NEMZETI HÍRKÖZLÉSI ÉS INFORMATIKAI TANÁCS

BLOCKCHAIN

…és a blockchain specifikus biztonsági kérdései…

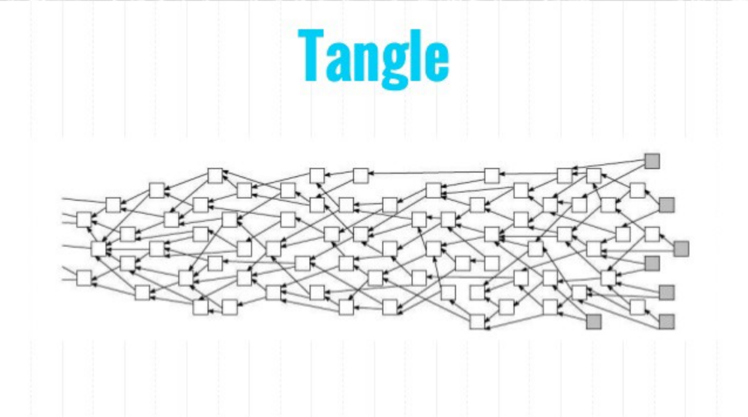
Sík Zoltán Nándor
Alelnök, NHIT

Blockchain vs. DLT 1

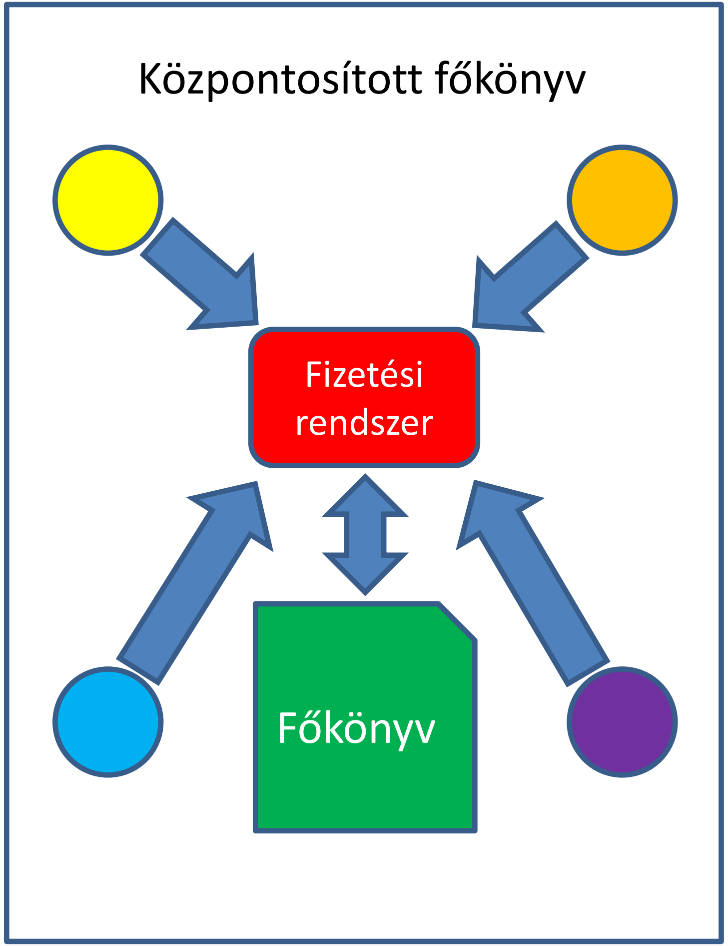
Mielőtt a blockchain-re rátérnénk…

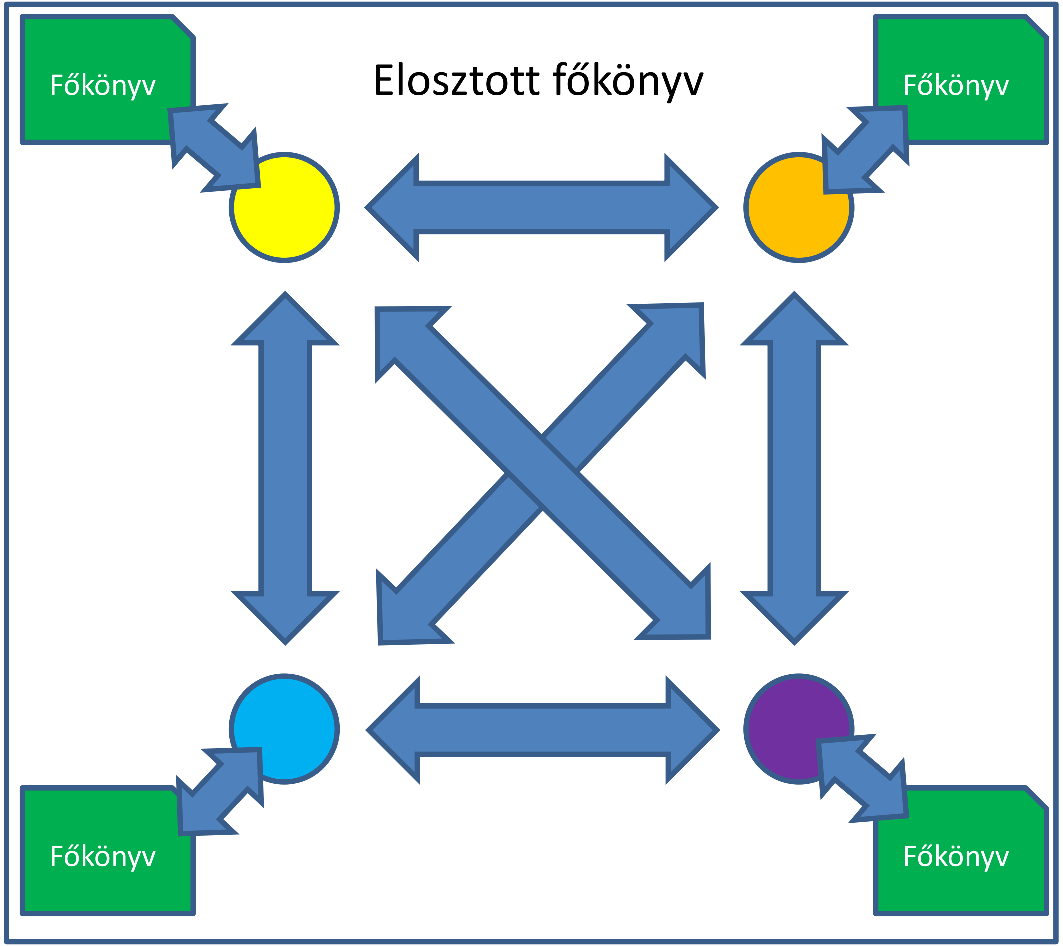
- **DLT** (Distributed Ledger Technology): olyan decentralizált adatbázis, amelyet a különböző résztvevők kezelnek, és nincs olyan központi hatóság, amely bíróként vagy megfigyelőként közreműködne. (…pl. a torrent is ilyen)
- **Blockchain**: olyan infokommunikációs rendszer, amely központ nélküli (decentralizált),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

- Tehát a blockchain egy olyan DLT, amely további kritériumokat tartalmaz
- „Plusz opció” – **okosszerződések** (smart contracts) – Nick Szabó (pont ma tart előadást egy budapesti blockchain konferencián)
- De van még más is, ami további kritériumokat tartalmazó DLT:
  - Tangle (lásd IOTA)
  - Inter Planetary File System (IPFS)
  - Hashgraph
  - …és még mit hoz a jövő



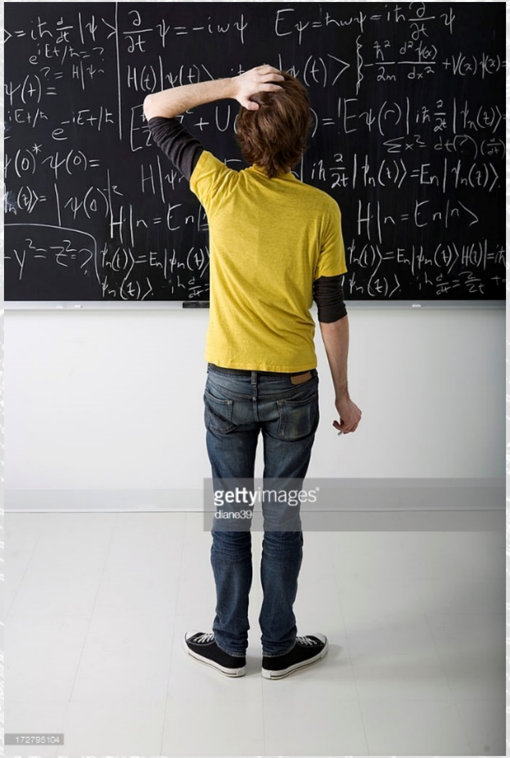
Központi és elosztott főkönyv közötti különbség



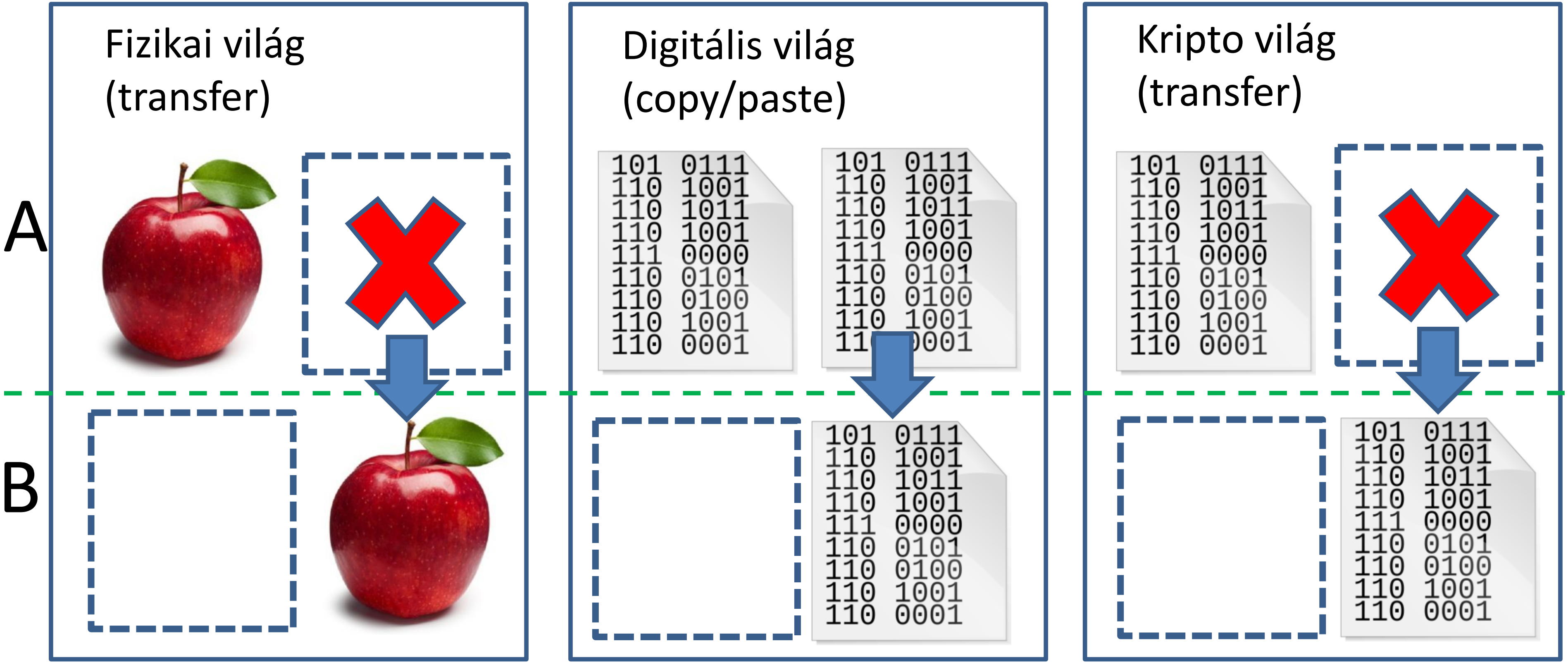


Blockchain:

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



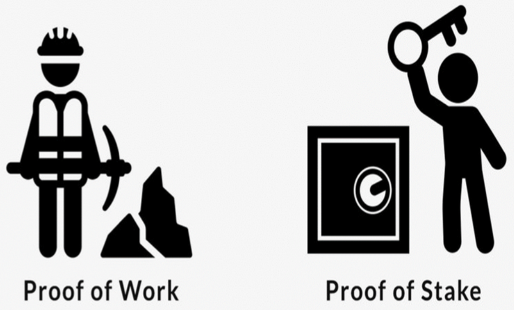
A „dolgok” közvetítése fizikai, digitális és kripto világban



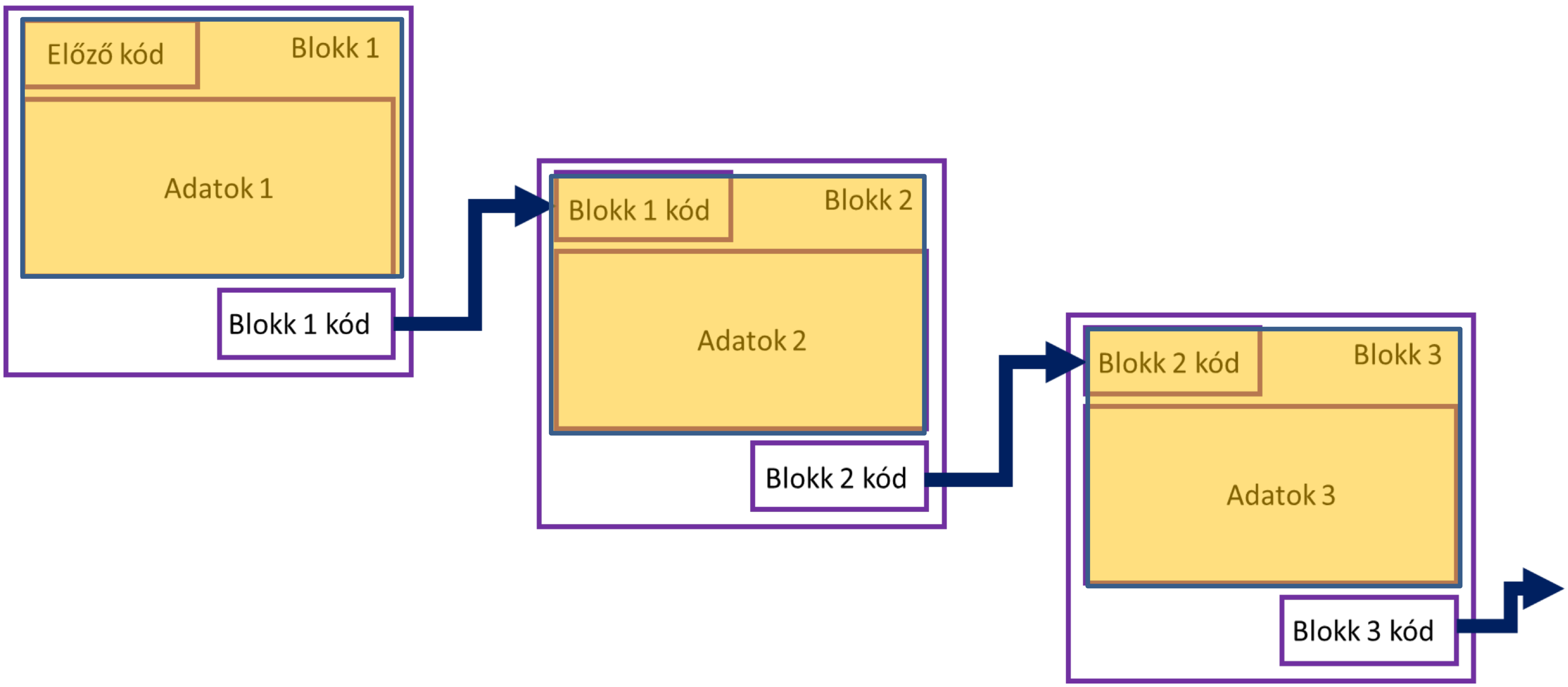
Konszenzus kényszer megoldások

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.



Általános blockchain



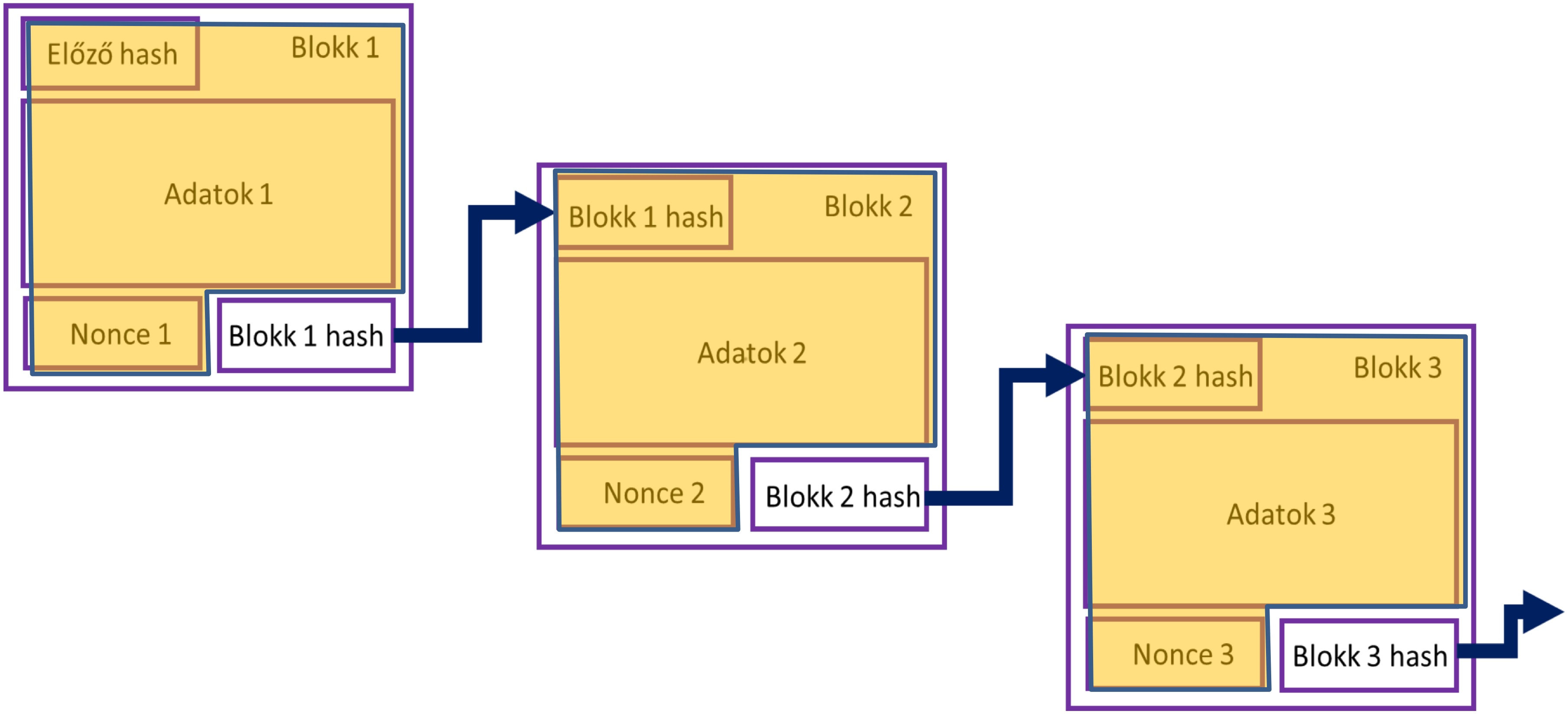
NEMZETI HÍRKÖZLÉSI ÉS INFORMATIKAI TANÁCS

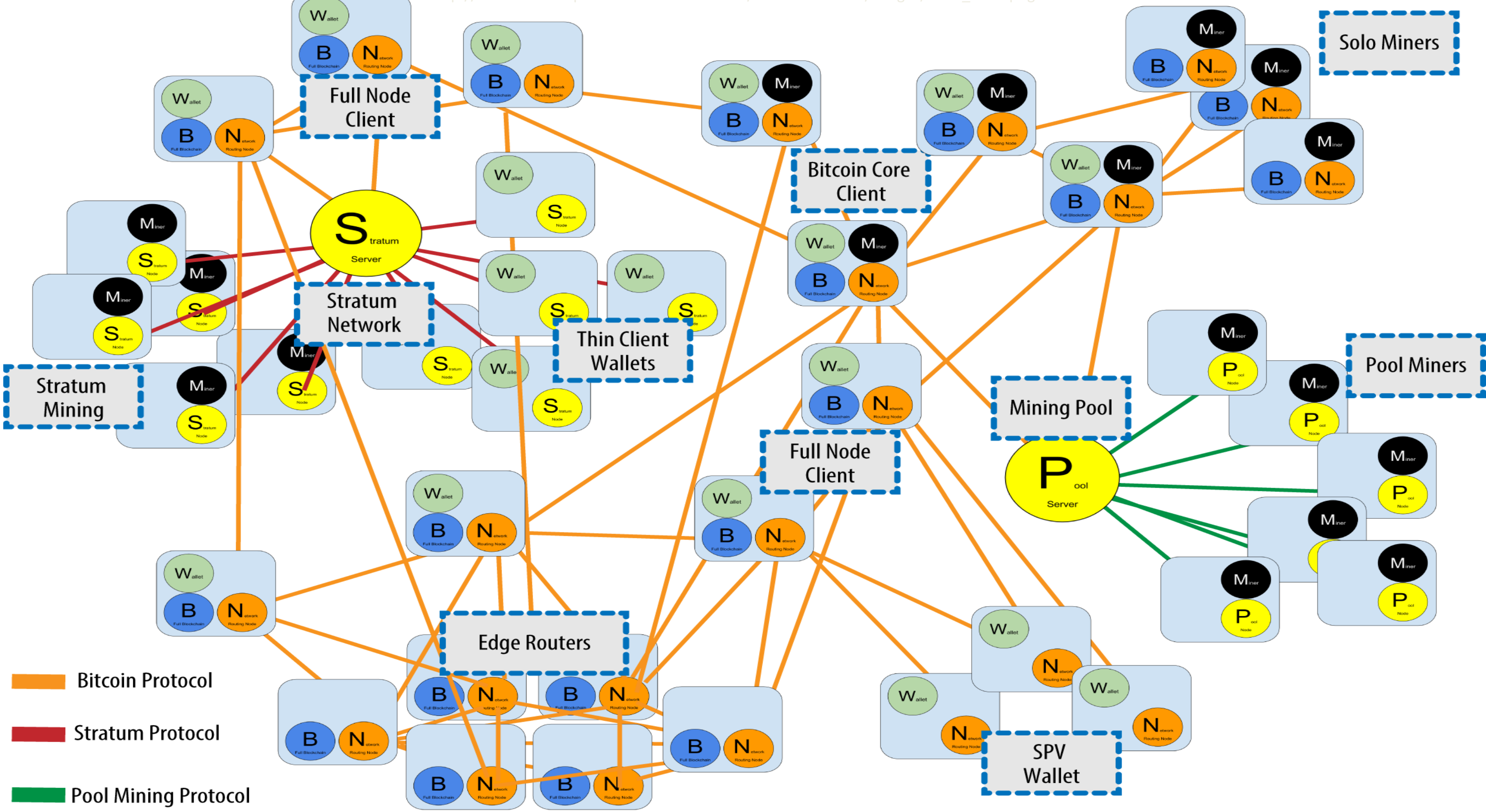
A Bitcoin rendszer – Proof of Work típus

– Október 31-én volt 10 éves a Bitcoin –

Satoshi Nakamoto White Paper-ét ekkor tette közzé

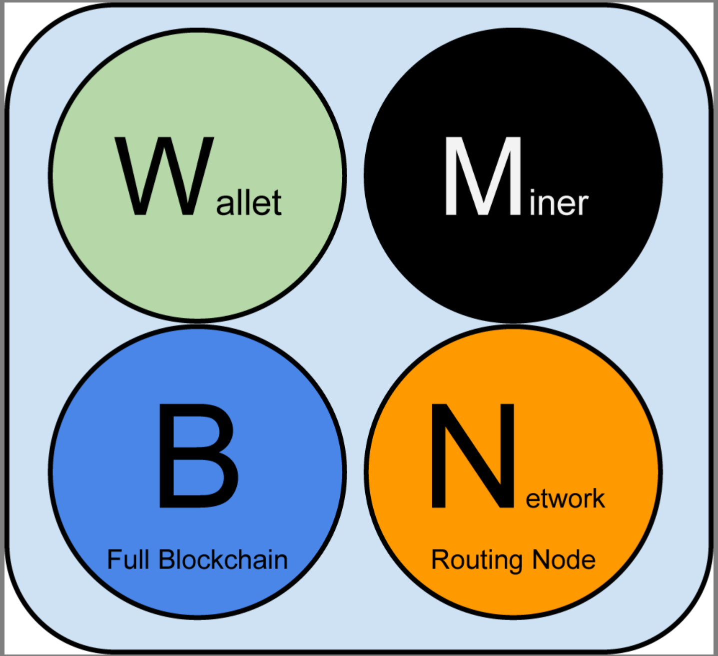
Blokkchain a nonce-szal (PoW)




Full Node Client
Solo Miners
Bitcoin Core Client
Stratum Server
Stratum Network
Stratum Mining
Thin Client Wallets
Mining Pool
Pool Miners
Pool Server
Full Node Client
Edge Routers
SPV Wallet
Bitcoin Protocol
Stratum Protocol
Pool Mining Protocol

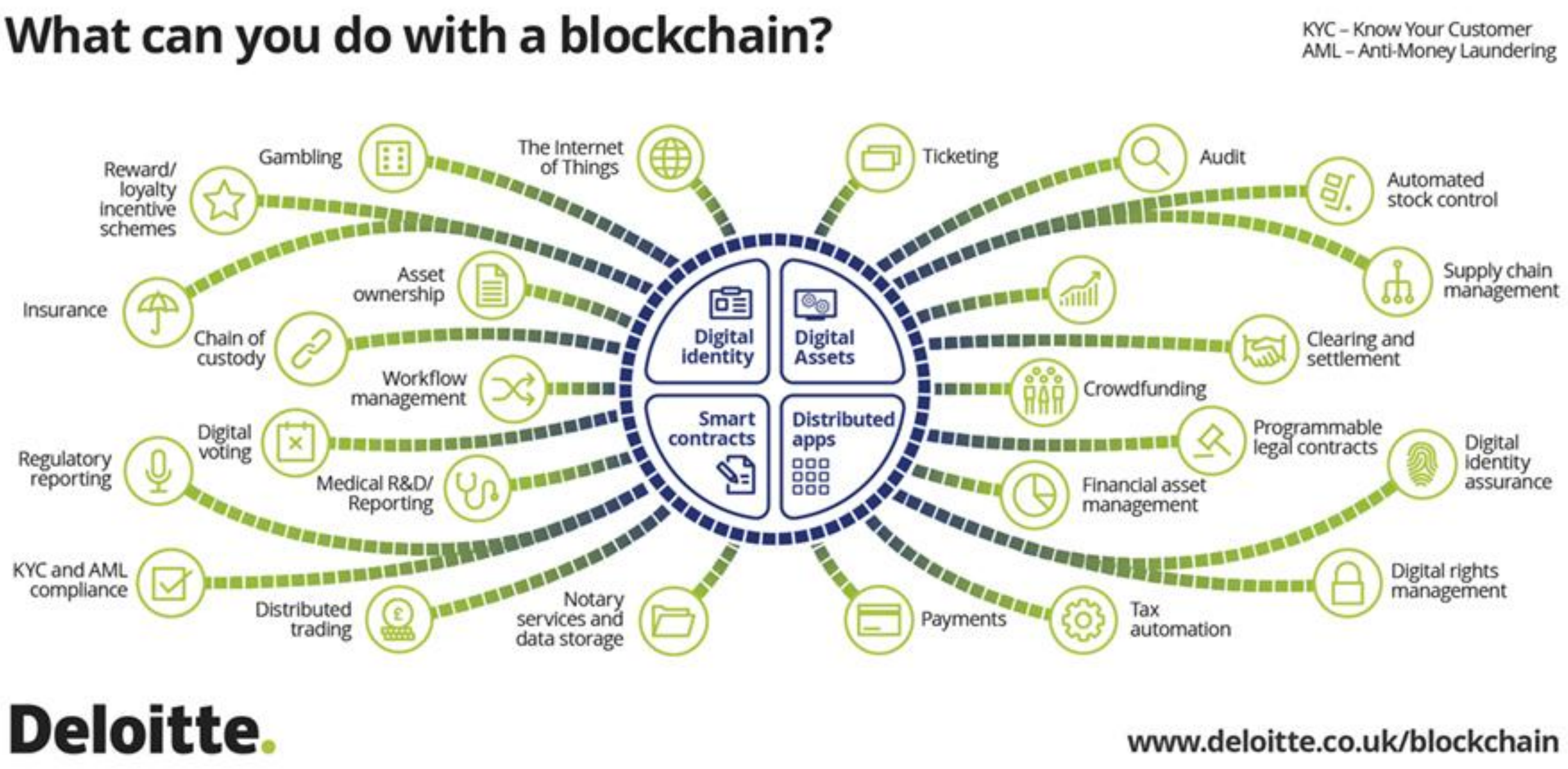
Funkciók (PoW blockchain-ek):

- W – Wallet
- B – Full blockchain
- N – Network routing node
- M – Miner
- P – Pool node/server vagy…
- S – Stratum node/server



Miért az „értékek” internete? – A kriptoeszközök piaci kapitalizációja

Blockchain felhasználási területek



Rank	Name	Sym.	Description	Rank	Name	Sym.	Description	Rank	Name	Sym.	Description
1	Bitcoin	BTC	Digital gold	34	TenX	PAY	Cryptocurrency credit card	67	Iconomi	ICN	Digital asset investment funds
2	Ethereum	ETH	Programmable contracts and money	35	MaidSafeCoin	MAID	Rent disk space	68	Aeternity	AE	Decentralized apps (prototype)
3	Bitcoin Cash	BCH	Bitcoin clone	36	BitcoinDark	BTCD	Zcoin close	69	DigiByte	DGB	Faster Bitcoin
4	Ripple	XRP	Enterprise payment settlement network	37	BitShares	BTS	Decentralized exchange	70	Bancor	BNT	Token Index Funds
5	Litecoin	LTC	Faster Bitcoin	38	Golem	GNT	Rent other people's computers	71	Ripio Credit	RCN	Co-signed Cryptocurrency Loans
6	Dash	DASH	Privacy-focused Bitcoin clone	39	PIVX	PIVX	Inflationary Dash clone	72	ATMChain	ATM	Advertising network
7	NEO	NEO	Chinese-market Ethereum	40	Gas	GAS	Pay fees on Neo	73	Gnosis	GNO	Decentralized prediction market
8	NEM	XEM	Batteries-included digital assets	41	TRON	TRX	In-app-purchases	74	VeChain	VEN	Supply chain item IDs
9	Monero	XMR	Private digital cash	42	Vertcoin	VTC	Bitcoin clone	75	Pura	PURA	Cryptocurrency
10	Ethereum Classic	ETC	Ethereum clone	43	MonaCoin	MONA	Japanese Dogecoin	76	Particl	PART	Privacy marketplace and chat
11	IOTA	MIOTA	Internet-of-things payments	44	Factom	FCT	Decentralized record keeping	77	KuCoin Shares	KCS	Profit-sharing exchange fees
12	Qtum	QTUM	Ethereum contracts on Bitcoin	45	Basic Attention	BAT	Decentralized ad network	78	Bitquence	BQX	Mint for cryptocurrency investments
13	OmiseGO	OMG	Banking, remittance, and exchange	46	SALT	SALT	Cryptocurrency-backed loans	79	FunFair	FUN	Decentralized casino
14	Zcash	ZEC	Private digital cash	47	Kyber Network	KNC	Decentralized exchange	80	ChainLink	LINK	External data for contracts
15	BitConnect	BCC	Madoff-like investment fund	48	Dogecoin	DOGE	Serious meme bitcoin clone	81	Power Ledger	POWR	Airbnb for electricity
16	Lisk	LSK	Decentralized applications in JavaScript	49	DigixDAO	DGD	Organisation manages tokenized gold	82	Nxt	NXT	Cryptocurrency and marketplace
17	Cardano	ADA	Layered currency and contracts	50	Veritaseum	VERI	Vaporware	83	Monaco	MCO	Cryptocurrency credit card
18	Tether	USDT	Price = 1 USD	51	Walton	WTC	IoT Blockchain	84	Cryptonex	CNX	Zerocoin clone
19	Stellar Lumens	XLM	Digital IOUs	52	SingularDTV	SNGLS	Decentralized Netflix	85	MCAP	MCAP	Mining investment fund
20	EOS	EOS	Decentralized applications on WebAssembly	53	Bytom	BTM	Physical assets as tokens	86	Storj	STORJ	Rent disk space
21	Hshare	HSR	Blockchain switchboard	54	Byteball Bytes	GBYTE	Decentralized database and currency	87	ZenCash	ZEN	Privacy-focused Bitcoin clone
22	Waves	WAVES	Decentralized exchange and crowdfunding	55	GameCredits	GAME	Video game currency	88	Nexus	NXS	Bitcoin clone
23	Stratis	STRAT	Decentralized applications in C#	56	Metaverse ETP	ETP	Chinese Ethereum plus identity	89	Neblio	NEBL	Decentralized application platform
24	Komodo	KMD	Decentralized ICOs	57	GXShares	GXS	Decentralized Chinese Equifax	90	Zeusshield	ZSC	Decentralized insurance
25	Ark	ARK	Blockchain switchboard	58	Syscoin	SYS	Decentralized marketplace	91	Streamr DATAcoin	DATA	Real-time data marketplace
26	Electroneum	ETN	Monero clone	59	Siacoin	SC	Rent disk space	92	ZCoin	XZC	Private digital cash
27	Bytecoin	BCN	Privacy-focused cryptocurrency	60	Status	SNT	Decentralized application browser	93	NAV Coin	NAV	Bitcoin with private transactions
28	Steem	STEEM	Reddit with money voting	61	0x	ZRX	Decentralized exchange	94	AdEx	ADX	Advertising exchange
29	Ardor	ARDR	Blockchain for spawning blockchains	62	Verge	XVG	Privacy Dogecoin	95	Open Trading	OTN	Decentralized exchange
30	Binance Coin	BNB	Pay Binance exchange fees	63	Lykke	LKK	Digital asset exchange	96	SmartCash	SMART	Zcoin clone with rewards
31	Augur	REP	Decentralized prediction market	64	Civic	CVC	Identity and Authentication App	97	Bitdeal	BDL	Bitcoin clone
32	Populous	PPT	Invoice trading futures	65	Blocknet	BLOCK	Decentralized exchange	98	Loopring	LRC	Decentralized exchange

Blockchain fajták

Blockchain and Distributed Ledger Technology

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

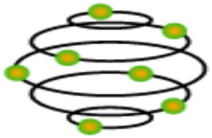
In a consortium blockchain, the consensus process is controlled by a pre-selected group – a group of corporations, for example. The right to read the blockchain and submit transactions to it may be public or restricted to participants. Consortium blockchains are considered to be "permissioned blockchains"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

Publikus blockchain előnyök/hátrányok

- 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

- 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?

Privát blockchain előnyök/hátrányok

- 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 terheli a környezetet (biztosan nem PoW alapon működik…)
- Gyorsabb, mint a publikus
- Különböző működési módú blockchain-ek
- Továbbfejleszthetőség

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

NEMZETI HÍRKÖZLÉSI ÉS INFORMATIKAI TANÁCS

A blockchain rendszer környezete

A legtöbb környezeti elem centralizált, ezért eséllyel és gazdaságosan támadható!

- Kriptotőzsdék (Centralizált, Decentralizált (Decentralized Exchange - DEX))
- Váltók (fiat/kripto)
- Fejlesztők (csak egy adott csoport fejleszt…)
- Mining farm-ok, pool-ok (átirányítás, wallet törés)
- Pénztárcák (exchange wallet, software wallet, hardware wallet, „paper wallet”)
- Villamos energia (PoW)
- Internet/hálózat
- Állami szabályozás, ill. annak hiánya

- Centralizált részek/környezet
  - Pénztárca (jelszó kiderül, vagy nincs meg – de: HDwallet-ek)
  - Kriptotőzsdék (inkább a centralizáltak)
  - Váltók (fiat/kripto)
  - Fejlesztők! (github, stb.)
  - PoW: Minerek, mining pool-ok, farm-ok
  - PoS: Forgerek
  - Áramfüggés, internet függés, sávszélesség függés

Matthew Mellon II
– kb. 1MRD USD értékű XRP-t vitt a sírba

- Ellenérdekeltség
  - Direkt ellenállás
  - Direkt támadás
  - FUD (Fear, Uncertainity, Doubt)
  - Média-hack
  - Ellenséges pénzpiaci műveletek
  - Piacbefolyásolás
  - Pénzügyi átjárhatóság tiltása
  - Állami/szabályozási lobbi

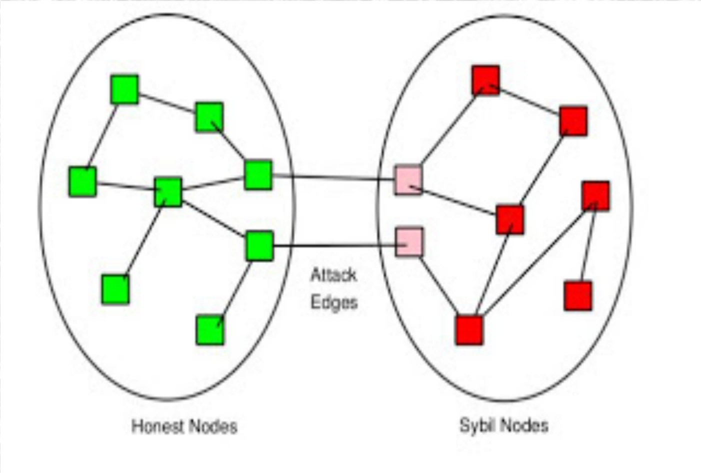
Blockchain sérülékenységek 3

- Állam/szabályozás
  - Szabályozás hiánya
  - Túlszabályozás (adminisztratív ellehetetlenítés)
  - Tiltás (kereskedelem, mining, HODL)
  - Engedélyhez kötés (pl. Howey test – security)
  - Direkt beavatkozás
  - Adóztatás
  - Stb.

- Blockchain protokoll hibák
  - Alaprendszer (in vivo kísérleti rendszerek – élveboncolás)
  - Skálázhatóság
  - Chain-ek közti átjárás
  - Software deployment
  - Smart contract-ok
  - Más rendszerekre kifejtett hibák (környezetterhelés, cryptojacking)
  - Megvalósítási hibák (fejlesztés)
  - Evolúciós hibák (pl. „csomósodás” (Pow/PoS is), skálázási gondok)

Maga a blockchain rendszer is támadható, nem csak a környezet…

- Wallet sérülékenység (hiba, jelszó vagy privát kulcs kompromittálódás, wallet „befagyás” – lásd Parity ETH wallet-ek)
- Coin történet lekövetése (privacy)
- Sybil attack (többszöröződés)
- Packet lehallgatás (data tampering)
- Distributed Denial of Service (DDOS)
- Időszinkron eltérítés
- Illegális tartalom bejuttatása a blockchain-be
- Hálózat szegmentálódás



Sybil attack

Forrás: https://cnt13.blogspot.com/2013/03/dr-jekyll-and-mr-hyde-detecting-sybils.html

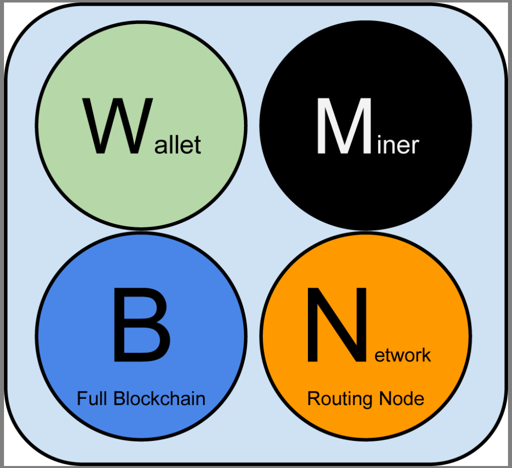
Mi ellen lehet támadni? (PoW eset)

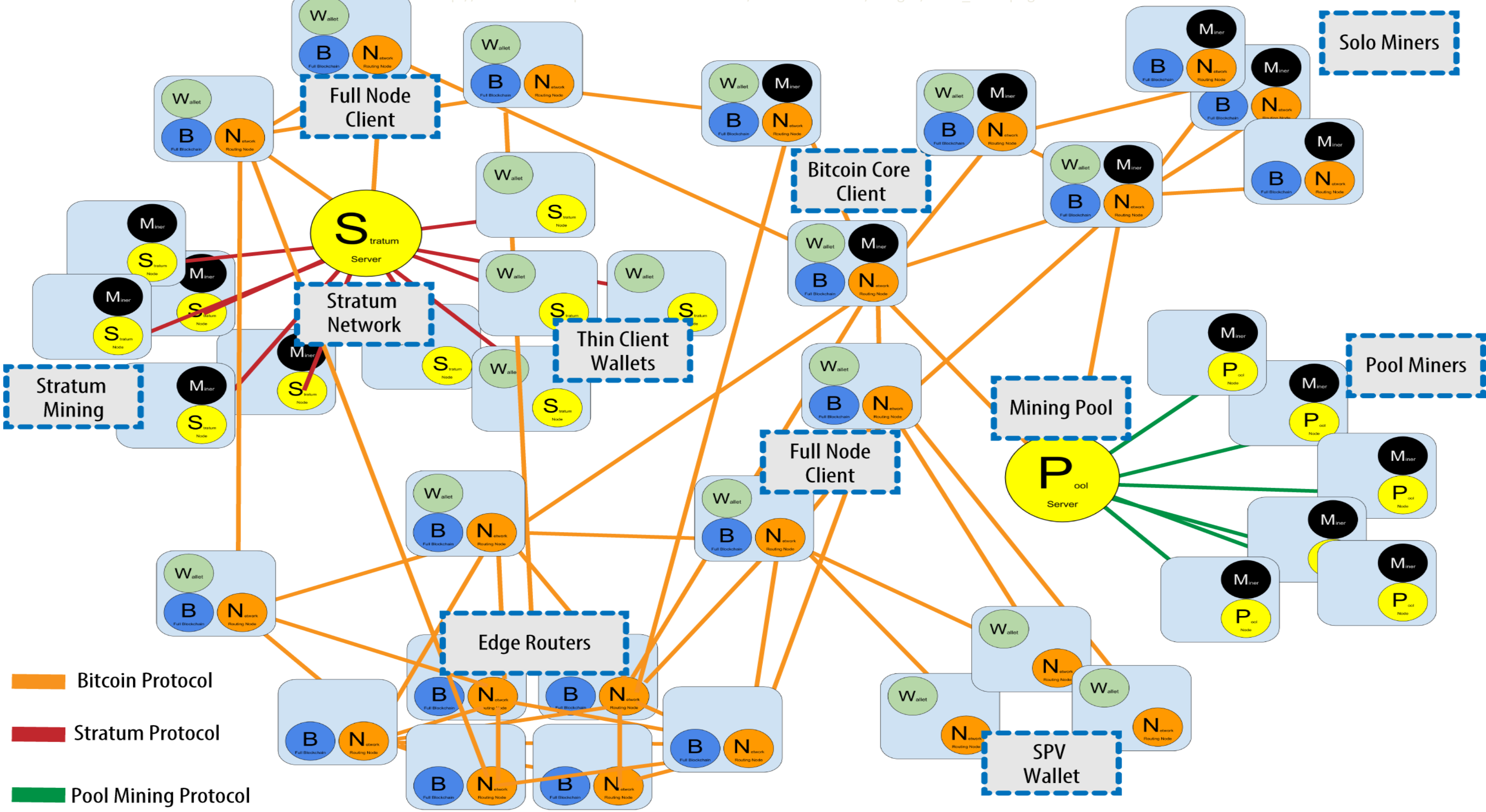
Funkciók

- W – Wallet
- B – Full blockchain
- N – Network routing node
- M – Miner
- P – Pool node/server vagy…
- S – Stratum node/server

Típusok

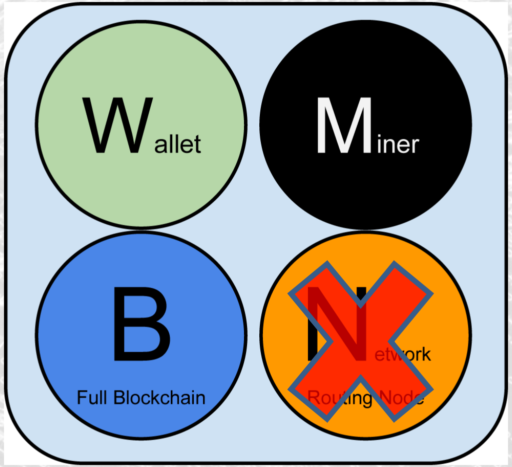
- Bitcoin core client – W,M,B,N
- Full node client – W,B,N
- Solo miner – M,B,N
- Edge router – B,N
- SPV wallet – W,N
- Thin client wallet – W,S
- Pool miner – M,P
- Stratum miner – M,S

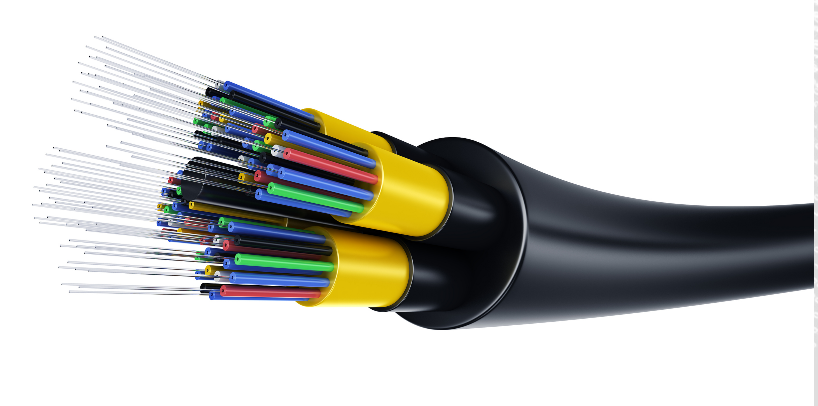



Full Node Client
Stratum Server
Stratum Network
Stratum Mining
Thin Client Wallets
Bitcoin Core Client
Solo Miners
Mining Pool
Pool Server
Pool Miners
Full Node Client
Edge Routers
SPV Wallet
Bitcoin Protocol
Stratum Protocol
Pool Mining Protocol

Network routing node elleni támadások

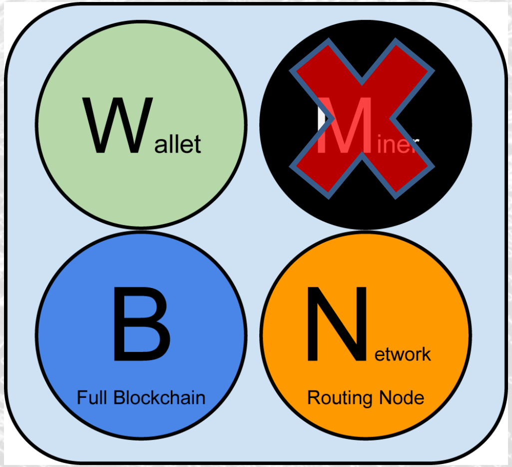
- Szokásos hálózatbiztonsági kérdések…
- Distributed Denial of Service (DDOS)
- Man-in-the-Middle (MITM)
- Hálózati kimaradás (elektromos hálózatot is beleértve)
- Fizikai támadás a hálózat ellen
- Stb.





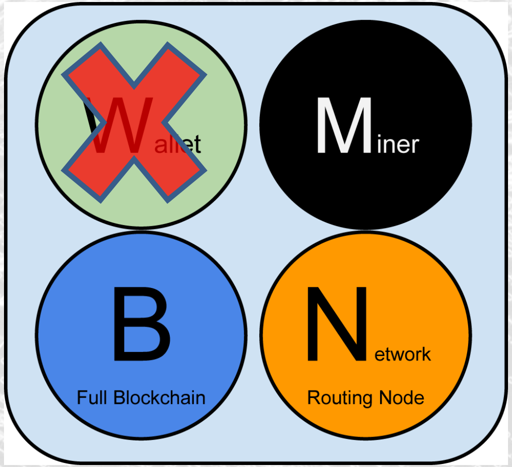
Miner ill. Pool/Stratum szerver elleni támadások

- Fizikai támadás
- Hálózatkimaradás (elektromos hálózatot is beleértve)
- MITM – Átirányítás
- Pool/Stratum szerver sérülékenységeinek kihasználása (ez az infrastruktúra nem szorosan tartozik a blockchain-hez)
- Stb.
- + Cryptojacking – gépek mining-ra való használata vírussal



Wallet elleni támadások

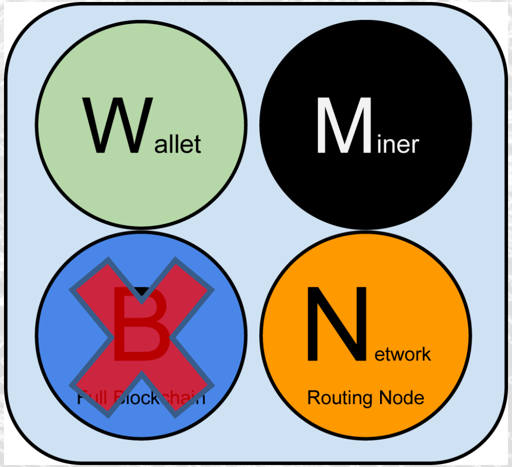
- Kriptográfiai kulcs kompromittálódása
- Jelszótörés
- Rossz smart contract-ok
- Fizikai kényszerítés, lopás
- Social engineering
- Környező rendszerek sérülékenységének kihasználása
  - Exchange wallet (Exchange hack)
  - Mining pool wallet (Pool hack)
  - Software wallet (keylogger)
  - Hardware wallet (??)
  - Stb.

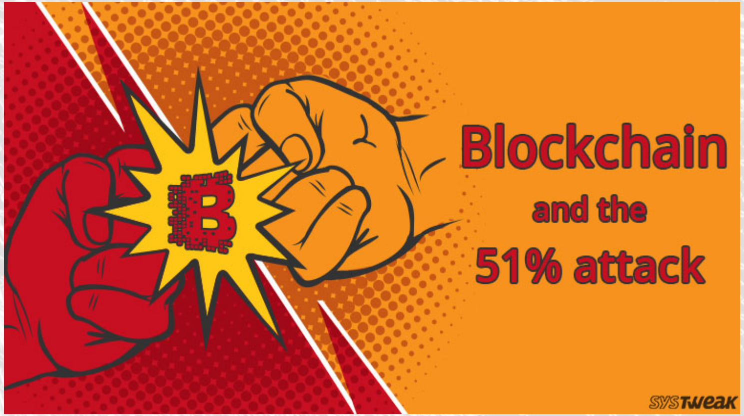


Céljuk: sikeres dupla költés (double spending), tranzakció hamisítás, konszenzus megtörése – lásd még: Bizánci tábornokok problémája

- Race attack („0/unconfirmed” attack)
- Finney attack („0/uncinfirmed” attack)
- Vector76 attack (one confirmation attack)
- Alternative history attack (pl. Success Probability (Hashpower=40%, Confirmation=6 blocks) = 50.398%) – Bitcoin esetén)
- Majority attack (51% attack – PoW eset)

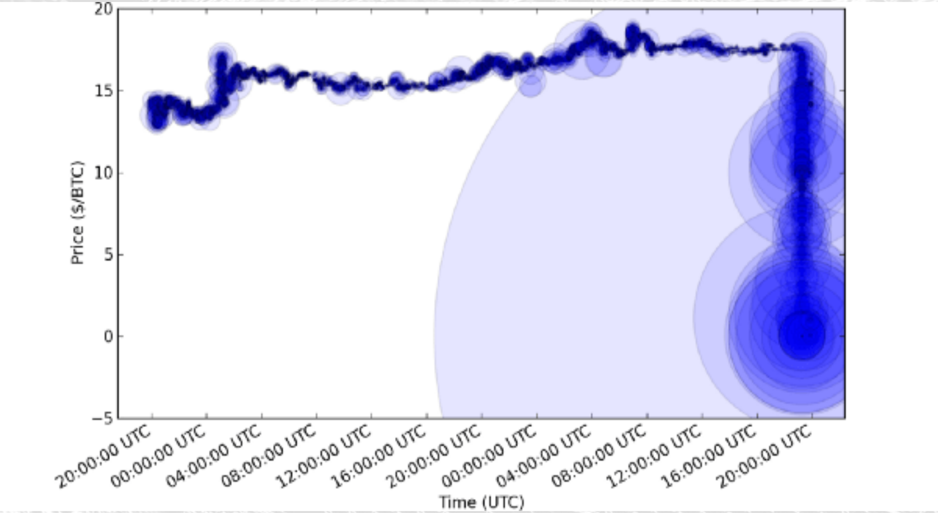
Lásd: https://en.bitcoin.it/wiki/Irreversible_Transactions





Protokoll hiba példák

- 51% attack és társai (PoW) – semmi sem tökéletes
- Nothing at Stake (PoS) – még nem használták ki
- Fork-ok (BTC/BCH, stb.) – Hard fork, soft fork
- Összebeszélés (PoS) – EOS (26-ból 16 tőzsde, ill. forger)
- Skálázhatóság – **Mt. Gox esete** – transatcion malleability
- Mégsem minden anonim – Bitcoin/Chainalysis
- Wallet/smart contract hiba – Parity Technologies hard wallet – „frozen ether”
- Smart contract megvalósítási hiba – **The DAO hacking** (utána ETH/ETC fork) – rekurzív hívás



A Mt. Gox Bitcoin tőzsde összeomlása percről percre

A „The DAO" hacker nyílt levele 1

===== BEGIN SIGNED MESSAGE =====
To the DAO and the Ethereum community,

I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting is rewarded with additional ether. **I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward.** It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAOs".

I am disappointed by those who are characterizing the use of this intentional feature as "theft". I am making use of this explicitly coded feature as per the smart contract terms and my law firm has advised me that my action is fully compliant with United States criminal and tort law. For reference please review the terms of the DAO:

"The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at **0xbb9bc244d798123fde783fcc1c72d3bb8c189413.** Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation."

A „The DAO” hacker nyílt levele 2

A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract. **Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology.** Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal.

I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm. Those accomplices will be receiving Cease and Desist notices in the mail shortly.

I hope this event becomes an valuable learning experience for the Ethereum community and wish you all the best of luck.

Yours truly,
"The Attacker"
===== END SIGNED MESSAGE =====

Message Hash (Keccak): 0xaf9e302a664122389d17ee0fa4394d0c24c33236143c1f26faed97ebbd017d0e
Signature: 0x5f91152a2382b4acfdbfe8ad3c6c8cde45f73f6147d39b072c81637fe8
1006061603908f692dc15a1b6ead217785cf5e07fb496708d129645f3370a28922136a32

Figyelmüket köszönve:

Sík Zoltán Nándor
Alelnök
Nemzeti Hírközlési és Informatikai Tanács
zoltan.sik@nhit.hu