# Blockchain

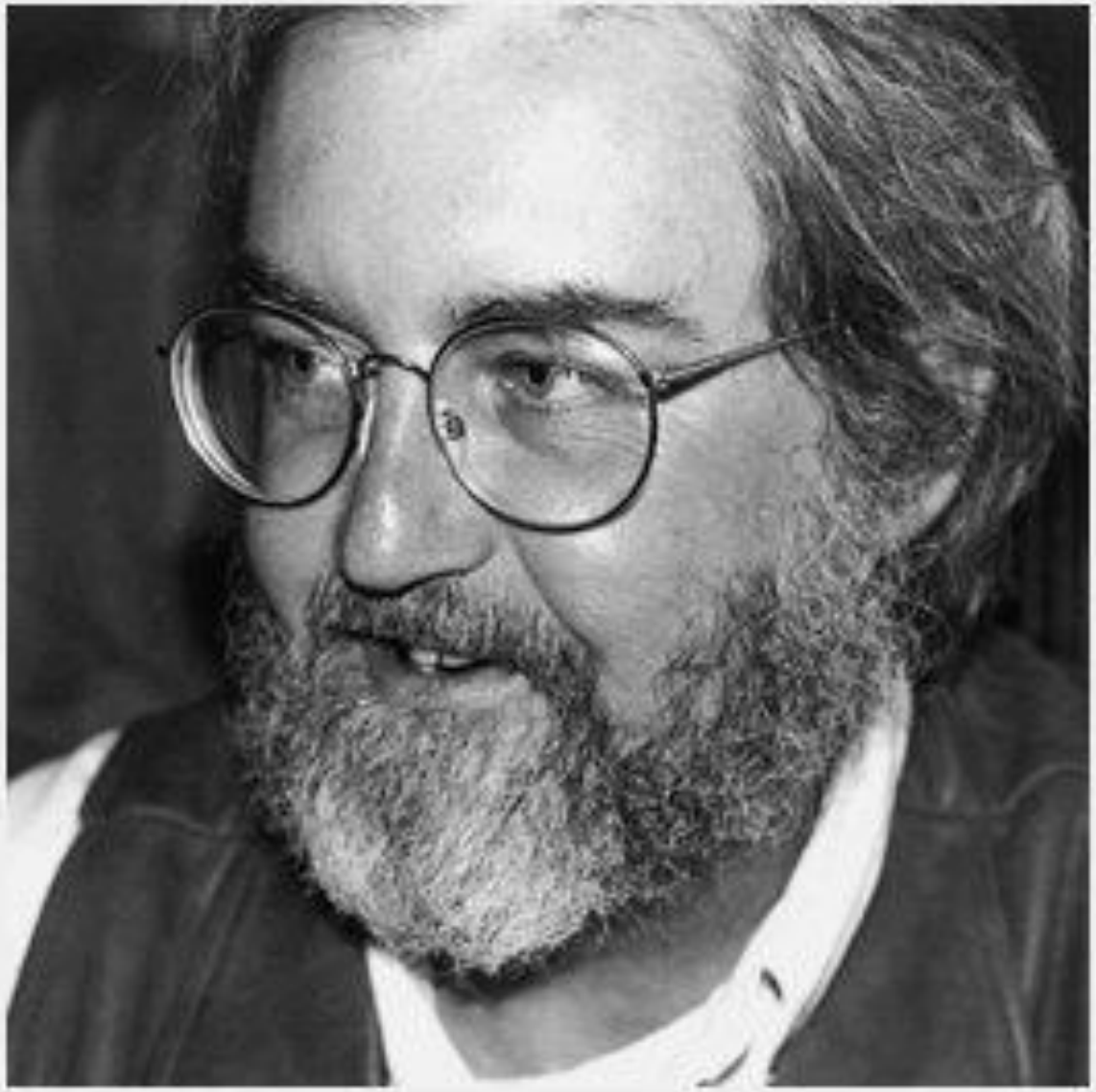
## …ÉS A KRIPTOVALUTÁK (!) SZEREPE A GAZDASÁGI ÉLETBEN

Sík Zoltán Nándor

*2018.04.11*

# Miről lesz szó? (csak röviden!)

- Miért kellett a blockchain?
- A Bitcoin rendszer
- A blockchain további használati lehetőségei
- Blockchain ma – Altcoinok, Tokenek, Tőzsdék, ICO-k, Startup-ok



TIMOTHY C. MAY (US - VIA SKYPE)

Author of The Crypto Anarchist Manifesto

# Timothy C. May

From Wikipedia, the free encyclopedia

**Timothy C. May**, better known as **Tim May**, is an American technical and political writer, and was an electronic engineer and senior scientist at Inte
He retired in 2003.

Contents [hide]



## Discovery of alpha particle effects on computer chips [edit]

As an engineer, May is most noted for having solved the "alpha particle problem", which was affecting the reliability of integrated circuits as device
where a single alpha particle could change the state of a stored value and cause a single event upset. May realized that the ceramic packaging wh
clay, was very slightly radioactive. [2] [3] Intel solved the issue by increasing the charge in each cell to reduce its susceptibility to radiation[4] and ado
products.[*citation needed*]

May co-authored the 1981 IEEE W.R.G. Baker Award-winning paper "Alpha-Particle-Induced Soft Errors in Dynamic Memories", published in the IE
*Devices* in January 1979 with Murray H. Woods.[5]

# The Crypto Anarchist Manifesto

Timothy C. May <tcmay@netcom.com>

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re- routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

--

.....
Timothy C. May | Crypto Anarchy: encryption, digital money,
tcmay@netcom.com | anonymous networks, digital pseudonyms, zero
408-688-5409 | knowledge, reputations, information markets,
W.A.S.T.E.: Aptos, CA | black markets, collapse of governments.
Higher Power: 2^756839 | PGP Public Key: by arrangement.

# Miért kellett a blockchain?

- Ki kellene kerülni a bankokat – megbízhatatlan a „megbízható harmadik fél”
- Első alkalmazás – a Bitcoin rendszer
- Technológiai innováció halmaz
- Új elem: Blockchain - a dupla költés elkerülésére


BANK
of
EVIL


A GONOSZ BANKJA

# A Bitcoin rendszer

# 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.


WHO IS
SATOSHI NAKAMOTO?

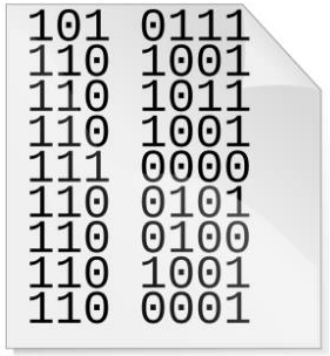
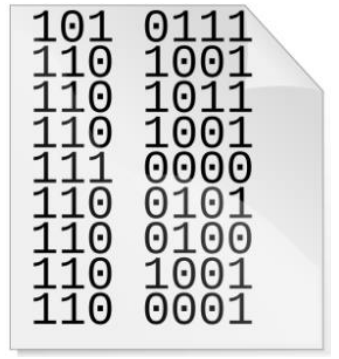
# 6 Discussion

Satoshi Nakamoto used the phrase "proof-of-work" repeatedly throughout the Bitcoin paper and Nick Szabo is the only author of the training corpus who used the same exact phrase in his blog post called *Bit gold*. It supports a theory that Nick Szabo is very close to Satoshi in terms of linguistic style. The document distances of every author of the corpus in 2-dimensional spaces using multidimensional scaling, MDS on sklearn were visualized. In Pic 1, the distance between Ian Grigg and Nick Szabo is the shortest, suggesting that Ian Grigg and Nick Szabo are closely related to each other, which might not be a coincidence. Wei Dai and Timothy C. May are far away from each other and Nick Szabo and Ian Grigg, possibly suggesting that Wei Dai and Timothy C. May are not strong candidates for Satoshi Nakamoto compared to Nick Szabo and Ian Grigg.

# A Bitcoin rendszer lényege 1

- Ne kelljen megbízható harmadik fél (bank), mégis megbízhatóan működjön
- A fizikai világhoz hasonló „értéket” kellene közvetíteni a digitális világban (ellentétben az információ sokszorozódásával, itt az cél, hogy az adott „dolog” egyszerre csak egy helyen „létezzen”)
- Mindig tudni kell, hogy ki rendelkezik az adott „értékkel”

# A „dolgok” közvetítése fizikai, digitális és kripto világban

| | Fizikai világ (transfer) | Digitális világ (copy/paste) | Kripto világ (transfer) |
|---|---|---|---|
| A |  |  |  |
| B |  |  |  |

# A Bitcoin rendszer lényege 2

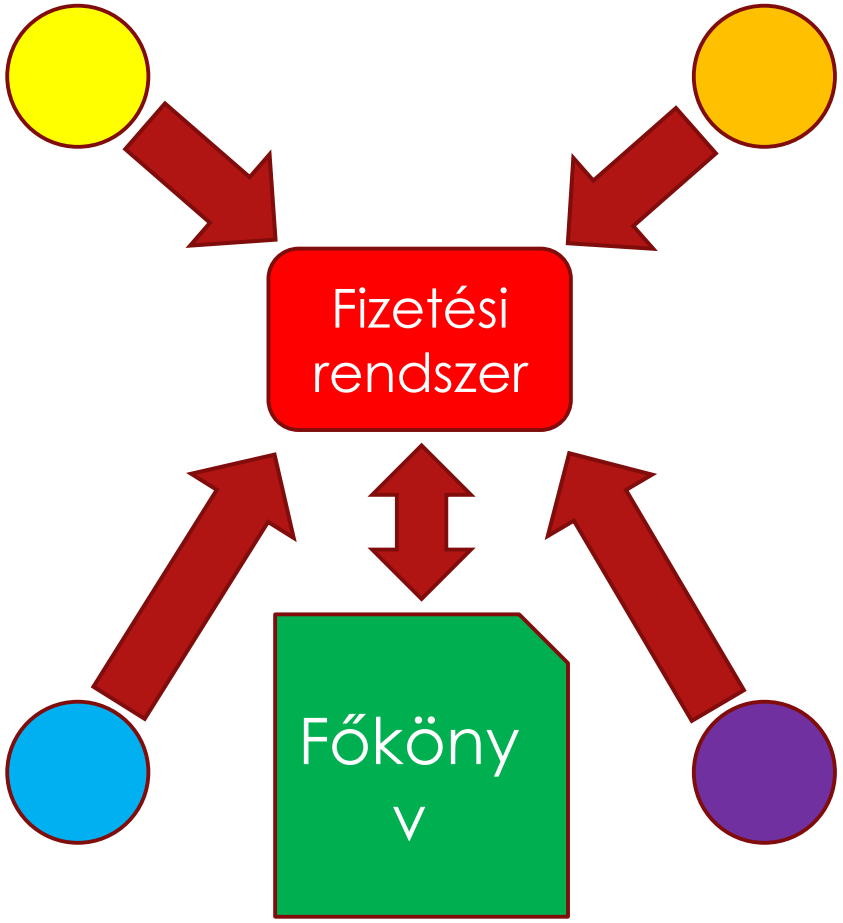
- Egyetlen, konszenzusos protokoll létezzen, és annak betartását mindenki ellenőrizhesse, és bárki részt vehessen a rendszerben, egyenrangú félként (nyílt forráskód)
- Limitált mennyiségű kriptopénz (21millió) – ne legyen értéktelen
- *Megjegyzés: nem ez volt az első kísérlet digitális pénzre, lásd: David Chaum (DigiCash), Wei Dai (B-money)*

# Mi kell ehhez?

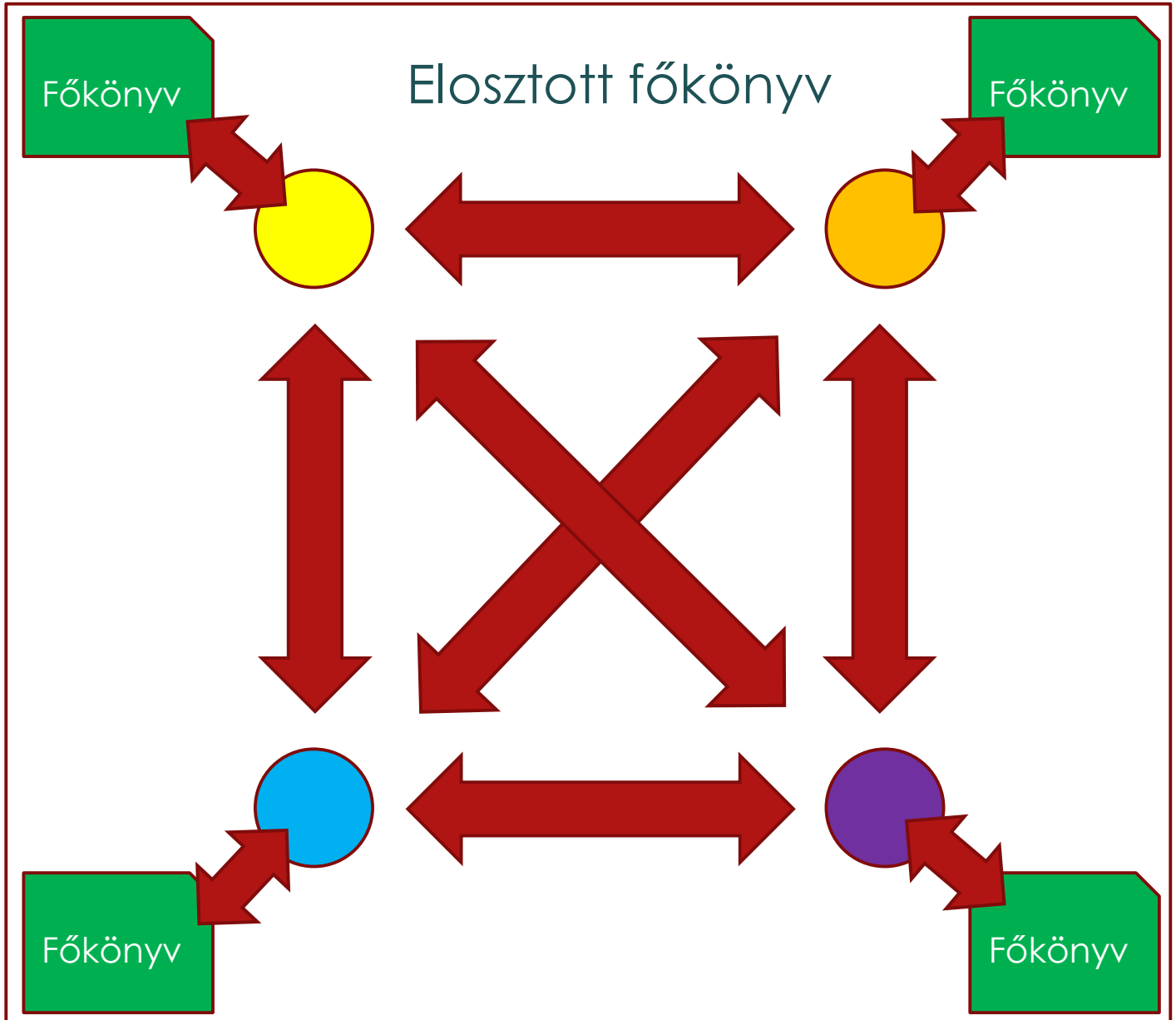
- Tranzakciók, és azok könyvelése
- Nyílt, és elosztott főkönyv (distributed ledger)
- Minden részvevő (full node) által könyvelve/ellenőrizve
- A tranzakciók anonim számlákhoz/tárcákhoz (wallet) rendeltek (hiszen a tranzakciókat minden „könyvelő” látja)
- Az egyes felek nem ismerik egymást, nem is bíznak egymásban…
- Csak a protokollban kell megbízni (nem a kódban, az lehet hibás!)
- A limitált (!) mennyiségű fizető eszköz (bitcoin), fokozatosan (!) kerül forgalomba (infláció elkerülése)

# Központi és elosztott főkönyv közötti különbség

## Központosított főkönyv




## Elosztott főkönyv



# Hogyan oldjuk meg?

- Anonim pénztárcák (wallet) létrehozása nyílt kulcsú rejtjelezési technológiával
- A tranzakciók is „csak” számsorok, két anonim tárca között
- Az el nem költött (unspent - UTXO) bitcoin a tárcába visszakerül
- Egyszer és mindenkorra le kell könyvelni
- Minden tranzakciót csak és kizárólag egyszer lehet könyvelni (double spending probléma megoldása)
- A főkönyv maga a blokklánc – megszakíthatatlan a kezdetektől (a genezis blokktól)

# A megoldás egy innováció halmaz

## Már meglévő elemek:

- Nyílt kulcsú rejtjelezés (Public Key Cryptography)
- Elektronikus aláírás (Electronic signature)
- Hash kód generálás (Hash = fix méretű lenyomat, kivonat)
- Munkabizonyíték (Proof of Work)
- Központ nélküli (Peer-to-peer) kommunikáció

## Új elem:

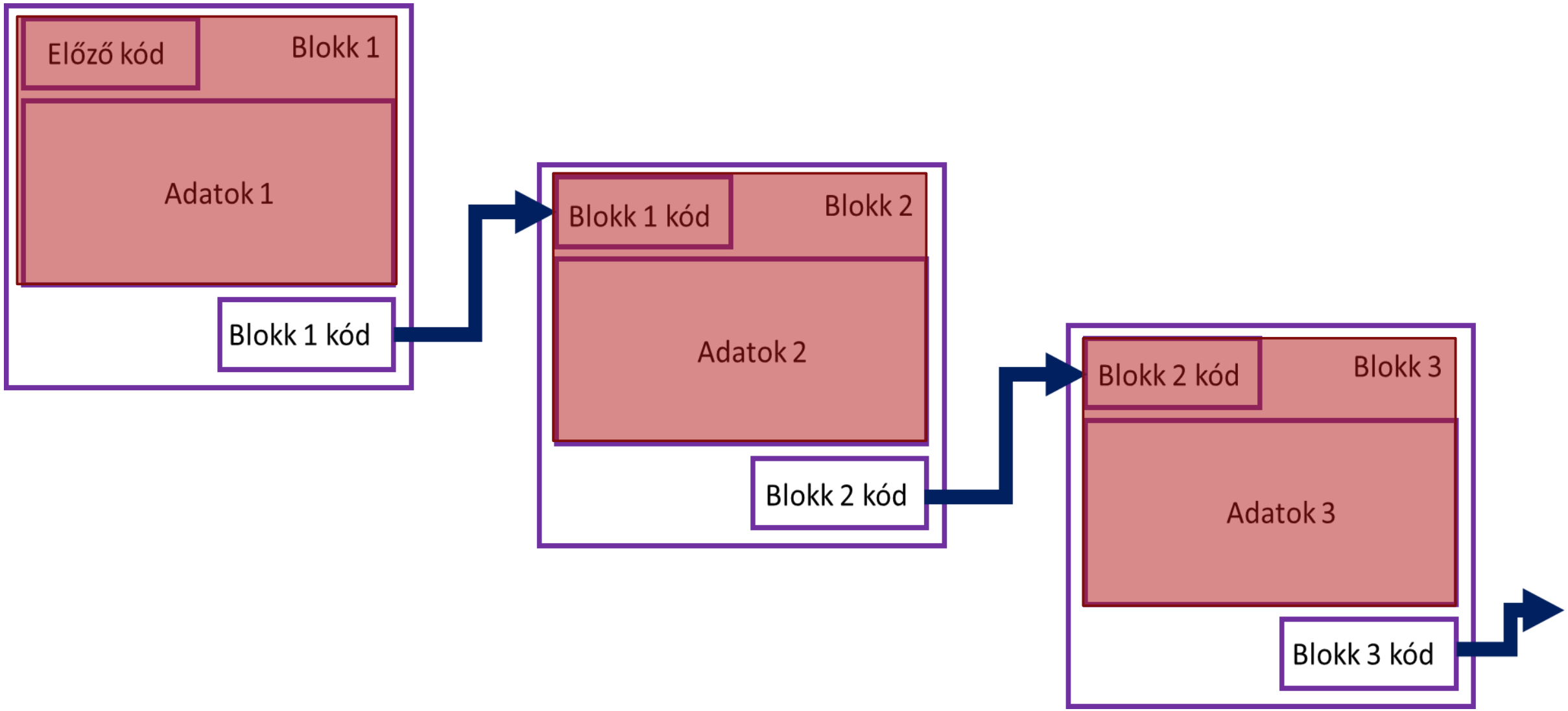
- (Publikus) blokklánc (blockchain)
  – ez túlmutat a Bitcoin rendszeren!

# Hol használjuk még ezeket?

## Példák a „mindennapi” használatra:

- Nyílt kulcsú rejtjelezés – minden web oldal, ami HTTPS://
- Elektronikus aláírás – elektronikus személyi igazolvány, e-banki azonosító kártyák, minden hivatalos helyről származó installált szoftver
- Hash kód generálás – az elektronikus aláírással aláírandó adat kivonatolása
- Munkabizonyíték – e-mail szerverek spam-elés megnehezítésére
- Központ nélküli kommunikáció – torrent hálózat
- Blockchain – ez egy új platform (az értékek internete, web 3.0…)

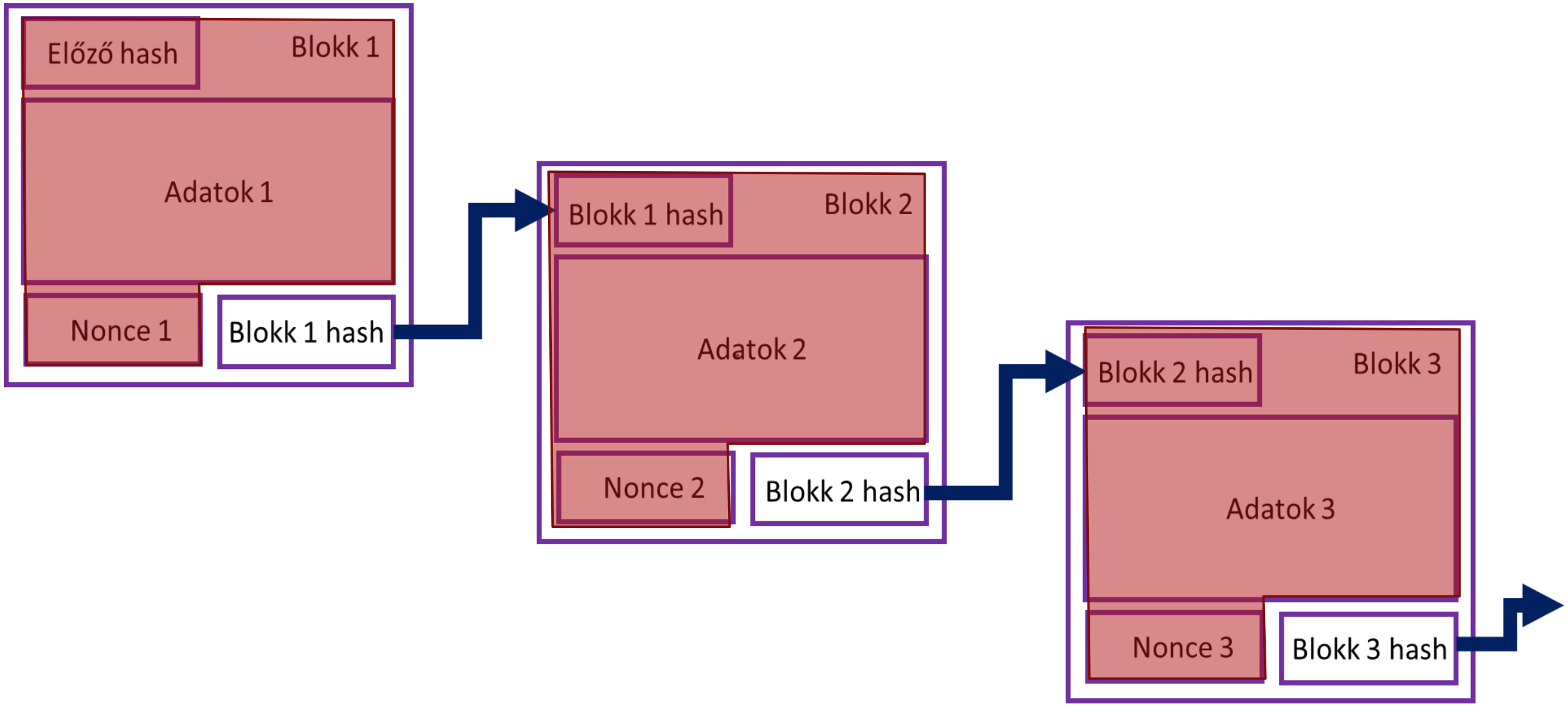
# Általános blockchain



# Ki könyvelheti a következő blokkot? 1

- Versengés kell hozzá - kockadobással döntjük el? … jó sok „kockával”
- Megoldás: Proof of Work – rengeteg „kockadobás”
- Feladat: kihozni egy olyan hash kódot a block végén, aminek első X számjegye mind nulla (X - bonyolultság)
- Nagyon bonyolult feladat – ehhez kell a „N-once” (nonce)

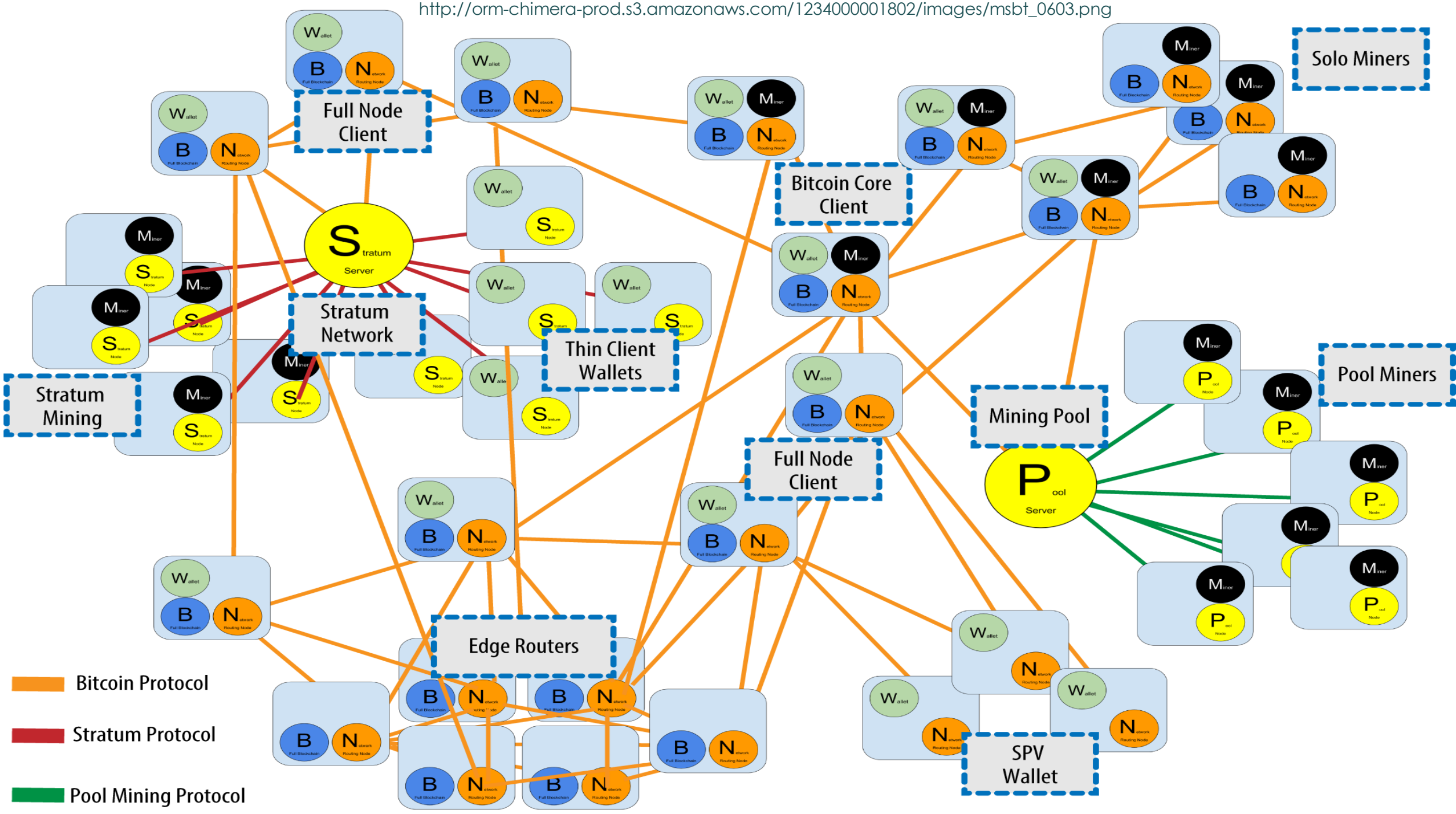
# Blokkchain a nonce-szal



# Ki könyvelheti a következő blokkot? 2

- Minden résztvevő (full node) ezen dolgozik
- Akinek elsőre sikerül az adott nonce-t megtalálni, annak a lapját fogadja el mindenki a következő főkönyvi lapnak
- Miért? Mert ez van leírva a protokollban, és mindenki ehhez tartja magát – KONSZENZUS!!!

http://orm-chimera-prod.s3.amazonaws.com/1234000001802/images/msbt_0603.png



# Block #514099

**BlockHash** 00000000000000004cfcf3859cbd0f82b7a9ebbb5e92f7fa8fa4ffb6de7dfc

## Summary

| | | | |
|---|---|---|---|
| **Number Of Transactions** | 773 | **Difficulty** | 3462542391191.563 |
| **Height** | 514099 (Mainchain) | **Bits** | 17514a49 |
| **Block Reward** | 12.5 BTC | **Size (bytes)** | 347908 |
| **Timestamp** | Mar 18, 2018 2:58:06 PM | **Version** | 536870912 |
| **Mined by** | | **Nonce** | 1299879262 |
| **Merkle Root** | d93679c33a70e3270dad9bcbcce43... | | |
| **Previous Block** | 514098 | | |

# Kérdések

- Miért nem lehet egy adott „összeget” kétszer elkölteni?
- Honnan tudják a node-ok, hogy milyen tranzakciók léteznek, amiket le kell könyvelni?
- Hogyan választják ki, hogy mely tranzakciók kerülnek az összeállítandó blokkba?
- Mi történik a lekönyveletlen tranzakciókkal?
- Mennyi időnként jön létre egy blokk?
- Mi van, ha egyszerre többen is sikeresen összeállítottak egy blokkot (találtak megfelelő nonce-ot)?
- Hogy keletkezik egyáltalán „bitcoin” a rendszerben?
- Mi van, ha valaki nem követi a protokollt?

# Miért nem lehet kétszer költeni?

- Mert minden tranzakció viszonylag gyorsan (Bitcoin rendszer esetén kb. 10 percenként – „blokkidő”) lekönyvelődik
- Csak egy blokklánc lesz érvényes (lásd később), ezért nincs olyan, hogy két különböző és érvényes (!) blokkban is lekönyvelésre kerül egy tranzakció
- A tranzakciókat nem lehet meg nem történtté tenni (nincs storno!)
- Minden előzmény blokk (a teljes főkönyv!) minden full node-nál (teljes csomópont) megvan, és ellenőrizhető

# Mely tranzakciók vannak még lekönyveletlenül?

- A node-ok egymás közt „elhíresztelik” a tranzakciókat
- Nem biztos, hogy minden node értesül minden tranzakcióról, mire a következő blokk összeáll
- De azért tovább híreszteli azokat, amik még nincsenek lekönyvelve
- Minden blokk mindenkihez eljut, miután valaki azt sikeresen összeállította és a többi full node elfogadta azt a lánc következő blokkjának

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon Mar 19 2018 23:34:00 GMT+0100 (Közép-európai téli idő ).

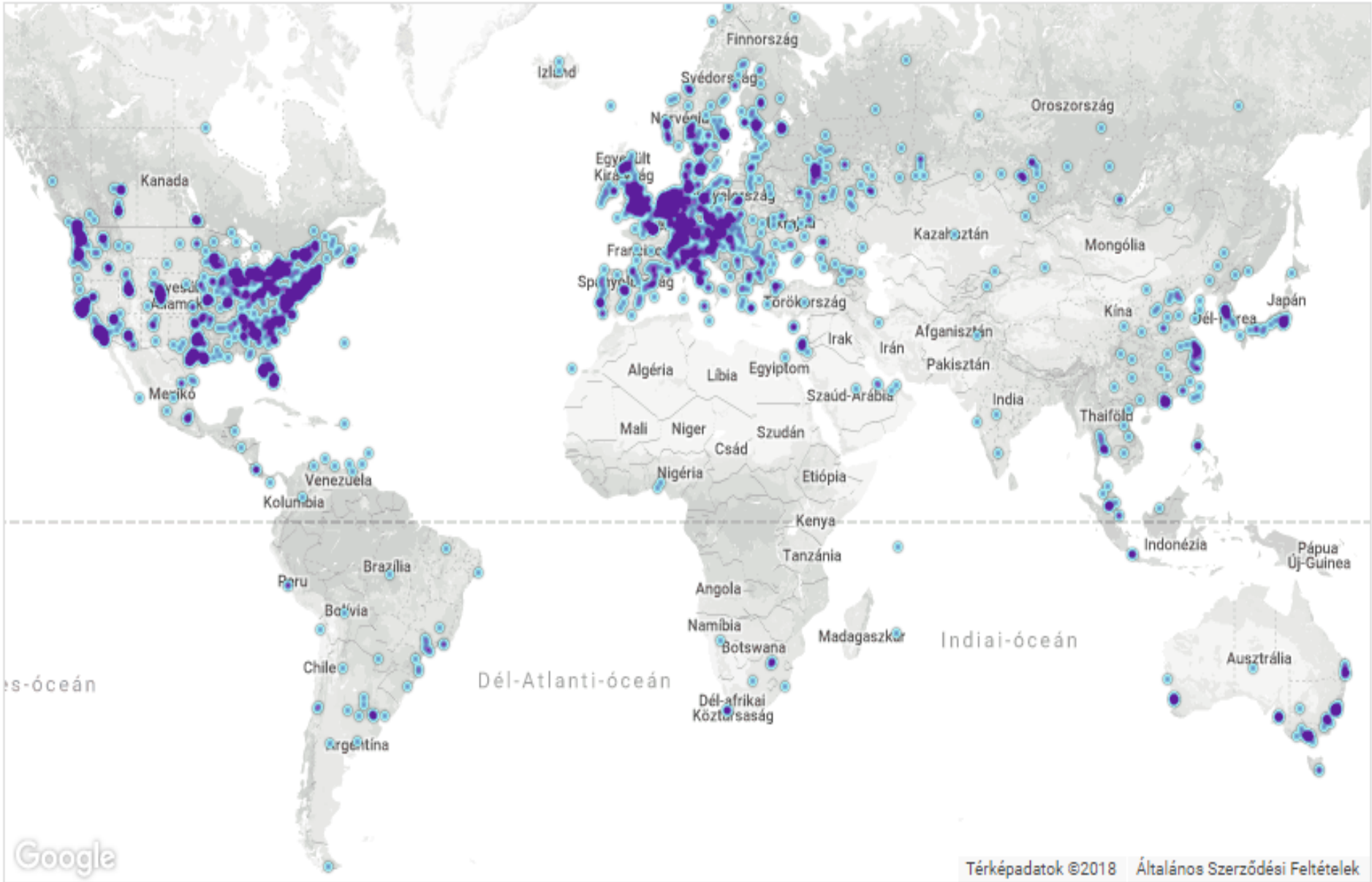
# 12274 NODES

24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

| RANK | COUNTRY | NODES |
|---|---|---|
| 1 | United States | 2768 (22.55%) |
| 2 | China | 2150 (17.52%) |
| 3 | Germany | 2007 (16.35%) |
| 4 | France | 686 (5.59%) |
| 5 | Netherlands | 505 (4.11%) |
| 6 | United Kingdom | 431 (3.51%) |
| 7 | Canada | 405 (3.30%) |
| 8 | Russian Federation | 363 (2.96%) |
| 9 | n/a | 309 (2.52%) |
| 10 | Singapore | 234 (1.91%) |

More (100) »




Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

# Hogyan választanak a lekönyveletlen tranzakciók közül?

- Az adott full node által ismert tranzakciókból összeállít egy (jelenleg még max. 1MB méretű) blokkot (1000 - 2000 tranzakció fér bele)
- Megjegyzés: a blokkméret ma az egyik legnagyobb skálázási gond – különböző megoldási javaslatok vannak – de ki javasol, és hogy fogadja el azt a közösség
- Minden tranzakció tartalmaz egy minimális könyvelési „díjat” is (ezt a node kapja). A könyvelő node igyekszik „optimalizálni” a saját díját

# Mi történik a lekönyveletlen tranzakciókkal?

- Ezeket minden node úgy tartja számon, hogy a következő blokkba még bekerülhet
- Ahogy telik az idő, egyre több node-hoz kerülnek el a lekönyveletlen tranzakciók, így egyre több az esélye, hogy valaki beemeli az általa összeállítandó blokkba

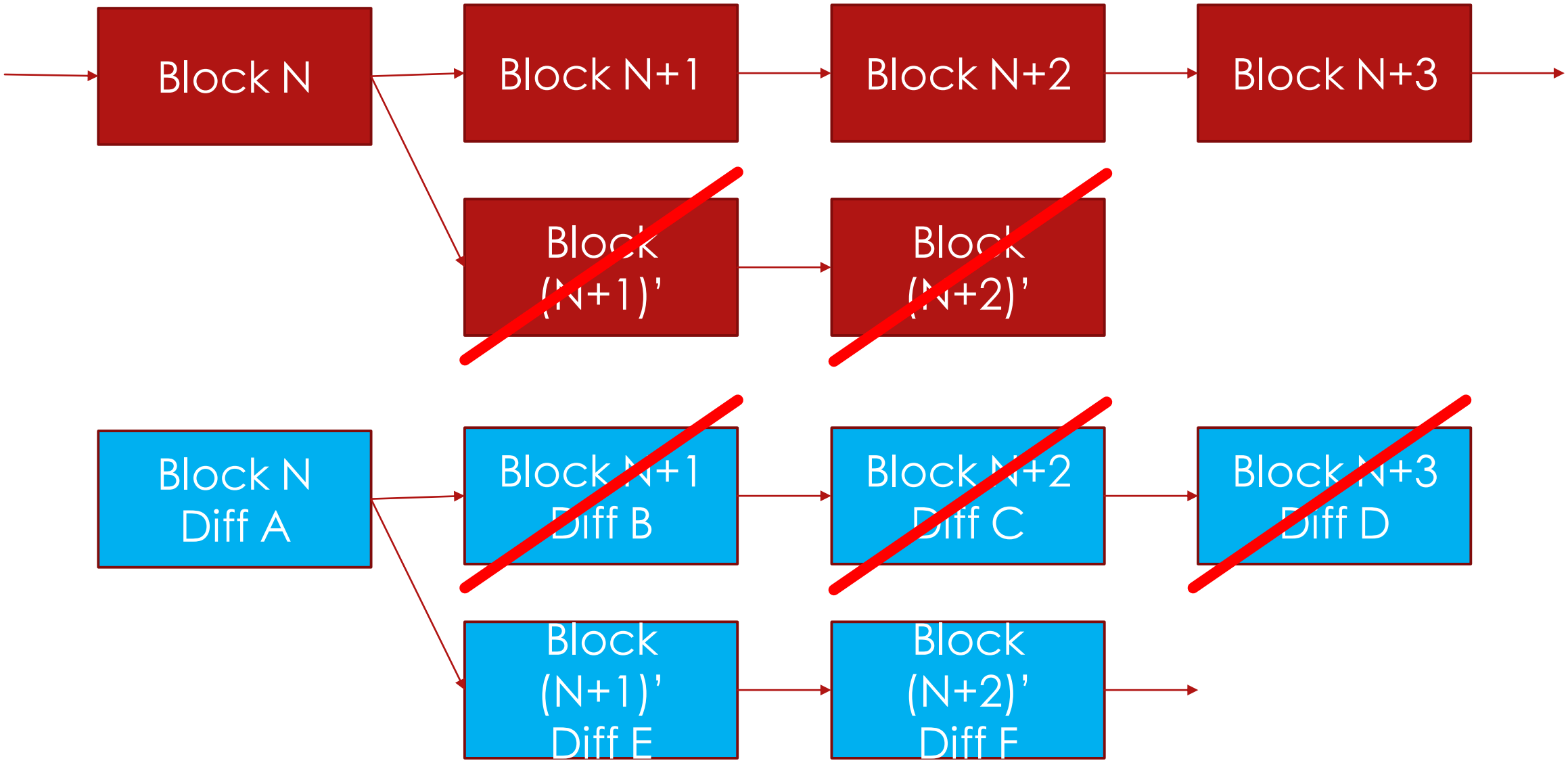
# Mennyi időnként jön létre egy blokk?

- A Bitcoin rendszer protokollja szerint kb. 10 percenként jön létre egy blokk
- Ez csak átlag idő, sok paramétertől függ
- A feladat bonyolultságát (difficulty) változtatja automatikusan a rendszer (1 óránként 75-300% között), hogy a többi paramétertől függetlenül tartani lehessen a 10 percet
- A bonyolultságot az jelenti, hogy hány darab nulla legyen a block hash elején azaz mennyi legyen az az X szám).
- Minél nagyobb X, annál nehezebb megtalálni a blokkhoz a megfelelő nonce-ot
- Megjegyzés: skálázási probléma, hogy a rendszer lassú. Manapság ez óriási gond (ezért is kellene a blokkméretet növelni)

# Mi van, ha egyszerre többen állítanak elő blokkot?

- Előfordul, hogy egymástól „távol” lévő node-ok kvázi egyszerre találnak megfelelő nonce-ot, és így állítanak elő blokkot.
- Ilyenkor valamilyen szabály kell, hogy melyik legyen az elfogadott blokklánc, nehogy „elágazzon” (fork) – hacsak nem szándékolt az elágazás (ez más témakör).
- Példák a szabályra:
  - Az a blokk a „nyerő”, amelyhez azóta már többen csatlakoztak, azaz azt véve alapul, már több utána következő blokkot állítottak elő. Azaz a hosszabb blokklánc lesz a nyerő, a rövidebb láncot eldobja a rendszer, akárhány blokkot is generáltak az adott blokk után

# „Nyerő” blokk kiválasztása

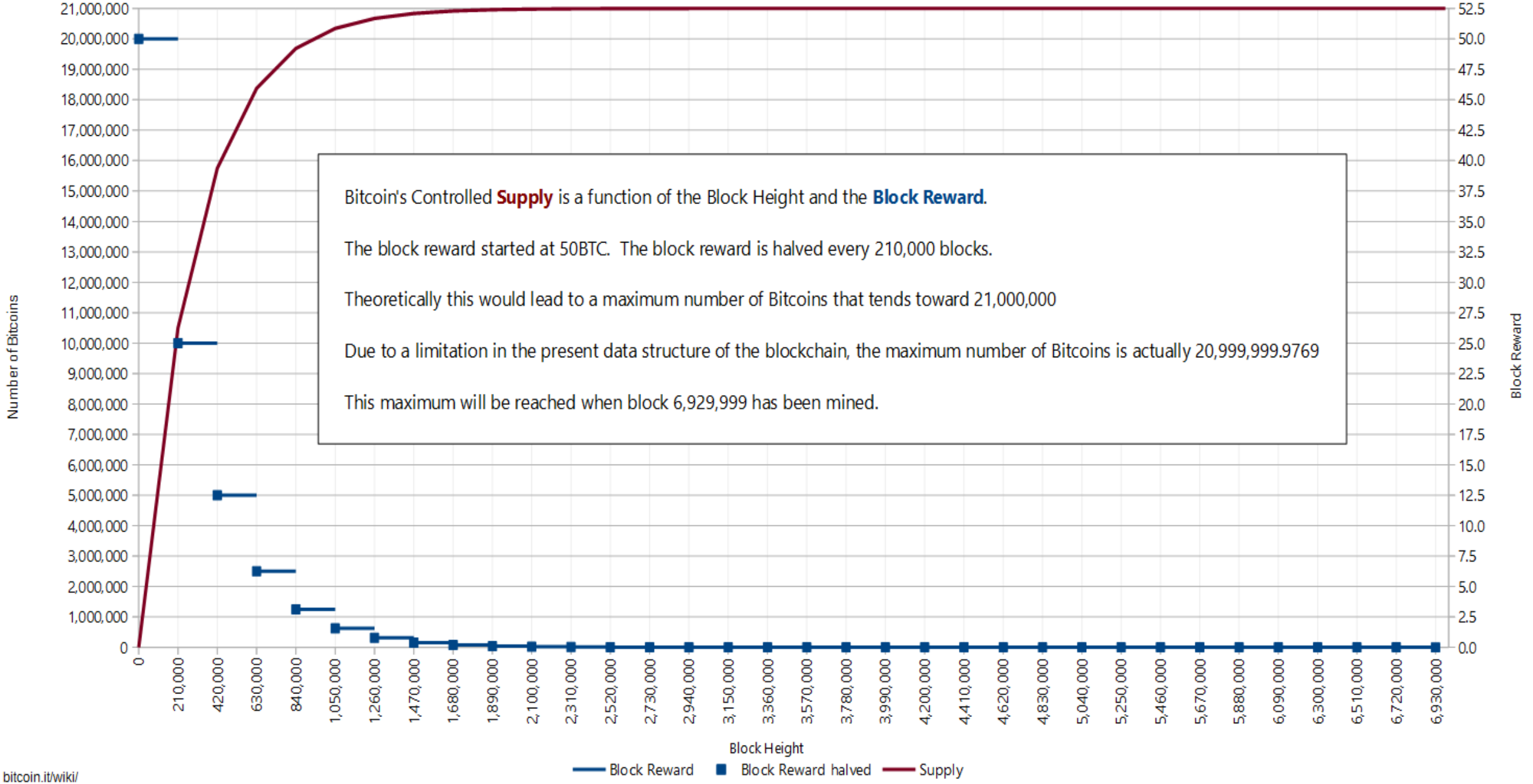


# Hogyan kerül a bitcoin a rendszerbe?

- A node-ok, amikor összeállítanak egy blokkot, megkapják a tranzakciókban lévő könyvelési díjat
- Emellett minden sikeresen összeállított, és a rendszer tagjai által elfogadott blokk után a „semmiből" keletkezik bitcoin, ami a blokkot könyvelő node jutalma (a siker mértéke az átlaghoz képest a luck)
- A semmiből a protokoll maga állítja elő a bitcoint, és ezt mindenki elfogadja (coinbase tranzakció)
- Eredetileg 50 BTC volt, de minden 210000. blokk után ez a jutalom feleződik. Jelenleg 12.5BTC a jutalom. Így kb 2140-re érik el, hogy mind a 21 millió BTC a rendszerben legyen. Utána már nem lesz jutalom.

# Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height




Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

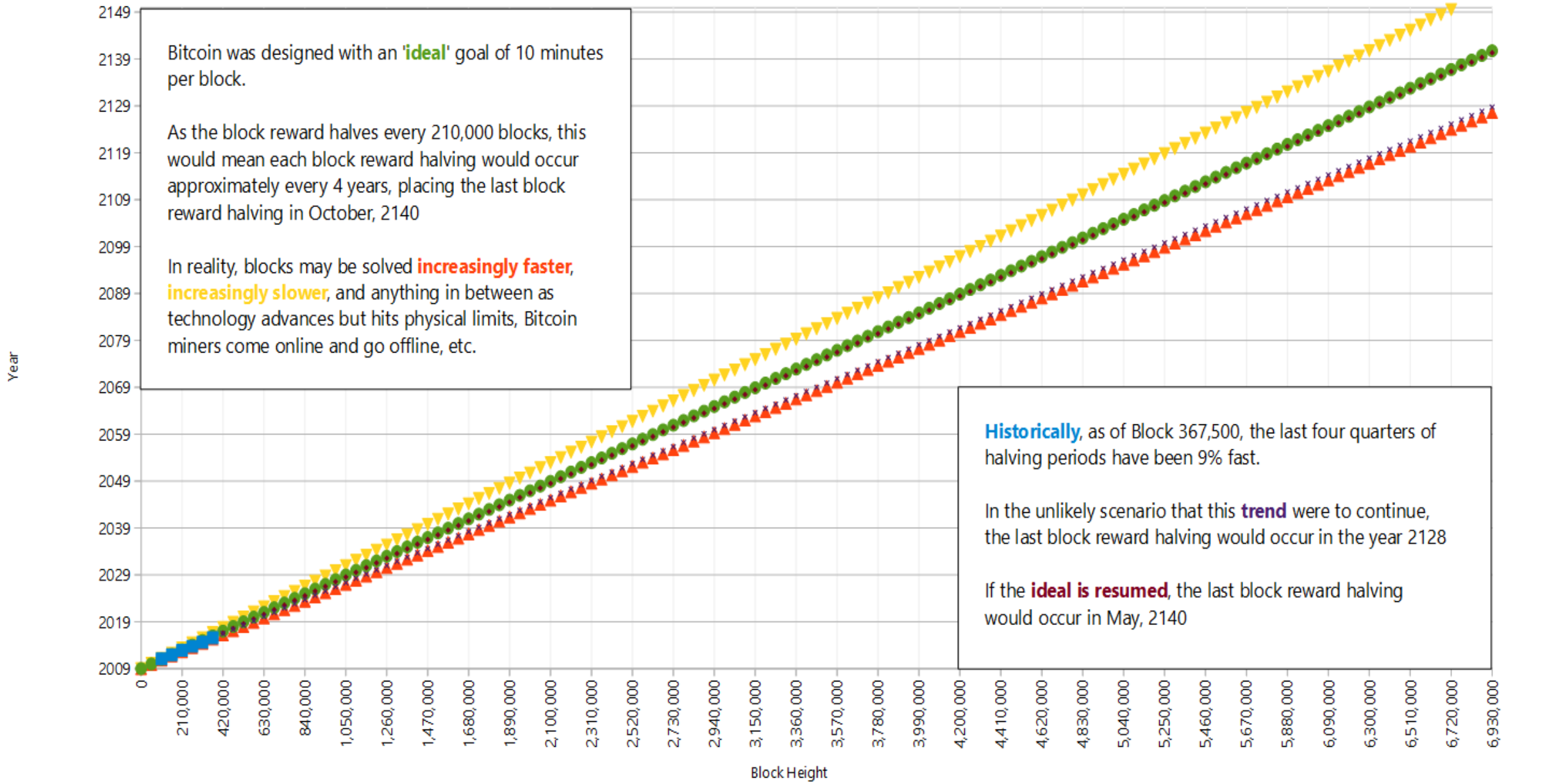
Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

# Bitcoin - Controlled Supply: timeline estimation

Estimated year of a given block height as an estimation of the network's hash rate




bitcoin.it/wiki/

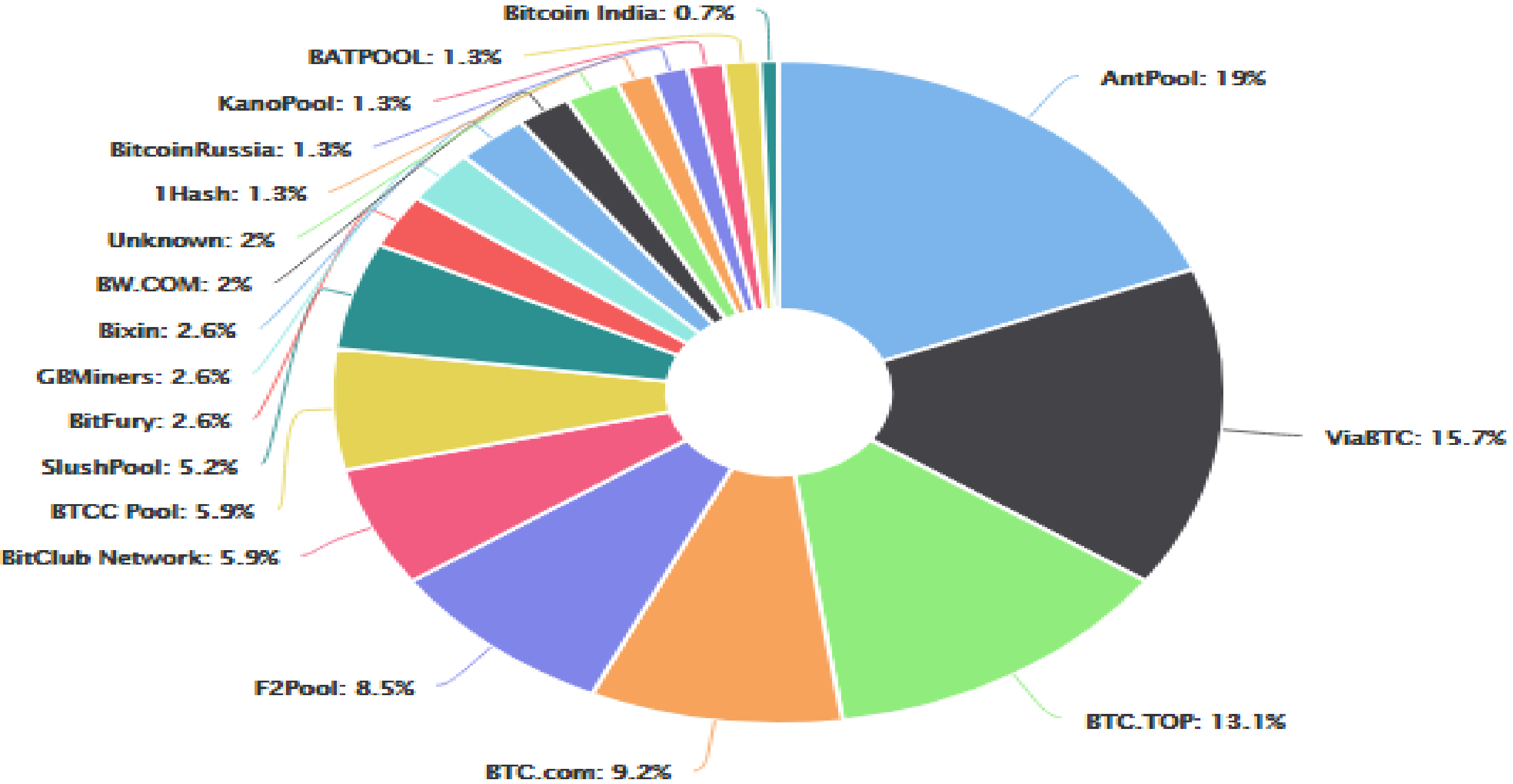
July 30th 2015

# Mi van, ha valaki nem követi a protokollt?

- Alapvetően a rendszer kizárja a „csalót”
- Ez addig működőképes, amíg valakinek nincs annyi számítási kapacitása, hogy ő állítja elő legnagyobb valószínűséggel a következő blokkokat is (51% attack)
- Ilyenkor már ő tudja megszabni a szabályokat
- Ennek elosztott rendszer lévén kicsi a valószínűsége
- Ha mégis, akkor lehet u.n. „hard fork”, azaz a rendszer kétfelé válik, az egyik csapat az, akik követik az új szabályt, a másik csapat, akik nem.

# A „kockadobás” – a node-ok, akik bányásznak

- A bányászat a PoW alapján a nonce megtalálása adott X difficulty mellett
- Óriási mértékű számítási kapacitás kell hozzá (petahash/sec)
- Nagyon fogyasztja az áramot…
- De a „reward” miatt megéri – Bitcoin rendszer esetén 10 percenként 12,5BTC keletkezik (mai árfolyamon, kb. 11800 USD/BTC-vel számolva 147,500 USD/10 perc, azaz 21,240,000 USD/nap keletkezik a semmiből… és akkor még nem mondtuk, hogy 2017 decemberében 20,000 USD/BTC is volt az árfolyam)


Bitcoin India: 0.7%
BATPOOL: 1.3%
KanoPool: 1.3%
BitcoinRussia: 1.3%
1Hash: 1.3%
Unknown: 2%
BW.COM: 2%
Bixin: 2.6%
GBMiners: 2.6%
BitFury: 2.6%
SlushPool: 5.2%
BTCC Pool: 5.9%
BitClub Network: 5.9%
F2Pool: 8.5%
BTC.com: 9.2%
BTC.TOP: 13.1%
ViaBTC: 15.7%
AntPool: 19%

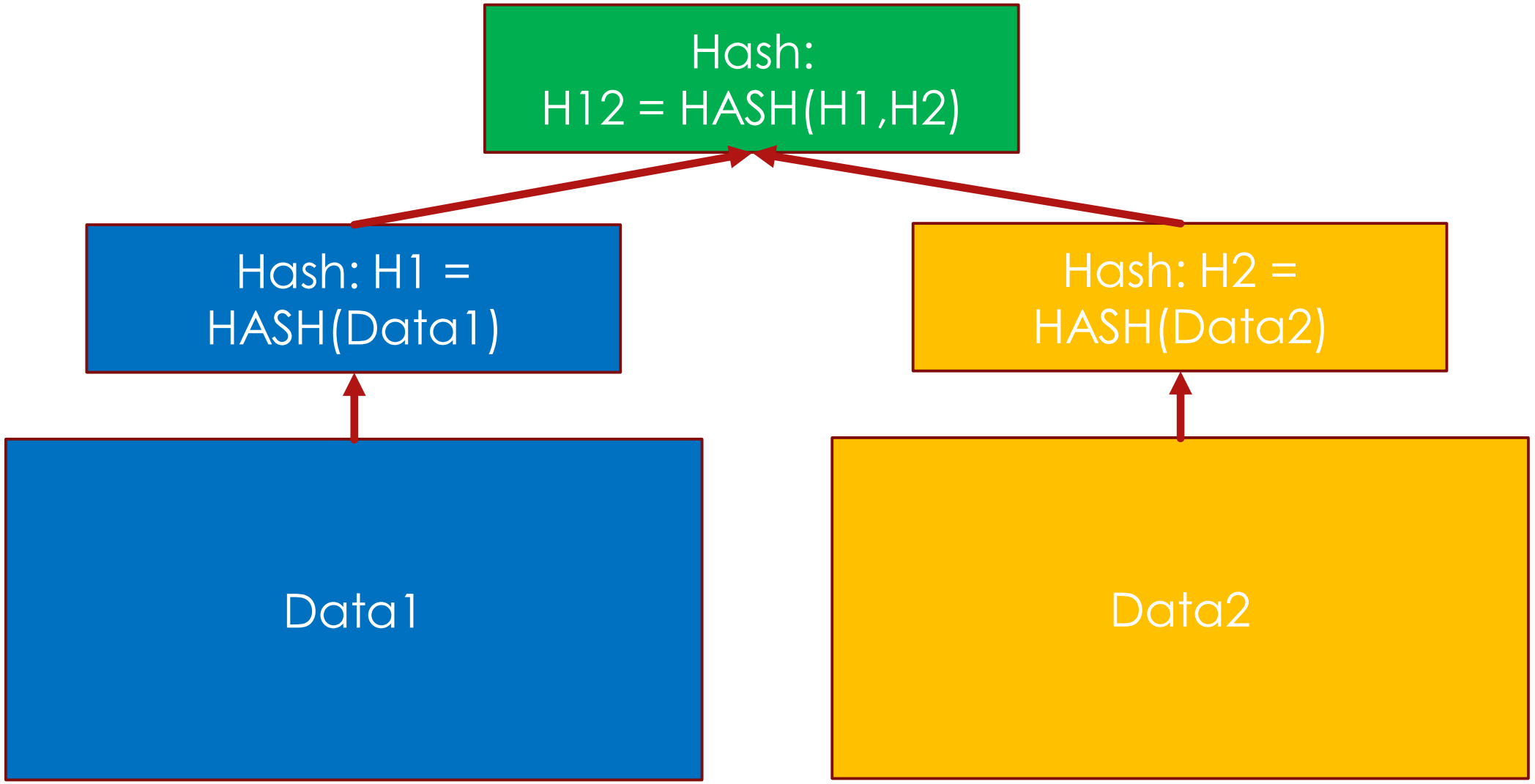
# Mit lehet csinálni bányászat (PoW) helyett?

- Léteznek más algoritmusok is, egyelőre kísérleti stádiumban
  - Proof of Stake (PoS) – Ethereum fogja használni (Casper kód, Serenity release-től)
  - Proof of Elapsed Time (PoET)
  - Proof of Authority (PoA)
  - Proof of Resource (PoR)
- Mineable, premined, non-mineable
- Mineable - Trusted 3rd Party nélküli, Publikus, PoW

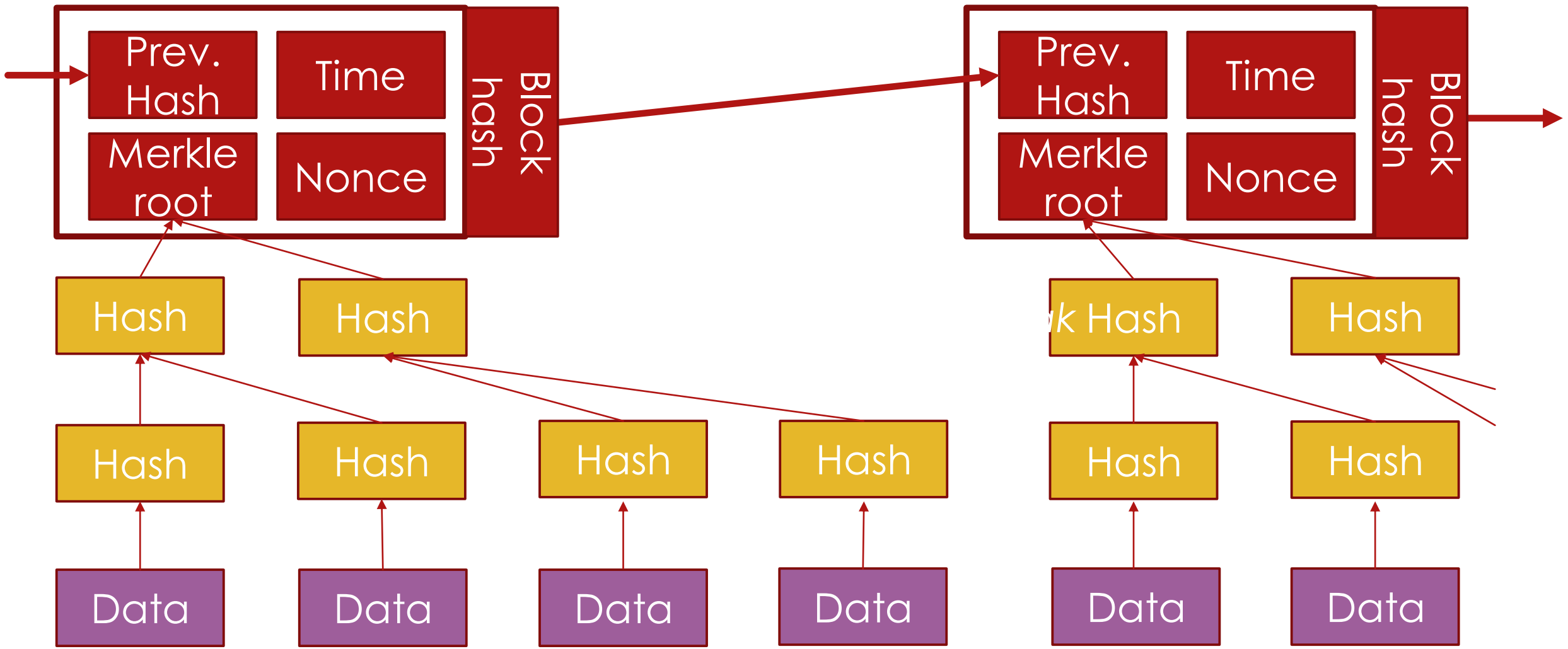
# Mi van ténylegesen a blockchain-ben?

- A blokkok az összes tranzakciót tartalmazzák
- A blockchain blokk fejrésze kevés adatot tartalmaz (Bitcoin rendszerben a blokk fej összesen 80 byte)
- A tényleges adatok nem a blokk fejrészében vannak, csak az adatok hashkódjainak „összege”, az u.n. Merkle fa gyökere, a Merkle-root
- A bányászatnál nem az összes adatot hash-elik újra és újra, csak a készülő blokk fejrésézben lévő adatokat. A Merkle root-ot csak egyszer állítják elő a node-ok
- Az ellenőrzésnél a full node a teljes blockchain adattartalmát ellenőrzi, az egyszerű node (light node, SPV node) csak a blokkok fejrészében lévő adatokat
- *Megjegyzés: több blockchain rendszer van, ahol a tényleges adatok a blockchain-en kívül vannak (off-chain) elhelyezve (pl. nagyobb tömegű adatok tárolására használt blockchain-ek, pl Siacoin, Filecoin, Storj, MaidSafe, Burstcoin) így a blockchain „csak” a hitelesség ellenőrzéséhez, illetve pl. az adat tényleges helyének meghatározásához használt hash kódokat tartalmazza*

# Merkle fa képzése (általános „HASH” függvényre)



# Merkle fa és a Merkle-root a blockchain-ben

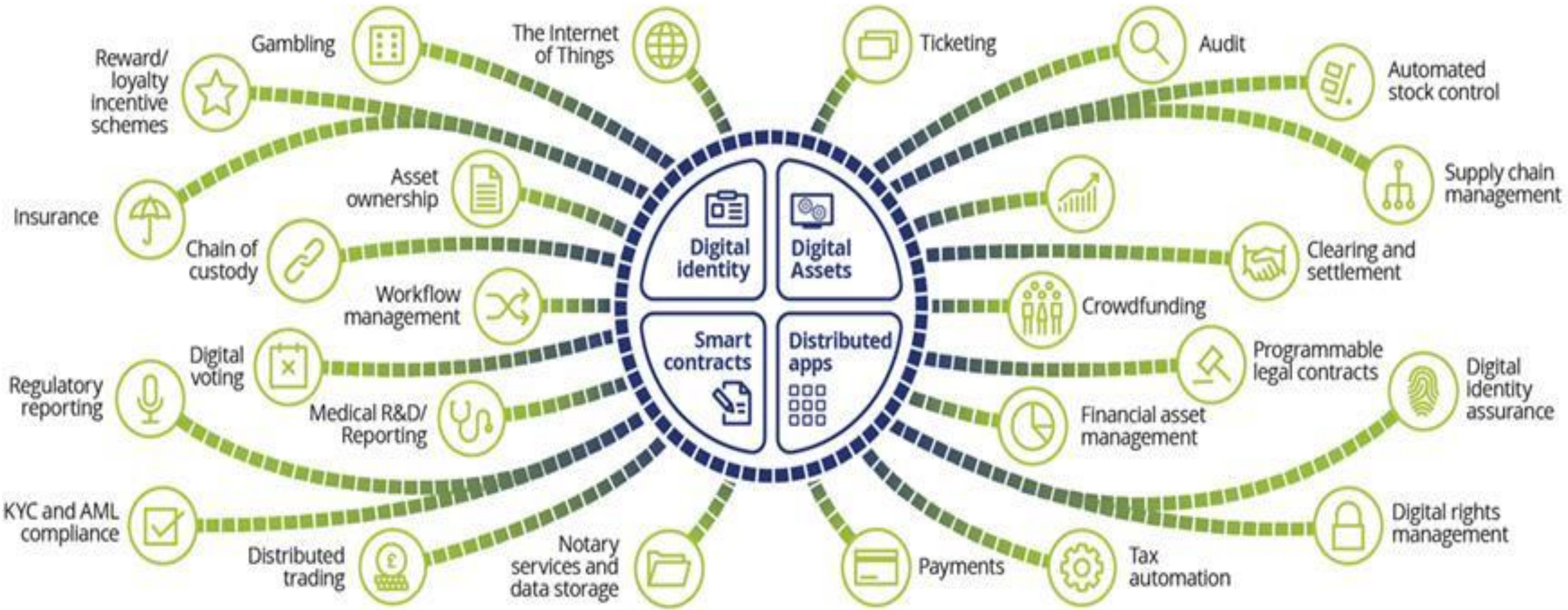


# Miért mutat túl a blockchain a bitcoin-on?

- Gyakorlatilag bármilyen adat tárolható benne (nem csak tranzakciók!), sőt végrehajtható kódok, (elosztott) programok (dApp – decentralized applications) is (lásd pl. okos szerződések az Ethereum rendszerben)
- A hitelesség biztosítása és mindenki által való könnyű ellenőrizhetősége a legnagyobb előny (ezért ez nem egy egyszerű adatbázis!)
- Elosztott (központ nélküli!) szervezetek/vállalatok hozhatók létre (DAO – Decentralized Autonomous Organization, ill. DAC - ~ Corporation)
- Óriási innovációs potenciál, elosztott világ, Web 3.0, értékek internete
- *Megjegyzés: ez nem csak a blockchain-re igaz, hanem más, újabb technológiai innovációkra is (pl. Tangle (IOTA alkalmazza), illetve hashgráf)*
- *Megjegyzés2: a (publikus) blockchain nagyon lassú és nagyon drága üzemeltetésű rendszer, ezért leginkább „digitális értékek" tárolására alkalmas*

# What can you do with a blockchain?

KYC – Know Your Customer
AML – Anti-Money Laundering




Deloitte.

www.deloitte.co.uk/blockchain

# BLOCKCHAIN SECTOR USE

- Fintech/
- Banking / Insurance
- Payments
- Smart contracts Legal / Compliance
- Government
- Health
- Corporate
- IoE / IoT
- Digital Identity
- Cyber Security
- Verified Data
- Ethereum

intelligentHQ

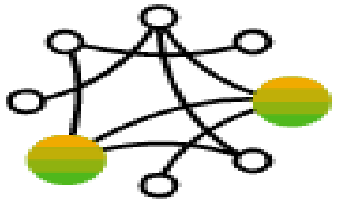
BLOCKCHAINAGE

# Blockchain típusok

- Publikus – megbízható harmadik fél nélküli
- Privát (permissioned) – megbízható harmadik fél/felek üzemeltetik – más a célja – itt nem is kell PoW (azaz bányászat)

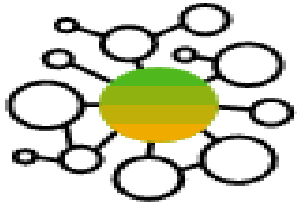
# 4 types of blockchain networks

Of the four ways to establish a blockchain network – currently, consortium is the most accepted model for business.



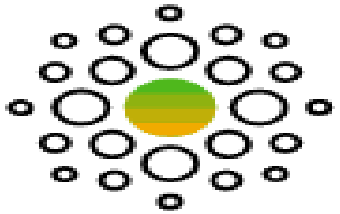
## Consortium blockchains

In a consortium blockchain, the consensus process is controlled by a pre-selected group – a group of corporations, for example. The right to read the blockchain and submit transactions to it may be public or restricted to participants. Consortium blockchains are considered to be "permissioned blockchains" and are best suited for use in business.



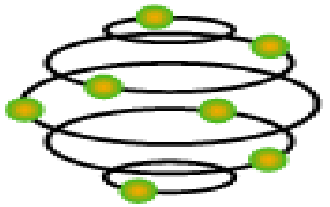
## Semi-private blockchains

Semi-private blockchains are run by a single company that grants access to any user who satisfies pre-established criteria. Although not truly decentralized, this type of permissioned blockchain is appealing for business-to-business use cases and government applications.



## Private blockchains

Private blockchains are controlled by a single organization that determines who can read it, submit transactions to it, and participate in the consensus process. Since they are 100% centralized, private blockchains are useful as sandbox environments, but not for actual production.



## Public blockchains

Anyone can read a public blockchain, send transactions to it, or participate in the consensus process. They are considered to be "permissionless." Every transaction is public, and users can remain anonymous. Bitcoin and Ethereum are prominent examples of public blockchains.

# A publikus blockchain előnyei

- Nem kell senkire rábízni magunkat
- Egymásban sem kell hinni, csak a konszenzus számít
- A protokoll az, amiben hinni kell (és nem a kód!)
- Nyílt forráskód (legtöbbször) – hányan tudják ellenőrizni?
- Gyakorlatilag megállíthatatlan, elosztott „gép”, óriási rendelkezésre állás
- Különböző működési módú blockchain-ek
- Továbbfejleszthetőség

# A privát blockchain előnyei

- Van/vannak megbízható harmadik fél/felek, de tehermentesített/ek
- Csak megbízható/hiteles adatok kerülhetnek a rendszerbe (ki és milyen adatot küldhet a rendszerbe)
- Az adatok (és azok rendszerbe kerülési ideje) a megbízható harmadik fél/felek nélkül is ellenőrizhetők
- Nem szükséges a drága PoW a blockchain előállításához (pl. PoS alapon működik)
- Gyorsabb, mint a publikus
- Különböző működési módú blockchain-ek
- Továbbfejleszthetőség

# A publikus blockchain hátrányai

- Nyílt forráskód, de ki ért hozzá, hogy fejlessze? – limitált létszám
- Nincs semmi védelem, ha meglopnak, csalnak
- Csak a rendszer határain belül biztosított a protokoll (vagy ott sem!)
- Saját magunknak kell védeni magunkat/értékeinket
- Pénz van benne – jönnek a csalók, hackerek, „scam artist”-ok, Ponzi séma (Onecoin, BitConnect)…
- Új, jobb protokollok is jöhetnek, így vége lehet az egésznek
- Quantum computer resistance?

# A privát blockchain hátrányai

- Mégiscsak van „megbízható” harmadik fél
- Nem olyan nagy a rendelkezésre állása, mint a publikusnak
- Megállítható/megállhat a működés (adott node(ok) kiesésével)
- Csak a rendszer határain belül biztosított a protokoll (vagy ott sem!)
- Korlátozott alkalmazhatóság
- GDPR???

# Hibák

- A rendszerek még „in vivo” kísérletiek
- Skálázás sokszor nem megodott
  - Bitcoin – BitcoinABC – hard fork – Bitcoin Cash (BCH)
  - Bitcoin – SegWit2x – kérdéses, hogy bejön-e
- Hard fork/soft fork (pl. UASF) – van itt konszenzus?
- Protokoll hibák
  - Bitcoin – transaction malleability – Mt. Gox
  - Ethereum – The DAO hacking – kényszerű fork – ETH/ETC
  - Ethereum – Parity Technologies – frozen Ether…
- Csak a rendszeren belül van „biztonság” protokoll hiba nélkül is

# Altcoin-ok, tokenek, kriptotőzsdék

- Mára kb. 1500 altcoin/token létezik
- Legjelentősebb az Ethereum
  - Vitalik Buterin találta ki (2014)
  - Turing complete script nyelv (Solidity)
  - Elosztott alkalmazások (dAapp)
  - Nick Szabó találta ki hozzá az okos szerződéseket
- De ma már kb. 20 „kriptopénz” piaci kapitalizációja van 1MRD USD felett (ez a szám volt már 34 is…)
- Ezeket kriptotőzsdéken kereskedik

Total Y2050 Marketcap: $381,115,961,418 | Total Current Marketcap: $240,924,508,109 | Bitcoin Dominance: 48.14%

## Flagged Assets USD | BTC

You haven't flagged any assets yet...

## Recent Quotes USD | BTC

You haven't viewed any assets yet...

## Daily Movers USD | BTC

**Top Gainers**

| | | |
|---|---|---|
| XVG | $0.09 | +28.78% |
| GNT | $0.24 | +20.02% |
| CVC | $0.24 | +14.60% |
| SALT | $2.24 | +12.13% |
| ICN | $0.94 | +12.11% |

**Top Losers**

| | | |
|---|---|---|
| PIVX | $3.88 | -2.32% |
| DGD | $207.26 | -1.84% |
| DCR | $48.47 | -1.45% |
| DASH | $295.55 | -1.26% |
| LTC | $114.09 | -0.75% |

## Cryptoasset Indexes

| | | |
|---|---|---|
| Bletchley 10 | 863.31 | +1.38% |
| Bletchley 20 | 1313.35 | +1.50% |
| Bletchley 40 | 205.3 | +5.55% |

## Sector Watch USD | BTC

**Daily Winners**

# Cryptoasset Categories

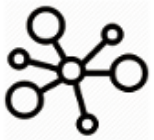
Cryptoassets can (mostly) be divided into 5 categories based on the types of networks on which they're used.

### Currency Tokens

Primarily used as Money / Store-of-Value

### Platform Tokens

Used as 'gas' on General Purpose Networks



### Utility Tokens

Built for Specifc-Use Networks

### Brand Tokens

Specific-Use on Single Entity's Network

### Security Tokens

Represent Claims on Off-Chain Assets

# Cryptoasset Sectors

Similar to how equities are often classified, cryptoassets can often apply to specific sectors of economic activity. Below are sectors identified for the assets we cover today.

### Advertising

Decentralized advertising platforms incentivize new markets through ad-network-specific onchain tokens.

### Distributed Computation

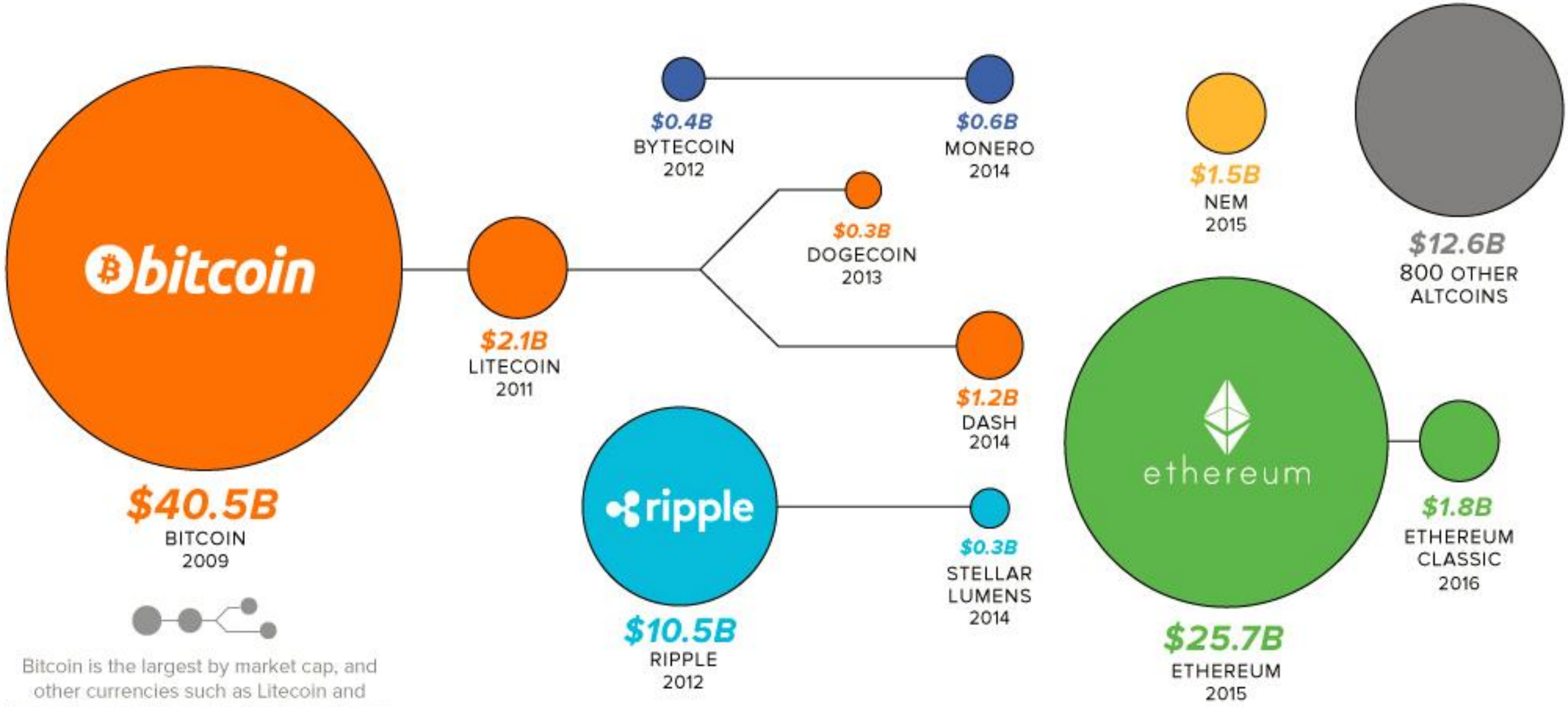
Distributed computation assets create a market for CPU/GPU power distributed globally across participating computers.

### Payment Platform

Payment platforms integrate multiple blockch platform for ease of payment, possibly emplo more complex applications.

### Distributed Storage

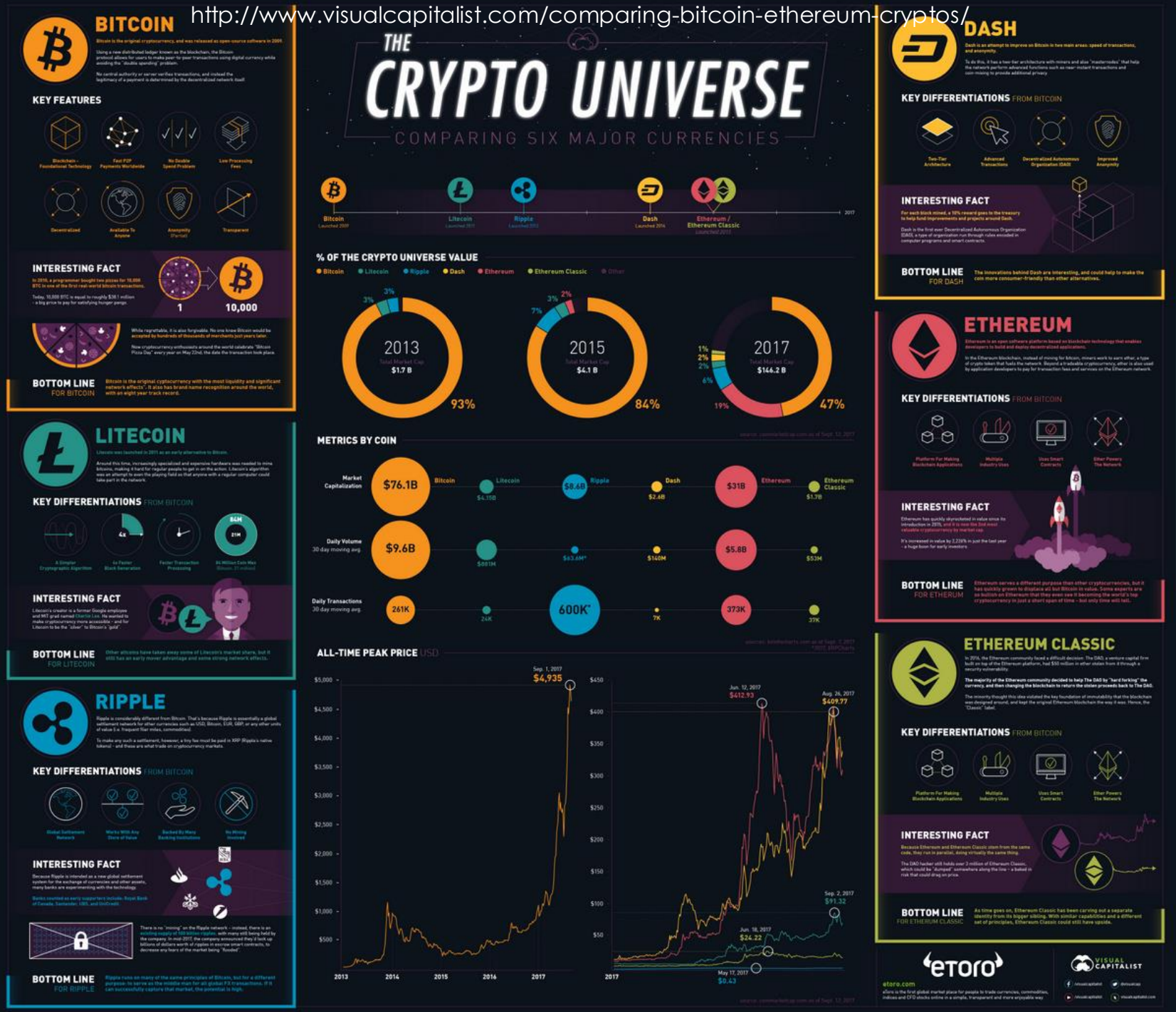
# THE CRYPTOCURRENCY UNIVERSE




Bitcoin is the largest by market cap, and other currencies such as Litecoin and Dogecoin were "forked" using its codebase.

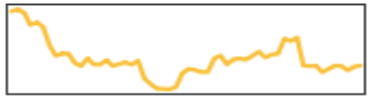
http://www.visualcapitalist.com/chart-coin-universe-keeps-expanding/

http://www.visualcapitalist.com/comparing-bitcoin-ethereum-cryptos/



# Top 100 Cryptocurrencies by Market Capitalization

All ▾ | Coins ▾ | Tokens ▾ | USD ▾ | Next 100 → | View All

| # | Name | Market Cap | Price | Volume (24h) | Circulating Supply | Change (24h) | Price Graph (7d) |
|---|---|---|---|---|---|---|---|
| 1 | Bitcoin | $114 866 726 325 | $6 769,25 | $4 126 460 000 | 16 968 900 BTC | 0,21% |  |
| 2 | Ethereum | $39 458 300 554 | $399,64 | $1 091 330 000 | 98 733 624 ETH | 1,19% |  |
| 3 | Ripple | $19 024 097 437 | $0,486618 | $156 894 000 | 39 094 520 623 XRP * | 0,28% |  |
| 4 | Bitcoin Cash | $10 898 670 191 | $638,63 | $210 485 000 | 17 065 650 BCH | 0,12% |  |
| 5 | Litecoin | $6 357 105 689 | $113,48 | $197 865 000 | 56 021 588 LTC | -1,17% |  |
| 6 | EOS | $4 698 720 281 | $5,99 | $198 586 000 | 784 639 632 EOS * | 2,27% |  |
| 7 | Cardano | $3 946 126 063 | $0,152201 | $54 416 000 | 25 927 070 538 ADA * | 1,23% |  |
| 8 | Stellar | $3 683 590 160 | $0,198563 | $27 094 600 | 18 551 241 469 XLM * | 1,24% |  |
| 9 | NEO | $3 310 892 000 | $50,94 | $105 497 000 | 65 000 000 NEO * | 0,44% |  |
| 10 | IOTA | $2 754 200 424 | $0,990887 | $20 523 900 | 2 779 530 283 MIOTA * | 0,95% |  |

# Top 100 Cryptocurrencies described in 4 words or less

by @eigenjoy

Updated November 7th, 2017

| | | | |
|---|---|---|---|
| 1 | Bitcoin | BTC | Digital gold |
| 2 | Ethereum | ETH | Programmable contracts and money |
| 3 | Bitcoin Cash | BCH | Bitcoin clone |
| 4 | Ripple | XRP | Enterprise payment settlement network |
| 5 | Litecoin | LTC | Faster Bitcoin |
| 6 | Dash | DASH | Privacy-focused Bitcoin clone |
| 7 | NEO | NEO | Chinese-market Ethereum |
| 8 | NEM | XEM | Batteries-included digital assets |
| 9 | Monero | XMR | Private digital cash |
| 10 | Ethereum Classic | ETC | Ethereum clone |
| 11 | IOTA | MIOTA | Internet-of-things payments |
| 12 | Qtum | QTUM | Ethereum contracts on Bitcoin |
| 13 | OmiseGO | OMG | Banking, remittance, and exchange |
| 14 | Zcash | ZEC | Private digital cash |
| 15 | BitConnect | BCC | Madoff-like investment fund |
| 16 | Lisk | LSK | Decentralized applications in JavaScript |
| 17 | Cardano | ADA | Layered currency and contracts |
| 18 | Tether | USDT | Price = 1 USD |
| 19 | Stellar Lumens | XLM | Digital IOUs |
| 20 | EOS | EOS | Decentralized applications on WebAssembly |
| 21 | Hshare | HSR | Blockchain switchboard |
| 22 | Waves | WAVES | Decentralized exchange and crowdfunding |
| 23 | Stratis | STRAT | Decentralized applications in C# |
| 24 | Komodo | KMD | Decentralized ICOs |
| 25 | Ark | ARK | Blockchain switchboard |
| 26 | Electroneum | ETN | Monero clone |
| 27 | Bytecoin | BCN | Privacy-focused cryptocurrency |
| 28 | Steem | STEEM | Reddit with money voting |
| 29 | Ardor | ARDR | Blockchain for spawning blockchains |
| 30 | Binance Coin | BNB | Pay Binance exchange fees |
| 31 | Augur | REP | Decentralized prediction market |
| 32 | Populous | PPT | Invoice trading futures |
| 33 | Decred | DCR | Bitcoin with alternative governance |

| | | | |
|---|---|---|---|
| 34 | TenX | PAY | Cryptocurrency credit card |
| 35 | MaidSafeCoin | MAID | Rent disk space |
| 36 | BitcoinDark | BTCD | Zcoin clone |
| 37 | BitShares | BTS | Decentralized exchange |
| 38 | Golem | GNT | Rent other people's computers |
| 39 | PIVX | PIVX | Inflationary Dash clone |
| 40 | Gas | GAS | Pay fees on Neo |
| 41 | TRON | TRX | In-app-purchases |
| 42 | Vertcoin | VTC | Bitcoin clone |
| 43 | MonaCoin | MONA | Japanese Dogecoin |
| 44 | Factom | FCT | Decentralized record keeping |
| 45 | Basic Attention Token | BAT | Decentralized ad network |
| 46 | SALT | SALT | Cryptocurrency-backed loans |
| 47 | Kyber Network | KNC | Decentralized exchange |
| 48 | Dogecoin | DOGE | Serious meme bitcoin clone |
| 49 | DigixDAO | DGD | Organisation manages tokenized gold |
| 50 | Veritaseum | VERI | Vaporware |
| 51 | Walton | WTC | IoT Blockchain |
| 52 | SingularDTV | SNGLS | Decentralized Netflix |
| 53 | Bytom | BTM | Physical assets as tokens |
| 54 | Byteball Bytes | GBYTE | Decentralized database and currency |
| 55 | GameCredits | GAME | Video game currency |
| 56 | Metaverse ETP | ETP | Chinese Ethereum plus identity |
| 57 | GXShares | GXS | Decentralized Chinese Equifax |
| 58 | Syscoin | SYS | Decentralized marketplace |
| 59 | Siacoin | SC | Rent disk space |
| 60 | Status | SNT | Decentralized application browser |
| 61 | 0x | ZRX | Decentralized exchange |
| 62 | Verge | XVG | Privacy Dogecoin |
| 63 | Lykke | LKK | Digital asset exchange |
| 64 | Civic | CVC | Identity and Authentication App |
| 65 | Blocknet | BLOCK | Decentralized exchange |
| 66 | Metal | MTL | Payments with rewards program |

| | | | |
|---|---|---|---|
| 67 | Iconomi | ICN | Digital asset investment funds |
| 68 | Aeternity | AE | Decentralized apps (prototype) |
| 69 | DigiByte | DGB | Faster Bitcoin |
| 70 | Bancor | BNT | Token Index Funds |
| 71 | Ripio Credit Net | RCN | Co-signed Cryptocurrency Loans |
| 72 | ATMChain | ATM | Advertising network |
| 73 | Gnosis | GNO | Decentralized prediction market |
| 74 | VeChain | VEN | Supply chain item IDs |
| 75 | Pura | PURA | Cryptocurrency |
| 76 | Particl | PART | Privacy marketplace and chat |
| 77 | KuCoin Shares | KCS | Profit-sharing exchange fees |
| 78 | Bitquence | BQX | Mint for cryptocurrency investments |
| 79 | FunFair | FUN | Decentralized casino |
| 80 | ChainLink | LINK | External data for contracts |
| 81 | Power Ledger | POWR | Airbnb for electricity |
| 82 | Nxt | NXT | Cryptocurrency and marketplace |
| 83 | Monaco | MCO | Cryptocurrency credit card |
| 84 | Cryptonex | CNX | Zerocoin clone |
| 85 | MCAP | MCAP | Mining investment fund |
| 86 | Storj | STORJ | Rent disk space |
| 87 | ZenCash | ZEN | Privacy-focused Bitcoin clone |
| 88 | Nexus | NXS | Bitcoin clone |
| 89 | Neblio | NEBL | Decentralized application platform |
| 90 | Zeusshield | ZSC | Decentralized insurance |
| 91 | Streamr DATAco | DATA | Real-time data marketplace |
| 92 | ZCoin | XZC | Private digital cash |
| 93 | NAV Coin | NAV | Bitcoin with private transactions |
| 94 | AdEx | ADX | Advertising exchange |
| 95 | Open Trading Ne | OTN | Decentralized exchange |
| 96 | SmartCash | SMART | Zcoin clone with rewards |
| 97 | Bitdeal | BDL | Bitcoin clone |
| 98 | Loopring | LRC | Decentralized exchange |
| 99 | Edgeless | EDG | Decentralized casino |
| 100 | FairCoin | FAIR | Bitcoin that rewards savers |

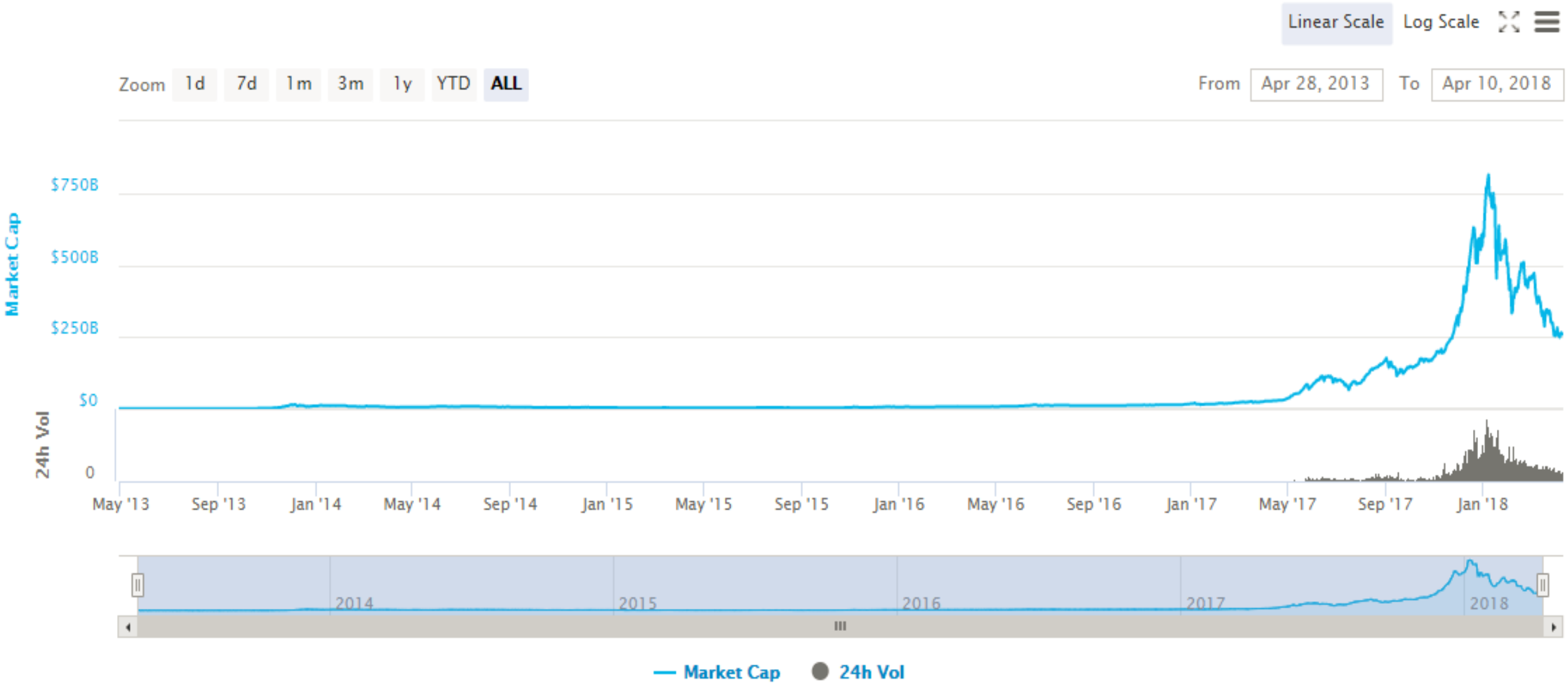


Ranked according to market cap on coinmarketcap.com as of November 7th, 2017

Caution: market cap is not an indicator of maturity or legitimacy

# Global Charts

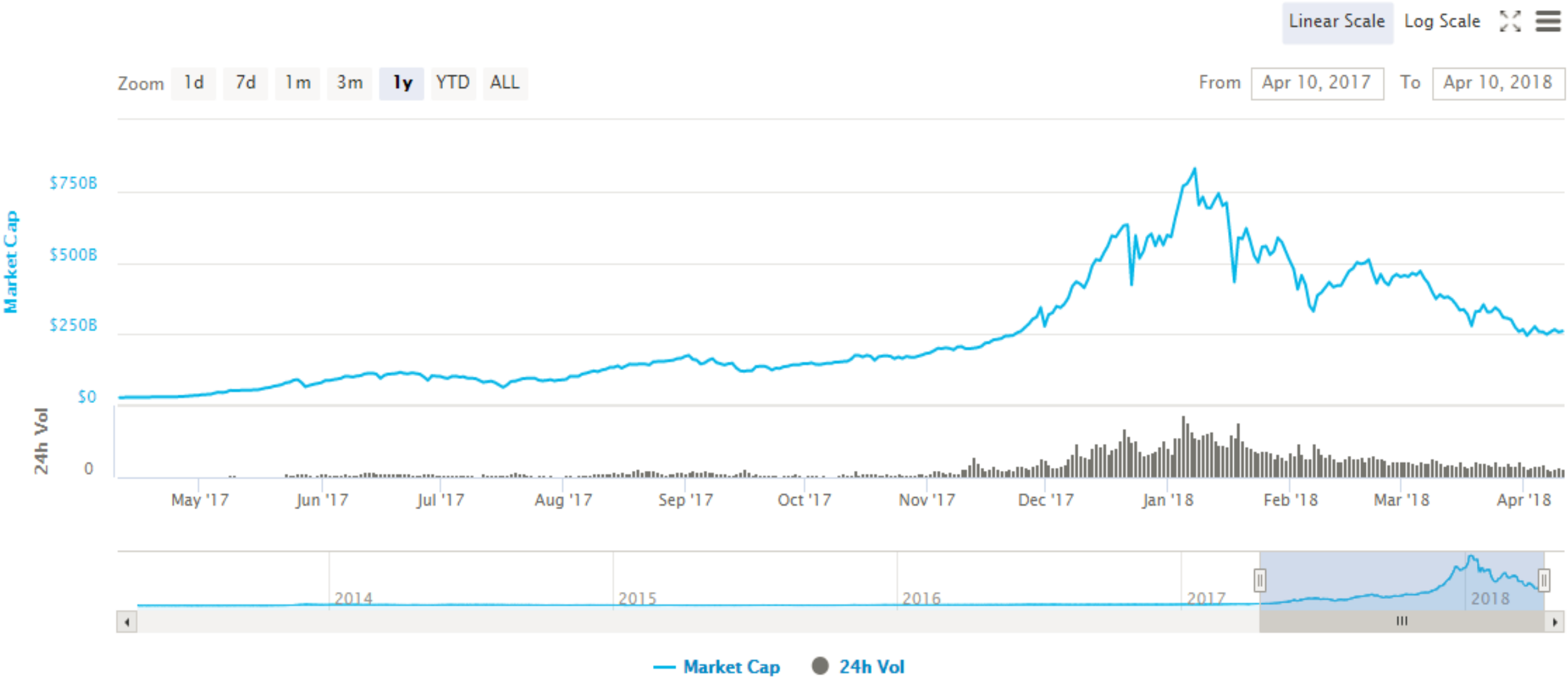
## Total Market Capitalization



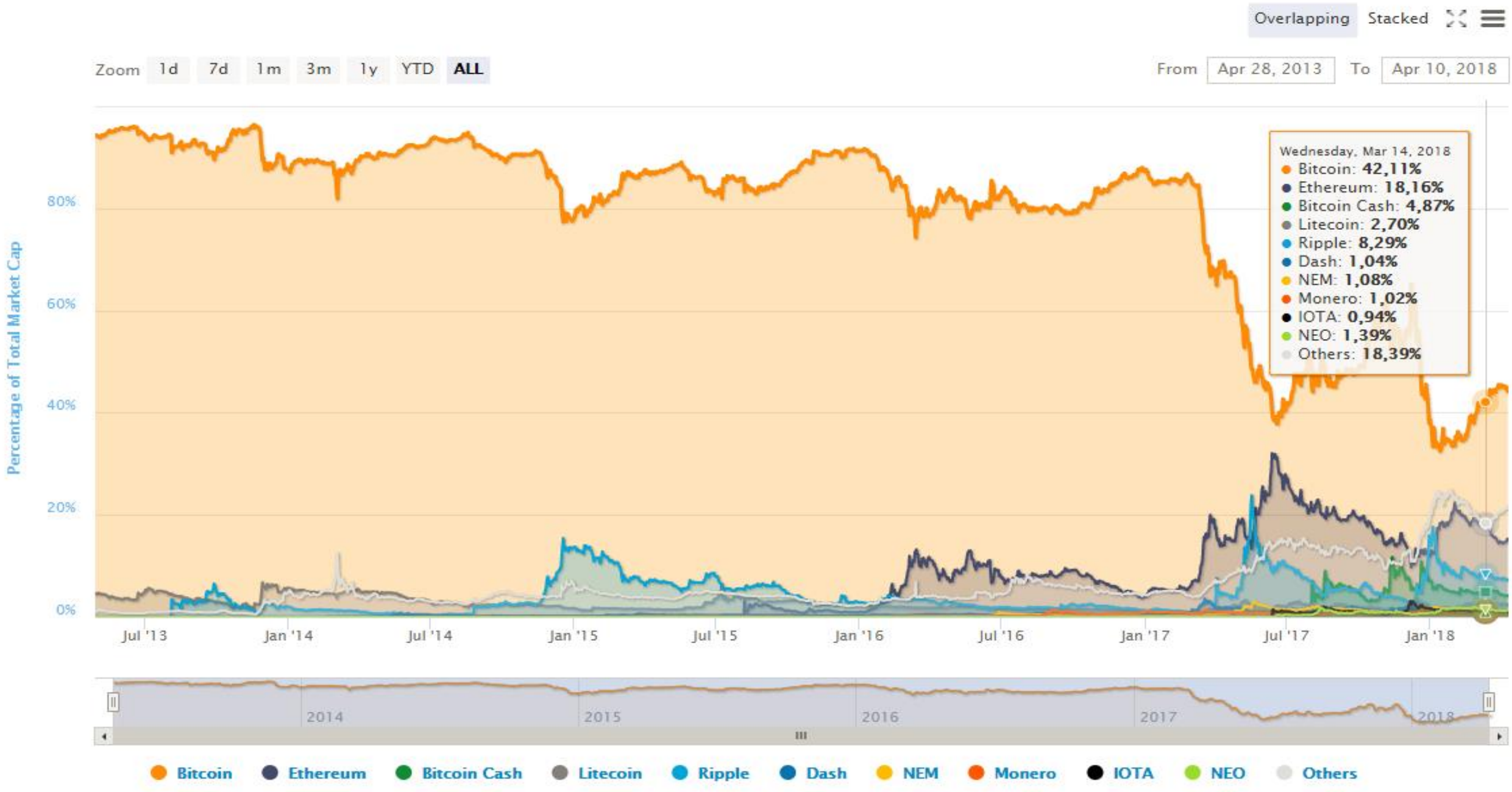

coinmarketcap.com

# Global Charts

## Total Market Capitalization



# Percentage of Total Market Capitalization (Dominance)



# Cryptocurrency Exchanges / Markets List

Indexing **191** cryptocoin exchanges with a total **24h volume of $2.11B** on **6727** trading pairs!

| Rank | Logo | Exchange Name | Markets | 24h Trades | 24h Volume | Marketshare | Last Update | Vote |
|---|---|---|---|---|---|---|---|---|
| 1 | | Bitfinex | 16 | >39,398,948 | $501,989,761 | 24% | 31 sec | |
| 2 | | Kraken | 57 | >37,948,351 | $198,156,433 | 9% | 40 sec | |
| 3 | | Coinbase GDAX | 12 | >27,310,798 | $192,027,688 | 9% | 35 sec | |
| 4 | | Bithumb | 12 | >18,241,901 | $186,279,254 | 9% | 1 min | |
| 5 | | Bitstamp | 11 | >20,840,381 | $142,261,446 | 7% | 1 min | |
| 6 | | coinone | 6 | >84,036,764 | $133,395,558 | 6% | 2 min, 43 sec | |
| 7 | | Bittrex | 254 | >64,911,519 | $125,800,821 | 6% | 3 min, 52 sec | |
| 8 | | HitBTC | 284 | >140,507,340 | $115,367,324 | 5% | 5 min, 49 sec | |
| 9 | | bitFlyer | 3 | >7,757,788 | $81,989,884 | 4% | 1 min, 20 sec | |

QLC Competition Has Now Concluded (04-08) | Binance Has Distributed March GAS (NEO) (04-06) | Binance Delists Centra (CTR) Token (04-05)

# ETH / BTC
Ethereum

| Last Price | 24h Change | 24h High | 24h Low | 24h Volume |
|---|---|---|---|---|
| 0.059540 $407.13 | 0.000740 +1.26% | 0.059517 | 0.058400 | 7,128.77 BTC |

groups 6 decimals

| Price(BTC) | Amount(ETH) | Total(BTC) |
|---|---|---|
| 0.059532 | 0.747 | 0.04447040 |
| 0.059530 | 8.244 | 0.49076532 |
| 0.059529 | 0.222 | 0.01321544 |
| 0.059528 | 6.526 | 0.38847973 |
| 0.059527 | 5.000 | 0.29763500 |
| 0.059526 | 0.076 | 0.00452398 |
| 0.059525 | 0.025 | 0.00148813 |
| 0.059523 | 0.051 | 0.00303567 |
| 0.059519 | 0.035 | 0.00208317 |
| 0.059517 | 1.495 | 0.08897792 |
| 0.059515 | 0.100 | 0.00595150 |
| 0.059513 | 1.156 | 0.06879703 |
| 0.059510 | 1.103 | 0.06563953 |
| 0.059498 | 0.258 | 0.01535048 |
| 0.059494 | 0.140 | 0.00832916 |
| 0.059493 | 14.285 | 0.84985751 |
| **0.059540↑** | | |
| 0.059443 | 6.656 | 0.39565261 |
| 0.059441 | 1.613 | 0.09587833 |
| 0.059440 | 25.632 | 1.52356608 |
| 0.059432 | 0.330 | 0.01961256 |
| 0.059429 | 0.003 | 0.00017829 |
| 0.059424 | 0.636 | 0.03779366 |
| 0.059417 | 0.804 | 0.04777127 |
| 0.059404 | 0.180 | 0.01069272 |
| 0.059403 | 1.230 | 0.07306569 |
| 0.059402 | 4.000 | 0.23760800 |
| 0.059400 | 33.681 | 2.00065140 |
| 0.059390 | 0.033 | 0.00195987 |
| 0.059386 | 0.313 | 0.01858782 |
| 0.059384 | 0.250 | 0.01484600 |
| 0.059381 | 0.310 | 0.01840811 |

Time | Min | Hour | 1D | 1W | Candlesticks | Depth


Limit | Market | Stop-Limit

**Buy ETH** BTC Balance: --

Price: 0.059514 BTC

Amount: ETH

25% 50% 75% 100%

Total: BTC

Login or Register to trade

**Sell ETH** ETH Balance: --

Price: 0.059514 BTC

Amount: ETH

25% 50% 75% 100%

Total: BTC

Login or Register to trade

Favorites | BTC | ETH | BNB | USDT

Change | Volume

| Pair | Price | Change |
|---|---|---|
| ADA/BTC | 0.00002250 | 1.99% |
| ADX/BTC | 0.00008912 | -0.51% |
| AE/BTC | 0.0001988 | 3.43% |
| AION/BTC | 0.0003003 | -1.25% |
| AMB/BTC | 0.00003854 | 0.73% |
| APPC/BTC | 0.00004712 | 4.22% |
| ARK/BTC | 0.0003199 | 5.86% |
| ARN/BTC | 0.00013798 | 1.36% |
| AST/BTC | 0.00003906 | 8.50% |
| BAT/BTC | 0.00002873 | 3.23% |
| BCC/BTC | 0.094584 | 0.19% |
| BCD/BTC | 0.002836 | -0.84% |
| BCPT/BTC | 0.00005430 | 2.80% |
| BLZ/BTC | 0.00004845 | 13.87% |

## Trade History

| | | |
|---|---|---|
| 0.059540 | 0.534 | 17:59:02 |
| 0.059511 | 0.047 | 17:59:02 |
| 0.059540 | 0.165 | 17:59:02 |
| 0.059511 | 1.645 | 17:59:01 |
| 0.059539 | 0.085 | 17:59:00 |
| 0.059511 | 0.973 | 17:59:00 |
| 0.059538 | 3.830 | 17:59:00 |
| 0.059538 | 2.629 | 17:59:00 |
| 0.059524 | 5.977 | 17:59:00 |
| 0.059511 | 0.071 | 17:59:00 |
| 0.059511 | 0.001 | 17:58:59 |
| 0.059511 | 0.026 | 17:58:59 |
| 0.059511 | 0.539 | 17:58:59 |
| 0.059511 | 0.033 | 17:58:59 |
| 0.059539 | 0.019 | 17:58:58 |
| 0.059539 | 0.251 | 17:58:58 |

# ICO-k

- ICO – Initial Coin Offering (hasonló az IPO-hoz, csak itt nem kap részesedést a cégből, aki befektet)
- Óriási innovációs potenciál
- Bárki, bárhol, bármihez gyűjthet alaptőkét
- Új kockázati tőkebefektetési forma
- Az „amerikai álom” a világon mindenütt jelen lehet
- De! - ICO-k 90%-a „bedől” – lásd Vaporware-ek, csalók
- De2! - Óriási hype, mindenki mindenre ad pénzt, „befektet”
- De3! - Túl sok pénz jön be egy-egy ICO-ra, nincsenek ekkora üzleti tervek (lásd Tezos – 20mUSD helyett 230mUSD-t gyűjtött), nem érdeke tényleg megcsinálni az innovációt a kitalálóknak

# Upcoming and Live ICOs

Subscribe to Updates

Submit an ICO

LIVE

**Crowd Machine**

ENDS IN: 407 days

UPCOMING

**Eligma**

STARTS IN: 7 days

LIVE

**SafeCrypt.io**

ENDS IN: 58 days

LIVE

**Quant Network**

ENDS IN: 20 days

UPCOMING

**Plaza Systems**

STARTS IN: 16 days

UPCOMING

**Coupit**

STARTS IN: 47 days

LIVE

**Streamity**

ENDS IN: 19 days

LIVE

**Unibright**

ENDS IN: 30 days

LIVE

**Omnitude**

ENDS IN: 15 days

Live ICOs | Upcoming ICOs | Finished ICOs | Fraud

Category

| NAME | CATEGORY | START DATE | ENDS IN |
|---|---|---|---|
| Quant Network Featured | Infrastructure | Apr 02nd 2018 00:00 UTC | 19 days |
| SafeCrypt.io Featured | Exchange | Mar 25th 2018 00:00 UTC | 57 days |


Ki nevet a végén?
IGN

http://www.kozszov.org.hu/dokumentumok/UMK_2017/4/06_Blockchain_filozofiaja.pdf



SÍK ZOLTÁN NÁNDOR
ALELNÖK
NEMZETI HÍRKÖZLÉSI ÉS INFORMATIKAI TANÁCS

# A blockchain filozófiája, avagy a fennálló társadalmi rendek felülvizsgálatának kényszere

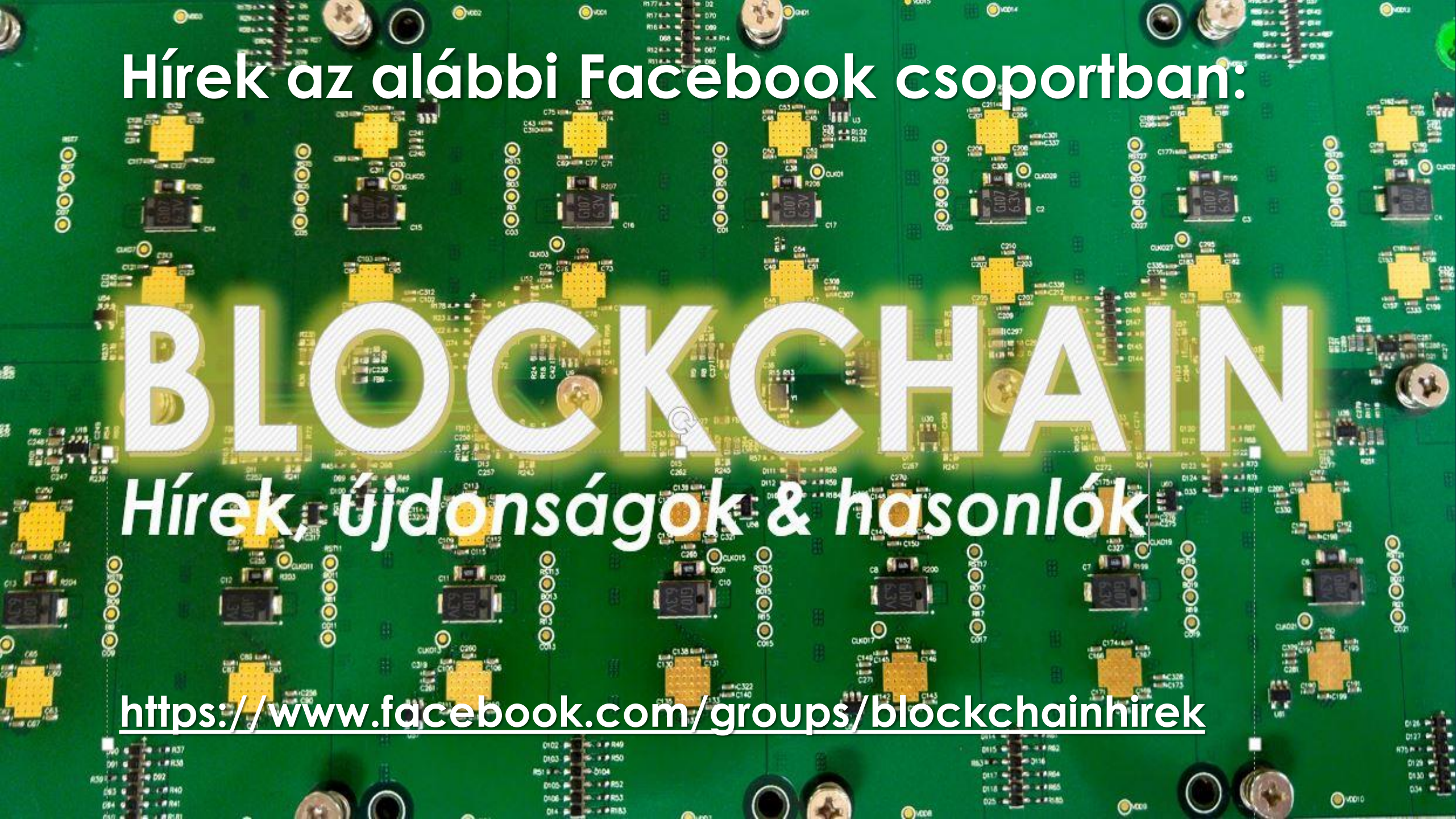
## Csak egy forradalmi innováció a sok közül?

Blockchain – jobb fordítás híján magyarul blokklánc[1]. A blockchain egy olyan információtechnológiai innováció, amely nevének már csak a hallatán is minden vezető állam, államszövetség politikai és gazdasági vezetőinek megremeg a szája széle. A jelen cikk írásának idejére gyakorlatilag a világ minden vezető hatalma tett már valamilyen nyilatkozatot blockchain „ügyben".

Tiltani, tűrni, vagy támogatni. Senki nem tudja, mit

Kim[12] a Világbank vezetője, Mario Draghi[13], az Európai Központi Bank elnöke. Ugyanígy megszólaltak más banki és pénzintézeti vezetők, mint pl. Jamie Dimon[14] a JPMorgan vezetője, vagy a nagy multicégek vezetői, mint pl. Bill Gates[15], és sorolhatnánk. Sőt, a blockchain még a politika középpontjába is került.[16] Naponta születnek nyilatkozatok, vélemények, állásfoglalások, leginkább abban a tekintetben, hogy hogyan lehet a blockchain-t kordában tartani, az erre alapuló megoldásokat szabályozni.

Mindemellett már számos tanulmány is foglalkozik a je-


Hírek az alábbi Facebook csoportban:
BLOCKCHAIN
Hírek, újdonságok & hasonlók
https://www.facebook.com/groups/blockchainhirek

# Figyelmüket köszönve:

Sík Zoltán Nándor

Alelnök

Nemzeti Hírközlési és Informatikai Tanács