

A blockchain a biztonságos adattárolás módja?

On-chain? Off-chain?

Sík Zoltán Nándor

Blockchain Kutatási Egyesület, alelnök

Egy kis „ismétlés”...

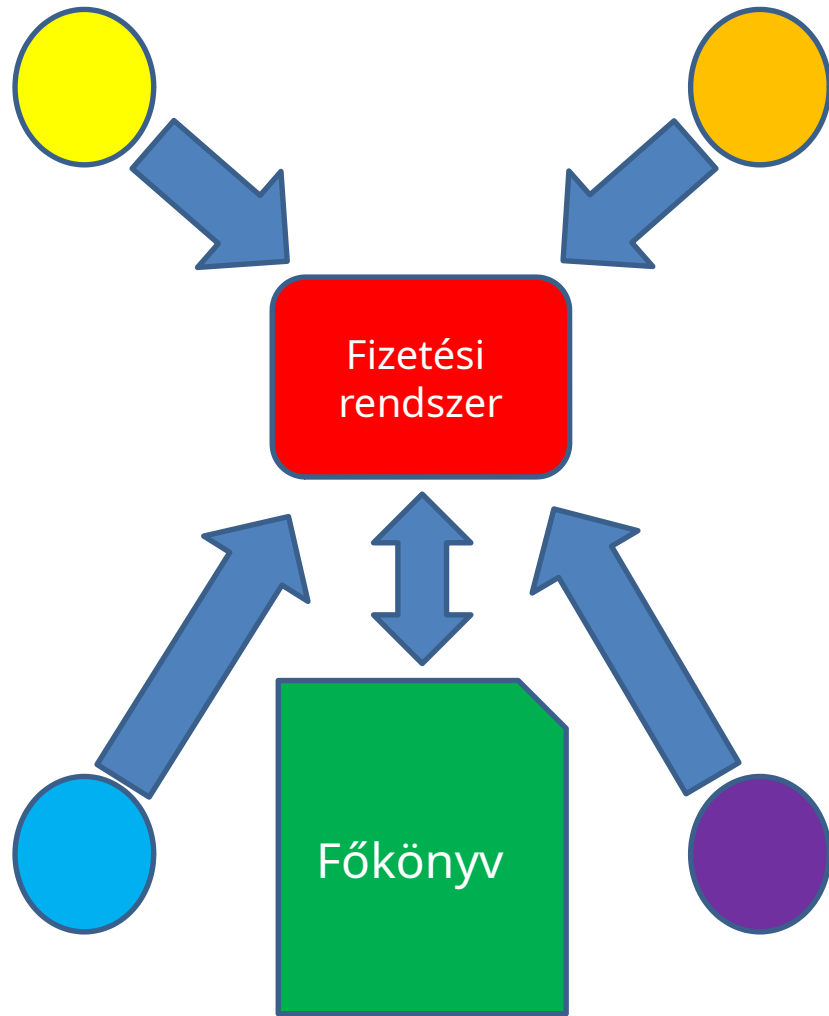
- **DLT** (Distributed Ledger Technology): olyan decentralizált adatbázis, amelyet a különböző résztvevők kezelnek, és nincs olyan központi hatóság, amely bíróként vagy megfigyelőként közreműködne. (...pl. a torrent is ilyen)
- **Blockchain**: olyan infokommunikációs rendszer, amely központ nélküli (decentralizált), adatbázisaként **láncba rendezett** adatblokkokat kezel, működése **egyenrangú** felek **konszenzus kényszerére**, valamint **kriptográfiai algoritmusok** használatára alapul.

Egy kis „ismétlés”...

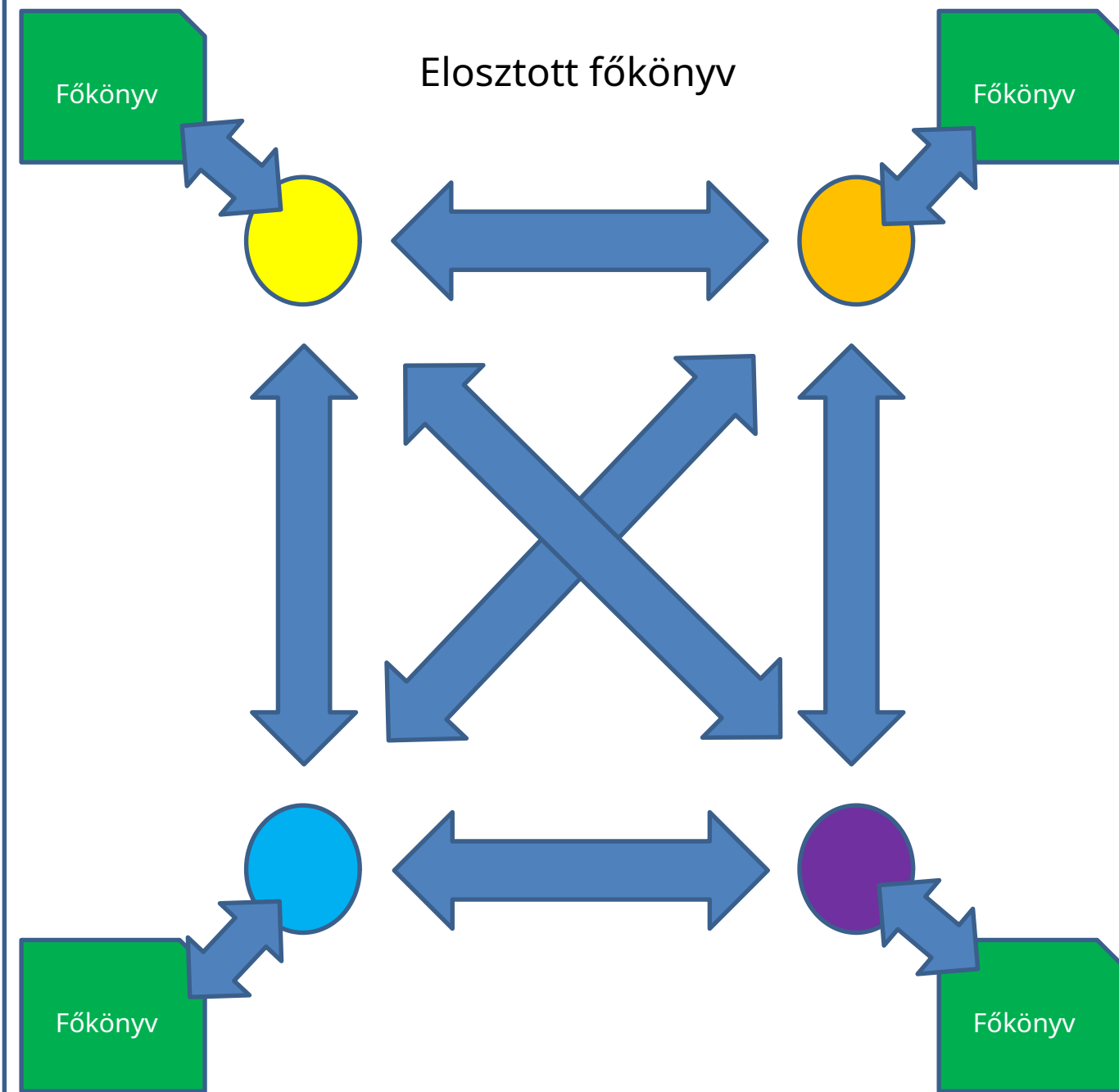
- Tehát a blockchain egy olyan DLT, amely további kritériumokat tartalmaz
- Megjegyzendő, hogy a blockchain nem elosztott, hanem replikált adatbázis (főkönyv)
- „Plusz opció” – **okosszerződések** (smart contracts)
- De van még más is, ami további kritériumokat tartalmazó DLT (nem blockchain!):
 - Tangle (lásd IOTA)
 - Hashgraph
 - Inter Planetary File System (IPFS) – ez most lényeges lesz...

Központi és elosztott főkönyv közötti különbség

Központosított főkönyv



Elosztott főkönyv



Blockchain - az „értékek” internete

Blockchain:

- Mi a megoldandó probléma:
 - Érték közvetítése a digitális világban
 - Azaz a dupla költség elkerülése
- Megoldáshoz – „trustless system”:
 - Maga a blockchain (kvázi visszafejthetetlenség, „alternatív valóság” elkerülése)
 - Kriptográfiai algoritmussal kódolt jelsorozat (az érték)
 - Konszenzus kényszer (blokk lezárók, validátorok)

A „dolgok” közvetítése fizikai, digitális és kriptó világban

A

Fizikai világ
(transfer)



Digitális világ (copy/paste)

```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```

```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```



```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```

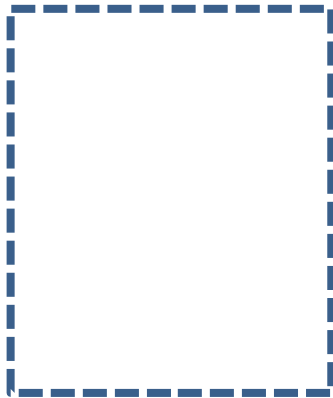
Kriptó világ
(transfer)

```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```

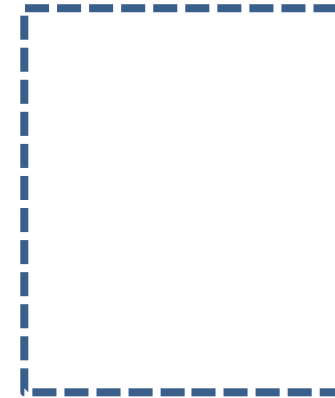


```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```

B



```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```



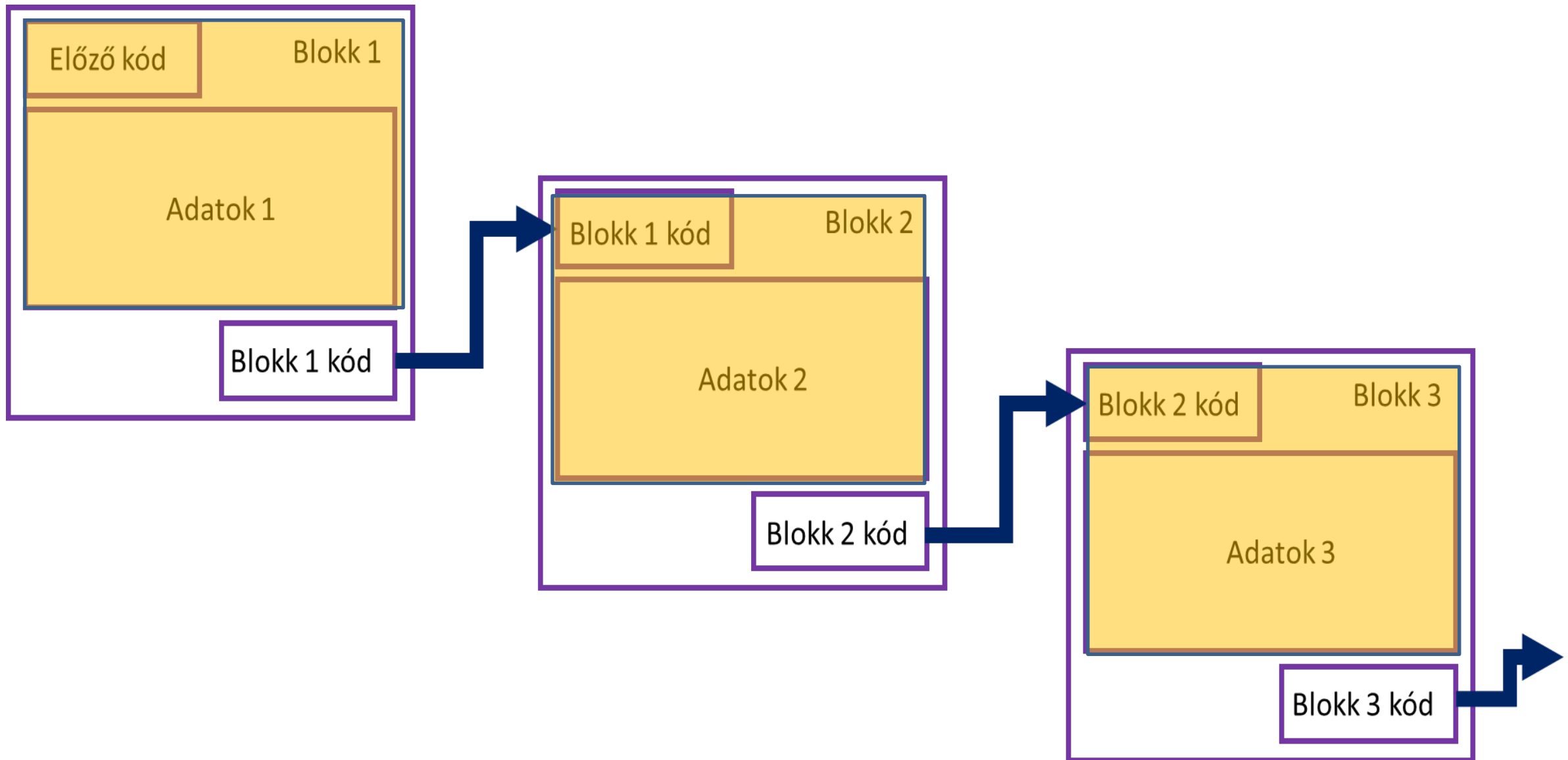
```
101 0111
110 1001
110 1011
110 1001
111 0000
110 0101
110 0100
110 1001
110 0001
```


Konszenzus kényszer megoldások

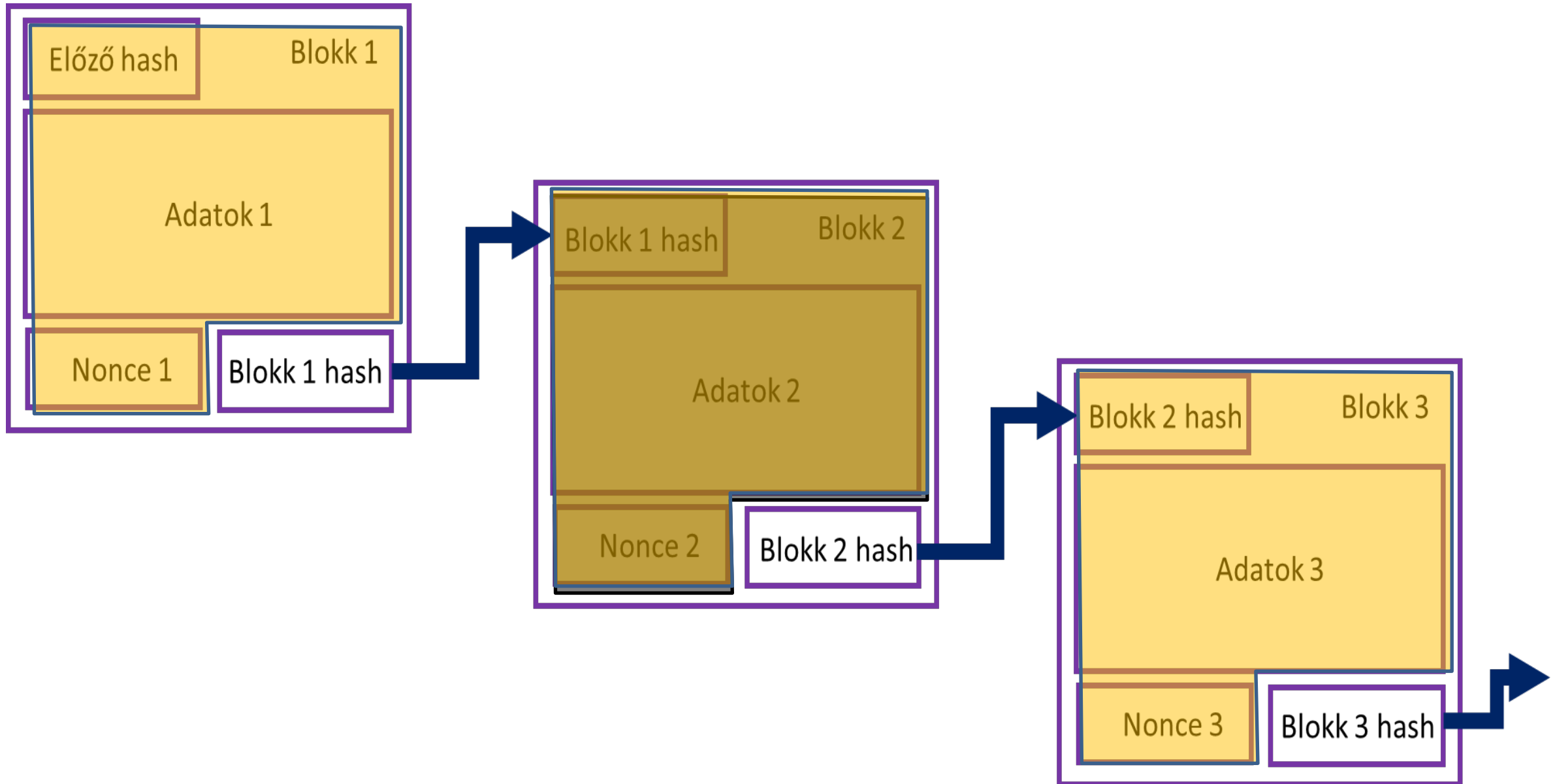
Különböző konszenzus kényszer megoldások léteznek:

- Proof of Work (PoW) – „mining” – Bitcoin és minden „mineable” coin, pl. Ethereum, Dash, Monero, Zcash
- Proof of Stake (PoS) – „minting” – pl. Ethereum fogja használni (Casper kód) – Reddcoin, Navcoin stb.
- Delegated PoS (dPoS) – EOS, Steem, Bitshares
- Proof of Assignment (PoA) – IOTW (IoT kezelés)
- Stellar/Ripple consensus protocol – Stellar, Ripple
- Delegated Byzantine Fault Tolerant (dBFT) – NEO
- Proof of Elapsed Time (PoET)
 - Hyperledger Sawtooth’s Lake project
- Proof of Resource (PoR)
 - „HDD mining” – Sia, Filecoin, Burstcoin, stb. – ez is lényeges lesz...

Általános blockchain



Blokkchain a nonce-szal (PoW)

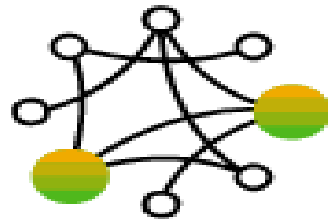


Blockchain típusok

- Publikus – megbízható harmadik fél nélküli
- Privát – megbízható harmadik fél/felek üzemeltetik – más a célja
 - itt nem is kell PoW (azaz bányászat)
 - sőt, „könyvelési díj” sem kell

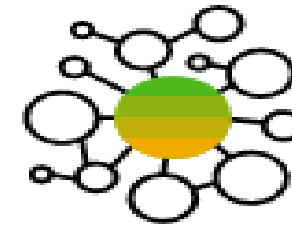
4 types of blockchain networks

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



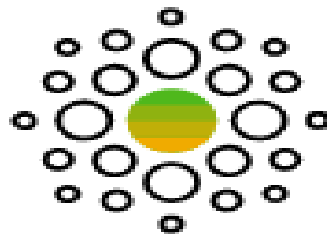
Consortium blockchains

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.



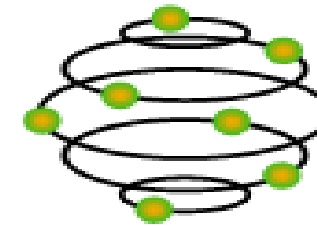
Semi-private blockchains

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.

Kriptoeszköz kategóriák

- **Currency Tokens** - Currency tokens are native blockchain assets intended to be used as money. Networks classified as currencies typically do not have many 'features' beyond those necessary to define and transfer the native blockchain asset.
- **Platform Tokens** - Platform tokens are required to use general purpose decentralized networks that support a wide variety of possible applications. Platform tokens are often used specifically to mediate use of the platform (ie, tokens are used to pay 'gas' in order to access the platform's functionality).
- **Utility Tokens** - Utility tokens are native to decentralized networks that are designed for specific application types. That is, they are open networks but designed with a specific use-case in mind. For example, decentralized storage and decentralized asset exchange are both use-types for which targeted networks (and their corresponding tokens) are being built. The terms 'Utility Tokens' and 'Protocol Tokens' are often used to describe the same type of token.

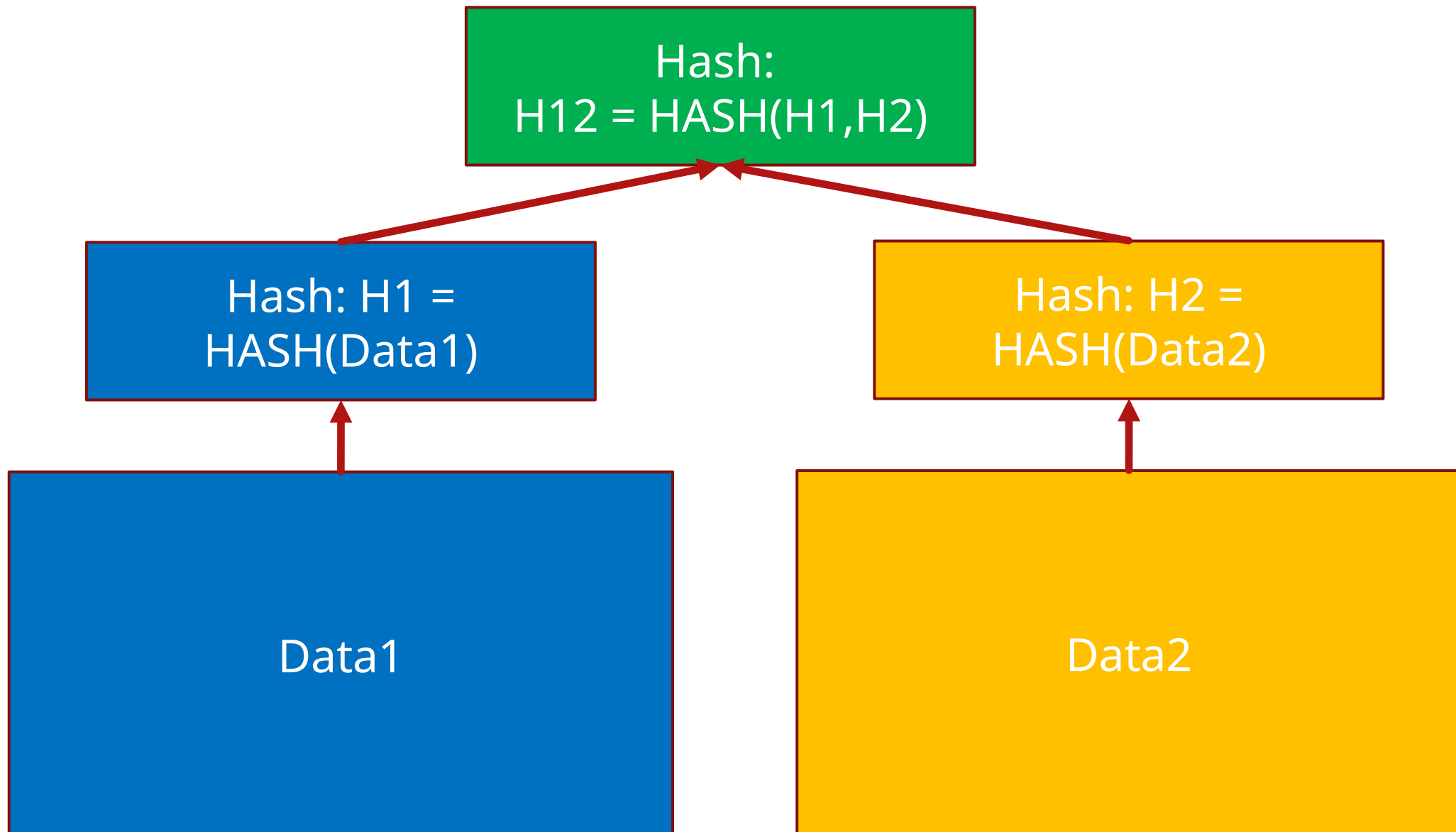
Kriptoeszköz kategóriák

- **Brand Tokens** - Brand tokens exist as tradeable digital assets for use mostly on one company/entity's platform. Some Brand Tokens may evolve into more generalized Utility Tokens over time.
- **Security Tokens** - Security tokens represent a claim on a specific cash-flow, or off-chain asset. Networks which generate fees-for-service that accrue to token holders, explicitly grant voting rights to token holders, or where tokens are said to be "backed" by some other asset, such as gold or company equity, are Security Tokens.

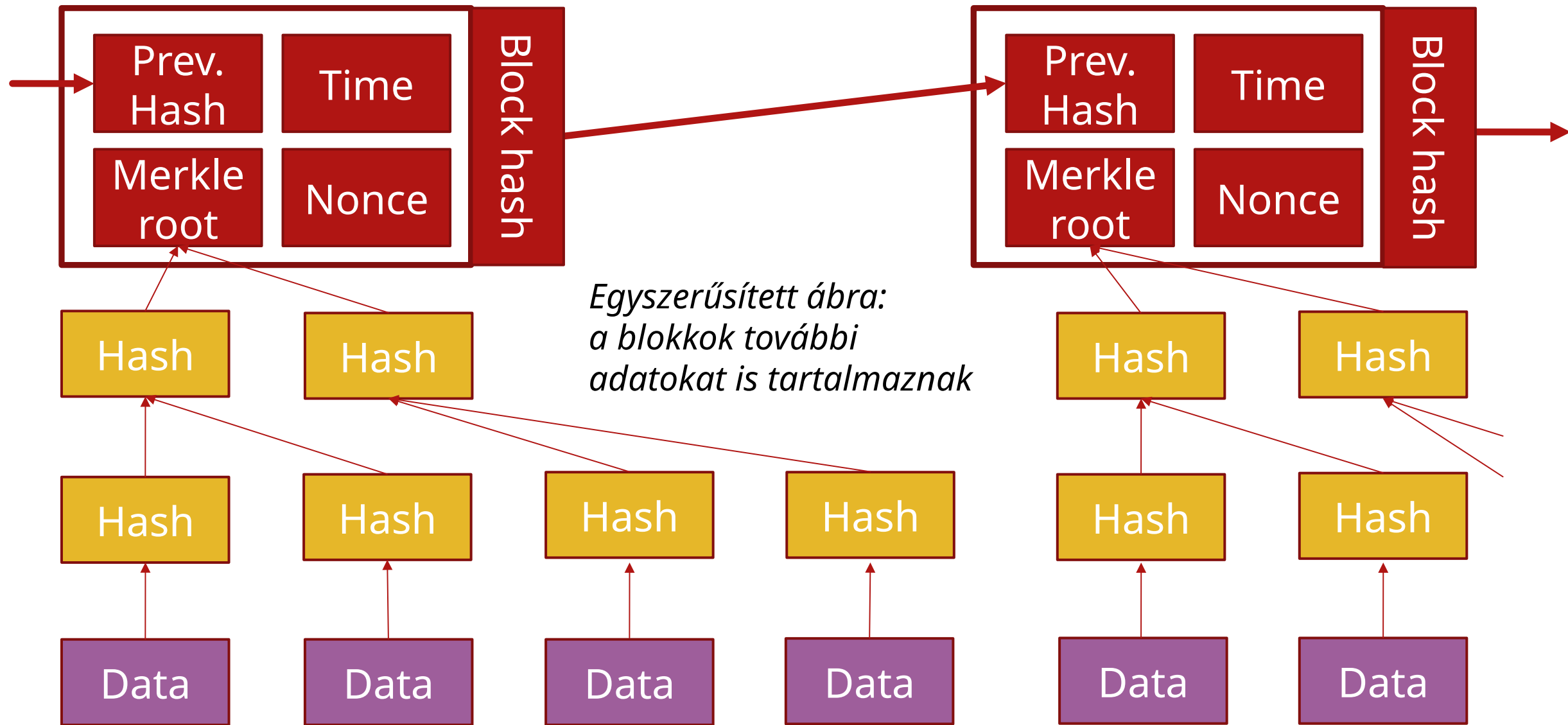
Mi van ténylegesen a blockchain-ben?

- 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 fejrészában 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 fejrészában 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 fejrészában lévő adatokat

Merkle fa képzése (általános „hash” függvényre)



Merkle fa és a Merkle-root a blockchain-ben

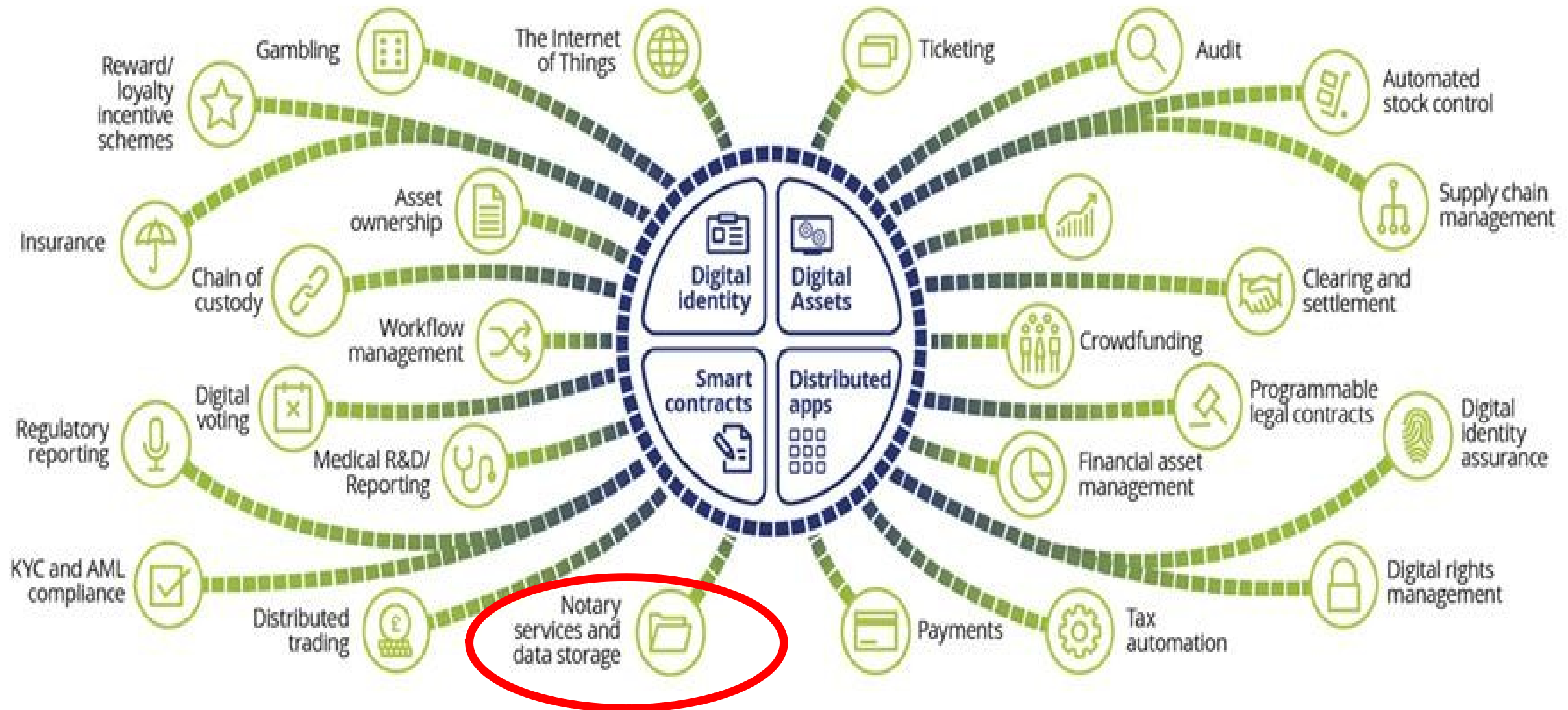


Blockchain adattárolásra?

- A blockchain biztonságosnak tűnik - tekintve az adattárolási lehetőségeket
- De: alapvetően a blockchain nem erre van kitalálva, hanem tranzakciós szemléletű (és lassú...)
- Ezért a hogyanra a válasz: tranzakciót kell a file tároláshoz rendelni
 - tárcák között
 - lehet saját tárcára is utalni

What can you do with a blockchain?

KYC – Know Your Customer
AML – Anti-Money Laundering





GDPR?

A GDPR megfelelelés a blockhainben nehezen megoldható

- Hagyományos adatbázisoknál (cloud-nál is) :CRUD – Create, Read, Update, Delete
- Blockchain-en CRAB – Create, Read, Append, Burn
 - Append – nincs Update
 - Burn – nincs Delete – helyette Burn – tranzakció egy olyan tárcába, aminek a privát kulcsát eldobtuk (fekete lyuk)

CIA alapelv

- Confidentiality – pro és kontra:
 - hacsak hash, akkor az nem utal a file-ra,
 - az adatokat mindenki látja, de lehet titkosítani
- Integrity – pro:
 - replikált (de legalább elosztott) adatbázis, hiba esetén helyreállítható az eredeti adat
- Availability – pro és kontra:
 - replikált adatok (minden/adott „node”-okon)
 - nem egyszerű és lassú a lekérdezés

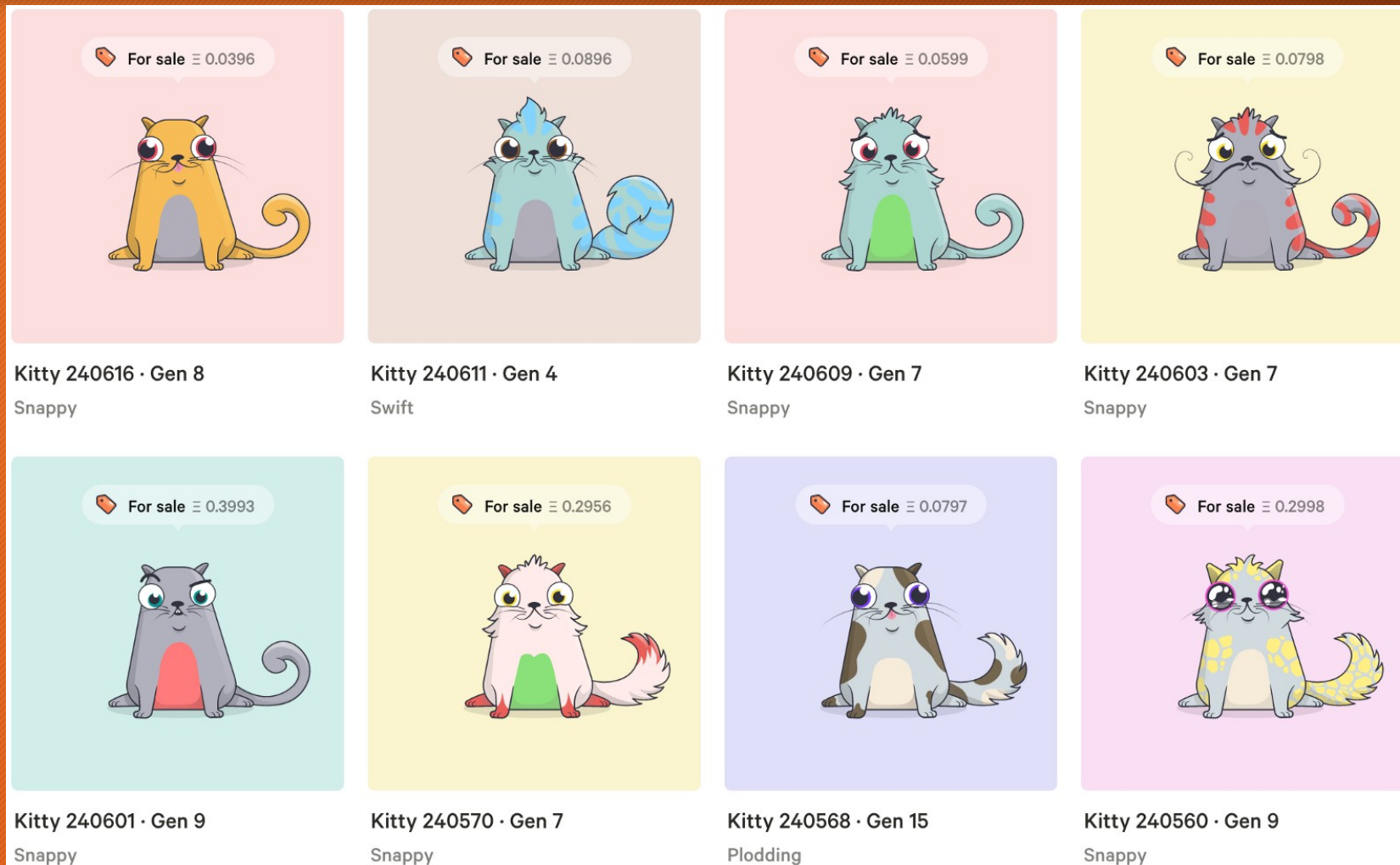
Megoldás típusok: on-chain

- a teljes adatot a blockchainben tároljuk
- Nagy mennyiségű adat tárolását a blokkméret határozza meg - vagy csak kevés adat fér bele, vagy szeletekben
- Alapértelmezésben mindenki látja az adatot
 - de lehet titkosítani (ez esetben a kulcsokat vhol másutt kell tárolni)
- Mindamellett hihetetlenül drága a tárolás
 - az ár az adatmennyiségtől függ
 - okos szerződésnél még annak végrehajtásáért is fizetni kell

Megoldás típusok: on-chain

- előnye:
- I – integráns, a replikáció miatt nem sok hibalahetőség lehet a tárolásban
- A - replikálva van az adat, mindenütt rendelkezésre áll
- hátránya:
- C – nyílt az adat, mindenki látja (hacsak nincs titkosítva, kulcs másutt tárolva – de mi van, ha elvész a kulcs?)
- A - nagyon nehéz a visszanyerése (lassú)
- Plusz: drága

Cryptokitties: non-fungible crypto assets



Megoldás típusok: off-chain

- Csak a hash kódot tároljuk a blockchainben, a tényleges adat másutt van
- előnye:
- C – az adat nem a chainben van, nem látja mindenki
- pluszban:
 - proof, hogy az adat az bitre megegyezik (hash biztosítja)
 - proof, hogy ki tette fel
 - proof, hogy mikor

Megoldás típusok: off-chain

- I – az az adatbázistól függ, nem a blockchaintől (elosztott adatbázisnál nagyobb az esély, hogy integráns marad)
- plusz: ellenőrizhető, hogy tényleg nem sérült-e meg az adat
- A – szintén az adatbázistól függ: az adatbázisban van tárolva, gyors a hozzáférés/lekérdezés
- plusz: csak a hash-t kell tárolni, nem drága (de azért „pénzbe” (crypto-ba) kerül)
- hátránya:
- a proof-on kívül semmi pluszt nem nyújt a blockchain

Adattároló blockchain megoldások

- Rengeteg kezdeményezés/megoldás - platform token, utility token
- Legismertebbek:
 - Maidsafe Safecoin (bevezetés: 2014.04.22)
 - Burstcoin (bevezetés: 2014.08.10)
 - Siacoin (bevezetés: 2015.06.07)
 - Storj (régebben Storj Coin X) (bevezetés: 2014.07.18)
 - IPFS – Inter Planetary File System) (bevezetés: 2017.08.11) (+Filecoin)

Safecoin

Safecoin is a digital token. It can be thought of as the oil in the engine of the SAFE Network, a built in way of ensuring that all users of the network are compensated for the value they provide. Let's find out how it works...

Global distribution without human intervention.

Safecoins are distributed entirely by the algorithms within the SAFE Network. Human beings are not involved in the process. Only 4.3 billion coins will ever be in circulation at one time and each will have its own unique identity. Safecoins will be recycled when users exchange them for network services, ensuring there is always a supply for users to earn.



Farming: an incentive for a crowd sourced Internet.

Safecoins are given as an incentive to users for providing their resource to the network. This resource is their: storage space, CPU, bandwidth and online time that enable the encrypted chunks of



Proof of Capacity

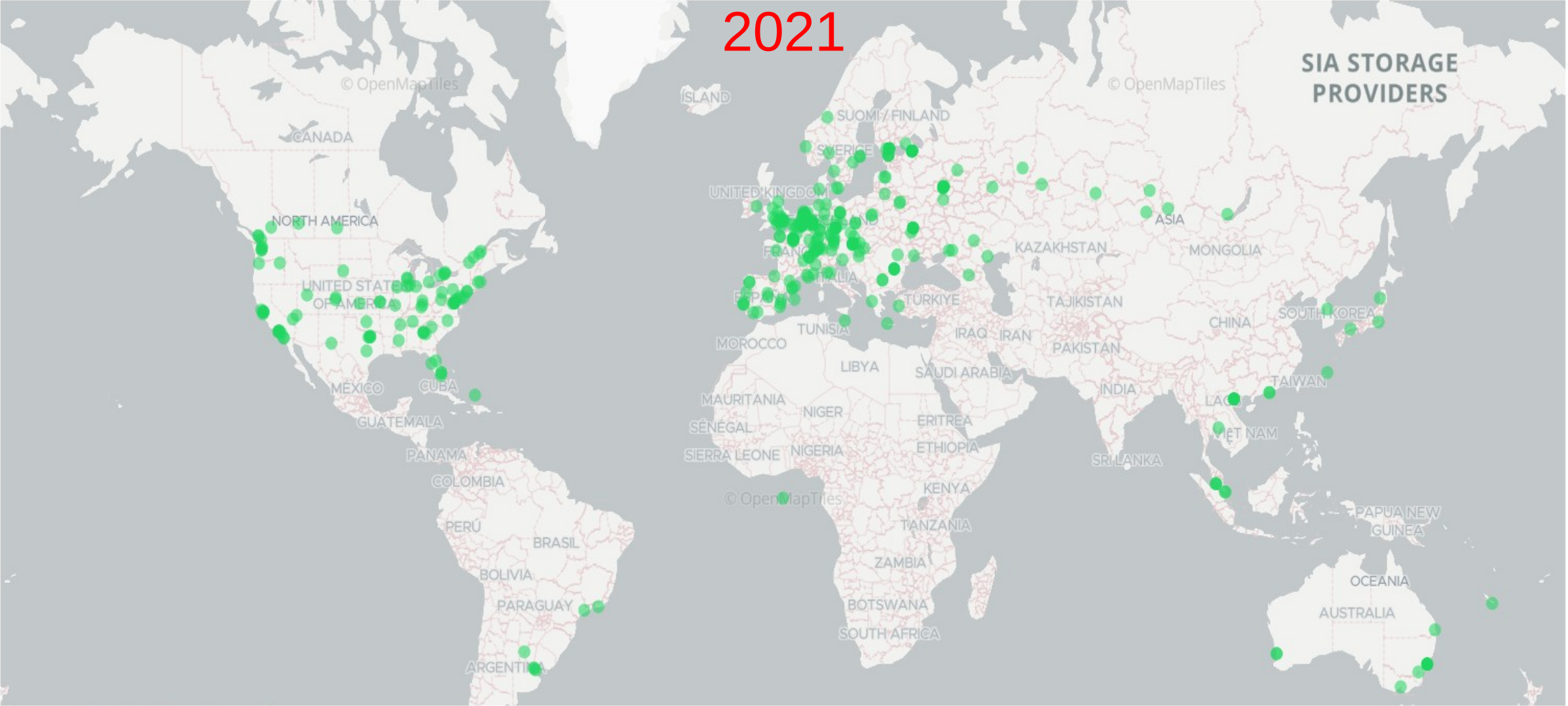
Proof of Capacity

[Home](#) / [Proof of Capacity](#)

Mining for everyone

The Burst mining system is unlike any other coin in existence: it uses your existing free space on your hard drive to mine coins. Because of this, it is naturally more decentralized, and very low on power usage. The difference between mining and simply running your computer not mining is so negligible you will not notice a difference on your power bill. Due to the nature of the mining process, and the fact that it is mineable most efficiently and cost effectively mined on consumer grade storage hardware, the coin lends itself to being much more decentralized by design. Everyone has free hard drive space, and purchase of another drive specific for Burst mining represents a small cost. Since the mining process itself doesn't take much power (as hard disks only average <5W power, just like charging a mobile phone) it makes sense to mine just because you can.

This opens the door to the general public in a way that had never been possible before with other more 'traditional' style mined crypto-currencies. The mining process is very easy on hardware, and to date not a single piece of hardware has been reported to have issues due to the BURST mining process running on it.



2.4PB

Storage Capacity

370

Storage Providers

591TB

Used Storage

1.2M

Downloads



STORJ

[Developers](#)

[Community](#)

[Help](#)

[Pricing](#)

[News](#) ▾

[Login](#)

[RENT YOUR DRIVE](#)

The Future of Cloud Storage

End-to-end encrypted, distributed object storage, where only you have access to your data. Powered by blockchain payments.



End-to-End Encryption

Distributed infrastructure



Blazing Fast

Peer-to-peer technology



Higher Availability

99.99999%



VS



PROS

- Sia cheaper than Storj
- Storage marketplace
- Fully decentralized

CONS

- Requires collateral for hosting
- Accepts only SIA coin as payment
- Requires entire blockchain download
- Currently can't stream videos

PROS

- Accepts various payment methods
- Fixed prices
- Allows to stream videos

CONS

- Storage cost 7x more than Sia
- No storage marketplace
- Has centralized bridge

SUBSCRIBE

HDD mining (PoR alapú bányászat)

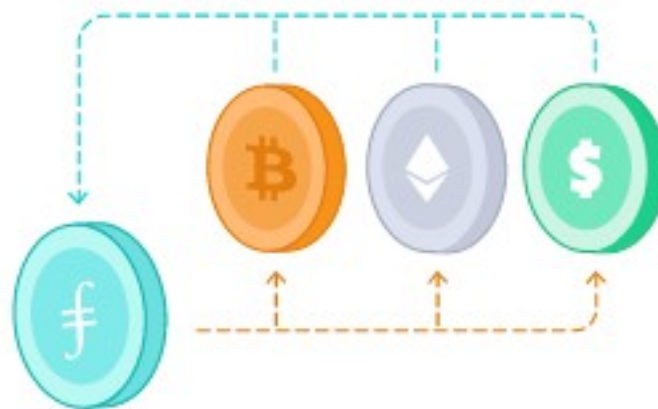
- A klasszikus PoW bányászat mellett létezik...
- Proof of Resource/Proof of Capacity típusú
- Csak Storage típusú coin-okra
- Tárhely kapacitás rendelkezésre bocsátása
- Sokkal kevesebb áram, mint a PoW
- (De: sokkal kevesebbet is fizet...)

A MASSIVE AMOUNT OF STORAGE SITS UNUSED IN DATA CENTERS AND HARD DRIVES AROUND THE WORLD.



EARN FILECOIN FOR HOSTING FILES

Put your unused storage to work by becoming a Filecoin miner. Use the Filecoin mining software to get paid for fulfilling storage requests on the Filecoin market.



EXCHANGE FILECOIN FOR USD, BTC, ETH AND MORE

The Filecoin currency will be traded on a number of exchanges and supported by multiple cryptocurrency wallets, allowing you to easily exchange Filecoin for other currencies like US Dollars, Bitcoin, and Ether.



RELIABLY STORE FILES AT HYPERCOMPETITIVE PRICES

Clients can tune their storage strategy to suit their needs, creating a custom balance between redundancy, speed of retrieval, and cost. The worldwide Filecoin storage and retrieval markets make vendors compete to give you flexible options at the best prices.

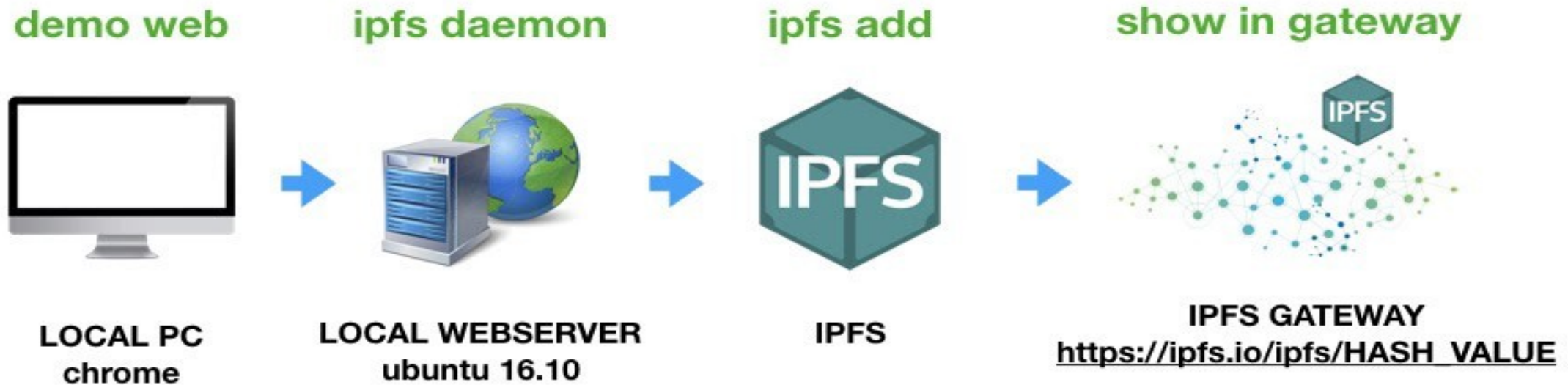
IPFS – a legismertebb „közbülső”...

- IPFS – Inter Planetary File System
- hasonló a torrent-hez
- az adatok nem a chain-ben vannak
- külön IPFS node-ok-ok vannak (kulcsokkal – hash a publikus kulcsa)
- DHT – distributed hash table

IPFS

- Magában a rendszerben csak az van, hogy hol az adat – hash alapján – content addressing
- Egy helyen nincs meg az összes adat, hanem csak az, amiben a node „érdekelt”
- De van pl. verziókövetés és duplikáció szűrés – hash, ill. hash változás alapján
- Viszont nincs keresési lehetőség, ismerni kell a hash kódot, hogy hozzá lehessen férni – le kell kérdezni az IPFS node-októl
- Megoldás az IPNS-t – human readable names

ADD FILE TO IPFS DEMO



Share files using IPFS

Share directly from your device — no cloud needed.

Add your files

1

Add files to share them directly from your device over the IPFS network. Anyone with the unique code in your share link can download your files, so don't add sensitive or copyrighted material. [Learn more.](#)

Keep this page open!

2

Because you're sharing directly from your device, it's important to keep this page open until the recipient downloads the files. If you're sharing with a group, others in the group can help you co-host the files by also keeping the share page open in their browsers.

Share the link

3

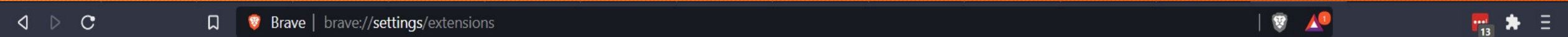
Every share link contains a unique fingerprint called a CID that enables the recipient's device to find that content on the IPFS network. [Learn more.](#)



Add files

Or add a folder

IPFS támogatás a Brave böngészőben



Beállítások

Brave jutalmak

Előzmények

Könyvjelzők

Letöltések

Kriptopénztárak



Beállítások



Kezdő lépések



Megjelenés



Új lap



Szinkronizálás



Pajzsok



Közösségi média
blokkolása



Keresőmotor



Kiterjesztések



Biztonsági ellenőrzés

További beállítások



A Brave névjegye
v 1.21.74

Crypto Wallets betöltése indításkor



Google bejelentkezés engedélyezése a bővítmények számára

[További információ](#)



Hangouts

Hangouts komponenseket használ, hogy lehetővé tegye a képernyőmegosztást és más funkciókat a böngészőben.



Módszer az IPFS források kezelésére

Kérés



IPFS nyilvános átjáró címe

<https://dweb.link>

Módosítás

Visszaállítás IPFS nyilvános átjáróra

Automatikus visszaállítás nyilvános IPFS átjáróra, ha a helyi csomópont nem érhető el.



IPFS források átirányítása a beállított IPFS átjáróra

Automatikusan a beállított átjárót használja IPFS megoldásokhoz, amikor egy IPFS-átjáró forrással találkozik.



IPFS Companion

IPFS Companion kiterjesztést használ a bővített IPFS támogatáshoz Brave-ben, beleértve a közönséges IPFS feladatokhoz a böngészőből.



Media Router

Média-útválasztó komponens használatával engedélyezi a Chromecastot a böngészőben.



Privát ablak Torral

Ezzel elrejtheti a felkeresett oldalak elől az IP címét.



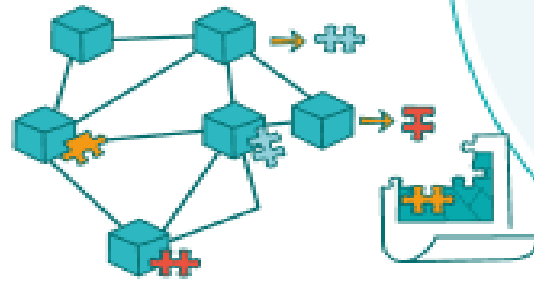
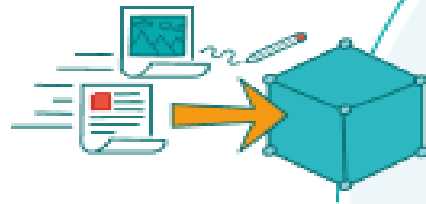
IPFS

- Skálázható, de lassú a visszanyerés egy hagyományos/cloud adatbázishoz képest
- Pénzbe (crypto) kerül – Ethereum rendszeren alapul – smart contract – „gas”-t fizetni kell
- IPFS node-oknak is fizetni kell a tárolásért
- De pl. jó DNS szolgáltatásra is, akár más domain tartomány feloldás, lásd pl. még Namecoin, vagy akár a Tor (bár annak nincs köze a blockchainhez)

IPFS 0.5.0 (2020.04.28)

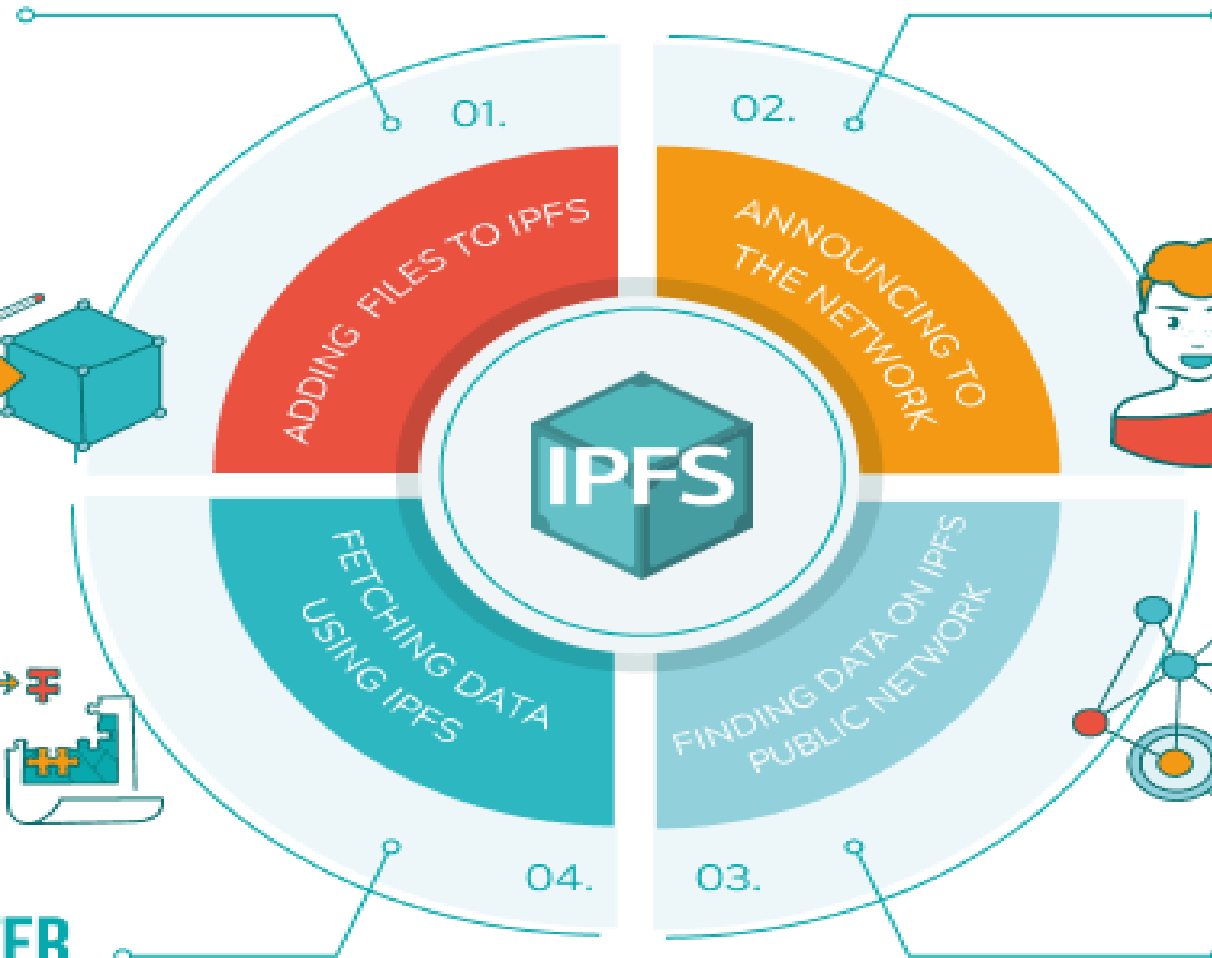
2X FASTER ADDING

Adding data using the Badger datastore is now 25x faster than flatfs.



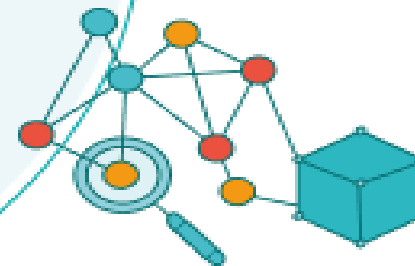
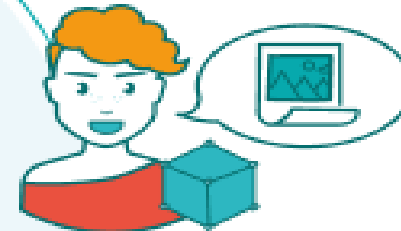
2-5X FASTER FETCHING

Fetching content once you're connected to multiple peers is over twice as fast!



2.5X FASTER PROVIDING

As nodes upgrade, providing will get faster. A fully upgraded 1K node test network shows a 25x speed-up!



2-6X FASTER FINDING

Finding the content you want in the network is now faster and more reliable.

Forrás: <https://blog.ipfs.io/2020-04-28-go-ipfs-0-5-0/>



Köszönöm a figyelmet!