BITCOIN ÎN 10 MINUTE

Tot ce ai vrut întotdeauna să știi despre Bitcoin

Brought to you by **Relai**

CE ESTE BITCOIN?

Bitcoin, cea mai de succes criptomonedă din lume, este pe prima pagină a ziarelor din întreaga lume. Mulți vor să profite de pe urma succesului său, în timp alții sunt indiferenți sau chiar sceptici. Moneda digitală a stârnit nenumărate discuții despre bani, investiții și tehnologie. Unii văd în Bitcoin un pur vehicul de speculație sau îl denunță ca pe un fenomen trecător, în timp ce alții vorbesc despre inovație, revoluție monetară sau chiar despre salvarea de actualul sistem monetar.

Diferite țări, inclusiv China, văd Bitcoin ca pe o amenințare și au declarat război criptomonedei. Alte guverne, precum cel din El Salvador, au introdus Bitcoin ca mijloc oficial de plată în speranța unei creșteri economice.

Dar ce este Bitcoin? O formă de bani? Aur digital? O modă pentru informaticieni și speculatori? Sau ceva cu totul altceva? În paragrafele următoare, vom răspunde la aceste întrebări și vom examina mai îndeaproape moneda digitală pentru a înțelege mai bine filozofia și funcționalitatea din spatele Bitcoin. Pentru a realiza acest lucru, este important să începem chiar cu originile proiectului.

POVESTEA BITCOIN

Începuturile Bitcoin datează de la începutul anilor ,90. În 1992, un grup de informaticieni din California a creat listă de corespondență pentru a face schimb de idei cu persoane care împărtășeau aceleași păreri despre criptografie, matematică, politică și filozofie. Aceștia s-au autointitulat „Cypherpunks“ - un joc de cuvinte de la cyberpunk (persoană din literatura științifico-fantastică care, pe bună dreptate, este sceptică față de societate) și cipher (referitor la procesul de codificare a informației, a codifica).

Gruparea “Cyberpunks”

Gruparea „Cypherpunks“ a devenit în curând o echipă eterogenă. În ciuda originilor lor diferite, erau uniți de convingerea că internetul va deveni în curând una dintre cele mai disputate arene pentru libertatea umană.

Pentru a se proteja împotriva amenințării de control, supraveghere și cenzură a internetului și pentru a păstra un internet liber și deschis, membrii grupării Cypherpunk au folosit o armă puternică: criptografia, practica prin care se codează și secretizează informațiile.

În manifestul lor din 1993, ei au declarat: „Cypherpunks scriu cod [informatic]. Știm că cineva trebuie să scrie software pentru a apăra confidențialitatea internetului și [...] noi vom fi aceia care îl vor scrie.

Dar de una singură, criptografia nu ar fi suficientă suficientă pentru un internet liber. Iar membrii grupării Cy-

pherpunk erau convinși de acest lucru: internetul nu poate fi cu adevărat liber dacă nu are banii săi. Bani independenți de state, bănci centrale și companii; o criptomonedă la fel de echitabilă și descentralizată ca Internetul însuși.

Experimente monetare

Dar crearea de bani independenți, digitali, a reprezentat o provocare tehnică pentru Cypherpunks. Încă din 1990, criptologul David Chaum a creat prima criptomonedă, numită eCash. Aceasta nu era descentralizată, dar asigura anonimatul datorită criptografiei. Cu toate acestea, eCash nu a reușit să se impună pe termen lung în fața altor sisteme de plată online. Compania din spatele proiectului a intrat în faliment după 8 ani de activitate, iar eCash a dispărut.

Au urmat alte încercări, dintre care s-a remarcat E-Gold. E-Gold a fost o criptomonedă susținută de aur, deschisă tuturor. Înființată în timpul erei "dot-com" în 1996, compania a atins un punct de atracție pentru cei interesați, procesând tranzacții în valoare de peste două miliarde de dolari pe an la apogeu.

Dar E-gold era controlată de o instituție centrală și, prin urmare, era vulnerabilă la atacuri. Problemele juridice au urmat curând, iar guvernul american a luat măsuri legale împotriva proiectului. În 2008, E-Gold a fost găsit vinovat de un tribunal american de spălare de bani și de încălcarea Patriot Act. Toate activele au fost înghețate, iar E-Gold a trebuit să își înceteze activitatea.
Prin aceste încercări eșuate, gruparea cypherpunk a învățat două lecții importante. În primul rând, atât eCash, cât și E-Gold fuseseră susținute de garanții. Aceste garanții s-au dovedit a fi un punct slab, deoarece puteau fi confiscate de către state. Prin urmare, o criptomonedă liberă nu ar trebui să aibă puncte centrale de atac, precum o companie înregistrată, un cont bancar sau o locație centralizată a serverului. Îi al doilea rând, atât guvernele, cât și autoritățile de reglementare nu au niciun interes în în a susține o formă de bani indepedentă de controlul statului.

Pentru Cypherpunks, întrebarea de bază, pentru care nu s-a găsit încă nicio soluție, a rămas: Cum poate funcționa o monedă digitală independentă fără o entitate centrală care să țină evidența contabilă și să se asigure că aceeași sumă de bani nu poate fi cheltuită de două ori? La urma urmei, dacă ar fi posibil să se rezolve problema dublei cheltuieli fără a se baza pe o entitate centrală, ar fi posibil să se creeze bani digitali liberi care să fie nativi pentru internet.

Un act mistic de creație

Din aceste motive, Cypherpunks a început să discute despre proiecte pentru o criptomonedă lipsită de o parte centrală și fără garanții. Două dintre cele mai importante concepte au fost

b-money (1998) și BitGold (2005). Aceste idei teoretice, care nu au fost niciodată implementate în practică, erau deja foarte asemănătoare cu Bitcoin în ceea ce privește designul lor. Pentru criptare era prevăzută o pereche de chei publice/private, iar crearea de monede digitale suplimentare urma să fie asigurată de Proof-of-Work (dovadă a muncii), așa cum este și în cazul Bitcoin. În Whitepaper-ul său, inventatorul Bitcoin a confirmat, de asemenea, că era la curent cu invențiile anterioare.

Deoarece b-money și BitGold se bazau pe un sistem de vot pentru consens (acordul cu privire la proprietatea asupra fiecărei unități monetare existente), acestea erau vulnerabile la atacuri rău intenționate care puteau manipula aceste alegeri. Astfel, proprietatea ar fi putut fi denaturată.

Pentru această ultimă problemă, care încă stătea în calea creării de noi bani pe internet, a fost prezentată o soluție în ziua de vineri, 31 octombrie 2008. În acel moment, documentul Bitcoin Whitepaper, în care Satoshi Nakamoto își explica conceptul de rețea de plăți descentralizată, a fost trimis prin e-mail către un grup de pasionați de criptografie. Două luni mai târziu, la 3 ianuarie 2009, rețeaua Bitcoin a intrat în funcțiune.

Reacțiile inițiale la noul sistem monetar au fost discrete. Câțiva entuziaști au început să testeze rețeaua și să raporteze erori. Cu toate acestea, la început, Satoshi Nakamoto însuși a fost cel care a asigurat funcționarea sistemului. Dar, încet-încet, vestea despre noii bani de pe internet s-a răspândit pe forumurile de informatică și tehnologie, iar interesul a crescut. După un an, rețeaua Bitcoin număra deja câțiva utilizatori. Cu toate acestea, moneda bitcoin în sine nu avea încă vreo valoare tranzacțională.

Cine este Satoshi Nakamoto?

Bitcoin Whitepaper, precum și toate comunicațiile electronice ale inventatorului Bitcoin, au fost semnate cu numele Satoshi Nakamoto. Cu toate acestea, adevărata identitate a inventatorului Bitcoin rămâne necunoscută până în prezent, deoarece se pare că a apelat la un pseudonim. Pentru a se adresa unor persoane care împărtășesc aceleași idei și, mai târziu, comunității de dezvoltatori Bitcoin, Nakamoto a folosit cel puțin trei adrese de e-mail diferite, pe care le-a criptat în detaliu pentru a ascunde adevărata identitate a expeditorului.

Diverse persoane au pretins deja că sunt Satoshi Nakamoto. Dar până în prezent, niciuna dintre ele nu a reușit să demonstreze acest lucru. Dovada supremă, și anume trimiterea de Bitcoin de la una dintre adresele de portofel care, cel mai probabil, îi aparține lui Satoshi, nu a fost încă furnizată de nimeni.

În plus, grupul celor care au comunicat „personal“ cu Satoshi Nakamoto prin intermediul internetului este fo-

arte restrâns. Satoshi Nakamoto a scris ultimul său mesaj către comunitatea Bitcoin la 12 decembrie 2010, dar acesta nu a fost în niciun caz un bilet de adio – creatorul Bitcoin a încetat pur și simplu să mai comunice din acel moment.

Cu toate acestea, retragerea lui Satoshi a fost în primă fază doar o îndepărtare de comunitatea mai largă. Nakamoto a continuat să adune în jurul său un mic grup de programatori de bază și i-a informat cu privire la dezvoltarea ulterioară a rețelei Bitcoin. Dar, în aprilie 2011, el a trimis un ultim mesaj și acestui grup. La fel de misterios cum a apărut în 2008, Nakamoto a dispărut aparent definitiv trei ani mai târziu.

„Ziua Pizza" în Comunitatea Bitcoin

Cum a ajuns Bitcoin să aibă valoare tranzacțională pentru prima dată? La început, Bitcoin putea fi minat și trimis între membrii rețelei, dar unitățile monetare digitale nu aveau nicio valoare. De asemenea, grupul celor care știau despre Bitcoin, ca să nu mai vorbim de cei care puteau să îl tranzacționeze, era încă foarte mic.

Un eveniment remarcabil s-a produs la data de 22 mai 2010, când o cerere neobișnuită a apărut pe forumul de internet bitcointalk.org. Un bărbat din Florida în vârstă de 28 de ani, numit Laszlo Hanyecz, a oferit 10.000 de Bitcoin către prima persoană dispusă să îi comande două pizza la domiciliu. Un student din California a acceptat oferta și a trimis către Laszlo două pizza mari în valoare de 41 de dolari. În schimb, Hanyecz a efectuat tranzacția a 10.000 de Bitcoin.

În urma acestui eveniment, ziua de 22 mai este sărbătorită anual de către bitcoineri ca fiind „Ziua Pizza". Tranzacția dintre Laszlo și furnizorul de pizza ilustrează trei lucruri:

- Unitățile monetare Bitcoin au valoare
- Bitcoinii pot fi folosiți ca mijloc de schimb și de plată

- Numărul de unități monetare suplimentare care intră în circulație scade constant, iar numărul maxim de 21 de milioane de monede va fi minat până în anul 2140. Bitcoin are un sistem predictibil si transparent de emitere, ce nu poate fi modificat. Datorita acestui fapt, cunoaștem rata inflației pe tot parcursul emiterii, iar din anul 2140 va deveni o moneda deflatio-

nara. Numărul de unități monetare suplimentare care intră în circulație scade constant, ceea ce poate duce la o creștere a valorii.

Cele două pizza au intrat în cărțile de istorie ca fiind cele mai scumpe din lume. Calculând costul lor cu prețul bitcoin din decembrie 2021, s-a plătit pentru ele suma incredibilă de 460 de milioane de dolari americani. Suma este fabuloasă. Dar și beneficiarul celor 10.000 de Bitcoin i-a cheltuit deja. Într-un interviu, el a declarat că a vândut bitcoinii primiți la scurt timp pentru a plăti o călătorie cu mașina - la prețul Bitcoin de astăzi, probabil și exemplul celei mai scumpe călătorii cu mașina din istoria omenirii.

„Ziua Pizza“ ilustrează, de asemenea, în mod impresionant de ce „hodling“ (un termen derivat din verbul din limba engleză care desemnează acțiunea de păstrare)- este atât de popular printre bitcoineri. „Hodling“ înseamnă să ții de bitcoinii pe care îi ai pe perioade îndelungate cu intenția de a nu îi vinde (probabil) niciodată. La urma urmei, cine vrea să cheltuie bitcoin astăzi, știind că ar putea valora dublu, triplu sau chiar de zece ori mai mult în anii următori?

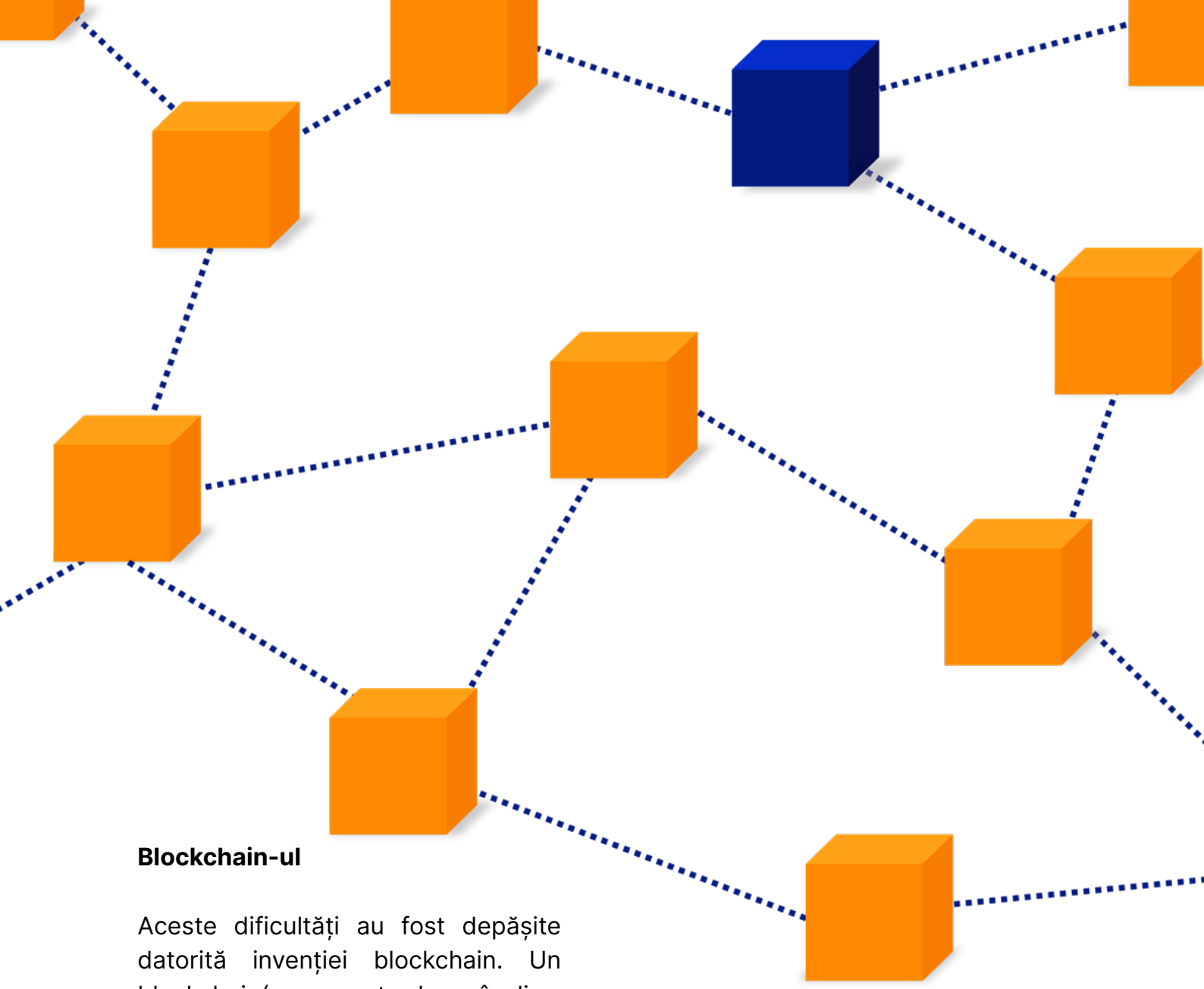
CUM FUNCȚIONEAZĂ BITCOIN?

După ce am aflat despre istoria Bitcoin, ne vom ocupa acum de modul său de funcționare. Scopul este de a înțelege cum funcționează rețeaua Bitcoin, ce probleme rezolvă și care sunt beneficiile sale practice.

Intenția din spatele Bitcoin este de a fi o rețea descentralizată. Niciun participant nu ar trebui să fie capabil să conducă singur rețeaua - puterea de decizie și supravegherea sunt distribuite între toți participanții. Acest lucru este important, deoarece niciun individ, niciun guvern și nicio companie nu poate schimba rețeaua în mod independent. Schimbările sunt posibile doar în mod colectiv, prin consensul tuturor participanților.

Bitcoin funcționează în așa fel încât fiecare participant la rețea deține și actualizează în permanență o copie identică a celui mai actualizat registru de proprietate - ca urmare, toată lumea știe întotdeauna cine deține în prezent Bitcoin și care sunt sumele. Astfel, nimeni nu poate pretinde că posedă mai multe monede decât prevede registrul contabil, deoarece fiecare participant la rețea poate verifica această afirmație în raport cu propria evidență. Falsurile pot fi dovedite extrem de ușor. .

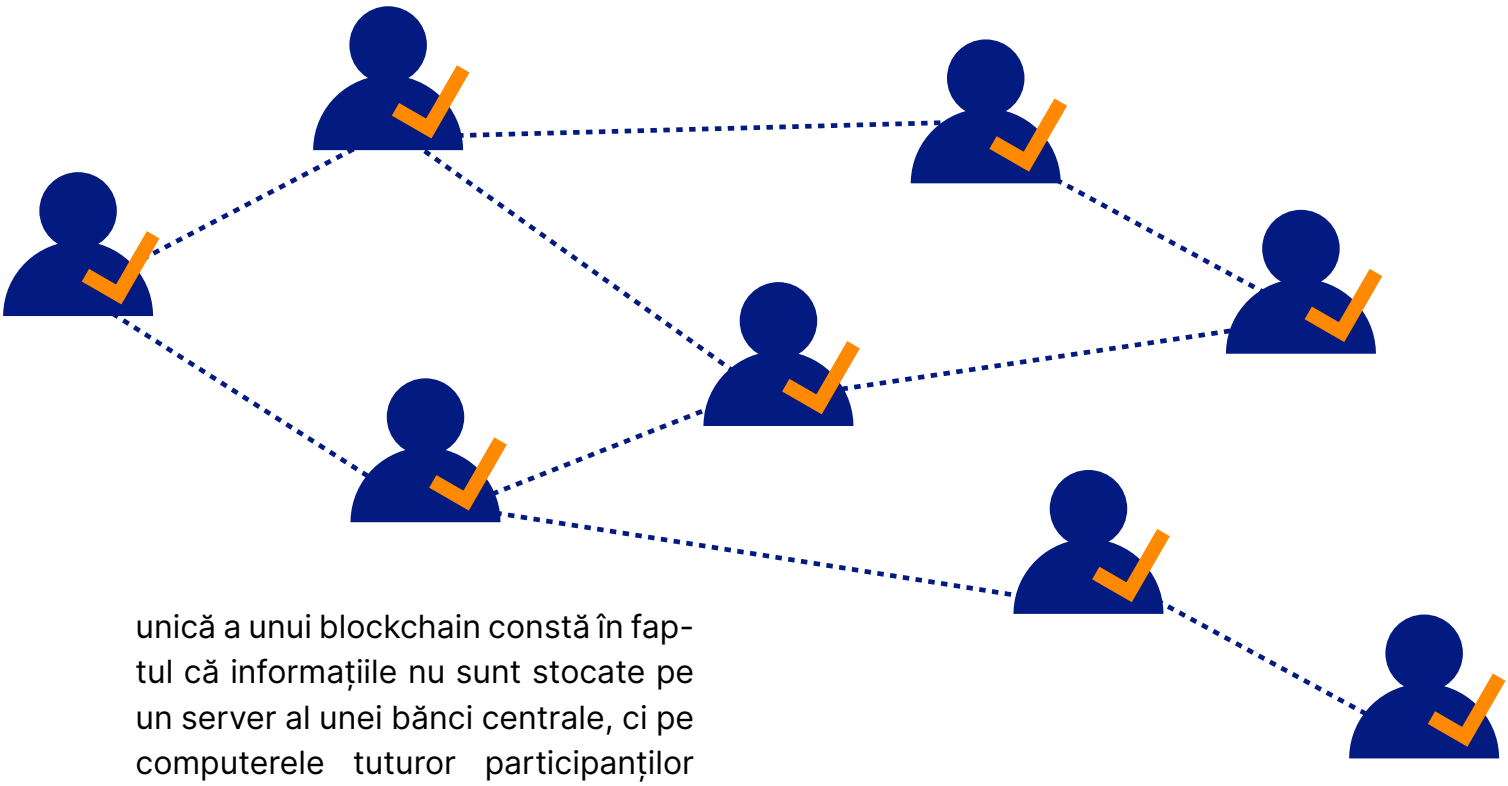
Înainte de lansarea Bitcoin, rețelele descentralizate se confruntau cu două provocări majore. În primul rând, cum se poate asigura că toți participanții primesc cele mai recente actualizări privind schimburile de proprietate – adică informații despre ce bitcoini au fost transferați și către cine. A doua provocare majoră este legată de felul cum participanții pot să verifice cu certitudine absolută că informațiile pe care le primesc sunt corecte.



Blockchain-ul

Aceste dificultăți au fost depășite datorită invenției blockchain. Un blockchain(care se traduce în limba română ca înlănțuire de blocuri) stochează informații și date în ordine cronologică. În cazul Bitcoin, toate tranzacțiile de la crearea sistemului și până astăzi sunt stocate în ordine cronologică în sute de mii de blocuri organizate într-un sistem informatic de coadă (modificarea informației se poate face doar începând cu blocul cel mai recent și necesită o cantitate uriașă de timp și resurse pentru a putea rescrie activitatea). Orice participant la rețea care dorește să afle cine deține fiecare Bitcoin poate urmări istoricul tranzacțiilor din blockchain și poate determina exact care sunt sumele. Astfel, dacă cineva dorește să trimită un bitcoin, orice terț poate verifica dacă persoana în cauză deține cu adevărat suma pretinsă.

Până în acest punct, mecanismul descris nu este nimic nou. Băncile folosesc un proces similar: dacă un client dorește să cheltuiască un franc elvețian, banca verifică istoricul tranzacțiilor pentru a vedea dacă francul mai aparține clientului sau dacă a fost deja cheltuit (trimis altcuiva). Cu toate acestea, caracteristică



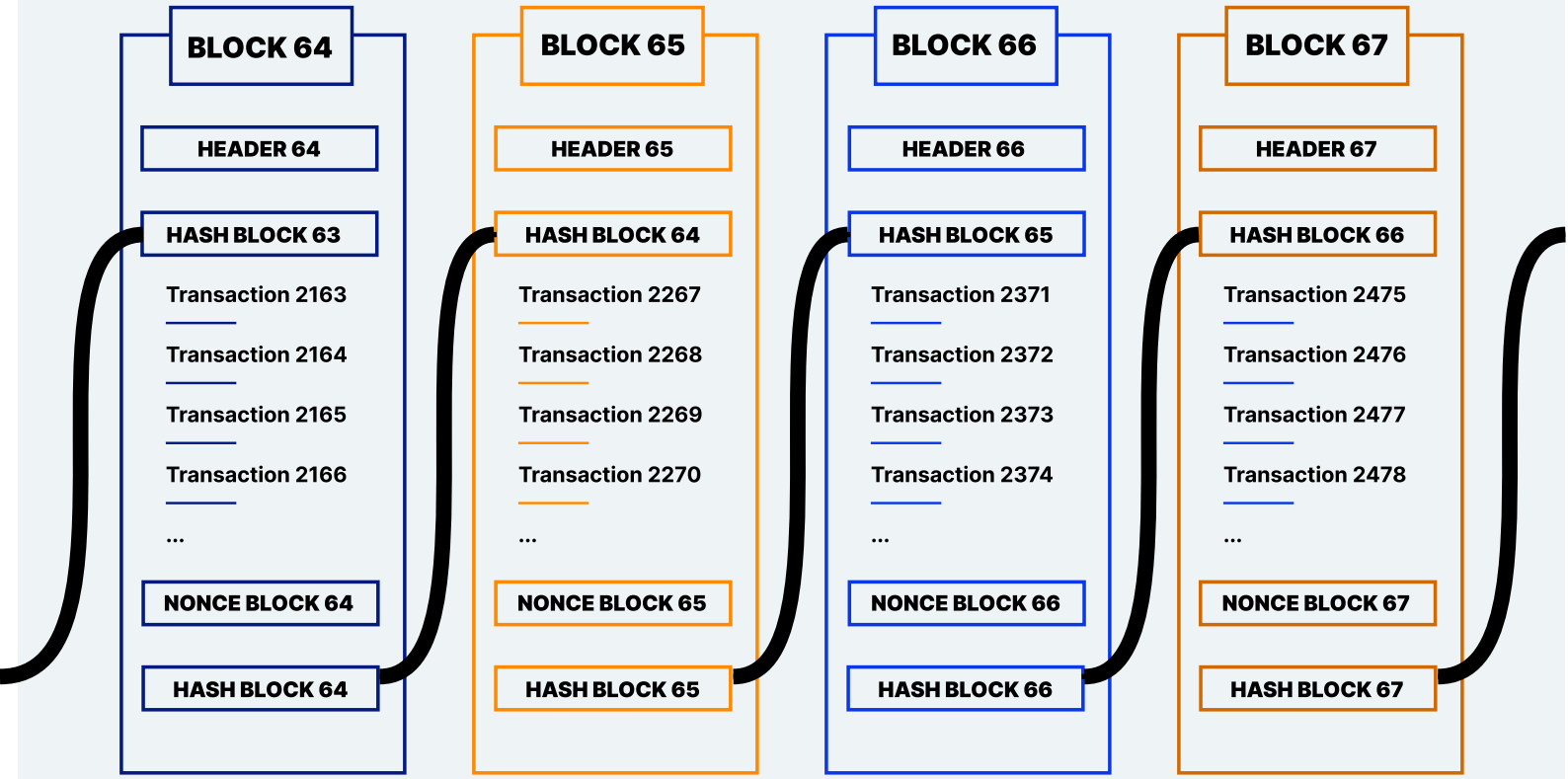
unică a unui blockchain constă în faptul că informațiile nu sunt stocate pe un server al unei bănci centrale, ci pe computerele tuturor participanților la rețea (așa-numitele noduri complete). Astfel, există în zeci de mii de copii ale registrului de tranzacții, răspândite în întreaga lume. Acesta este, de asemenea, motivul pentru care Bitcoin nu poate fi pur și simplu șters - pentru a face acest lucru, ar trebui să fie eliminate în același timp evidențele contabile stocate în toate computerele participante din întreaga lume.

Cu toate acestea, provocarea cu care se confruntă blockchain-ul este că fiecare participant la rețea trebuie să fie capabil să determine cu certitudine absolută că propria copie a registrului este corectă și că nicio tranzacție eronată sau frauduloasă nu intră în sistem. Deoarece, la fiecare 10 minute se adaugă la blockchain un nou bloc cu tranzacții recente, blockchain-ul este în continuă creștere și trebuie actualizat în permanență pe toate computerele participante, din toate colțurile lumii.

Aceste blocuri nou atașate trebuie să poată fi verificate de toate nodurile validatoare. Verificarea se face cu ajutorul unor reguli neschimbabile care sunt definite în codul informatic al rețelei Bitcoin. Aceste reguli definesc exact ce tranzacții sunt permise și care încalcă principiile fundamentale. Prin urmare, fiecare utilizator care descarcă o copie a blockchain-ului poate verifica dacă toate tranzacțiile sunt conforme cu regulile stabilite. În cazul în care o tranzacție se abate de la reguli, adică dacă este incorectă sau frauduloasă, aceasta este respinsă de participanții la rețea (noduri complete) și nu este inclusă în blockchain.

Mineritul Proof-of-Work (PoW)

Rețeaua Bitcoin dispune de un mecanism de limitare a adăugării de noi blocuri. Dacă oricine ar putea adăuga noi tranzacții și blocuri la înlănțuirea existentă, rețeaua ar ajunge în haos – blockchain-ul nu ar putea să se ac-



Antetul, rezultatul funcției hash a blocului anterior, toate tranzacțiile blocului curent și un număr aleatoriu (denumit „nonce“) sunt introduse într-o funcție matematică. Numărul aleatoriu se modifică până când rezultatul funcției hash are suficiente zerouri ca prefix. Acest proces se numește minerit.

tualizeze la nivel mondial suficient de repede, păstrând în același timp toate calitățile intacte.

Pentru a preveni acest lucru, Bitcoin funcționează cu un mecanism Proof-of-Work. Pentru ca cineva să câștige dreptul de a adăuga un nou bloc la înlănțuire, trebuie să furnizeze o dovadă că a muncit pentru a-l produce. O ilustrare simplă a acestui proces este un grup de oameni care caută ace într-un car cu fân. Cel care găsește primul un ac are dreptul de a adăuga un nou bloc în blockchain. În plus, cel care l-a găsit este recompensat cu noi unități bitcoin care se adaugă la cantitatea maximă de 21 de milioane, împreună cu sumele rezultate din comisioanele de tranzacție plătite de utilizatori pentru a avea transferurile incluse în acest bloc. De îndată ce blocul a fost atașat, procesul de căutare o ia de la capăt.

În realitate, minerii execută o funcție matematică de tip hash (algoritmul hash SHA-256) în căutarea unor numere specifice. Numărul hash al blocului anterior, tranzacțiile din blocul curent și un număr aleatoriu (nonce) sunt procesate împreună. Numărul aleatoriu este modificat până când funcția hash emite un rezultat cu un număr minim de zerouri de început. De exemplu, blocul #700000, creat la 11 septembrie 2021, a avut numărul hash valid:

0000000000000000000590fc0f3eba193a278534220b2b37e9849e1a770ca959.

Căutarea acestui număr, un proces denumit generic minerit, are două funcții principale:

– leagă blocurile între ele într-un mod matematic și criptografic, astfel încât toată lumea să poată verifica instant ordinea corectă. În același timp, mecanismul Proof-of-Work face aproape imposibilă modificarea acestei ordini.
– întârzie adăugarea de noi blocuri astfel încât, în medie, intervalul de timp dintre aceste blocuri să se păstreze în jurul valorii de 10 minute. Astfel, toți participanții la rețea din întreaga lume au suficient timp pentru a se actualiza la aceeași stare recentă a blockchain-ului.

Pe scurt, minerii asigură funcționarea rețelei Bitcoin. Datorită lor, noi tranzacții sunt procesate și adăugate la înlănțuirea de blocuri. Nodurile complete păstrează copii ale registrului, se asigură că regulile sunt respectate și se asigură că nicio tranzacție frauduloasă nu intră în sistem.

21 de milioane de Bitcoin

Deși în mod constant se adaugă blocuri la blockchain-ul Bitcoin, iar minerii sunt recompensați pentru această muncă prin BTC proaspăt-emis, masa monetară totală este limitată la 21 de milioane de Bitcoin. Pe scurt, nu vor exista niciodată mai mult de 21 de milioane de Bitcoin. Dar aceste 21 de milioane de monede nu s-au aflat în circulație de la început. Mai degrabă, ele sunt eliberate de codul Bitcoin în conformitate cu un program strict de emitere.

Când a fost lansat Bitcoin, codul a eliberat 50 de noi unități monetare pentru mineri la un interval de timp de aproximativ 10 minute. La patru ani din momentul lansării, numărul de bitcoini eliberați la zece minute a fost redus la jumătate. Acest proces se numește „înjumătățire“ și descrie fenomenul prin care recompensa per bloc pentru mineri scade la jumătate la fiecare 4 ani (210.000 de blocuri descoperite). În prezent, există deja 19 milioane de bitcoin în circulație. Restul de monede vor fi minate până în anul 2140. După aceea, minerii vor fi compensați doar prin intermediul comisioanelor de tranzacție pe care le primesc de la participanți.

Cantitatea strict limitată de unități bitcoin este una dintre proprietățile fundamentale ale criptomonedei și face din BTC o marfă extrem de rară. Această raritate digitală absolută este, de asemenea, o condiție prealabilă importantă pentru ca Bitcoin să funcționeze ca monedă de rezervă pe perioade lungi de timp. Este și motivul pentru care Bitcoin este adesea numit aur digital sau aur 2.0.

Rezultatul: proprietate digitală

Examinând combinația dintre toate caracteristicile rețelei Bitcoin, se poate vedea importanța acestei invenții.

Pentru prima dată în istorie, există un bun digital care este disponibil doar într-un număr strict limitat. Bitcoinii nu pot fi copiați sau duplicați.

Datorită acestei realizări, bitcoin este deseori numit proprietate digitală. Pentru că, așa cum fiecare bucată de pământ de pe planetă este unică și există o singură dată, fiecare unitate bitcoin este, de asemenea, unică și există o singură dată în spațiul digital.

Iar aceste unități bitcoin oferă drepturi absolute de proprietate. Doar persoana care deține cheia privată corespunzătoare, o combinație de numere și litere compusă din 64 de caractere, poate muta monedele asociate. Cu alte cuvinte, fără această cheie privată, Bitcoin nu poate fi furat, confiscat sau blocat. Acest lucru permite proprietarului să dețină un control absolut asupra resurselor sale financiare, indiferent dacă este milionar, refugiat politic sau creditor persecutat. Pentru prima dată de la invenția computerului, este posibil să deții cu adevărat active digitale.

DE CE BITCOIN?

Dar de ce avem toată această agitație în jurul Bitcoin? Pentru că posibilitatea de a deține cu adevărat un activ digital poate fi revoluționară. Dar de ce ar vrea cineva să dețină bitcoin?

Cel mai bun din ambele lumi

În secolele trecute, mijlocul principal de plată era reprezentat de metale prețioase. Mai târziu a apărut numerarul sub formă de monede și bancnote. Aceste forme de bani aveau avantajul de a putea fi stocate și cheltuite independent de terți. Expresia „numerarul este libertate tipărită“ rezumă foarte bine acest lucru. Cu toate acestea, dezavantajul metalelor prețioase și al banilor lichizi este că sunt dificil de utilizat în spațiul digital al internetului. Prin urmare, cel puțin de la apariția cumpărăturilor online, cardurile de debit și de credit s-au impus în rândul populației generale.

Dar acum, când majoritatea oamenilor folosesc banii digitali în conturi bancare în loc de numerar, riscurile de fraudă cauzată de contrapartidă sunt în creștere. Dacă, de exemplu, o instituție financiară își declară insolvența, economiile clienților ar putea fi pierdute. Sau, așa cum s-a întâmplat în Cipru în 2013, dacă retragerile de numerar sunt limitate drastic, se instituie controale de capital și are loc o expropriere forțată asupra conturilor de economii. În aceste situații, oamenii nu mai dețin controlul asupra banilor lor. Sau, așa cum se întâmplă în prezent în multe țări occidentale, clienții bancari nu au permisiunea de a trimite bani rudelor pentru că acestea locuiesc în Cuba, Iran,sau o altă țară aflată sub incidența unor sancțiuni. Astfel, părțile implicate într-o astfel de tranzacție depind de o terță parte care să le aprobe toate operațiunile.
Odată cu trecerea de la banii pe suport de hârtie la banii digitali, stocați

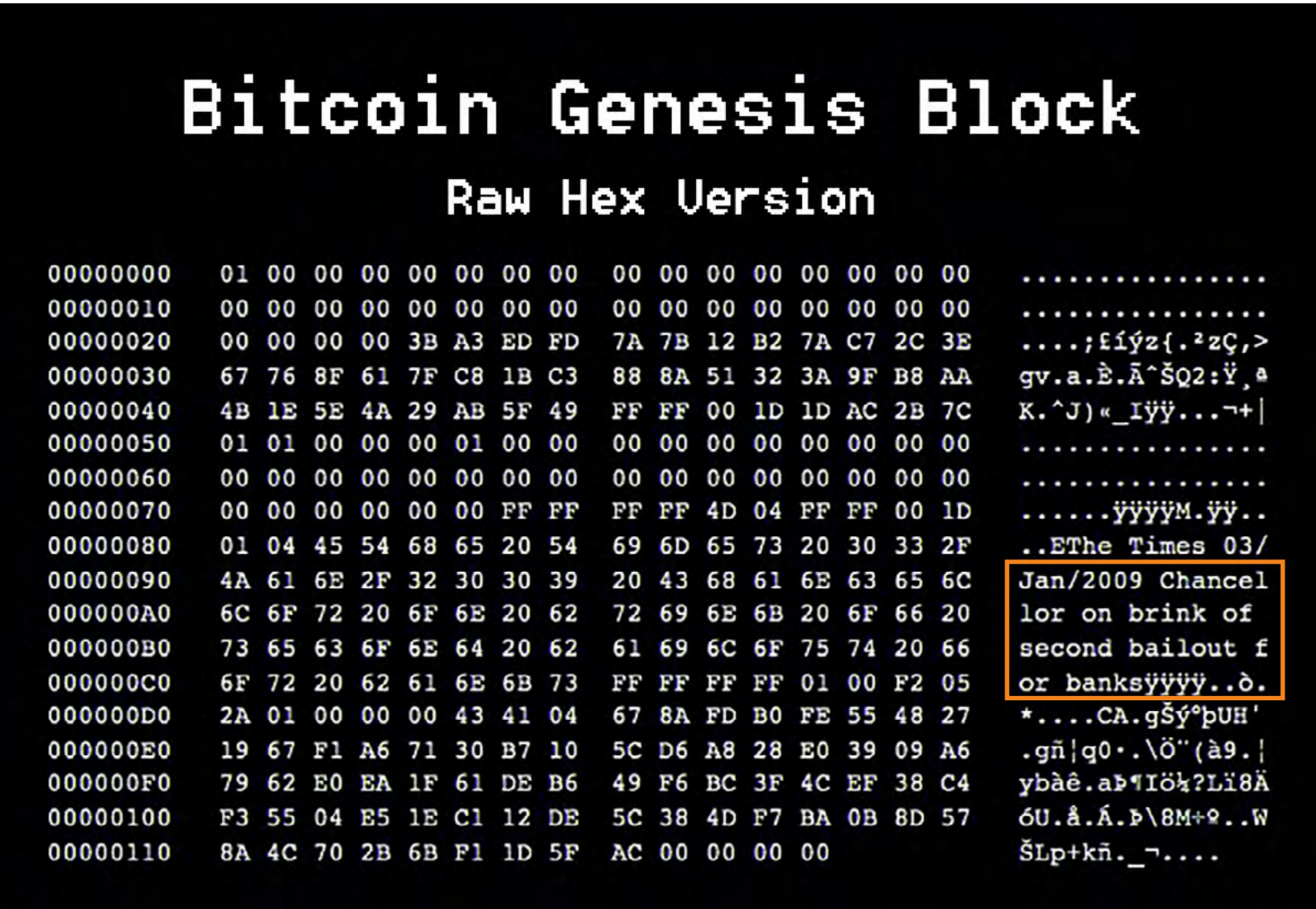
în conturi bancare, în cele din urmă nu mai deținem controlul asupra propriilor noastre economii. Până acum însă, acest dezavantaj a fost prețul pe care a trebuit să îl plătim pentru a participa la o viață digitalizată.

Bitcoin oferă o soluție la această dilemă. Ca monedă digitală, este ideal pentru a fi utilizat în spațiul digital. În același timp, Bitcoin poate fi stocat ca proprietate digitală fără a fi nevoie să se bazeze pe terțe părți (bănci) pentru păstrarea în siguranță. Astfel, proprietarii de Bitcoin își pot depozita monedele - sub formă de chei private - sub saltea sau oriunde consideră că este cel mai sigur.

Perfect Timing

Bitcoin a fost creat în timpul crizei financiare globale din 2008/2009. Pe primul bloc al lanțului de blocuri Bitcoin - numit și blocul Genesis - Satoshi Nakamoto a lăsat un mesaj puternic. El a citat un titlu publicat în ziarul The Times, care spunea: „Cancelarul este pe punctul de a acorda un al doilea plan de salvare pentru bănci“.

Prin acest act, Satoshi a exprimat filozofia critică față de stat a grupării Cypherpunks. În timpul crizei financiare din 2008, băncile centrale au pus în circulație cantități uriașe de bani noi pentru a salva băncile. În cele din urmă, însă, oamenii de rand au plătit pentru asta, deoarece eco-



nomiile lor și-au pierdut valoarea prin diluarea din cauza excesului de bani. Acest fapt i-a confirmat încă o dată pe Cypherpunk în neîncrederea lor în stat și în băncile centrale și le-a întărit convingerea că este nevoie urgentă de bani independenți de stat.

Aceeași procedură, doar că la scară mai mare, s-a repetat de la izbucnirea pandemiei Covid-19. Numai în 2020, masa monetară din SUA a fost extinsă cu 50%, iar în alte țări - inclusiv în Elveția - presa digitală de tipărire funcționează în mod constant. O consecință directă a acestei situații este reprezentată de ratele scăzute record ale dobânzilor - chiar și de ratele negative ale dobânzilor în Elveția - și de inflația puternică a activelor.

Acoperirea împotriva devalorizării monedei

Prin urmare, Bitcoin a fost lansat în cel mai bun moment posibil. Rareori problema banilor a fost mai relevantă și semnele de întrebare au fost mai mari decât astăzi. Cu oferta sa limitată de 21 de milioane, Bitcoin oferă un contrast plăcut față de bilanțurile în continuă creștere ale băncilor centrale. Rezerva sa limitată oferă protecție împotriva diluării capitalului propriu, așa cum s-a observat în cazul tuturor monedelor din lume în ultimele decenii.

Datorită configurației sale specifice, Bitcoin este conceput pentru a asigura conservarea puterii de cumpărare pe perioade lungi de timp. Deoarece Bitcoin este rar, ar trebui să se descurce chiar mai bine în această sarcină decât aurul, care are un flux net de intrare de 1-2% în fiecare an. În plus, costurile de stocare și transport ale Bitcoin sunt, de asemenea, semnificativ mai mici în comparație cu aurul, ceea ce permite, de asemenea, o mai bună conservare a valorii în timp.

Protecția proprietății

O altă problemă pe care Bitcoin o atenuează este protecția proprietății. În timp ce aurul sau banii lichizi trebuie, de obicei, depozitați în condiții de siguranță, cu costuri mari, pentru a fi protejați de furt, Bitcoin poate fi depozitat și transportat cu costuri practic zero. Chiar și sume substanțiale pot fi luate oriunde în lume cu ajutorul unui cod format din douăsprezece sau douăzeci și patru de cuvinte. Odată memorat și distrus fizic, acest cod nu mai poate fi furat de nimeni, ceea ce face ca Bitcoin din spatele codului să fie în siguranță și îi permite proprietarului său să le ia cu el în mormânt, dacă dorește.

CUMPĂRĂ BITCOIN

Există două modalități de a intra în posesia Bitcoin. Fie câștigi Bitcoin ca miner, fie cumperi Bitcoin de la o altă persoană. Deoarece mineritul cu dispozitive casnice a devenit practic imposibil în zilele noastre, singura cale rămasă pentru nou-veniți este să cumpere Bitcoin.

Burse criptografice și brokeri

Cel mai simplu mod de a cumpăra Bitcoin este prin intermediul unui schimb de cripto-monede sau al unui broker. Acestea funcționează în mod similar cu platformele de tranzacționare a acțiunilor. După deschiderea unui cont personal, franci elvețieni, euro sau dolari americani pot fi transferați prin transfer bancar sau prin card de credit. Odată ce banii au ajuns în contul personal de la bursa de tranzacționare, Bitcoin poate fi cumpărat 24/7 cu câteva clicuri la prețul curent al pieței. În Europa, este posibilă cumpărarea de Bitcoin fără înregistrare, verificare sau depunerea de bani mai întâi cu ajutorul popularei aplicații de investiții exclusiv în Bitcoin, Relai.

Peer-to-peer (Între egali)

Ca o alternativă la bursele de criptomonede, Bitcoin poate fi, de asemenea, achiziționat direct de la alți participanți pe piață prin intermediul platformelor peer-to-peer, fără a implica o bursă. Acest lucru permite un mai mare anonimat, deoarece nu trebuie dezvăluite date personale în acest proces.

ATM-uri Bitcoin

Există, de asemenea, posibilitatea de a retrage Bitcoin prin intermediul ATM-urilor. Acestea sunt deja disponibile în multe țări, inclusiv în Elveția, Germania, România și Austria. La ATM-urile Bitcoin, Bitcoin poate fi cumpărat în mod anonim cu numerar

sau cu cardul de credit. Nu este necesar nici un cont și nici un portofel cripto existent.

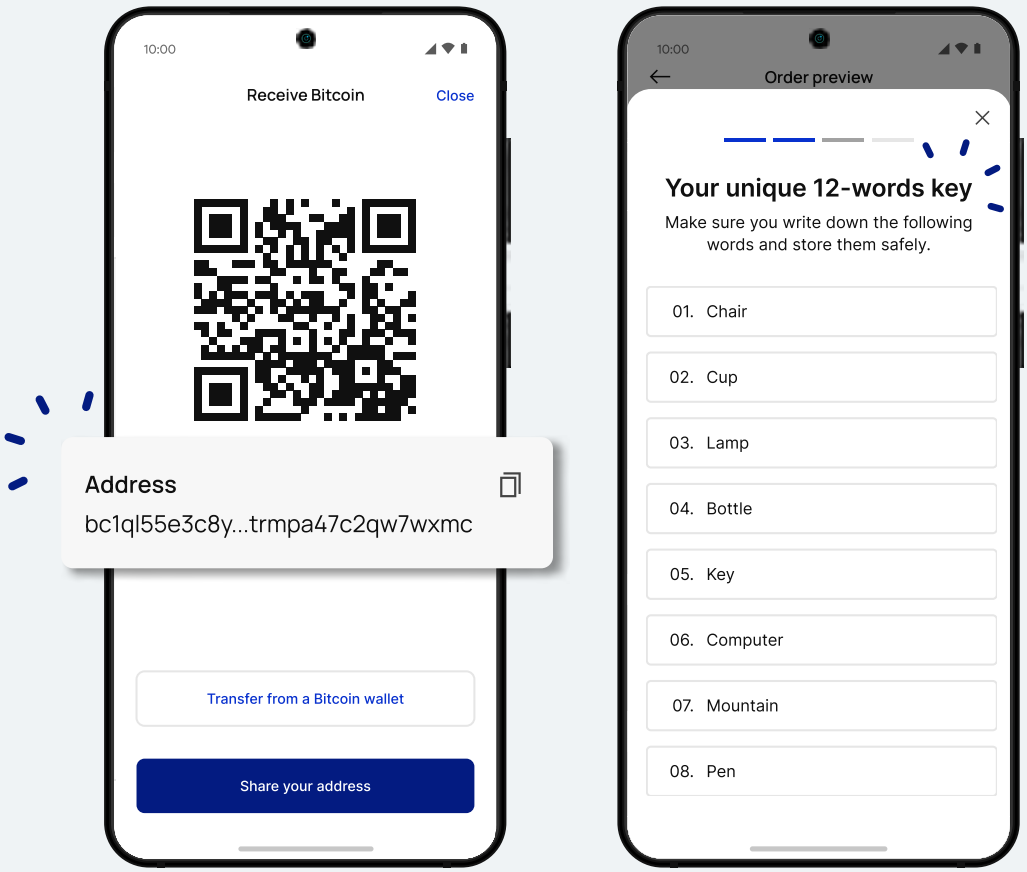
Stocați Bitcoin în siguranță

Odată ce monedele Bitcoin au fost achiziționate, se pune problema manipulării și depozitării lor în siguranță. Bitcoin și criptomonedele sunt guvernate de principiul: „nu sunt cheile tale, nu sunt monedele tale“. Pentru a deține cu adevărat Bitcoin, trebuie să fiți în posesia cheilor private corespunzătoare. Această expresie oarecum tehnică înseamnă că aveți cu adevărat controlul asupra Bitcoin-ului dvs. doar dacă îl păstrați într-un portofel digital personal, ale cărui chei private le dețineți.

Atâta timp cât monedele tale sunt depozitate pe o bursă de cripto-monede, acestea se află sub controlul bursei respective. În cazul în care bursa este spartă, dă faliment sau este frauduloasă, Bitcoin ar putea fi pierdute pentru totdeauna.

Custodie proprie

Spre deosebire de un cont bancar, Bitcoin vă oferă opțiunea de a vă stoca unitățile monetare într-un portofel personal. Acest lucru vă permite să fiți propria bancă și are avantajul că aveți control absolut asupra Bitcoin-ului dumneavoastră. În schimb, acest lucru vine și cu responsabilități. Cheia privată, care se prezintă adesea sub forma a douăsprezece sau douăzeci și patru de cuvinte, trebuie să fie stocată și păstrată în siguranță chiar de către proprietarul Bitcoin respectiv. Manipularea incorectă sau



neglijentă poate duce la pierderea irevocabilă a Bitcoin-ului.

Portofele: Portofele digitale

Portofelele digitale ajută la stocarea în siguranță a Bitcoin sau, mai exact, a cheilor private. Bitcoin în sine sunt întotdeauna stocate pe blockchain și nu pot fi transferate într-un portofel. Doar cheile de acces la Bitcoin pot fi stocate într-un portofel.

Astfel, portofelele au fost create pentru a stoca cheile private în siguranță și într-un mod simplu. În plus, acestea permit trimiterea și primirea de Bitcoin cu doar câteva click-uri. Astfel, portofelele sunt un instrument util pentru utilizarea Bitcoin.

Portofele software

Cele mai comune portofele sunt portofelele software. Portofelele software pot fi configurate ca aplicații desktop sau ca aplicații pentru smartphone. În timpul configurării, cheile private ale portofelului sunt enumerate sub forma a douăsprezece sau douăzeci și patru de cuvinte (frază de pornire). Aceste cuvinte sunt sinonime cu Bitcoin din portofelul respectiv. Oricine cunoaște aceste cuvinte are controlul asupra monedelor. Prin urmare, cuvintele trebuie să fie scrise în mod analog, de preferință pe hârtie, în secret și păstrate în siguranță. În cazul în care computerul sau smartphone-ul se pierde sau este furat, portofelul poate fi restaurat în orice moment cu ajutorul acestor cuvinte.

Portofelele software au avantajul că pot fi configurate rapid și sunt ușor de utilizat. Cu toate acestea, deoarece portofelele software sunt programe informatice instalate pe un dispozitiv și conectate direct la internet, există întotdeauna riscul atacurilor hackerilor

Portofele hardware

Dacă țineți la securitate, ar trebui să folosiți un portofel hardware. Aceste dispozitive mici stochează codurile de acces pentru Bitcoin pe un dispozitiv asemănător unui stick USB care este conectat la computer doar atunci când este necesar. Dispozitivul este conceput în așa fel încât nici măcar un computer infectat cu un software rău intenționat nu poate accesa codurile.

Atunci când se configurează un portofel hardware, sunt generate douăsprezece sau douăzeci și patru de cuvinte (fraza de pornire), care trebuie scrise în mod analogic și păstrate în siguranță. Dacă portofelul hardware se pierde vreodată, acesta poate fi restaurat cu ajutorul cuvintelor. Exemple de portofele hardware sunt BitBox și Trezor.

Made in Switzerland

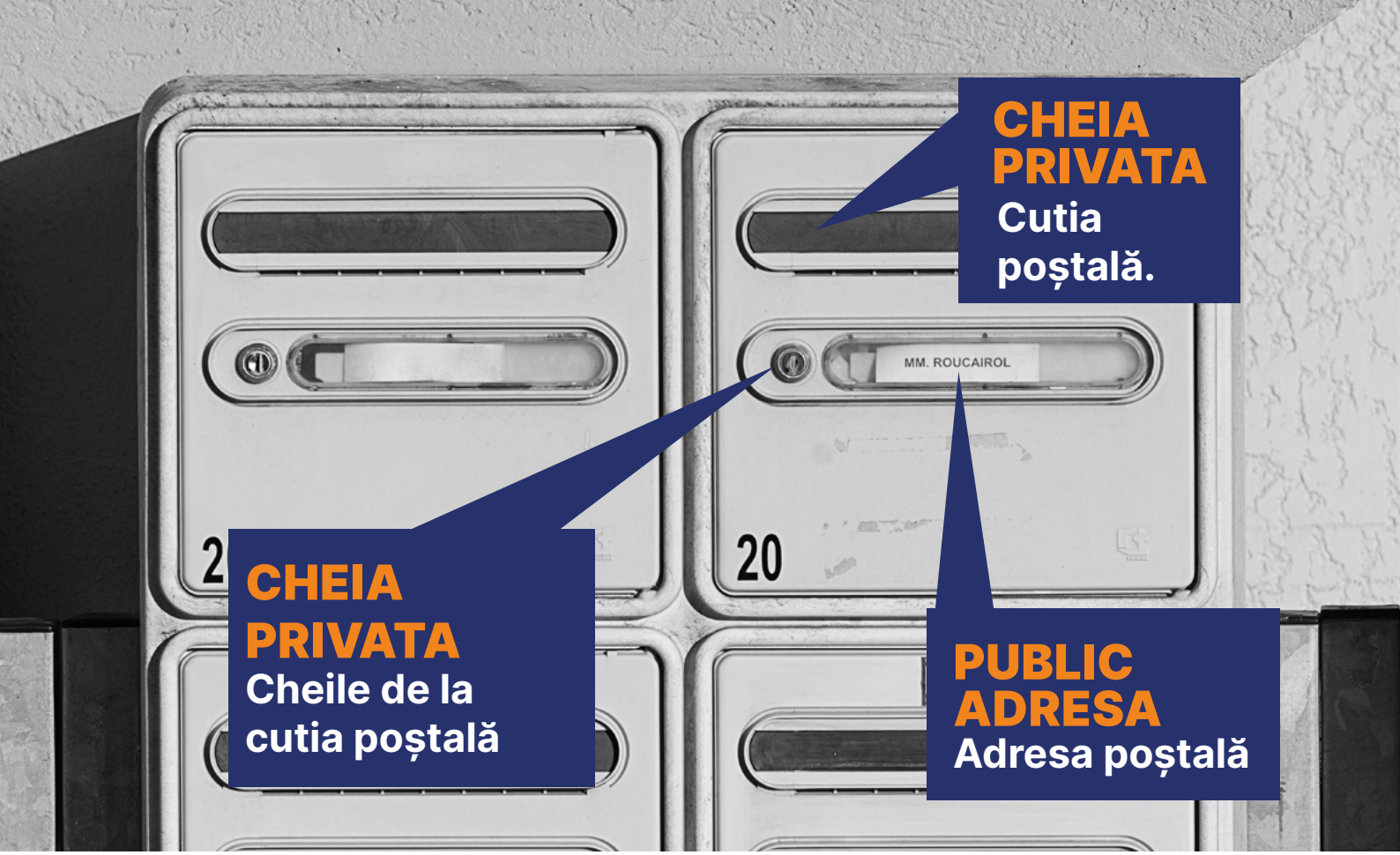
EUROPE'S EASIEST BITCOIN APP

Relai

Download on the App Store

GET IT ON Google Play

Buy bitcoin in 1 minute from as little as 10 EUR/CHF without verification.



Trimiteți și primiți Bitcoin

Trimiterea și primirea de Bitcoin este foarte ușoară. Fiecare portofel Bitcoin are o adresă publică generată de așa-numita cheie publică. Aceasta servește drept adresă de primire, similară unui IBAN. Oricine are această adresă poate trimite Bitcoin către portofelul corespunzător. Adesea, adresa este afișată sub forma unui cod QR, ceea ce simplifică și mai mult utilizarea.

Dacă doriți să trimiteți Bitcoin cuiva, puteți fie să introduceți adresa Bitcoin a destinatarului în portofelul dvs. la rubrica „trimite“, fie să scanați codul QR corespunzător. Taxele de tranzacție suportate sunt deduse automat din portofelul expeditorului. Valoarea comisioanelor de tranzacție variază în funcție de gradul de încărcare a rețelei și poate fi consultată aici. Este nevoie în medie de 10 minute pentru ca transferul să ajungă la destinatar. Cu toate acestea, poate dura și mai mult, în funcție de valoarea comisionului de tranzacție pe care sunteți dispus să îl plătiți.

Plătiți cu Bitcoin

Când a fost creat Bitcoin, s-a sperat că într-o zi Bitcoin va putea fi folosit pentru a plăti bunurile de zi cu zi. Și, în teorie, acest lucru este posibil astăzi. Unele departamente fiscale guvernamentale, organizații non-profit și un număr din ce în ce mai mare de companii acceptă Bitcoin ca mijloc de plată. Dar, deoarece tranzacțiile prin intermediul rețelei Bitcoin pot fi costisitoare și durează cel puțin 10 minute, acest lucru are sens doar pentru sume mai mari. Pentru a trimi-

te Bitcoin ieftin și rapid, este nevoie de o soluție alternativă.

Rețeaua Lightning - mai rapidă și mai ieftină

Prin urmare, un strat suplimentar a fost construit deasupra rețelei Bitcoin. Această rețea, numită Lightning, permite plata cu Bitcoin în câteva secunde, la un cost minim. În țări precum El Salvador, rețeaua Lightning este deja utilizată în mod activ și cu succes.

Prin urmare, în viitor, plata bunurilor de uz cotidian cu Bitcoin se va face în mare parte prin intermediul rețelei Lightning. Dezvoltările în acest domeniu sunt în plină desfășurare. Twitter, de exemplu, a introdus recent o funcție „bacșiș" care utilizează rețeaua Lightning. În plus, aplicația Strike oferă plăți în întreaga lume în diverse valute la cost zero prin intermediul rețelei Lightning. Prin urmare, este de așteptat ca, în viitor, doar sumele mari să fie decontate direct prin intermediul rețelei Bitcoin, în timp ce toate celelalte tranzacții vor fi efectuate prin intermediul rețelei Lightning.

Deoarece prin intermediul rețelei Lightning se trimit în principal sume mai mici, în loc de Bitcoin se utilizează ca unitate de cont Satoshis, sau pe scurt Sats. 1 Bitcoin este egal cu 100.000.000 de Satoshis. Pentru a utiliza rețeaua Lightning, trebuie configurat un portofel Lightning.

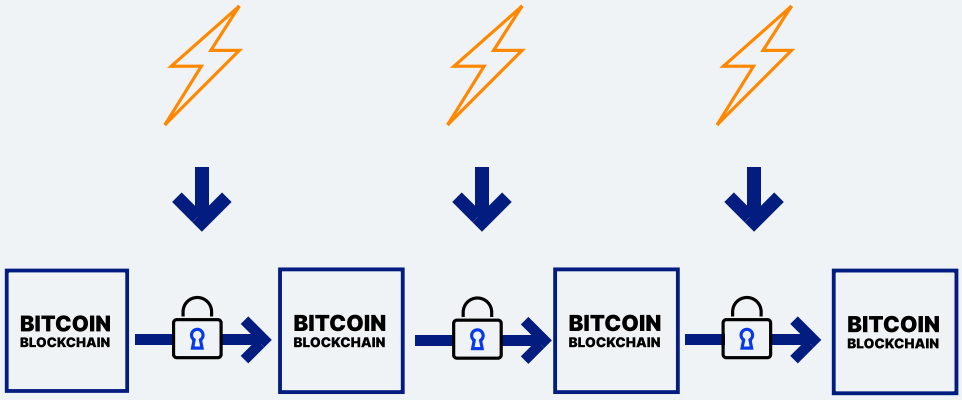
O PRIVIRE ÎN VIITOR

În cei peste zece ani de existență, Bitcoin a trecut prin multe suișuri și coborâșuri. Criptomoneda a fost declarată moartă sau a căzut în uitare în rândul publicului larg de mai multe ori după pierderi mari de preț. Cu toate acestea, Bitcoin s-a răspândit inexorabil în întreaga lume în ultimul deceniu.

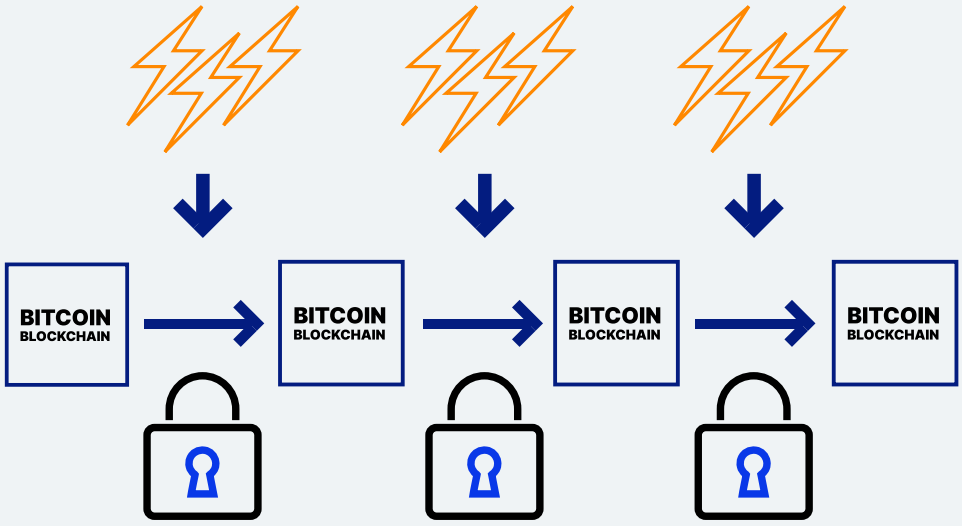
Bitcoin și energia

Una dintre primele preocupări care apare deseori în legătură cu dezvoltarea Bitcoin este consumul de energie al rețelei Bitcoin. Mineritul Bitcoin consumă deja o cantitate semnificativă de energie electrică la nivel mondial. Iar acest consum este posibil să crească în viitor, pe măsură ce tot mai mulți oameni se vor implica în mineritul Bitcoin.

Cu cât se utilizează mai puțină energie sub formă de putere de calcul pentru a construi blockchain-ul Bitcoin, cu atât este mai ușor să îl modificăm ulterior.



Cu cât se utilizează mai multă energie sub formă de putere de calcul pentru crearea blockchain-ul Bitcoin, cu atât este mai greu de modificat ulterior.



Când vorbim despre Bitcoin și energie, este important să înțelegem că volumul de energie care intră în rețeaua Bitcoin este esențial pentru securitatea rețelei. Cu cât mai multă energie intră în rețea, cu atât mai sigură este aceasta. Acest lucru se datorează faptului că, pentru ca blockchain-ul Bitcoin să fie modificat, aceeași cantitate de putere de calcul - și, prin urmare, de energie - care a fost investită pentru a crea blockchain-ul în primul rând trebuie să fie cheltuită din nou. Cu toate acestea, având în vedere că milioane de computere din întreaga lume furnizează putere de calcul rețelei Bitcoin, este aproape imposibil ca o persoană, o organizație sau un stat să adune vreodată suficientă putere de calcul pentru a face chiar și cele mai mici modificări ale blockchain-ului. Prin urmare, puterea de hashing și consumul de energie asociat reprezintă o caracteristică de securitate importantă a rețelei Bitcoin.

În plus, computerele de minerit Bitcoin au avantajul că pot fi amplasate oriunde în lume. Deoarece minerii au nevoie de cea mai ieftină energie electrică posibilă pentru a fi profitabili, aceștia se localizează adesea în locuri în care există o mulțime de surplusuri și, prin urmare, energie ieftină. Pe termen lung, este posibil ca acest

lucru să se întâmple în locuri unde există multă energie regenerabilă, deoarece aceasta produce cea mai ieftină energie electrică.

Potrivit Consiliului de minerit Bitcoin, minerii Bitcoin utilizează în prezent aproximativ 56% energie regenerabilă, iar tendința este în creștere. Mulți experți Bitcoin consideră că, în viitor, mineritul Bitcoin va fi alimentat cu energie regenerabilă de până la 100%.

Cu toate acestea, până când acest lucru nu se va întâmpla, consumul de energie al Bitcoin se reduce la întrebarea dacă banii și depozitul de valori sigure și nefalsificabile merită această cheltuială de energie - sau nu.

El Salvador - Bitcoin ca monedă națională

În urmă cu câțiva ani, vizionarii credeau deja că este posibil ca Bitcoin să fie recunoscută într-o zi ca mijloc legal de plată de către statele naționale. În vara anului 2021, a sosit momentul: El Salvador a fost prima țară din lume care a introdus Bitcoin ca mijloc legal de plată. În magazine, restaurante și la furnizorii de servicii de tot felul, plata nu se poate face doar cu dolari americani, ci și cu Bitcoin. În acest scop, cetățenilor le-a fost pus la dispoziție un portofel Bitcoin personalizat, care permite efectuarea plăților prin intermediul rețelei Lightning în câteva secunde și la un cost minim.

Alte țări, precum Ucraina, Brazilia și Panama, discută în prezent proiecte de lege similare. În cazul în care și alte țări ar urma exemplul El Salvadorului, acest lucru ar duce, pe de o parte, la o creștere și mai mare a cererii de Bitcoin și, mai important, la consolidarea credibilității Bitcoin ca „bani“. Prin urmare, acceptarea Bitcoin ca mijloc legal de plată în tot mai multe țări reprezintă o etapă decisivă în procesul de adaptare globală a Bitcoin.

Legi și reglementări

Aceste evoluții au făcut ca statele naționale, băncile centrale și companiile să fie nevoite să se ocupe intensiv de criptomonede. Diferite state, inclusiv Elveția, au emis reglementări și orientări cu privire la criptomonede. Acest pas este salutat de mulți participanți pe piață, deoarece creează siguranță juridică atât pentru proiectele crypto, cât și pentru investitorii implicați.

Reglementări se întrevăd la orizont și în SUA, care au adoptat până acum o abordare de laissez-faire. Forma exactă pe care o vor lua aceste noi legi de reglementare din SUA este monitorizată îndeaproape de comunitatea crypto la nivel mondial, deoarece va avea un impact major asupra întregului sector crypto.

Alte criptomonede

Bitcoin nu este nici pe departe singura criptomonedă din zilele noastre. În prezent, există peste 16.000 de criptomonede și active diferite. Aceste monede și jetoane au caracteristici și funcționalități diferite și nu au fost concepute toate ca „monede“ sau bani. Unele sunt mai mult ca niște acțiuni, în sensul că valoarea lor reflectă succesul unui proiect criptografic. Altele sunt necesare pentru a utiliza un anumit serviciu. Iar altele - așa-numitele token-uri meme - sunt în primul rând monede de distracție.

Pentru a evita pierderile, este, prin urmare, recomandabil să vă uitați mai atent la moneda respectivă și la proiectul din spatele ei înainte de a face orice investiție.

Monedele digitale ale băncii centrale (CBDC)

Criptomonedele sunt în tranziție de la o fază nereglementată a Vestului Sălbatic la o lume reglementată a criptofinanțelor. Această evoluție nu a lăsat băncile centrale nevătămate, și au fost lansate idei potrivit cărora băncile centrale ar trebui să emită propriile criptomonede. Aceste „monede digitale ale băncilor centrale“, sau CBDC, ar combina, spun susținătorii, stabilitatea unei monede de stat cu avantajele unei monede bazate pe blockchain. Pe scurt, ele ar crea numerar digital, ca să spunem așa.

Cu toate acestea, în funcție de de-
signul său, un CBDC poate lua forme fundamental diferite.
Diferite țări au lansat teste pilot cu diferite tipuri de CBDC, iar CBDC au fost deja lansate în câteva țări. Cu toate acestea, se așteaptă cu nerăbdare dacă și în ce formă vor fi lansate CBDC-uri de către zone monetare puternice din punct de vedere economic, cum ar fi SUA, UE sau China.

Concurența banilor

În ultimele decenii, societatea noastră s-a obișnuit atât de mult cu monedele de stat, încât, până de curând, mulți dintre noi abia dacă puteau imagina alte tipuri de bani. Dar nu cu mult timp în urmă, circulația în paralel a diferitelor tipuri de bani făcea parte din viața de zi cu zi. Existau bancnote de la diverse bănci, monede din diferite metale și alte valori monetare care puteau fi folosite ca mijloc de plată.

Odată cu Bitcoin, monedele nestatale sunt acum din nou disponibile ca alternativă la cele statale. Până în prezent, majoritatea guvernelor au tolerat Bitcoin. Într-o anumită măsură, acest lucru s-ar putea datora naturii sale descentralizate, care face ca Bitcoin să fie dificil de atacat. Pentru cetățeni, acest lucru înseamnă că o alternativă digitală la banii statului este acum disponibilă alături de aur și argint. Efectele acestei concurențe monetare suplimentare vor fi interesante de observat în viitor.

BITCOIN, CE URMEAZĂ?

Dacă vă întrebați ce ar trebui să faceți cu toate aceste informații, permiteți-mi să vă fac o sugestie. Intrarea în lumea Bitcoin nu costă nimic, nici timp, nici bani. Dar veți cunoaște o tehnologie care este pe cale să ne schimbe lumea și viitorul.

Prin urmare: Creați un cont pe o bursă de criptomonede sau descărcați un portofel pe smartphone și cumpărați Bitcoin pentru 50 RON. Sau cereți unui coleg să vă trimită niște Bitcoin în portofelul dumneavoastră. Dar puneți mâna pe Bitcoin cel puțin o dată.

Pentru că, dacă Bitcoin va reuși să pătrundă și va deveni la fel de omniprezent ca și internetul, nu numai că veți ști despre el în mod teoretic, dar veți fi folosit și dumneavoastră Bitcoin. Uneori, acest lucru face diferența, deoarece vă oferă o imagine și o senzație a tehnologiei, ceea ce vă plasează în fața majorității oamenilor.

DESPRE

AUTOR

Daniel Jungen este economist și jurnalist financiar cu experiență în domeniul activelor criptografice. Daniel este co-fondator a InsightDeFi, un butic de cercetare specializat în tot ceea ce înseamnă cripto. Împreună cu partenerii săi de la InsightDeFi, aceștia publică un buletin informativ bisăptămânal ((în limba germană) despre Bitcoin, DeFi și Crypto.

RELAI

Fondată în Elveția de Julian Liniger și Adem Bilican, după ce s-au luptat să găsească un spațiu sigur și fără probleme pentru a cumpăra Bitcoin, Relai face economisirea și investițiile în bitcoin accesibile tuturor. Aplicația destinată exclusiv Bitcoin este concepută pentru a fi simplă și intuitivă, permițând oricărei persoane din Europa să cumpere și să vândă Bitcoin în câteva minute, fără a fi nevoie de înregistrare, verificare sau depuneri. Auditată în mod independent și cu peste 35 de milioane de franci elvețieni investiți în Bitcoin prin intermediul platformei sale, Relai le oferă consumatorilor șansa de a debloca noi mijloace de economisire și de investiție.

Aflați mai multe la Relai.app.

Mulțumim lui @ciprianhodl care a tradus această carte electronică din engleză în română.“

De asemenea, îi mulțumesc lui @TheVladCostea și lui @liviudm pentru că au revizuit traducerea și au oferit sfaturi.