UNIVERSITATEA TITU MAIORESCU

GRAD DE ÎNCREDERE RIDICAT

Blockchain

Agenda

- Introducere
- Context istoric și concepte precursoare
- Fundamentele teoretice ale Blockchain
- Apariția Bitcoin și White Paper-ul lui Satoshi Nakamoto
- Structura tehnică a unui Bloc Bitcoin
- Mecanismul Proof-of-Work (PoW) și dificultatea
- Evoluția Blockchain si aparatitia Ethereum (Mecanismul Proof-of-Stake)
- Alte retele Blockchain
- Demo – Blockchain privat si lansarea si tranzactionarea unui Token (OVI)
- Întrebări și Discuții

Mihai Ghita

- 30 de ani experienta in IT
- Master in Securitate Cibernetica
- Am lucrat pentru lideri din industria IT
  - Oracle
  - Quest
  - Symantec
  - Veritas
- 7 ani de Global IT, in McDonald's Corporation
- Doctorand la Academia Tehnica Militara – Criptografie si Blockchain
- Asistent Universitar la Titu Maiorescu

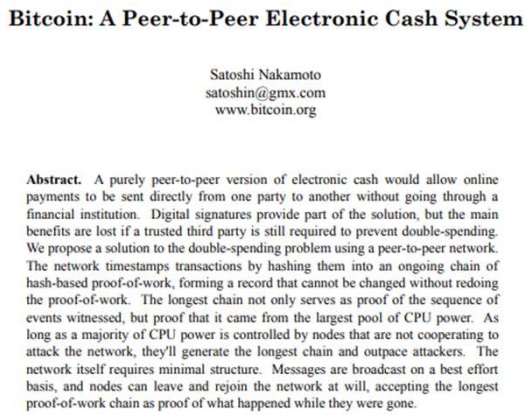
Originea și Evoluția Tehnologiei Blockchain

Contextul tehnologiei Blockchain

- Promisiunile Tehnologiei Blockchain
  - Sistem sigur și transparent
  - Transfer și stocare descentralizată a valorii și datelor
- Asocierea Inițială cu Bitcoin
  - Prima criptomonedă apărută
- Extinderea Aplicabilității
  - Industria financiară
  - Lanțurile de aprovizionare
  - Sectorul guvernamental
  - Sănătate
  - Identitate digitală

Context istoric și originile Blockchain

- Precursorii conceptului de registru distribuit
  - Ideea de registre distribuite și structuri de date imuabile a existat înainte de Bitcoin
  - 1979 – Ralph Merkle brevetează arborele de hash (Merkle Tree).
  - Cercetători și dezvoltatori explorau metode de timestamping digital și certificare a autenticității fișierelor în anii '90
  - Lucrarea lui Stuart Haber și W. Scott Stornetta din 1991 descria un sistem pentru înregistrarea documentelor digitale
  - Hashcash, creat de Adam Back în 1997, folosea un mecanism de tip „proof-of-work" pentru protecția împotriva spamului
- Apariția Bitcoin și rolul lui Satoshi Nakamoto
  - În 2008, Satoshi Nakamoto a publicat lucrarea „Bitcoin: A Peer-to-Peer Electronic Cash System"
  - Bitcoin este o monedă digitală descentralizată bazată pe o rețea P2P și blockchain



Bitcoin: A Peer-to-Peer Electronic Cash System

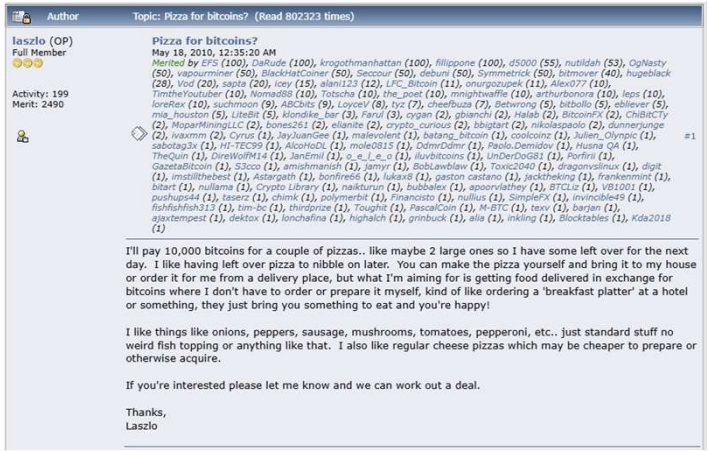
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

An	Eveniment-cheie	Impact
1979	Ralph Merkle patentează „hash tree”.	Structura Merkle permite verificarea eficientă a seturilor mari de date.
1991	Haber & Stornetta: „How to Time-Stamp a Digital Document”.	Lanț de hash-uri cu marcaj temporal – prim model tip blockchain.
1997	Adam Back publică Hashcash.	Introduce Proof-of-Work ca „cost computațional”.
1998	Wei Dai propune b-money.	Ideea unui cash anonim distribuit.
2005	Nick Szabo publică Bit Gold.	Lanț Proof-of-Work + timestamp, precursor Bitcoin.
31 oct 2008	Satoshi publică white-paper Bitcoin.	Combinație completă: PoW, rețea P2P, rezolvare double-spending.
3 ian 2009	Genesis Block Bitcoin.	Lansarea primei criptomonede funcționale.
2014	Faliment Mt. Gox.	Evidențiază riscul custodiei centralizate, impuls pentru reglementare.
30 iul 2015	Ethereum lansează rețeaua Frontier.	Introducerea smart-contractelor Turing-complete.
17 iun 2016	The DAO hack (3,6 M ETH).	Hard-fork ETH ↔ ETC, lecție despre securitatea contractelor.
24 aug 2017	SegWit activat pe Bitcoin.	Rezolvă maleabilitatea, crește capacitatea, pregătește Lightning.
2017	ICO-mania (~5 mld USD).	Model de finanțare directă via token-uri, atrage atenția autorităților.
15 mar 2018	Lightning Network mainnet-beta.	Plăți Bitcoin off-chain, sub-secundă, fee infime.
16 mar 2020	Solana mainnet-beta.	Debit mii TPS cu Proof-of-History și PoS.
14 nov 2021	Taproot activat pe Bitcoin.	Semnături Schnorr, MAST, scripturi mai private/eficiente.
15 sep 2022	Ethereum Merge (PoS).	Reduce consumul de energie cu ~99,9 % și scade emisia ETH.
31 aug 2021 – 2023	Arbitrum One depășește 1 mld tranzacții.	Confirmă scalarea Ethereum prin roll-up L2.
10 ian 2024	SEC aprobă Spot Bitcoin ETF-uri.	Integrare BTC în piețele financiare tradiționale.
13 mar 2024	Upgrade Dencun (EIP-4844) pe Ethereum.	Proto-Danksharding: cost redus pentru datele roll-up-urilor.
2025	Generalizarea L2 (Base, zkSync) & app-chains (Polygon CDK).	Peisaj multi-chain, lichiditate cross-chain.

„Bitcoin Pizza Day”

- Programatorul “laszlo” (Laszlo Hanyecz) postează oferta de a plăti **10 000 BTC** pentru două pizza Papa John’s.
- În seara de 22 mai, utilizatorul „jercos”(Jeremy Sturdivant) acceptă oferta, cumpără pizza cu cardul şi primește cei 10 000 BTC.
- Tranzacția demonstrează că bitcoinul poate fi folosit ca **monedă de schimb reală**; 22 mai este sărbătorit anual în comunitate drept „Pizza Day”.
- La cursul de pe BitcoinMarket (~0,003 USD/BTC) cele două pizza costau ≈ 30 USD; la prețurile din 2025, valoarea istorică a ajuns să depășească un miliard USD.



Author | Topic: Pizza for bitcoins? (Read 802323 times)

laszlo (OP)
Full Member
Activity: 199
Merit: 2490

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM
Merited by EFS (100), DaRude (100), krogothmanhattan (100), fillippone (100), d5000 (55), nutildah (53), OgNasty (50), vapourminer (50), BlackHatCoiner (50), Seccour (50), debuni (50), Symmetrick (50), bitmover (40), hugeblack (28), Vod (20), sapta (20), icey (15), alani123 (12), LFC_Bitcoin (11), onurgozupek (11), Alex077 (10), TimtheYoutuber (10), Nomad88 (10), Totscha (10), the_poet (10), rmightwaffle (10), arthurbonora (10), leps (10), loreRex (10), suchmoon (9), ABCbits (9), Loycev (8), tyz (7), cheefbuza (7), Betwrong (5), bitbollo (5), ebliever (5), mia_houston (5), LiteBit (5), klondike_bar (3), Farul (3), cygan (2), gbianchi (2), Halab (2), BitcoinFX (2), ChiBitCTy (2), MoparMiningLLC (2), bones261 (2), elianite (2), crypto_curious (2), bbigtart (2), nikolaspaolo (2), dunnerjunge (2), ivaxmm (2), Cyrus (1), JayJuanGee (1), malevolent (1), batang_bitcoin (1), coolcoinz (1), Julien_Olympic (1), sabotag3x (1), HI-TEC99 (1), AlcoHoDL (1), mole0815 (1), DdmrDdmr (1), Paolo.Demidov (1), Husna QA (1), TheQuin (1), DireWolfM14 (1), JanEmil (1), o_e_l_e_o (1), iluvbitcoins (1), UnDerDoG81 (1), Porfirii (1), GazetaBitcoin (1), S3cco (1), amishmanish (1), jamyr (1), BobLawblaw (1), Toxic2040 (1), dragonvslinux (1), digit (1), imstillthebest (1), Astargath (1), bonfire66 (1), lukaxs (1), gaston castano (1), jackiheking (1), frankenmint (1), bitart (1), nullama (1), Crypto Library (1), naikturun (1), bubbalex (1), apoorvlathey (1), BTCLiz (1), VB1001 (1), pushups44 (1), taserz (1), chimk (1), polymerbit (1), Financisto (1), nullius (1), SimpleFX (1), invincible49 (1), fishfishfish313 (1), tim-bc (1), thirdprize (1), Toughit (1), PascalCoin (1), M-BTC (1), texv (1), barjan (1), ajaxtempest (1), dektox (1), lonchafina (1), highalch (1), grinbuck (1), alia (1), inkling (1), Blocktables (1), Kda2018 (1)

#1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

laszlo (OP)
Full Member
Activity: 199
Merit: 2490

→ **Re: Pizza for bitcoins?**
May 22, 2010, 07:17:26 PM
Merited by EFS (100), fillippone (62), paxmao (10), vizique (10), o_e_l_e_o (4), icopress (4), dragonvslinux (2), xtraely (2), Farul (2), vapourminer (1), cAPSLOCK (1), bitbollo (1), ABCbits (1), Searing (1), DdmrDdmr (1), Husna QA (1), BitcoinFX (1), DireWolfM14 (1), 600watt (1), TheBeardedBaby (1), Toxic2040 (1), Heisenberg_Hunter (1), nullama (1), Spray. (1), TotSamiy (1), Aricoin (1), dektox (1)

#11

I just want to report that I successfully traded 10,000 bitcoins for pizza.

Pictures: http://heliacal.net/~solar/bitcoin/pizza/

Thanks jercos!

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

sirius
Bitcoiner
Sr. Member
Activity: 429
Merit: 1052

Re: Pizza for bitcoins?
May 22, 2010, 10:10:25 PM
Merited by EFS (10), Aricoin (1)

#12

Congratulations laszlo, a great milestone reached

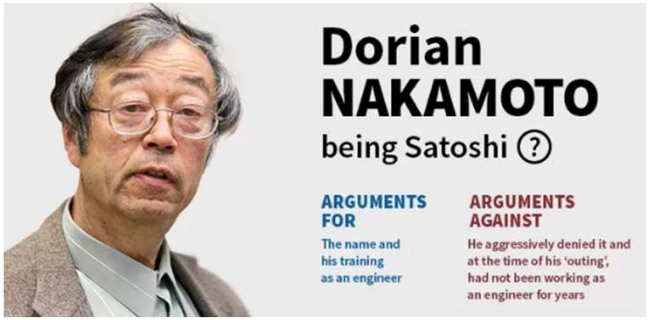
„Bitcoin Pizza Day”

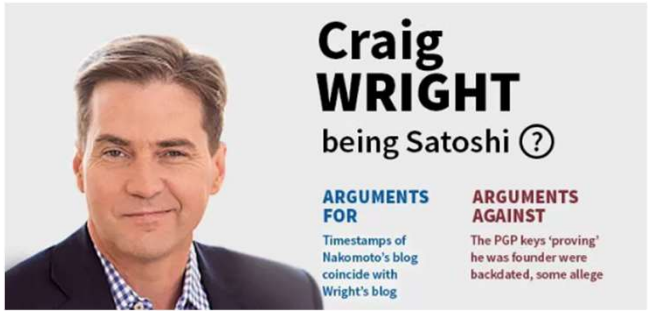
- **12.Jun.2010** - This is an open offer, by the way. I will trade 10,000 BTC for 2 of these pizzas any time as long as I have the funds (I usually have plenty). If anyone is interested, please let me know ... My 1-year-old daughter really enjoys pizza too! She just smears it all over her face if you give her a whole slice, but she does eventually manage to get most of it in her mouth (minus a few loose toppings of course).

- **04.Aug.2010** - Well, I didn't expect this to be so popular, but I can't really afford to keep doing it since I can't generate thousands of coins a day anymore. Thanks to everyone who bought me pizza already but I'm kind of holding off on doing any more of these for now.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

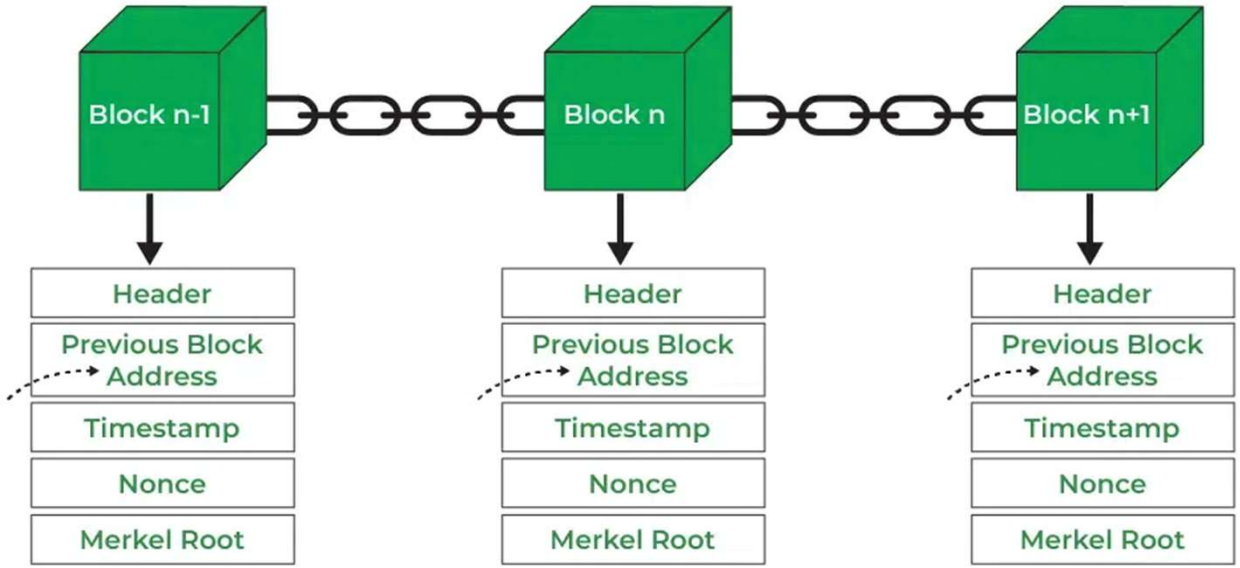
Satoshi Nakamoto





Fundamente teoretice ale Blockchain

- Definiție și Principii de Bază
  - Blockchain-ul este un registru digital distribuit și imuabil
  - Blocurile sunt interconectate prin criptografie
  - Principii: Descentralizare, Imuabilitate, Transparență, Securitate criptografică
- Elementele unui Blockchain
  - Bloc: Conține informații despre tranzacții și un hash al blocului anterior
  - Hash: Rezultatul unei funcții criptografice care mapează datele la un șir unic de caractere
  - Nod: Computer care rulează protocolul blockchain și menține o copie a lanțului de date
  - Rețea P2P: Structură de distribuție a datelor fără entități centrale de control
- Funcționarea unui Blockchain
  - Validarea: Tranzacțiile noi sunt verificate și introduse într-un bloc nou
  - Ordinea: Blocurile sunt adăugate într-o secvență strictă



Fundamente teoretice ale Blockchain

Aplicații și utilizări actuale ale Blockchain

Criptomonede și contracte inteligente

- Criptomonede populare: Bitcoin, Ethereum, Litecoin, Ripple
- Transfer rapid, global și cu comisioane reduse
- Contracte inteligente: cod software automatizat pe blockchain
- Executare automată la îndeplinirea condițiilor prestabilite
- Implementarea acordurilor și proceselor fără intermediari

Domenii adiționale

- Logistică și lanțuri de aprovizionare: trasabilitate și transparență
- Sănătate: stocarea și partajarea securizată a datelor medicale
- Sector public: gestionarea identității digitale și a sistemelor de vot electronic
- Energie: piața peer-to-peer pentru tranzacționarea energiei solare
- Asigurări: procese de despăgubire automatizate prin contracte inteligente

Scalabilitate și consum energetic

- Scalabilitatea blockchain-urilor
  - Probleme majore în rețelele publice
  - Volume mari de tranzacții îngreunează rețeaua
  - Creșterea timpilor de confirmare în mecanisme PoW
  - Bitcoin procesează doar câteva tranzacții pe secundă
  - Rețelele centralizate procesează mii sau zeci de mii de tranzacții
- Consum energetic al blockchain-urilor PoW
  - Consumul energetic este substanțial
  - Discuții despre impactul asupra mediului
  - Necesitatea unor protocoale mai eficiente (de ex. PoS)

Proof of Work (PoW)

- Conceptul de Proof of Work
  - Primul mecanism de consens implementat în blockchain (Bitcoin)
  - Nodurile specializate (mineri) concurează pentru a rezolva puzzle-uri criptografice complexe
- Funcționare
  - Minerii folosesc putere de calcul pentru a rezolva puzzle-uri
  - Primul care găsește soluția validează blocul de tranzacții și obține o recompensă
- Securitate
  - Securitatea se bazează pe dificultatea de a falsifica istoricul
  - Ar necesita o putere de calcul uriașă pentru a falsifica
- Avantaje
  - Securitate foarte ridicată împotriva atacurilor
- Dezavantaje
  - Consum energetic mare, viteza de procesare relativ mica

Proof of Work (PoW)

Header-ul unui bloc conține informațiile care sunt efectiv introduse în algoritmul de hashing. Acesta include:

- ☑ **Version** — Versiunea protocolului (indică regulile folosite).
- ☑ **Previous Block Hash** — Hash-ul blocului anterior (pentru a lega blocurile între ele).
- ☑ **Merkle Root** — Hash-ul rădăcinii arborelui Merkle (pentru a sumariza toate tranzacțiile din bloc).
- ☑ **Timestamp** — Data și ora la care blocul a fost creat (format UNIX timestamp).
- ☑ **Bits** — Dificultatea target pentru algoritmul de proof-of-work.
- ☑ **Nonce** — O valoare aleatorie folosită pentru a găsi un hash valid.

Hash=SHA-256(SHA-256(Header bloc))

Hash-ul rezultat este apoi comparat cu o valoare numită **target difficulty** (dificultatea target).

- Dificultatea definește cât de greu este să găsești un hash valid.
- Un hash este considerat valid dacă este **mai mic sau egal** cu valoarea target.

Minerii ajustează continuu valoarea **nonce** și recalculează hash-ul până când acesta îndeplinește condițiile impuse de dificultatea target.

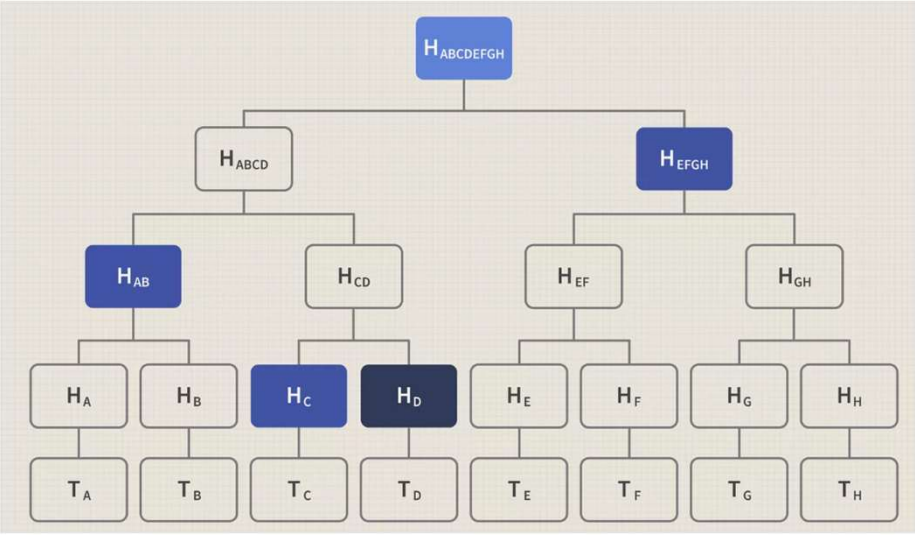
Proof of Work (PoW)

- Un procesor de **3 GHz** are **3 miliarde de cicluri pe secundă**. Numărul de calcule **SHA-256 pe secundă** depinde de câte cicluri sunt necesare pentru a efectua un singur hash. De exemplu:
- Dacă un hash SHA-256 necesită aproximativ **100 de cicluri**, atunci:
  - 3 miliarde ÷ 100 ≈ **30 de milioane de SHA-256 pe secundă**.
- Dacă un hash necesită **150 de cicluri**, atunci:
  - 3 miliarde ÷ 150 ≈ **20 de milioane pe secundă**.
- Dacă un hash necesită **200 de cicluri**, rezultatul este:
  - 3 miliarde ÷ 200 ≈ **15 milioane pe secundă**.
- În concluzie, în funcţie de implementare şi de optimizările folosite (precum utilizarea de instrucţiuni dedicate sau optimizări la nivel de asamblare), un procesor de **3 GHz** ar putea calcula undeva între **15 şi 30 de milioane de SHA-256 pe secundă**.

Proof of Work (PoW)

- Timpul mediu necesar pentru a mina un bloc de Bitcoin cu un singur Antminer S19 depinde de puterea de hash a dispozitivului și de dificultatea rețelei. Să presupunem că Antminer S19 are o putere de aproximativ **95 TH/s** și că rețeaua Bitcoin operează la un nivel total de hash rate de ordinul exahash-urilor (EH/s). În condiții ideale, întreaga rețea găsește un bloc la fiecare **10 minute**, iar șansa unui singur miner de a găsi blocul este proporțională cu fracțiunea puterii sale de hash din totalul rețelei.
- De exemplu, dacă rețeaua are aproximativ **350 EH/s** (adică **350.000.000 TH/s**), atunci:
- **Fracțiunea puterii tale** = 95 TH/s ÷ 350.000.000 TH/s ≈ **$2{,}7 \times 10^{-7}$**
- Astfel, timpul mediu pentru a găsi un bloc pe cont propriu ar fi:
- **Timp mediu** = 10 minute ÷ ($2{,}7 \times 10^{-7}$) ≈ **37 milioane de minute**, adică aproximativ **70 de ani**.

Proof of Work (PoW)



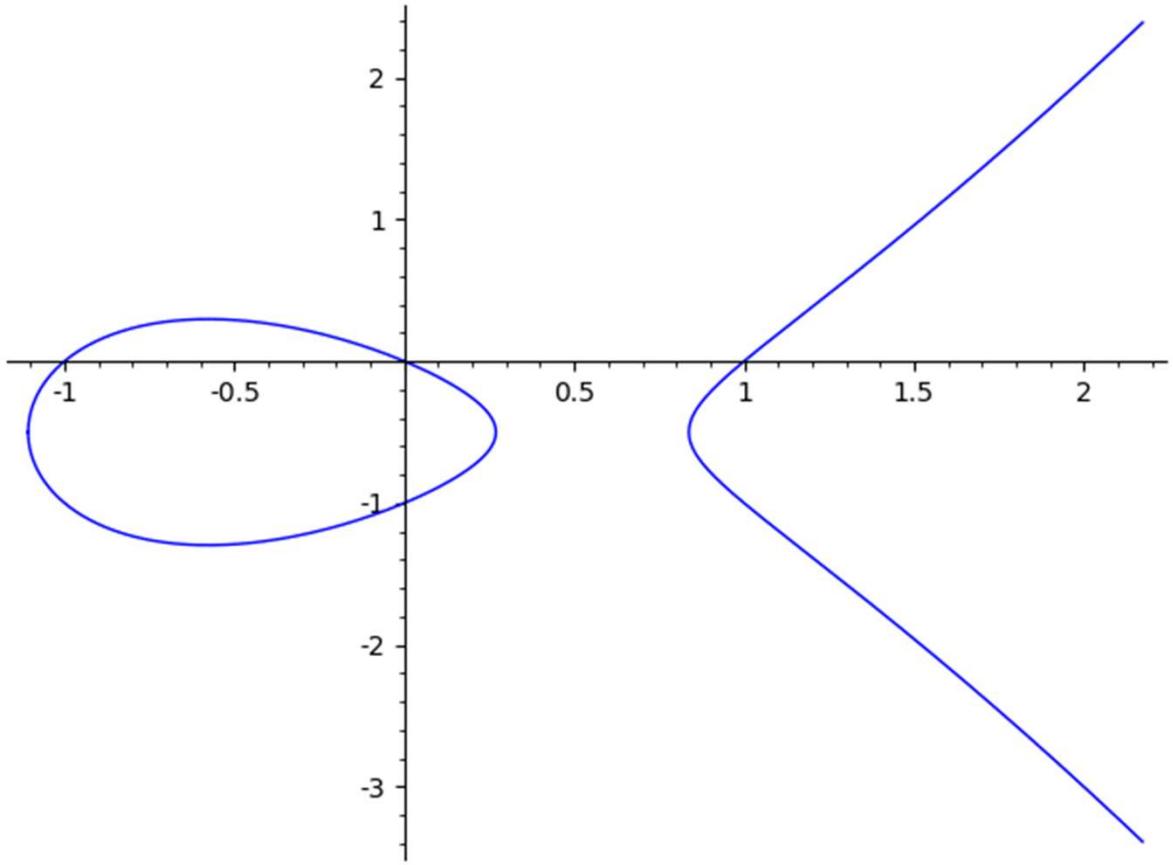
ECDSA este o variantă a algoritmului DSA (Digital Signature Algorithm), dar folosește **criptografia cu curbe eliptice** pentru a genera chei mai mici și mai eficiente fără a compromite securitatea.

ECDSA este esențial pentru securitatea Bitcoin și este folosit pentru:

- **Semnarea tranzacțiilor** (autentificarea expeditorului)
- **Verificarea autenticității tranzacțiilor** (validarea de către noduri)
- **Protejarea cheilor private ale utilizatorilor**

Bitcoin folosește curba eliptică **secp256k1**, definită astfel: $y^2=x^3+7$ (mod p)

Prin urmare, daca k este cheia privata, cheia publica este k * G (G se numeste generator)

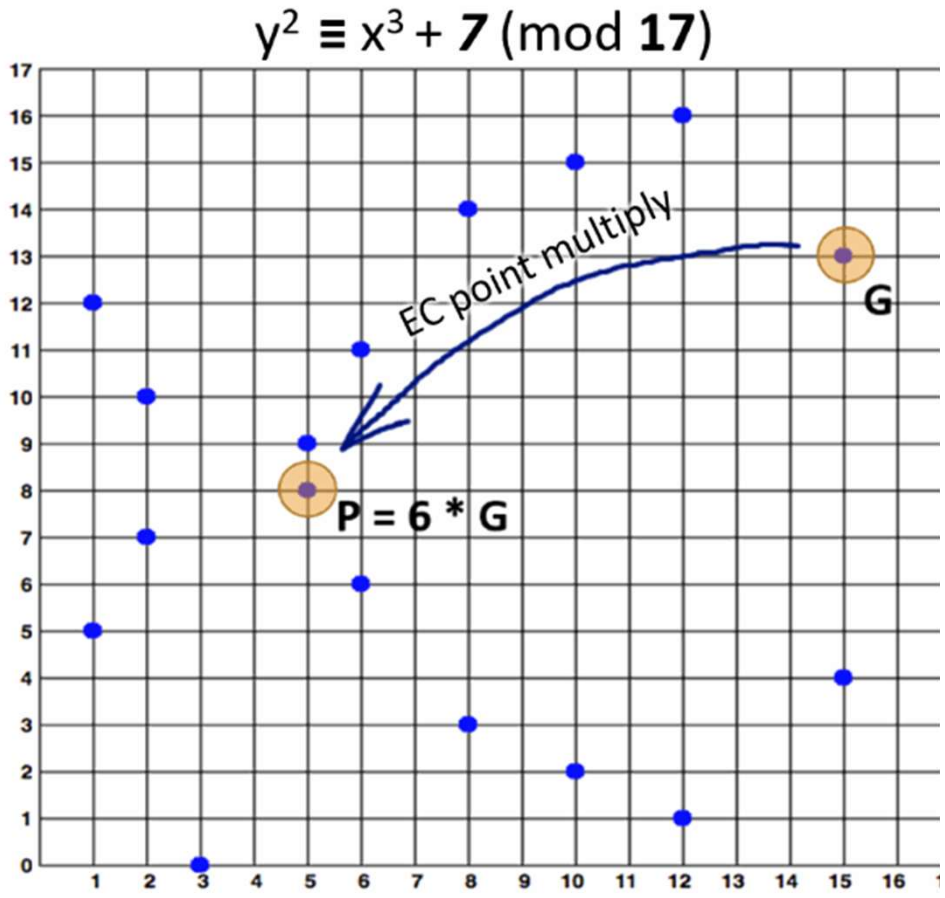


Proof of Work (PoW)

Elliptic Curve

- $y^2 = x^3 + a*x + b \pmod{p}$

- $a = 0$
- $b = 7$
- $p = 17$



Proof of Work (PoW)

```
# y² = x³ + ax + b (mod p)

$a = 0
$b = 7


# prime field

$p = 115792089237316195423570985008687907853269984665640564039457584007908834671663
#=> 2**256 - 2**32 - 2**9 - 2**8 - 2**7 - 2**6 - 2**4 - 1

# number of points on the curve we can hit ("order")

$n = 115792089237316195423570985008687907852837564279074904382605163141518161494337

# generator point (the starting point on the curve used for all calculations)

$G = {
x: 55066263022277343669578718895168534326250603453777594175500187360389116729240,
y: 32670510020758816978083085130507043184471273380659243275938904335757337482424,
}
```

Portofele (wallets)

- Hardware wallets
  - Exemple: Ledger, Trezor
  - Asigură cel mai înalt nivel de securitate
  - Stocare offline a cheilor private
- Software wallets
  - Disponibile pe desktop și mobil
  - Ușor de folosit
  - Expuse potențial la hacking dacă dispozitivul este compromis
- Web wallets
  - Accesate prin browser (ex. Metamask)
  - Convenabile
  - Vulnerabile atacurilor online

Bursele de tranzacționare (exchanges)

- Exchanges
  - Platforme pentru cumpărarea, vânzarea sau tranzacționarea criptomonedelor
  - Permite schimbul de criptomonede sau monede fiat
- CEX (Centralized Exchanges)
  - Exemple: Binance, Coinbase, Kraken
  - Cer înregistrare
  - Au infrastructură proprie
- DEX (Decentralized Exchanges)
  - Exemple: Uniswap, SushiSwap, PancakeSwap
  - Folosesc contracte inteligente pentru tranzacții peer-to-peer
  - Cresc anonimitatea și controlul utilizatorilor asupra fondurilor

Evoluția Blockchain și Apariția Ethereum

Primele Aplicații și Limitări ale Bitcoin

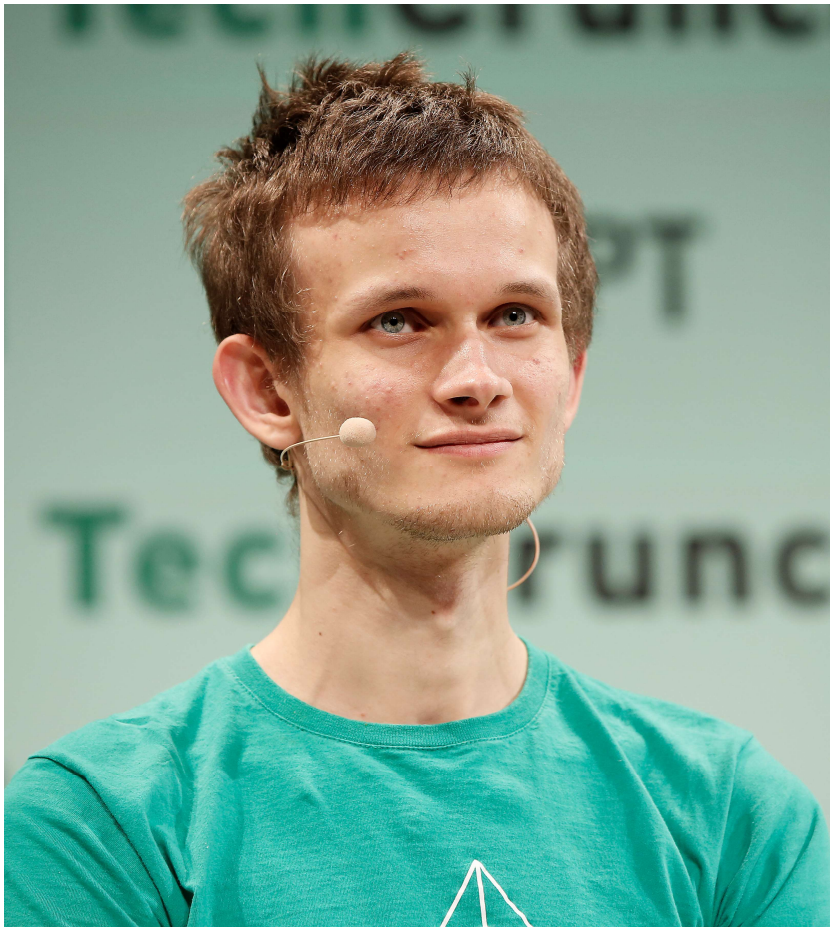
- Bitcoin ca sistem financiar descentralizat
  - Transfer de valoare (BTC)
  - Stocare de date minime (script opcodes)
- Popularitatea Bitcoin
  - Investitori și entuziaști
- Limitările protocolului Bitcoin
  - Nu susține aplicații complexe
- Necesitatea unei platforme blockchain generaliste
  - Capabilă să ruleze coduri de programare elaborate

Probleme și Limitări ale Primei Generații de Blockchain

- Scalabilitate și viteză de procesare
  - Bitcoin procesează aproximativ 7 tranzacții pe secundă
  - Sistemele centralizate (ex. Visa, MasterCard) procesează mii de tranzacții pe secundă
  - Blockchain-ul PoW necesită timp pentru minare și confirmare (~10 minute între blocuri la Bitcoin)
- Consum energetic
  - Mineritul PoW este extrem de costisitor energetic
  - Mii de mineri concurează să rezolve un puzzle criptografic
  - Creșterea popularității Bitcoin a amplificat consumul de energie la nivel global
- Funcționalități restrânse
  - Scriptul Bitcoin permite funcții simple
  - Nu a fost conceput pentru contracte inteligente complexe
  - Prima generație de blockchain nu putea găzdui direct aplicații descentralizate (DApps)

Ideea lui Vitalik Buterin

- Vitalik Buterin, programator rus-canadian
  - A propus un nou concept în 2013
- Conceptul de „blockchain cu un limbaj de scripting integrat”
  - Permite rularea contractelor inteligente
- Publicarea White Paper-ului Ethereum
  - Detaliază o platformă de calcul globală, descentralizată
  - Bazată pe un blockchain customizabil



Nick Szabo – The Quiet Master

- Nick Szabo este un informatician, criptograf și teoretician al dreptului, recunoscut în special pentru contribuțiile sale în domeniul contractelor inteligente (smart contracts) și al monedelor digitale.
- Nick Szabo a conceput ideea de contracte inteligente.
- În anii '90, el a scris „Smart Contracts: Building Blocks for Digital Markets”, în care a detaliat cum pot fi create contracte auto-executabile, unde termenii acordului sunt codificați și executați automat pe calculatoare.
- El a propus conceptul de Bit Gold, considerat unul dintre precursorii Bitcoin. Bit Gold a fost gândit ca un sistem descentralizat de monedă digitală, care ar fi funcționat fără intermediari financiari tradiționali.
- De-a lungul timpului, au existat speculații conform cărora Nick Szabo ar putea fi Satoshi Nakamoto, pseudonimul creat de fondatorul Bitcoin. Totuși, Szabo a negat aceste afirmații și nu există dovezi concludente în acest sens.

Lansarea Proiectului Ethereum

- Inițierea proiectului
  - Vitalik Buterin și co-fondatorii săi au organizat un crowd-sale în 2014
  - Scopul a fost finanțarea proiectului Ethereum
- Formarea Ethereum Foundation
  - Entitate non-profit pentru gestionarea dezvoltării protocolului
- Lansarea rețelei principale
  - Rețeaua Mainnet Ethereum a fost lansată în iulie 2015

Diferențele față de Bitcoin

- Limbaj Turing-complet
  - Ethereum introduce un limbaj de programare numit Solidity
  - Permite crearea de contracte inteligente elaborate
- Timp de bloc
  - Ethereum are un timp de bloc de ~12-15 secunde
  - Bitcoin are un timp de bloc de ~10 minute
  - Permite confirmări mai rapide pe Ethereum
- Viziunea de „calculator global”
  - Ethereum este o platformă pentru aplicații descentralizate (DApps)
  - Suportă tokenuri suplimentare prin standardele ERC-20 și ERC-721

Proof of Stake (PoS)

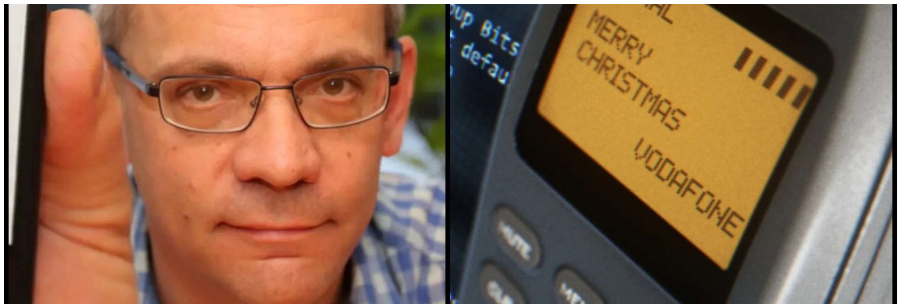
- Proof of Stake (PoS) ca alternativă la PoW
  - Reduce consumul energetic
  - Crește viteza tranzacțiilor
- Validarea blocurilor în PoS
  - Nu se bazează pe puterea de calcul
  - Se bazează pe deținerea unei sume de criptomonede
- Avantaje ale PoS
  - Consum energetic mult mai redus
  - Scalabilitate mai bună
- Dezavantaje ale PoS
  - Posibilă tendință de centralizare
  - Cei mai mari deținători pot controla rețeaua

Ethereum (ETH)

- Lansare și Fondatori
  - Lansat în 2015 de Vitalik Buterin și echipa sa
- Inovații Cheie
  - Introducerea contractelor inteligente
  - Aplicații descentralizate (DApps)
- Tranziții Tehnologice
  - Tranziție de la PoW la PoS (Ethereum 2.0 / The Merge)
- Ecosistem și Utilizări
  - Ecosistem vast
  - Motorul principal pentru DeFi și NFT-uri

NFT - “MERRY CHRISTMAS”

- December 3, 1992. Primul SMS trimis vreodata.
- Neil Papworth i l-a trimis lui Richard Jarvis, unul din directorii Vodafone.
- Jarvis avea un Orbitel "mobile" phone, care cantarea 2 kg.
- SMS-ul a fost vandut in 2022, ca NFT, pentru 132,680 EUR



Contractele Inteligente (Smart Contracts)

- Definiție a contractelor inteligente
  - Fragmente de cod stocate și executate pe blockchain
  - Rulează automat la îndeplinirea unor condiții prestabilite
- Rolul contractelor inteligente
  - Elimină nevoia unui intermediar
  - Validează și execută automat contractele
  - Exemplu: contract de asigurare care se activează automat la un eveniment specific

Exemple de Utilizare

- ICO-uri (Initial Coin Offerings)
  - Lansarea de tokenuri prin contracte inteligente pe Ethereum
  - Finanțare pe modelul crowdfunding
- DeFi (Decentralized Finance)
  - Aplicații de împrumut
  - Schimburi descentralizate (DEX)
  - Platforme de lichiditate și dobândă
  - Exemple: Uniswap, MakerDAO, Aave
- NFT-uri (Non-Fungible Tokens)
  - Standardul ERC-721 pentru tokenuri unice și indivizibile
  - Utilizare pentru opere de artă digitale, obiecte de colecție, elemente de joc
  - Exemple: CryptoKitties, Axie Infinity

Stablecoins (Tether, USDC, DAI)

- Tether (USDT)
  - Prima și cea mai folosită stablecoin
  - Ancorată la dolar
- USD Coin (USDC)
  - Lansată de consorțiul Centre
  - Creată de Coinbase și Circle
- DAI
  - Stablecoin descentralizat
  - Emis prin platforma MakerDAO
  - Acoperit de criptomonede puse drept garanție

Caracteristicile Cheie ale Ethereum

- Limbaje de programare
  - Solidity: inspirat de JavaScript, C++ și Python
  - Vyper: stil apropiat de Python
  - Permite scrierea logicilor complexe pe blockchain
- Mecanism de consens
  - Inițial Proof of Work (PoW)
  - Trecerea la Proof of Stake (PoS)
  - Etape: Beacon Chain, The Merge
  - Nodurile validatoare pun la stake ETH pentru a valida blocurile
- Ecosistemul aplicațiilor descentralizate (DApps)
  - Platformă programabilă atrage mii de dezvoltatori și proiecte
  - Crearea unui ecosistem DeFi

Lansarea de Token-uri - ERC20

În cazul unui token conform standardului ERC20, trebuie implementate următoarele funcții (și evenimente) esențiale:

- **totalSupply() -** Returnează numărul total de token-uri aflate în circulație.
- **balanceOf(address account) -** Permite obținerea soldului (numărul de token-uri) deținut de o anumită adresă.
- **transfer(address recipient, uint256 amount) -** Transferă o anumită cantitate de token-uri din contul apelantului către adresa destinatarului.
- **approve(address spender, uint256 amount) -** Aprobă o anumită cantitate de token-uri pe care o altă adresă (spender) o poate cheltui din contul apelantului.
- **allowance(address owner, address spender) -** Returnează cantitatea de token-uri pe care un anumit spender este aprobat să le cheltuiască din contul unui owner.
- **transferFrom(address sender, address recipient, uint256 amount) -** Permite transferul token-urilor de la o adresă sursă la o adresă destinație, folosind suma aprobată prin **approve**

Expansiunea Conceptului de DeFi

- Contracte inteligente pe Ethereum
  - Infrastructură pentru sistem financiar paralel
  - Eliminarea intermediarilor bancari
- Servicii oferite de DeFi
  - Împrumuturi
  - Tranzacționare
  - Stablecoins
  - Yield farming
- Investiții și interes
  - Investiții uriașe atrase
  - Interesul instituțiilor tradiționale pentru blockchain

Provocări și Perspective Viitoare

- Tranziția la Ethereum 2.0 (The Merge)
  - Adoptarea completă a Proof of Stake
  - Optimizarea rețelei prin sharding
  - Cresterea numărului de tranzacții procesate pe secundă
  - Scăderea costurilor pentru utilizatori
  - Implementarea etapizată a sharding-ului și noilor actualizări
- Provocări și perspective viitoare
  - Scalabilitate (Layer 2, sharding)
    - Probleme de congestionare a rețelei și comisioane ridicate
    - Soluții de sharding și adoptarea de soluții Layer 2
  - Aspecte juridice și reglementări
    - Combaterea fraudei și spălării banilor

Tranziția la Ethereum 2.0 (The Merge)

- Adoptarea Proof of Stake
  - Principalul obiectiv al Ethereum 2.0
  - Creșterea eficienței energetice
- Optimizarea rețelei prin sharding
  - Crescând numărul de tranzacții pe secundă
  - Scăzând costurile pentru utilizatori
- Etapele ulterioare după The Merge
  - The Surge
  - The Verge
  - The Purge
  - The Splurge

Tranziția la Ethereum 2.0 (The Surge)

- The Surge

- Obiectiv principal: Creșterea semnificativă a scalabilității rețelei și a capacității de procesare a tranzacțiilor.
- Mijloace tehnice: Introducerea sharding-ului (împărțirea bazei de date/lanțului în fragmente paralele), care le va permite validatorilor să proceseze doar o parte din date, în loc de întregul blockchain.
- Rezultat așteptat: Viteze mult mai mari ale tranzacțiilor, reducerea congestiei și a comisioanelor, făcând rețeaua mai potrivită pentru aplicații de masă (DeFi, NFT-uri etc.).

Tranziția la Ethereum 2.0 (The Verge)

- The Verge

- Obiectiv principal: Simplificarea și optimizarea nodurilor, astfel încât validarea să devină mai ușoară și mai rapidă.
- Mijloace tehnice: Introducerea unor structuri precum Verkle trees, care vor reduce volumul de date pe care un nod trebuie să îl stocheze și proceseze.
- Rezultat așteptat: O rețea cu noduri mai „ușoare”, care pot porni mai rapid și pot funcționa cu resurse hardware mai mici, facilitând astfel descentralizarea.

Tranziția la Ethereum 2.0 (The Purge)

- The Purge

- Obiectiv principal: Curățarea și simplificarea istoricului on-chain, respectiv reducerea complexității istorice și a datoriilor tehnice acumulate de-a lungul timpului.
- Mijloace tehnice: Eliminarea datelor istorice care nu mai sunt strict necesare validării actuale, optimizarea procesului de sincronizare a nodurilor și eliminarea unor componente vechi care încetinesc rețeaua.
- Rezultat așteptat: Un blockchain mai compact, cu cerințe de stocare mai mici și timpi mai buni de sincronizare, toate contribuind la creșterea eficienței rețelei.

Tranziția la Ethereum 2.0 (The Splurge)

- The Splurge

- Obiectiv principal: Integrarea unor îmbunătățiri adiționale și „rafinări” care nu sunt critice pentru scalabilitate de bază, dar care aduc un plus de funcționalitate, ușurință în utilizare și securitate.
- Mijloace tehnice: O serie de update-uri mai mici și de „fine-tuning” – pot include optimizări ale mașinii virtuale Ethereum (EVM), update-uri de contracte, noi propuneri EIP (Ethereum Improvement Proposals) etc.
- Rezultat așteptat: O rețea Ethereum mai „lustruită”, finalizând implementarea elementelor care fac platforma completă și robustă pe termen lung.

Rețele Blockchain

Bitcoin (BTC)

- Lansare: 3 ian 2009 (genesis); whitepaper 31 oct 2008.
- Fondator: Satoshi Nakamoto; cod C++ (Bitcoin Core).
- Consens: Proof-of-Work SHA-256; ~10 min/bloc; dificultatea se ajustează la 2016 blocuri.
- Aprovizionare fixă 21 M BTC; halving-ul 2024 → 3,125 BTC/bloc.
- Model UTXO; mărime efectivă ~4 MB cu SegWit.
- Layer-2: Lightning Network – >5 000 noduri, 63 000+ canale (Q2 2025).
- Soft-fork-uri: SegWit (2017), Taproot (2021).
- Script limitat; cercetare pentru Covenants & OP_CAT.
- Ecosistem: over-the-counter, ETF-uri spot (SUA 2024), custodie instituţională.

Ethereum (ETH)

- Lansare mainnet: 30 iul 2015; fondatori Vitalik Buterin, Gavin Wood.
- Trecere la Proof-of-Stake (Merge) 15 sep 2022; >1,2 M validatori (~44 M ETH).
- Slot 12 s; reward net ≈ 3,2 % APR; retrageri enable Shanghai (apr 2023).
- EIP-1559 (2021) arde parte din taxă; >4,3 M ETH arse până iun 2025.
- Proto-danksharding EIP-4844 (Dencun, 2024) → «blobs» ieftine pt L2.
- VM: EVM; limbaje Solidity, Vyper, Yul; posibil MEV-Burn & PBS în viitor.
- L2 ecosistem: Arbitrum, Optimism, zkSync, Starknet; TVL total ~61 mld USD.
- Tokenomics: inflaţie netă negativă în perioade de trafic ridicat («ultrasound ETH»).
- Tooling: Geth, Besu, Prysm, Lighthouse; limbaj principal Go/Rust.

BNB Smart Chain (BNB)

- Lansare: sept 2020; paralel cu BNB Beacon Chain (2019).
- Consens: Proof-of-Staked-Authority (PoSA); 21 validatori re-aleşi zilnic.
- Blocuri ~3 s; finalitate aproape instant (2 blocuri).
- EVM-compatibil; fork Geth în Go; BNB utilitar pentru taxă & guvernanţă.
- Taxe tipice < $0,05; setate la 3–5 gwei.
- opBNB (2023) – L2 pe OP-Stack; throughput sporit, taxe sub-cent.
- Punte Binance Bridge >20 lanţuri; BEP-20 token standard.
- Ecosistem: PancakeSwap TVL ~3,2 mld, Venus Lending, memecoins asiatice.
- Risc centralizare: set redus de validatori şi control Binance Labs.

Solana (SOL)

- Mainnet-beta: mart 2020; fondatori Anatoly Yakovenko, Raj Gokal.
- Consens: PoH (Proof-of-History) ca ceas + Tower BFT PoS.
- Timp bloc ≈ 400 ms; peste 65 k TPS teoretic (2 k real on-chain).
- Runtime paralel Sealevel; programe BPF compilate din Rust, C.
- Validatori ≈ 3 800; hardware: 128 GB RAM, NVMe; comision 0,000005 SOL.
- Upgrade-uri: QUIC network, stake-weighted QoS, Firedancer validator (Jump, 2024).
- Tokenomics: inflaţie iniţială 8 % → 1,5 % anual (până 2030).
- Ecosistem: DEX Jupiter, NFT Compression, Saga phone & Solana Mobile Stack.
- Stack programabil: Anchor framework, Sealevel VM, SVM Move-like.

TRON (TRX)

- Mainnet: mai 2018; fondator Justin Sun.
- Consens: DPoS cu 27 Super Representatives; bloc 3 s.
- TVM (TRON Virtual Machine) compatibil EVM; limbaje Solidity, Java.
- Model Energy & Bandwidth → tx fee ≈ 0; USDT TRC-20 circulă masiv (>45 % din supply).
- Staking yield ≈ 4 %; voturi prin TRX burn → tronpower.
- Side-chains Sun Network; BTTC cross-chain cu Ethereum & BSC.
- Ecosistem: JustLend, JustStables, APENFT; pieţe emergente Africa/Asia.
- Critici: centralizare, domnie Justin Sun; liste negre la nivel contract.

Polygon (MATIC) – PoS & zkEVM

- Originar ca Matic (2017); rebrand Polygon 2021.
- Polygon PoS: hibrid Plasma + PoS; bloc ≈ 2 s; >100 validatori Heimdall.
- Gas fee < $0,002; burning EIP-1559 implementat (2022).
- zkEVM mainnet mart 2023: roll-up cu zk-SNARK Groth16, compatibil EVM bytecode.
- Polygon CDK (2024) – toolkit pt zk-roll-up la cheie; DA opţional Celestia.
- Proiecte: Aavegotchi, Quickswap, Lens Protocol (social).
- Token suply 10 mld MATIC; deflaţie slabă via burn; staking ≈ 5 % APR.
- Roadmap: AggLayer inter-roll-up liquidity, zk-prover Type 2 upgrade.

Zilliqa (ZIL)

- **Zilliqa** este un blockchain public de **înaltă performanță**, cunoscut pentru faptul că a fost **primul blockchain care a implementat cu succes sharding-ul pe rețea principală (mainnet)**. Lansat în **2019**, Zilliqa a fost conceput pentru a rezolva problemele de **scalabilitate** întâlnite în rețele ca Ethereum și Bitcoin.

Algoritm de consens	Hybrid: Practical Byzantine Fault Tolerance (PBFT) + Proof of Work (PoW – doar pentru identificare)
Timp de bloc	~45 secunde (cu mini-blocuri la fiecare ~2 secunde)
TPS (tranzacții/secundă)	> 2.800 TPS (testat)
Token nativ	**ZIL**
Sharding	Da – nativ, implementat încă de la lansare
Smart contracts	Da – scrise în limbajul **Scilla** (proprietar)
EVM compatibil	Parțial – compatibilitate extinsă planificată
Taxe de tranzacție	Foarte mici (~0.001 ZIL)

Comparatie

Rețea	Consens & hardware minim	Noduri publice (estimare)	Set validatori / mineri	Timp bloc	Finalitate tipică	Debit L1 real / teoretic	VM / limbaj primar
Bitcoin	Proof-of-Work SHA-256 (ASIC)	~21 900	Hashrate 930 EH/s (pool-uri)	≈10 min	~60 min (6 conf.)	3-7 TPS	Bitcoin Script
Ethereum	Proof-of-Stake (32 ETH; 8 GB RAM)	~13 900	≈1,2 mil validatori Beacon	12 s	≈12 min (2 epoch)	15 TPS / >10k TPS cu L2	EVM (Solidity/Vyper)
BNB Smart Chain	PoSA (8 CPU / 32 GB RAM)	~215	45 validatori activi	≈3 s	<10 s (2 blocuri)	~200 TPS	EVM (Go fork)
Solana	PoH + Tower BFT (32 core / 256 GB RAM)	~5 170	≈1 400 validatori	0,4-0,5 s	<2 s	2 000 TPS / 50 k peak	Sealevel (Rust/C)
TRON	DPoS (16 CPU / 32 GB RAM)	mii (cloud, n/a exact)	27 SR + 127 candidați	≈3 s	≈1 bloc	~2 000 TPS	TVM (EVM-like)
Polygon PoS	Heimdall + Bor PoS (8 CPU / 32 GB RAM)	~200	≤105 validatori	≈2 s	<10 s	60 TPS / 7 000 teoretic	EVM (Solidity)

Blockchain-uri fara moneda nativa

- În 2025 cele două rețele **fără monedă nativă** (deci fără comisioane plătite în coin-uri, minerit sau stimulente speculative) care domină prin **scală** și **număr de participanți** sunt:

Criteriu	**AntChain** (Ant Group, China)	**IBM Food Trust** (Hyperledger Fabric, global)
Tip rețea	Platformă enterprise multi-lanț	Consorțiu unic pentru supply-chain alimentar
Participanți / conturi	**până la 1 miliard** de conturi și **1 miliard de tranz./zi** declarate de Ant Group businesswire.com	**≈ 500 de organizații** (retaileri, fermieri, procesatori) confirmate de IBM foodinstitute.com
Token nativ	**Nu există** – toate operațiunile folosesc conturi fiat / Alipay; AntChain a subliniat explicit că nu creează criptomonedă reuters.com	**Nu există** – rețea permisionată, costurile sunt abonamente SaaS/custodie, fără crypto-fees
Tehnologie	Framework proprietar + BFT; noduri operate de Ant și parteneri enterprise; integrat cu AI, IoT, confidențialitate calculabilă	**Hyperledger Fabric** (open-source); noduri deținute de fiecare membru al lanțului de aprovizionare
Domenii de utilizare	Certificate NFT „digital collectibles”, trasabilitate logistici, asigurări medicale, leasing IT, shipping, drepturi de autor	Trasabilitate ingrediente (Walmart, Carrefour), audit siguranță alimentară, recall rapid (< 2 sec)

Appendix - Epoch

În Ethereum 2.0, după tranziția de la **Proof-of-Work (PoW)** la **Proof-of-Stake (PoS)** (realizată prin upgrade-ul "The Merge"), conceptul de **epoch** (epocă) joacă un rol esențial în mecanismul de consens și în menținerea siguranței și eficienței rețelei.Ethereum 2.0 folosește o ierarhie de timp clară pentru organizarea blocurilor și activităților validatorilor:

Ethereum 2.0 folosește o ierarhie de timp clară pentru organizarea blocurilor și activităților validatorilor:

☑ **Slot** (Slot temporar) — Este cea mai mică unitate de timp în rețeaua Ethereum PoS.

- **Durata unui slot:** 12 secunde
- În fiecare slot, un validator este desemnat să propună un bloc.

☑ **Epoch (Epocă)** — Este o colecție fixă de **32 de sloturi**.

- **Durata unei epoci:** 32 × 12 secunde = **384 secunde** (aproximativ 6,4 minute).
- La sfârșitul fiecărei epoci, se face o evaluare a validatorilor și a stării rețelei.

➔ Ethereum nu are o limită fixă pentru câte blocuri trebuie să fie incluse într-o epocă

Appendix - Epoch

Epoch-ul este un element fundamental în procesul de consens Proof-of-Stake din Ethereum 2.0. Acesta are mai multe roluri cheie:

a) Propunerea blocurilor

- În fiecare slot, un validator este ales aleatoriu pentru a propune un bloc.
- Acest bloc conține tranzacțiile recente și informațiile privind starea blockchain-ului.

b) Atestarea (Attestations)

- Restul validatorilor din rețea (care nu propun un bloc) sunt responsabili pentru "atestarea" (confirmarea) blocurilor propuse.
- Atestările sunt esențiale pentru a stabili consensul asupra lanțului corect.

c) Finalitatea (Finality)

- Finalitatea este procesul prin care blocurile devin **definitiv confirmate** și nu mai pot fi modificate.
- Ethereum folosește un mecanism denumit **Casper FFG (Friendly Finality Gadget)** pentru a stabili finalitatea blocurilor.
- Pentru ca o epocă să fie considerată **finalizată**, trebuie să fie urmată de încă două epoci consecutive în care validatorii confirmă acea stare a lanțului.

Appendix - Epoch

În Ethereum 2.0, validatorii sunt aleși în mod pseudo-aleatoriu pentru fiecare slot și fiecare epocă:

- **Validator desemnat**: Un validator specific este ales pentru a propune blocul într-un anumit slot.
- **Comitet de validatori (Committee)**: În fiecare slot, un grup de validatori (comitet) este selectat pentru a oferi atestări (confirmări) asupra blocului.

Acest comitet este format din minimum 128 validatori pentru a garanta descentralizarea și securitatea.

➡ Această metodă reduce riscul ca un singur validator rău-intenționat să influențeze rețeaua.

La sfârșitul fiecărei epoci, se efectuează:

☑ **Recompense** pentru validatorii activi și sinceri.
☑ **Penalizări (Slashing)** pentru validatorii care au încercat să manipuleze rețeaua sau au fost offline în mod repetat.

Recompensele și penalizările sunt calculate în funcție de performanța validatorului și contribuția acestuia la rețea.

✔ Asigură finalitatea și stabilitatea blockchain-ului.
✔ Permite rotația eficientă a validatorilor pentru a preveni manipularea rețelei.
✔ Permite aplicarea sancțiunilor pentru comportamente malițioase.
✔ Garantează că tranzacțiile sunt confirmate ireversibil și nu mai pot fi modificate.