era internetului global și suntem abia la începutul accesului corporațiilor la cele mai intime detalii ale vieților noastre personale. Se apropie rapid problema datelor personale referitoare la sănătate și fitness, la fel și cea a deplasărilor noastre zilnice de ici-colo, intimitatea din căminele noastre și cam tot ce-ți vine în minte. Mulți oameni pur și simplu nu realizează numeroasele compromisuri microfaustiene pe care le fac în fiecare zi online. Prin simpla utilizare a site-urilor web, consumatorii îi autorizează pe proprietarii acestora să transforme firimiturile digitale în hărți detaliate care aduc beneficii comerciale private.

Dacă nu ne reorientăm spre noua paradigmă, nu este de domeniul științifico-fantastic să anticipăm sute de milioane de avatururi bâzâind în centrele de date ale zilei de mâine. Prin tehnologia blockchain, poți să-ți stăpânești avatarurile personale la fel ca în lumea virtuală din Second Life, dar cu implicații în lumea reală. Eul tău virtual ar putea să-ți protejeze informațiile personale, transmițând doar datele necesare în orice schimb social sau economic, să lucreze sub comanda ta și să se



asigure că ești recompensat pentru oricare dintre datele tale care au valoare pentru altcineva. Este o trecere de la *big data* la date private. Poți să îi dai numele de „little data”^{*}.

6. Drepturile conservate

Principiu: Drepturile de proprietate sunt transparente și executorii. Libertățile individuale sunt recunoscute și respectate. Noi considerăm acest adevăr evident, și anume că fiecare dintre noi ne naștem cu anumite drepturi inalienabile care ar trebui și care pot fi protejate.

Problemă de rezolvat: Prima eră a economiei digitale s-a axat pe găsirea unor modalități de a exercita mai eficient aceste drepturi. Internetul a devenit un mediu pentru noi forme de artă, de știri și de divertisment, pentru determinarea drepturilor de autor pentru poezii, cântece, povești, fotografii și înregistrări audio și video. Am putea să aplicăm și pe mai departe Codul Comercial Uniform pentru a reuși să facem și online lucrurile pe care codul a reușit să le accelereze în spațiul fizic, cum ar fi eliminarea nevoii de a negocia și de a crea contracte pentru absolut fiecare articol, precum un tub de pastă de dinți, indiferent cât de mic este prețul acestuia. Chiar și atunci, trebuia să avem încredere în intermediari care să gestioneze tranzacțiile, ei având puterea să refuze tranzacția, să o întârzie și să rețină banii în propriile conturi (bancherii numesc fondurile acestea „flotante”) sau s-o confirme doar pentru a o anula mai târziu. Ei se așteptau ca un anumit procent de oameni să înșele și acceptau un anumit nivel de fraudă ca inevitabil.

În această mare explozie de eficiență, drepturile legitime au fost călcate în picioare, nu doar dreptul la viață privată și la siguranță, ci și libertatea cuvântului, reputația și participarea egală. Oamenii ne puteau cenzura, calomnia și bloca în mod anonim suportând costuri sau riscuri mici. Realizatorii de filme, care erau dependenți de veniturile obținute din sindicalizare, filme la

^{*}Date mici. (n.tr.)



cerere, vânzări crescute de DVD-uri și drepturi de difuzare prin cablu pentru filme lansate cu câteva decenii mai devreme, s-au trezit că fluxul lor de venituri se diminuează până ajunge cât un firicel pentru că fanii lor încărcau pe net fișierele digitale pe care alții să le descarce gratuit.

Progres remarcabil: Confirmarea muncii necesare pentru a crea noi monede marchează temporal tranzacțiile, astfel încât doar prima cheltuire a monedei va fi confirmată și achitată. În combinație cu ICP, blockchainul nu se limitează la prevenirea unei duble cheltuiiri, ci confirmă și proprietatea fiecărei monede aflate în circulație, toate tranzacțiile fiind permanente și irevocabile. Cu alte cuvinte, nu putem tranzacționa în blockchain un lucru care nu ne aparține, indiferent dacă este vorba de o proprietate reală, o proprietate intelectuală sau de drepturi asociate statutului de persoană. Și nu putem tranzacționa nici lucruri pe care nu suntem autorizați să le tranzacționăm în numele altcuiva jucând rol de intermediere, poate ca avocat sau ca manager al unei companii. Și nu putem să înăbușim libertatea de expresie, de asociere și religioasă a oamenilor.

Haluk Kulin de la Personal BlackBox a exprimat aceasta cel mai bine: „În miile de ani de interacțiuni sociale ale oamenilor, de fiecare dată când le-a fost răpit dreptul de a participa, au revenit și au distrus sistemul. Noi descoperim că nu este sustenabil să le răpim acordul nici măcar în lumea digitală”⁴⁰. Ca Registru al Tuturor Lucrurilor, blockchainul poate funcționa ca registru public, prin instrumente cum ar fi Proof of Existence (PoE) (confirmarea existenței), un site care creează și înregistrează rezumate criptografice ale unor acte, titluri, chitanțe sau licențe în blockchain. Proof of Existence nu păstrează o copie după vreun act original; hash-ul documentului este calculat pe computerul utilizatorului, nu pe site-ul PoE, asigurându-se în felul acesta confidențialitatea conținutului. Chiar și în cazul în care o autoritate centrală închide Proof of Existence, confirmarea rămâne în blockchain.⁴¹ Așadar, blockchainul oferă mijloace de a dovedi proprietatea și de a păstra înregistrări necenzurate.



Pe internet nu am putea să asigurăm în mod necesar respectarea drepturilor contractuale sau să supraveghem implementarea. Și de aceea, pentru tranzacțiile mai complexe care angrenează mai multe drepturi și mai multe părți, avem acum la dispoziție *contractul inteligent*, un fragment de cod cu un scop special care execută un set complex de instrucțiuni în blockchain. „Acea intersectare a descrierilor legale cu softul este fundamentală și contractele inteligente reprezintă primul pas în direcția aceasta”, a spus Steve Omohundro, președintele *think tank*-ului* Self-Aware Systems. „După ce principiile felului în care codificăm digital legea încep să fie mai bine înțelese, cred că fiecare țară va începe să o facă... Fiecare jurisdicție ar urma să-și codifice legile, precis și digital, și ar urma să existe programe de traducere între ele... Eliminarea frecușului provocat de toate detaliile juridice va constitui un câștig economic enorm.”⁴²

Un contract inteligent oferă mijloacele pentru repartizarea drepturilor de utilizare unei alte părți, la fel cum un compozitor ar putea să cedeze o melodie finalizată unui producător de muzică. Codul contractului ar putea să includă termenul sau durata atribuirii, dimensiunea drepturilor de autor care ar urma să curgă din contul în bitcoini al producătorului în cel al compozitorului în perioada stabilită și alte câteva condiții pentru încetarea contractului. Spre exemplu, în cazul în care contul compozitorului a primit mai puțin de un sfert de bitcoin pe o perioadă de treizeci de zile consecutive, atunci toate drepturile ar reveni automat compozitorului, iar producătorul ar urma să nu mai aibă acces la opera compozitorului înregistrată în blockchain. Pentru a pune în mișcare acest contract inteligent, atât compozitorul, cât și producătorul – poate chiar și reprezentanții echipei contabile și a celei juridice ale producătorului – ar urma să semneze, utilizându-și cheile private.

* *Think tank* – grup sau instituție organizate în vederea cercetării intensive și a rezolvării de probleme, în special în domeniul tehnologiei, strategiei sociale și politice sau al armamentului. (n.red.)