Blockchain technológia és virtuális fizetőeszközök

Hash kódok

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

Egyszerű hash kód: egyszerű hash

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.
    - 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.
- **Digitális aláírás**: hitelesítéskor elég a hash-t aláírni digitálisan, nem kell a teljes dokumentumot.
- **Proof of work**: lásd az alábbiakban.

Blockchain alapok

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.*

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?

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.

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?

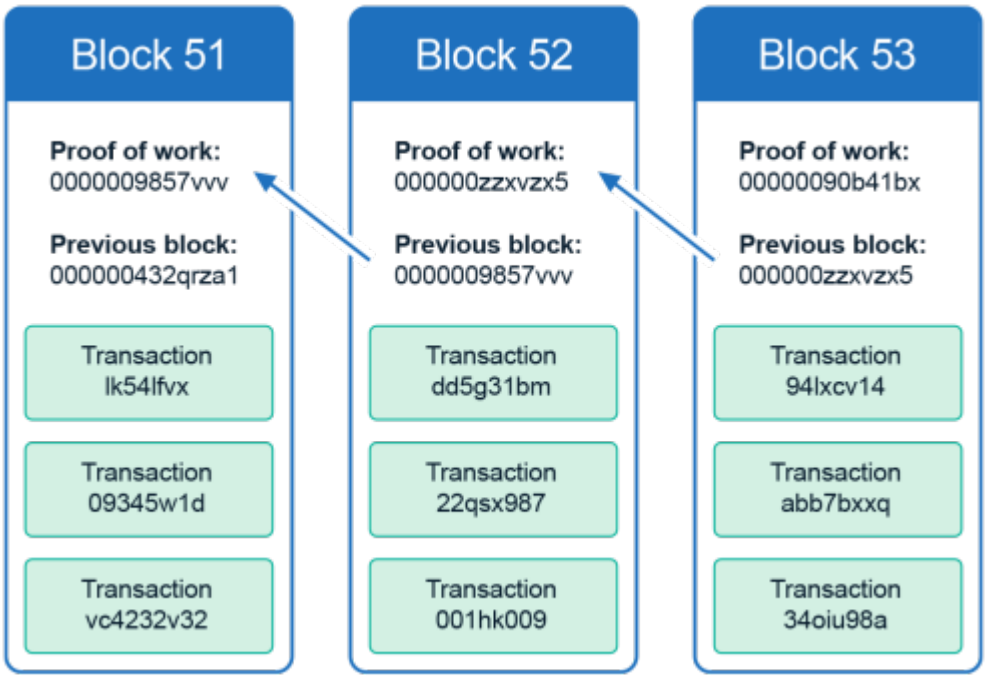
Blokk létrehozása: Egy adott blokk tartalmazza a tranzakciók listáját, a korábbi blokk hash-ét és más adatokat. A bányászok versenyeznek, hogy megtalálják azt a számot (a nonce-ot), amely megfelel bizonyos feltételeknek.

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/



Szavazás alapú hitelesítés

A hálózat résztvevői (csomópontok) szavaznak arról, hogy egy adott blokk vagy tranzakció érvényes-e. A csomópontok rendelkeznek azzal az információval, amely alapján megállapíthatják a tranzakciók helyességét (pl. elegendő egyenleg, aláírások hitelessége).

A hálózat meghatároz egy küszöbértéket (pl. 51% vagy 67%), amelyet el kell érni az elfogadáshoz. Például, ha két blokk érkezik egy időben, a többségi szavazás dönt.

Valóságos blokklánc: https://www.blockchain.com/explorer/assets/btc

"Jogos" alkalmazások

- Elektronikus szavazás (e-voting): A blockchain hálózat minden szavazatot hitelesít, és a többségi döntés automatikusan végrehajtásra kerül.
- Decentralizált Autonóm Szervezetek (DAO-k): A szavazás biztosítja a közösség által irányított működést, például a források elosztásáról vagy projektek jóváhagyásáról.
- Jogviták kezelése: A szavazási alapú konszenzus használható decentralizált döntéshozatalban, például okosszerződések vitás helyzeteinek feloldására.

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).

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract FlightDelayInsurance {
    struct Policy {
        address insured;  // A biztosított személy címe
        uint256 premium;  // A biztosítási díj (premium)
        uint256 payout;   // A kártérítési összeg
        bool active;      // Aktív-e a biztosítás
```

```
        bool paidOut;     // Kifizetés megtörtént-e
    }

    address public owner; // A biztosító címe
    mapping(string => Policy) public policies; // Járatszámhoz kötött
biztosítási szerződések

    event PolicyPurchased(address indexed insured, string flightNumber,
uint256 premium, uint256 payout);
    event CompensationPaid(address indexed insured, string flightNumber,
uint256 amount);

    constructor() {
        owner = msg.sender; // A szerződést deployoló fél lesz a biztosító
    }

    modifier onlyOwner() {
        require(msg.sender == owner, "Csak a biztosító végezheti ezt a
műveletet.");
        _;
    }

    // Biztosítás vásárlása
    function purchasePolicy(string memory flightNumber, uint256 payout)
public payable {
        require(msg.value > 0, "Biztosítási díjat (premium) kell fizetni.");
        require(policies[flightNumber].insured == address(0), "Ehhez a
járathoz már van biztosítás.");

        policies[flightNumber] = Policy({
            insured: msg.sender,
            premium: msg.value,
            payout: payout,
            active: true,
            paidOut: false
        });

        emit PolicyPurchased(msg.sender, flightNumber, msg.value, payout);
    }

    // Kártérítés kifizetése késés esetén (az orákulum adatai alapján)
    function payCompensation(string memory flightNumber) public onlyOwner {
        Policy storage policy = policies[flightNumber];
        require(policy.active, "Ez a biztosítás már nem aktív.");
        require(!policy.paidOut, "A kártérítést már kifizették.");

        // Kifizetés
        policy.paidOut = true;
        policy.active = false;

        payable(policy.insured).transfer(policy.payout);
```

```
        emit CompensationPaid(policy.insured, flightNumber, policy.payout);
    }

    // Szerződés egyenlegének lekérdezése
    function getBalance() public view onlyOwner returns (uint256) {
        return address(this).balance;
    }

    // Külső forrásból származó információk frissítése (orákulum
szimulációja)
    function handleFlightDelay(string memory flightNumber) public onlyOwner
{
        // Ez a függvény szimulálja a repülési késés adatok fogadását
        // és automatikusan meghívja a kártérítést kifizető függvényt
        payCompensation(flightNumber);
    }
}
```

Virtuális fizetőeszközök előnyei és kihívásai

- **Előnyök**:
  1. **Decentralizáció**: Közvetítő nélküli tranzakciók, alacsony költségek.
  2. **Globális elérhetőség**: Bárhol használható, ahol internetkapcsolat van.
  3. **Gyorsaság**: A tranzakciók gyorsabban feldolgozhatók, mint a hagyományos bankrendszerekben.
- **Kihívások**:
  1. **Volatilitás**: A kriptovaluták árfolyama gyakran ingadozik, ami kockázatot jelent a felhasználók számára.
  2. **Szabályozási kockázatok**: A szabályozás hiánya vagy változékonysága problémákat okozhat a jogi megfelelés terén.
  3. **Biztonsági kérdések**: Bár a blockchain biztonságos, a felhasználói fiókok, pénztárcák feltörhetőek, ha nem megfelelő védelmet használnak.