Információ hitelesítés a blockláncon

Daniel Szego
In: https://www.linkedin.com/in/daniel-szego/

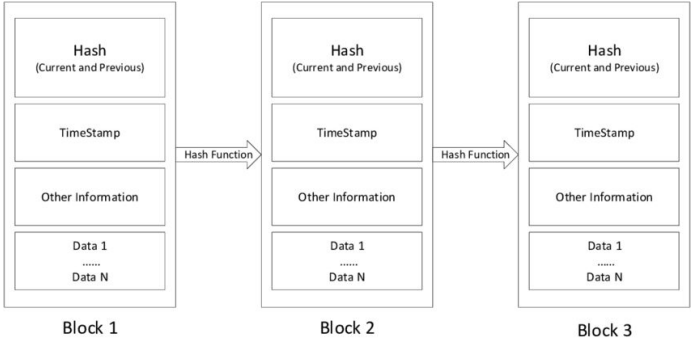
Blocklánc

Információ hitelesítési szempontból:

Beírjuk az adatot a blockclncba és az ott marad.

Kérdések:

- Milyen adat ?
- Mennyire marad ott ?
- Mire jó ?



Adat a blockláncban

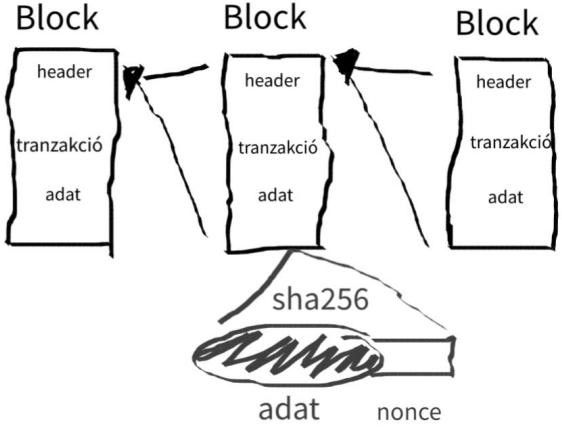
Nem nyújt titkosítást (publikus, félig publikus)

Az adat nem törölhető: GDPR

Sok adatot nem tárol a blockchain

Adat hash értékét szokták beírni, de (!) dictionary attack

Adat + véletlen nonce hash értéke



Perzisztencia: konszenzus - számítási garancia

Minden egyes block plusz számítási garancia. **Példa**:

Bitcoin hashrate 230.13 EH/s = 230 * 10^18

1 év = 31,536,000s = 31 * 10^6s

1 év garancia = 7 * 10^25 hash számítás

Kimerítő kulcskeresés:
2^256 = 1.1 10^77 << 7*10^25
(olyan mintha 84 bites kulcs mérettel dolgoznánk)

Perzisztencia: Konszenzus - közgazdasági garancia

Minden egyes block plusz közgazdasági garancia. **Példa**:

Tezos Active Staking capital 672,992,992 XTZ (* 1.8 USD) = 1.2 milliárd dollár

1 éves garanciára: 30s blocktime, (31,536,000s / 30s) * 1.2*10^9 = 1.2 * 10^15 = 1.2 billiárd dollár biztosítás

Perzisztencia: konszenzus - intézményi garancia

Minden egyes plusz blockot konzorciumot fenntartó intézmények többsége / túlnyomó többsége “érvényesnek” értékelte.

Ha az intézmények többségét / túlnyomó többségét meghackelik, a blockchain újra felépíthető => a beírt adat változtatható / törölhető

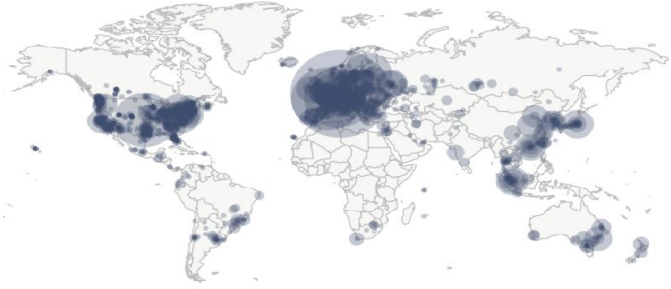
Perzisztencia: Geográfiai elosztottság

Csomópontok geográfiai lokalizációja.

Nyilvános blockchain csomópontok a világon mindenhol elosztva megtalálhatóak.

Konzorciumi blockchain csomópontok tipikusan geográfiailag koncentráltak

Csomópontok megsemmisülése / hálózati szeparáció

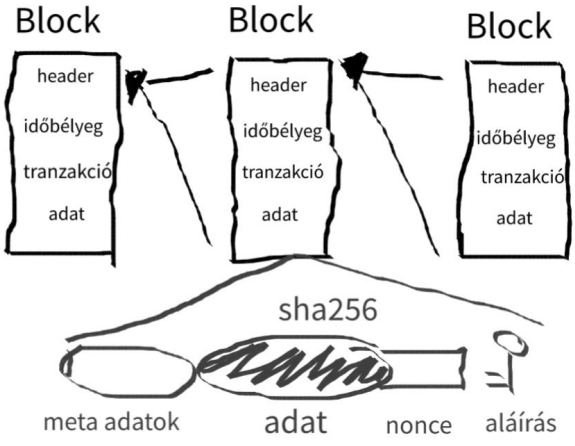


Alkalmazás: adat integritás

Egyszerű adat / információ integritás

Mentett adatok: például szerződések konzisztenciája pl:

Transzferált adatok, például adatátvitel két pont között

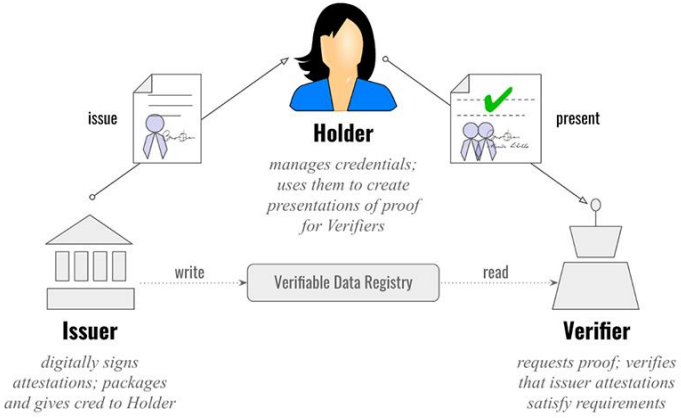


Alkalmazás: verifiable credentials

Komplex adatintegritás: a dokumentum aláírva a kibocsátó és a tulajdonos által, a nyilvános kulcsok és a dokumentum hash a blockchainben.

Blockchain and identity stack: Hyperledger Indy, https://www.hyperledger.org/use/hyperledger-indy

EBSI (European Blockchain Service Infrastructure)



Kérdések & diszkusszió

Daniel Szego
In: https://www.linkedin.com/in/daniel-szego/