Blockchain technológia és virtuális fizetőeszközök

A blockchain technológia ~2010-től forradalmasította az adatok kezelését és a virtuális fizetőeszközök működését. A decentralizált rendszerek, mint a Bitcoin és az Ethereum, lehetővé tették az emberek számára, hogy *közvetítők nélkül hajtsanak végre különböző tranzakciókat.*

Blockchain alapok

A blockchain egy **decentralizált adatbázis**, amely az adatok folyamatosan növekvő listáját, úgynevezett blokkokat tartalmazza. Minden blokk kapcsolódik az előzőhöz egy kriptográfiai algoritmus révén, biztosítva a lánc integritását és biztonságát.

- **Decentralizáltság**: A blockchain technológia alapja, hogy nincs központi hatóság, ami irányítaná vagy ellenőrizné az adatokat.
- **Átláthatóság**: Minden résztvevő láthatja a tranzakciókat, de a résztvevők személyazonossága anonim marad.
- **Változtathatatlanság**: Miután egy blokk hozzáadásra kerül a lánchoz, nem lehet azt módosítani anélkül, hogy az egész láncot ne változtatnák meg, ami rendkívül nehéz.

Hogyan működik a blockchain?

Eredeti cikk, szerzője álnéven írta:
https://web.archive.org/web/20140320135003/https://bitcoin.org/bitcoin.pdf

A blockchain technológia működési elve egyszerű, és rendkívül biztonságos:

1. A tranzakciók adatainak csoportosítása blokkokba.
2. A blokkok hozzáadása a lánchoz, miután a résztvevők (node-ok) konszenzusra jutottak, hogy a tranzakciók érvényesek.
3. Minden blokk tartalmazza az előző blokk kriptográfiai lenyomatát, ezzel biztosítva a lánc folyamatosságát és változtathatatlanságát.

Hash kódok

A hash egy fix hosszúságú alfanumerikus (számokból és betűkből álló) kód, amely az eredeti adat rövidített ujjlenyomata.

Hash-függvények főbb jellemzői

- Determináltság
  - Egy adott bemenet mindig ugyanazt a hash értéket adja vissza
- Fix hosszúságú kimenet

    - A bemenet méretétől függetlenül a hash kód mindig ugyanakkora hosszúságú. Az SHA-256 hash-függvény kimenete mindig 256 bit (64 hexadecimális karakter)
- Ütközés-ellenállás (Collision resistance)
    - Két különböző bemenet nem generálhatja ugyanazt a hash kódot. Ez a tulajdonság kritikus a biztonságos alkalmazásokban, bár az ütközés lehetősége soha nem zárható ki teljesen.
- Egyirányúság
    - A hash-ből nem lehet visszafejteni az eredeti adatot (matematikailag egyirányú)
- Jó a szórása
    - A bemenet kis módosítása (akár egyetlen karakter változtatása) jelentősen megváltoztatja a hash kódot.

Példa:

Hello, World! → `a591a6d40bf420404a011733cfb7b190`

hello, World! → `934acb356d42d04c21a261c15bf6a95d`

Ismertebb változatok

MD5: Régi, de már nem biztonságos hash-függvény.

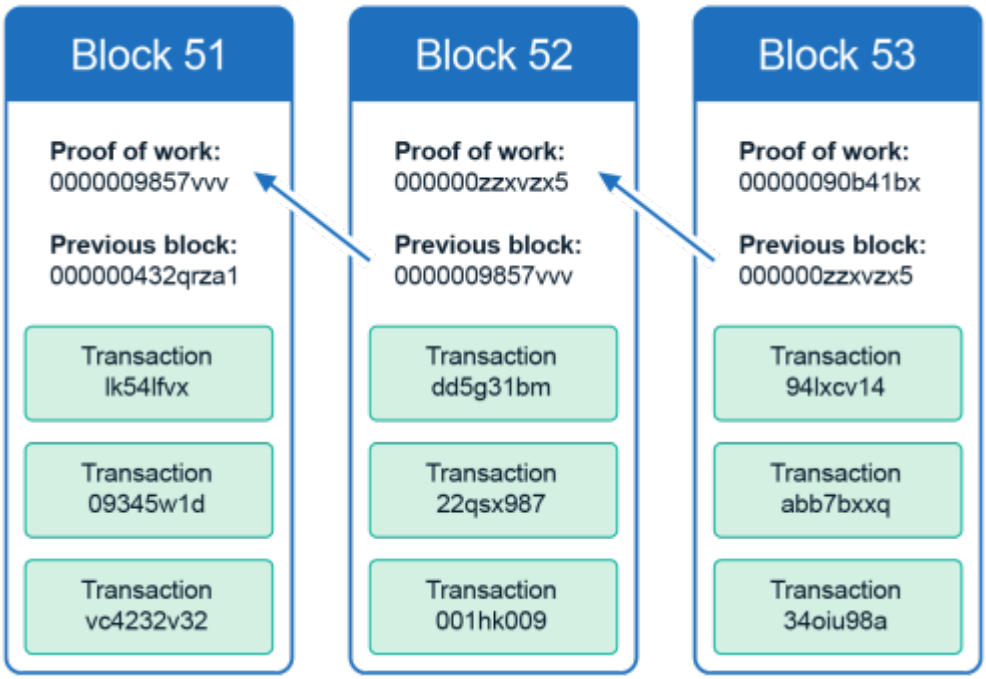
SHA-1: Jobb, de már gyenge, nem ajánlott használata.

SHA-256 (Secure Hash Algorithm): A modern blockchain rendszerekben (pl. Bitcoin) használt hash.

SHA-3: Újabb szabvány, még erősebb biztonság.

Hash alkalmazási területei

- **Jelszótárolás**: a jelszavakat nem tároljuk közvetlenül, hanem a hash kódját.
- **==== Blokklánc felépítése ==== === Proof of work === A Proof-of-Work (**PoW**) egy olyan konszenzusmechanizmus, amelyet blockchain hálózatok, például a Bitcoin, használnak a tranzakciók hitelesítésére és új blokkok hozzáadására a lánchoz. A** PoW **célja a hálózat biztonságának garantálása és a résztvevők közötti egyetértés (konszenzus) elérése központosított hatóság nélkül.** Hogyan működik? Blokk létrehozása**: Egy adott blokk tartalmazza a tranzakciók listáját, a korábbi blokk hash-ét és más adatokat. A bányászok versenyeznek, hogy megtalálják azt a számot (a nonce-ot), amely megfelel bizonyos feltételeknek.** Feladat**: A blokk tartalmából egy olyan hash-t kell generálni, amely megfelel a hálózat által meghatározott nehézségi szintnek. A gyakorlatban a hash-nek *egy bizonyos számú nullával* kell kezdődnie. A bányászok ezt próbálgatással (brute force) oldják meg, a hash-t addig számolják újra különböző nonce értékekkel, amíg megfelel a kritériumnak. Online szimulátor: https://blockchain-academy.hs-mittweida.de/2021/05/proof-of-work-simulator/**



Valóságos blokklánc: https://www.blockchain.com/explorer/assets/btc ===== Kriptovaluták ===== A blockchain technológia legismertebb alkalmazásai a kriptovaluták**, amelyek a hagyományos valutákhoz hasonlóan működnek, de digitális formában léteznek, és a blockchainen keresztül kerülnek kibocsátásra és nyomon követésre.** * Bitcoin**: Az első és legismertebb kriptovaluta, amelyet 2008-ban hoztak létre Satoshi Nakamoto álneve alatt. Célja egy közvetítők nélküli, decentralizált fizetési rendszer kialakítása.** * Ethereum**: Egy másik jelentős blockchain platform, amely nemcsak kriptovalutát (Ether) kínál, hanem lehetővé teszi okosszerződések (smart contracts) és decentralizált alkalmazások (DApps) futtatását. ===== Jogi vonatkozások ===== A kriptovaluták és a blockchain technológia használata számos jogi kérdést vet fel, különösen mivel a szabályozás gyakran elmarad a technológia fejlődésétől.** * Szabályozás**: Sok ország még dolgozik a kriptovaluták szabályozásán. Néhány ország elfogadja és szabályozza a kriptovaluták használatát, míg mások tiltják vagy szigorúan ellenőrzik azokat.** * Pénzmosás elleni törvények**: A kriptovaluták anonimitása lehetővé teheti a pénzmosást vagy illegális tevékenységek finanszírozását, ezért sok ország pénzmosás elleni törvényeket vezet be, hogy ellenőrizzék a kriptovaluta-tranzakciókat.** * Adózás**: A kriptovalutákat adózás szempontjából vagyoni eszközöknek tekintik, ezért az azokkal való kereskedésből származó nyereséget adóztatják. ===== Okosszerződések (Smart Contracts) ===== Az** okosszerződések **olyan önvégrehajtó szerződések, amelyek a blockchainen futnak. A szerződések feltételeit program formájában írják meg, és azok automatikusan végrehajtásra kerülnek, amikor a meghatározott feltételek teljesülnek.** * 1. példa**: Egy biztosítási szerződés, amely automatikusan kártérítést fizet, ha egy előre meghatározott esemény bekövetkezik (pl. egy járat késik). ===== Virtuális fizetőeszközök előnyei és kihívásai =====** * Előnyök**: -** Decentralizáció**: Közvetítő nélküli tranzakciók, alacsony költségek. -** Globális elérhetőség**: Bárhol használható, ahol internetkapcsolat van. -** Gyorsaság**: A tranzakciók gyorsabban feldolgozhatók, mint a hagyományos bankrendszerekben.** * Kihívások**: -** Volatilitás**: A kriptovaluták árfolyama gyakran ingadozik, ami kockázatot jelent a felhasználók számára. -** Szabályozási kockázatok**: A szabályozás hiánya vagy változékonysága problémákat okozhat a jogi megfelelés terén. -** Biztonsági kérdések**: Bár a blockchain biztonságos, a felhasználói fiókok, pénztárcák feltörhetőek, ha nem megfelelő védelmet használnak.