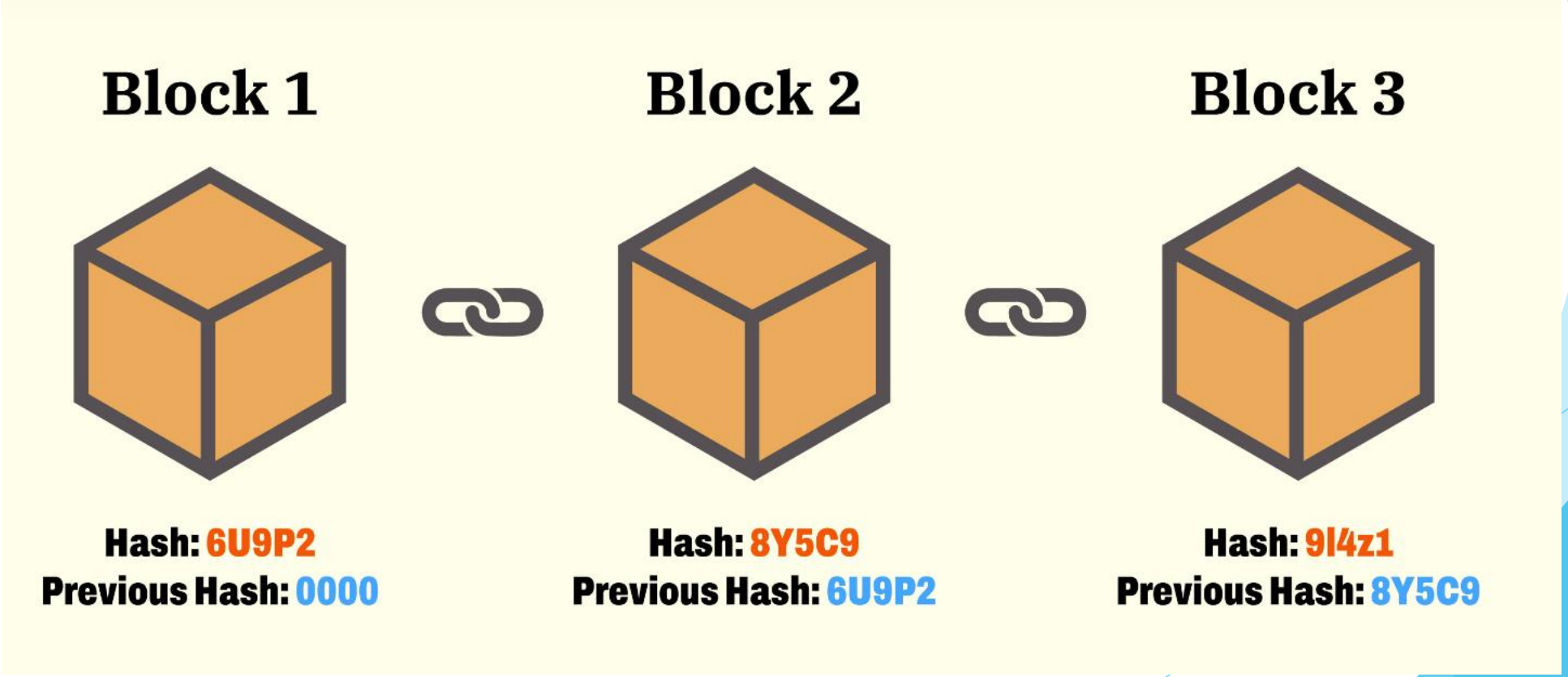
BlockChain

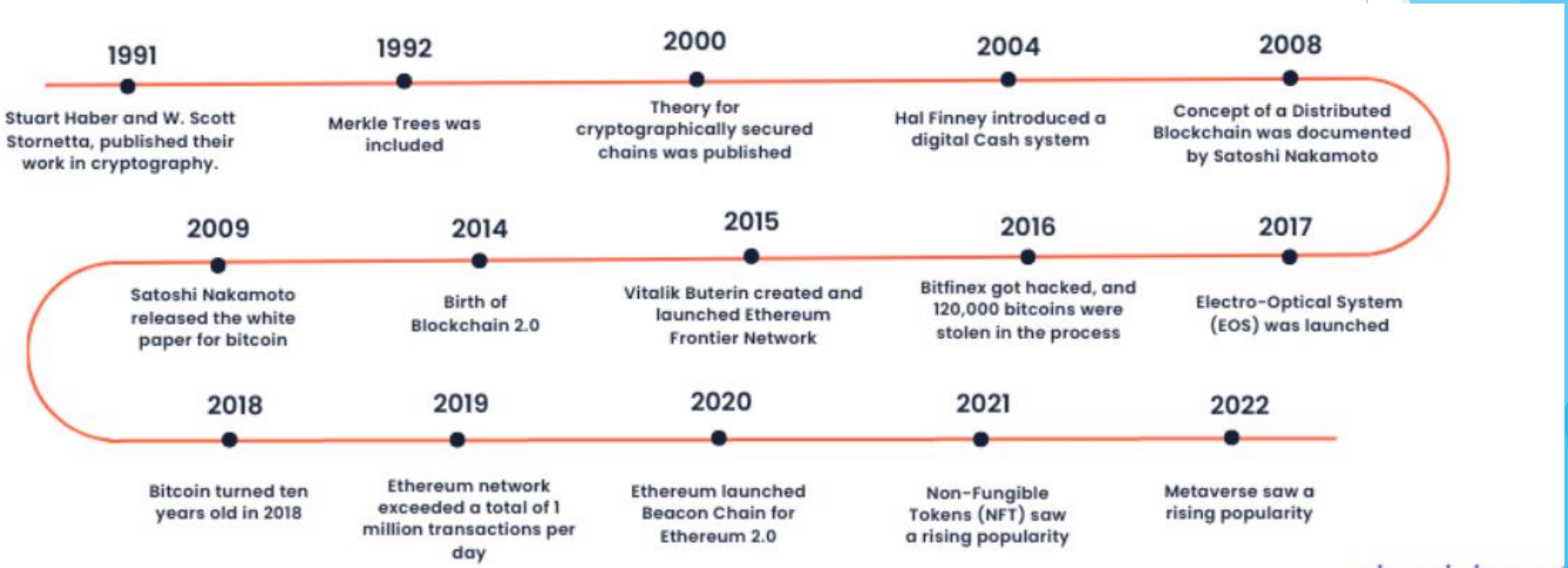
Adam Plavčan

Čo je to Blockchain?

"Blockchain je decentralizovaný digitálny účtovný záznam, ktorý zaznamenáva transakcie naprieč mnohými počítačmi tak, aby jednotlivý záznam nemohol byť zmenený bez zmeny všetkých následných záznamov.„



Stručná história:



Základné vlastnosti

- Distribuovaná databáza:
  Decentralizácia (Odstránenie sprostredkovateľov)

  !Pravda je zdieľaná, nie je diktovaná autoritou!
- Transparentnosť
- Nemennosť

SHA256("Guess #23") =
100100001110100111011011111110110
000000000011101111000001011001011
111000111101100010110101110001000
111100101010000000011011001010000
000001111100000101100111110111000
100010001100111011111000100001100
100100011101000011010111100001100
011001100101101001000100011011010

Cryptographic hash function

SHA256("???") =
100111110011110001011110010010111
110111101110110100110110101001010
010101000100010111011101101001000
100001010111001010110011001111101
001110010001110000010110011000010
001100101011001111101011001001000
000101010110100010100010000100100
110000011000011110010011100001000

Desired output

Inverse is infeasible

SHA256 → Proof of work

Sign(Message, sk) = Signature

Verify(Message, Signature, pk) = T/F

Ledger

Alice pays Bob 20 LD

Alice pays You 30 LD

Charlie pays You 100 LD

1073765433

Probability: $\frac{1}{2^{30}} \approx \frac{1}{1{,}000{,}000{,}000}$

30 zeros

SHA256

000000000000000000000000000011
001100010110111011001001001101 10
100000000100011001011011010001 1
101111111001110001100100101110 00
110110111011100101011011010001 11
000111100010000010001001100001 10
111001110001101000011000100100 01
100001011000100110100001010000 00

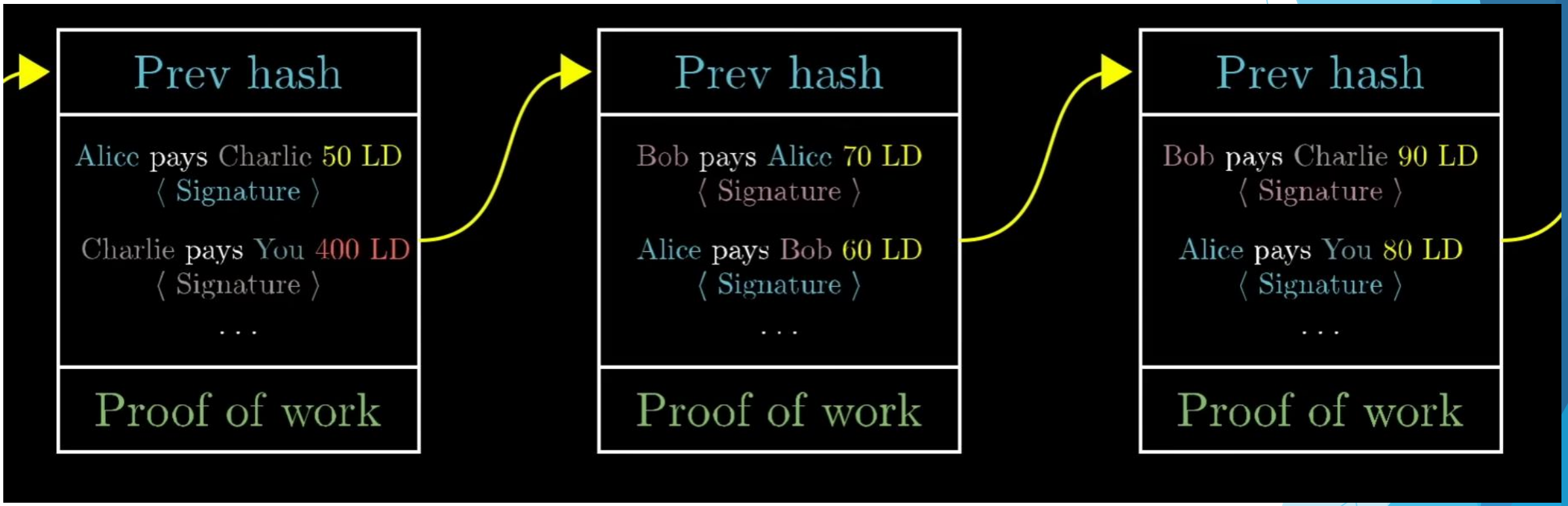
Konsenzus mechanizmus: Koncept PoW

- Všetky tranzakcie sa rozosielajú do siete
- Ťažiary („hádači“) vytvárajú z transakcií bloky
- Bloky sa zapisujú do reťazca
- Každý má prístup ku kópii reťazca

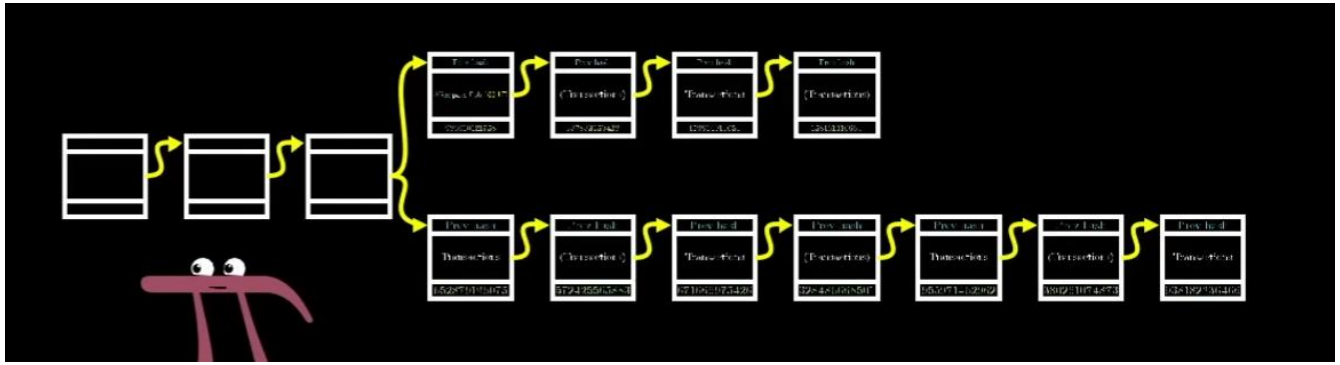
$$\text{Currency} = \text{Transaction history}$$

PoW – Tvorba bloku

- Ťažiary odpočúvajú transakcie
- Z určitého množstva transakcií a odkazu na predošlí blok sa vytvorí nový blok
- K novému bloku sa snažia nájsť nový hash (hádajú hádanku)
- Víťaz lotérie, ktorý vygeneroval spávny hash rozosiela nový blok do siete a získava odmenu
- PoW slúži ako opatrenie proti tvorbe podvodných blokov


Prev hash
Alice pays Charlie 50 LD
⟨ Signature ⟩
Charlie pays You 400 LD
⟨ Signature ⟩
. . .
Proof of work
Prev hash
Bob pays Alice 70 LD
⟨ Signature ⟩
Alice pays Bob 60 LD
⟨ Signature ⟩
. . .
Proof of work
Prev hash
Bob pays Charlie 90 LD
⟨ Signature ⟩
Alice pays You 80 LD
⟨ Signature ⟩
. . .
Proof of work

Problém dvojitej útraty:

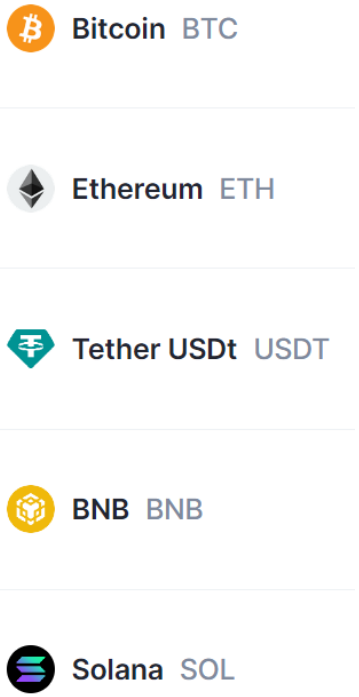


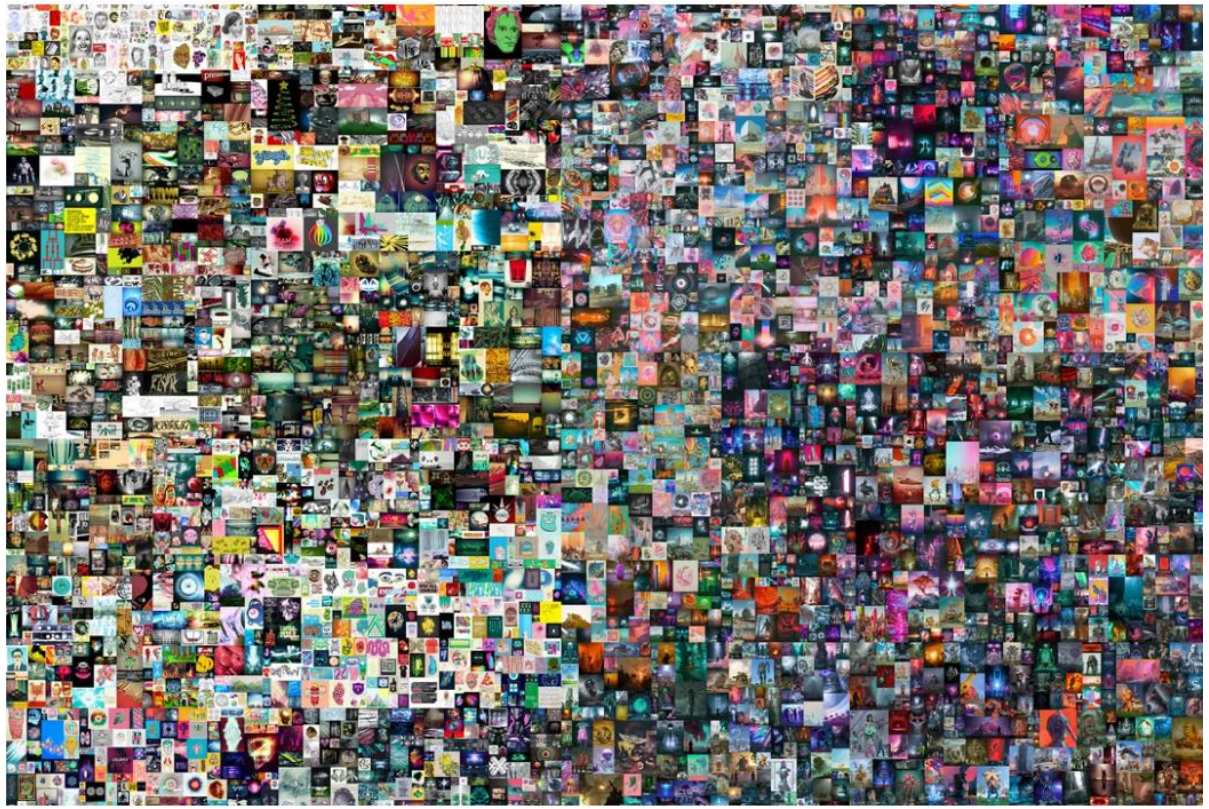
- Netreba veriť hneď poslednému bloku, treba počkať na ďalšie bloky, tým sa overí stabilita, teda v prípade vetvenia sa preferuje dlhšia vetva
- Uživatelia aj ťažiary majú motiváciu pokračovať v najdlhšej vetve
- Zmemožnenie falšovania

Aplikácie

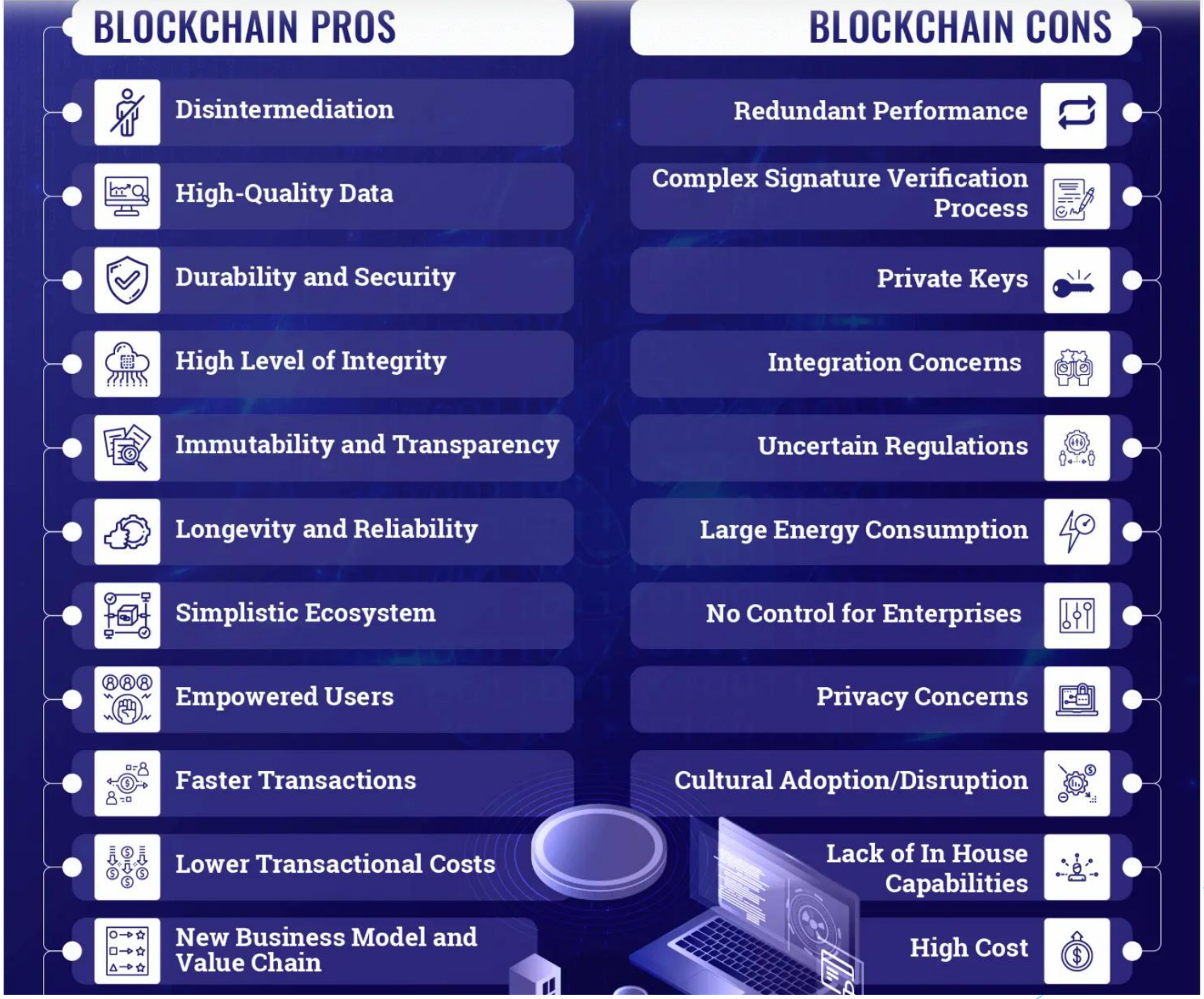
- Kryptomeny
- Smart kontrakty (If ... Then ...)

  Program, ktorý sa automaticky vyhodnotí v závislostiach na podmienkach kontraktu, zaručené vykonanie a transparentnosť kódu
- NFTs (Non-fungible token = Nezameniteľný token)
- DeFi = ! odstránenie prostredníkov a regulácii !



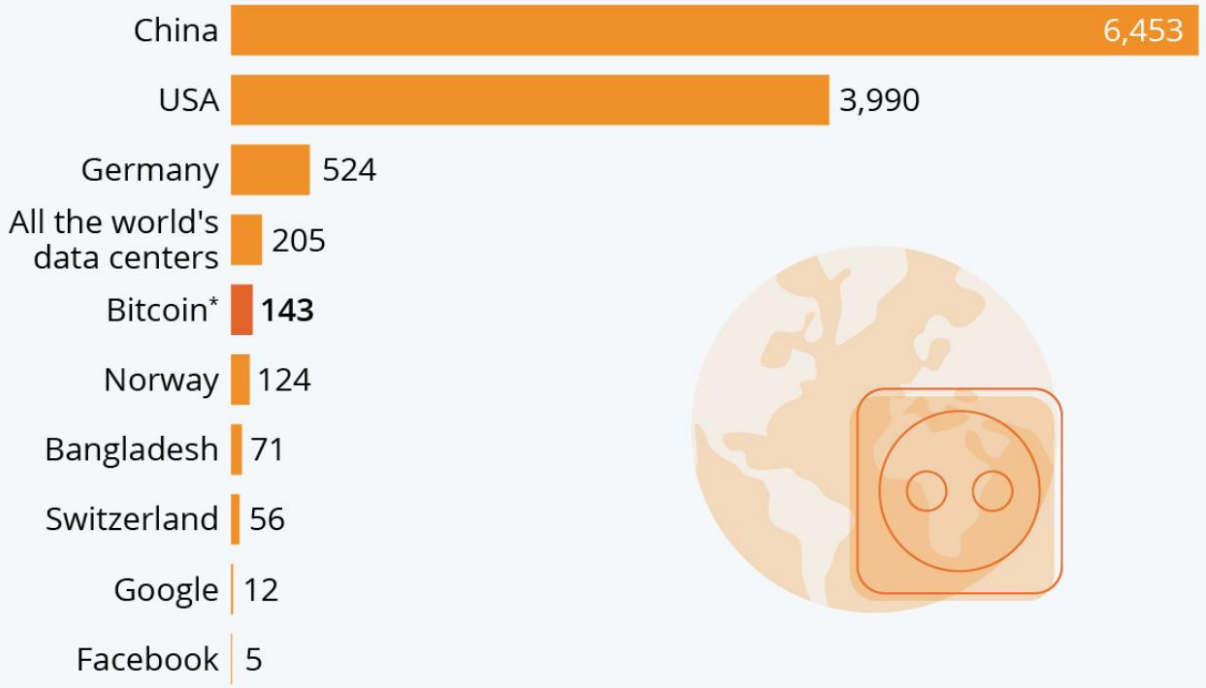


NFTs


BLOCKCHAIN PROS
Disintermediation
High-Quality Data
Durability and Security
High Level of Integrity
Immutability and Transparency
Longevity and Reliability
Simplistic Ecosystem
Empowered Users
Faster Transactions
Lower Transactional Costs
New Business Model and Value Chain
BLOCKCHAIN CONS
Redundant Performance
Complex Signature Verification Process
Private Keys
Integration Concerns
Uncertain Regulations
Large Energy Consumption
No Control for Enterprises
Privacy Concerns
Cultural Adoption/Disruption
Lack of In House Capabilities
High Cost

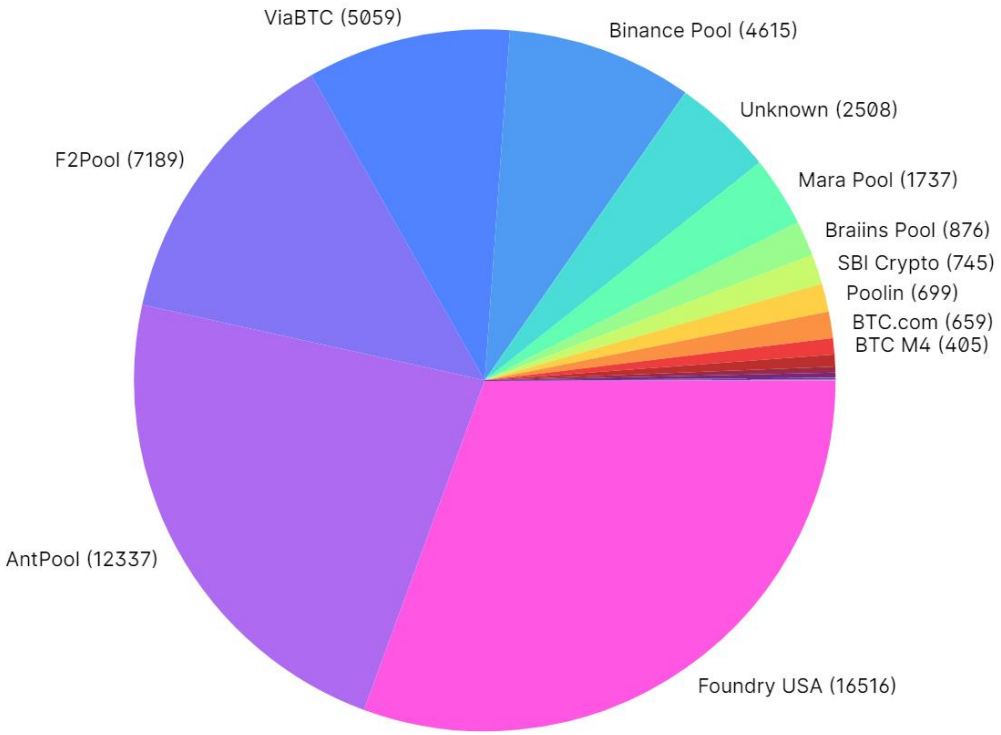
Bitcoin Devours More Electricity Than Many Countries

Annual electricity consumption in comparison (in TWh)



* Bitcoin figure as of May 05, 2021. Country values are from 2019.
Sources: Cambridge Centre for Alternative Finance, Visual Capitalist

Mining pools



Miner / Pool	Percent	Blocks Mined
Foundry USA	30.598%	16516
AntPool	22.856%	12337
F2Pool	13.318%	7189
ViaBTC	9.372%	5059
Binance Pool	8.550%	4615
Unknown	4.646%	2508
Mara Pool	3.218%	1737
Braiins Pool	1.623%	876
SBI Crypto	1.380%	745
Poolin	1.295%	699
BTC.com	1.221%	659
BTC M4	0.750%	405
Ultimus	0.547%	295
Kucoin	0.274%	148
Luxor	0.235%	127
1THash	0.059%	32
BTC M19	0.024%	13
Solo CKPool	0.022%	12
Zulu Pool	0.004%	2
KanoPool	0.004%	2
Titan	0.002%	1
CKPool	0.002%	1

Zdroje

- https://assets-global.website-files.com/5e5fcd39a7ed2643c8f70a6a/60ae0e84e7b6be8373534c4e_Bitcoin-whitepaper-original-CZ%20(1).pdf
- https://www.youtube.com/watch?v=bBC-nXj3Ng4
- https://www.youtube.com/watch?v=S9JGmA5_unY
- https://www.youtube.com/watch?v=XLcWy1uV8YM
- https://www.youtube.com/watch?v=17QRFlml4pA
- https://www.youtube.com/watch?v=pyaIppMhuic&ab_channel=WhiteboardCrypto
- https://101blockchains.com/pros-and-cons-of-blockchain/
- https://www.statista.com/chart/18632/estimated-annual-electricity-consumption-of-bitcoin
- https://www.blockchain.com/explorer/charts/pools

Ďakujem za Vašu pozornosť!