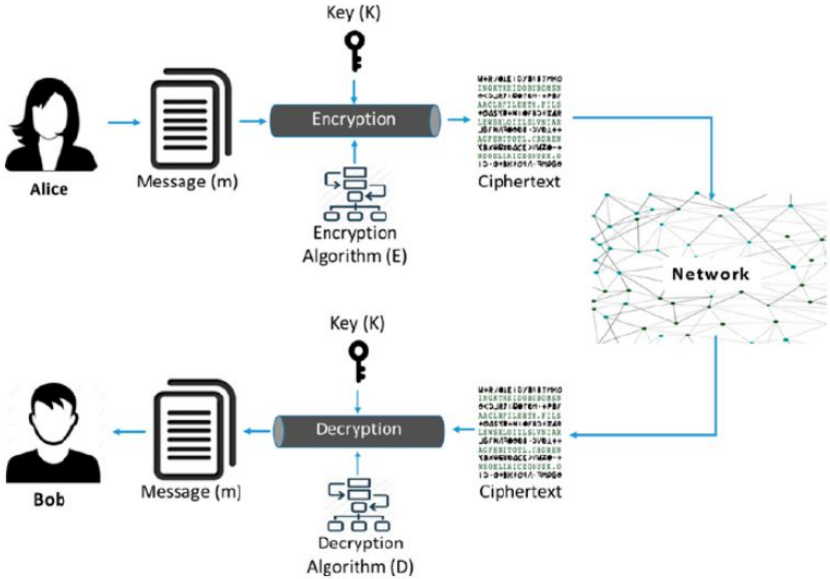
Blockchain technológia

Kovács László, ME

Információ védelmi modellek

Védelmi funkciók céljai:
- adatok titkosítása
- adat integritás védelem
- kliens hitelesítés
- eredeti állapot megőrzése

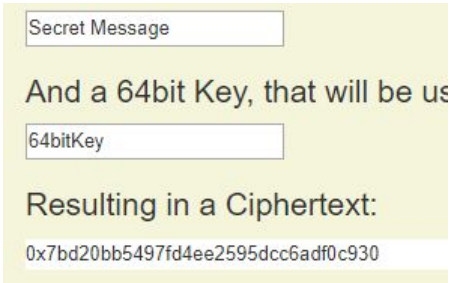
Kódolás és dekódolás
- egykulcsú vagy
- kétkulcsú
- adatfolyam vagy
- blokk kódolás



Egykulcsú védelem

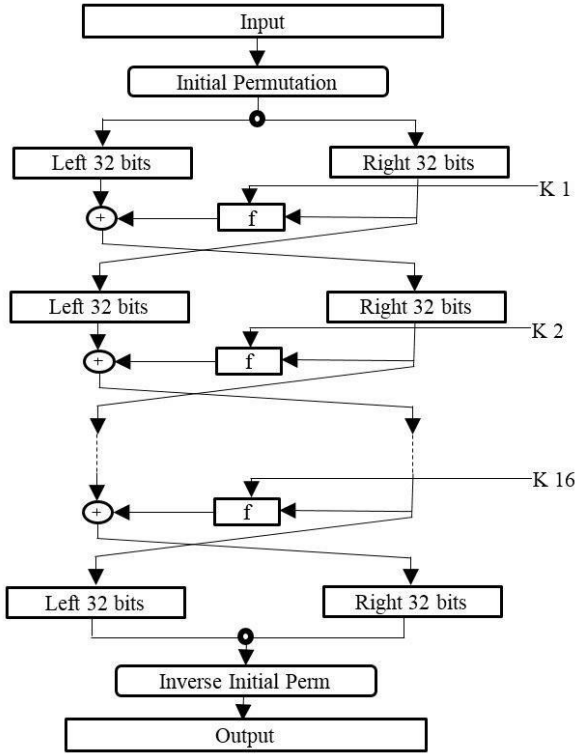
- a kulcs szimmetrikus szerepű (kódolás és dekódolás)
- hatékony algoritmusok
- hardver implementációk
- nagytömegű adatok kódolása
- DES : alap módszer
- XOR alapú
- probléma a kulcs megosztása

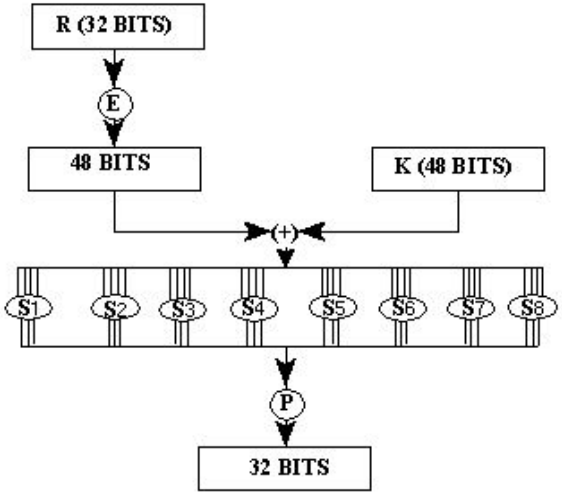
A	B	A ⊕ B
0	0	0
1	0	1
0	1	1
1	1	0



DES titkosítás

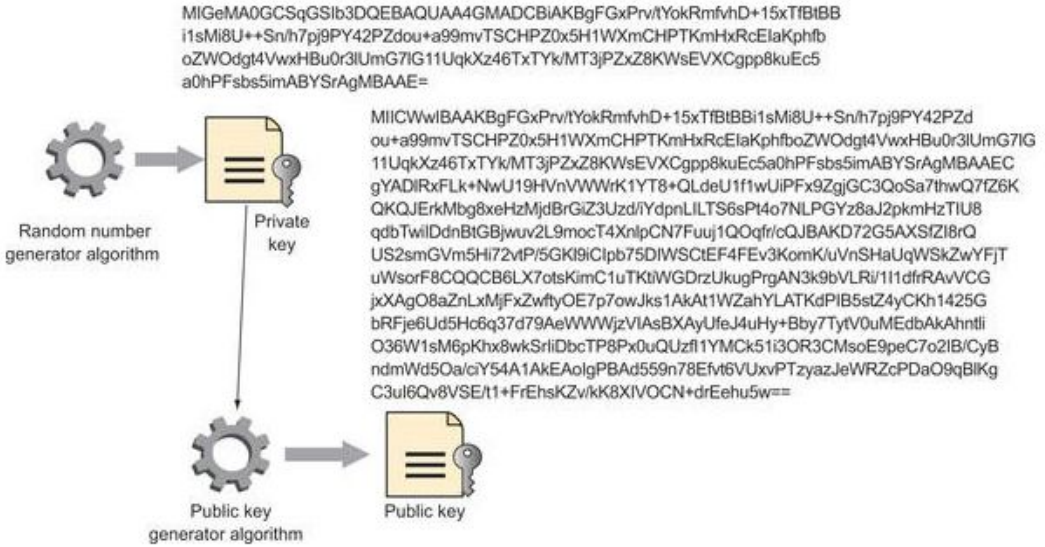
- blokk kódolás
- egykulcsú
- bitműveleteken alapul
- XOR
- kiterjesztés
- S-BOX
- az erősség a kulcs hosszától függ
- brute-force





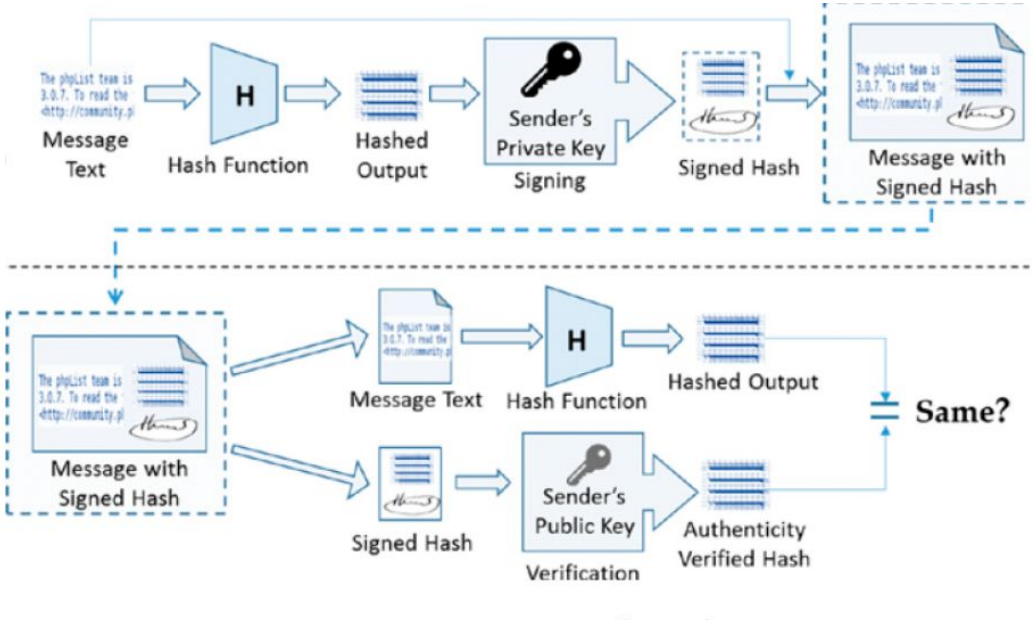
Kétkulcsú védelem

- egy kulcspár él, külön a kódolásra és külön a dekódolásra
- hatékony kódolás
- hardver implementációk
- számolás igényesebb
- kisebb méretű adatok kódolása
- RSA : alap módszer
- hatványozás, prímszám, moduló alapú
- kulcspárok generálása és kezelése



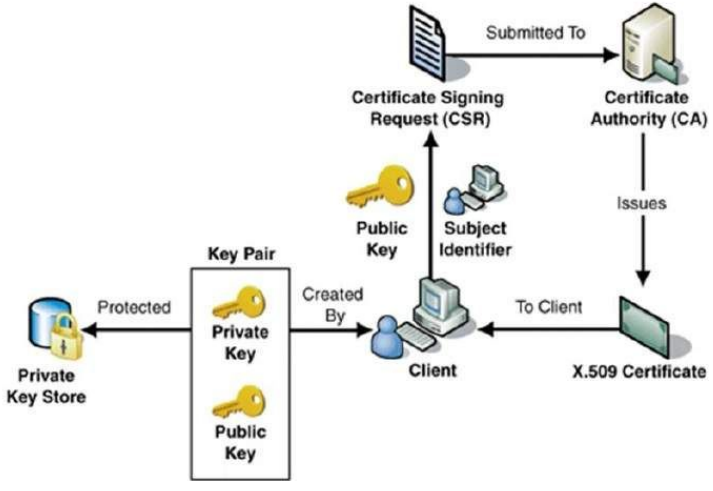
DSA titkosítás

- digitális aláírás
- üzenet eredetiségét garantálja
- a küldő személyet garantálja
- üzemethez ujjlenyomat készítése
- ujjlenyomat kódolása (K1)
- üzenet küldése, fogadása
- kapott ujjlenyomat dekódolása (K2)
- kapott üzenethez ujjlenyomat
- a két ujjlenyomat összevetése
- ha egyezik, akkor OK



PKI architektúra

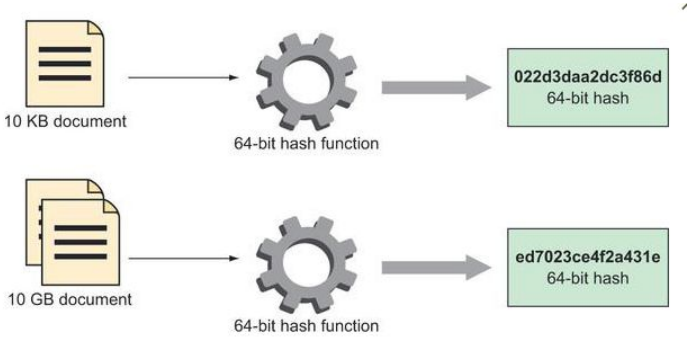
- biztonságos adatkezelés, adatküldés keretrendszere
- hálózati üzenetek titkosítása
- digitális aláírás
- kulcs-szerverek
- ujjlenyomat
- integritás ellenőrzés
- titkosítási primitívek

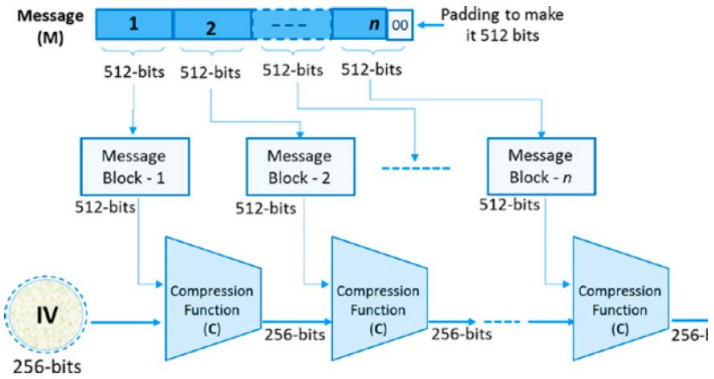


[Applications]		
System Security-Enabling Services	Secure Protocols	Security Policy Services
	Protocol Security Services	
	Long-Term Key Services	Supporting Services
	Cryptographic Services	
	Cryptographic Primitives	

Digitális ujjlenyomat, Hash függvény

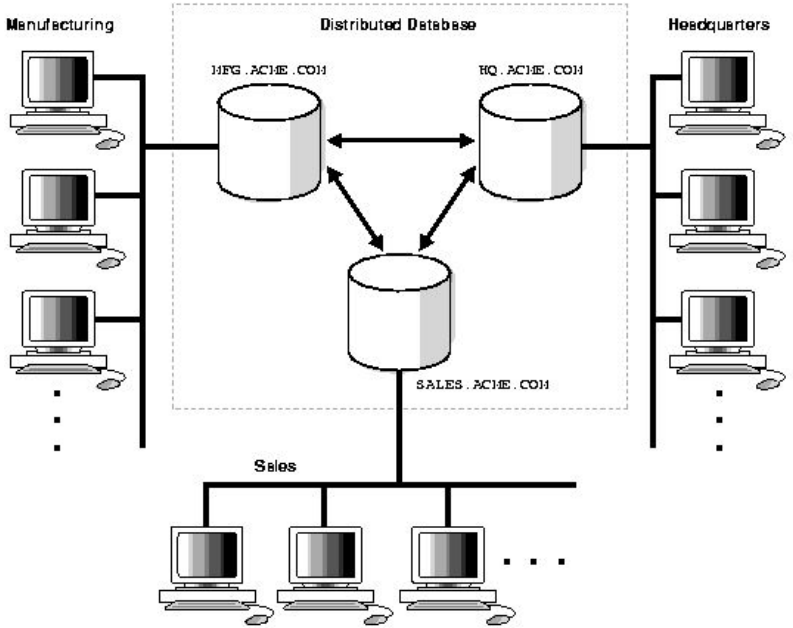
- a hosszabb adatsorhoz egy rövidebb leírás
- ha az adatsor változik, a a leírás is változik nagy eséllyel
- az adat rendszerint egész számként értelmezett
- v = H(x)
- v fix méretű
- H() determinisztikus
- H() ütközésmentes
- egyirányú kódolás
- (x mod m) alapú
- SHA: alap algoritmus





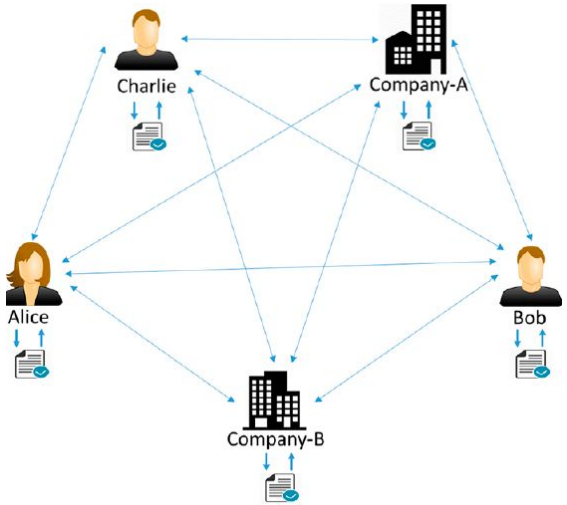
Elosztott DBMS, tranzakció

- hagyományos adatbázis komponensek
- adatok elosztott tárolása és kezelése
- központi vezérlés
- virtuális egység kívülről nézve
- hatékonyság és rendelkezésre állás növekedés
- UPDATE problémák
- hierarchikus tranzakciók



Elosztott ledgers

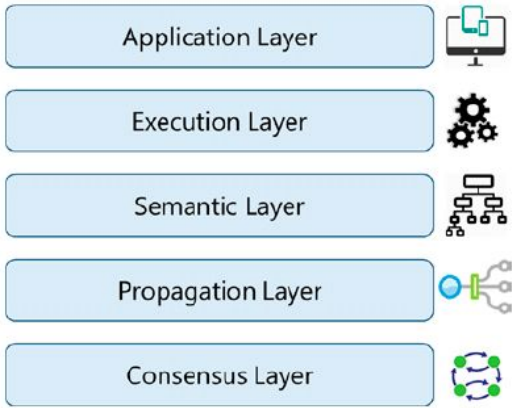
- 2018: Satoshi : “Bitcoin: A Peer-to-Peer Electronic Cash System”
- speciális elosztott adatbázis
- centralizált központi felügyelet kiváltása (nincs központi szerver)
- végrehajtott tranzakciók listája
- peer to peer tranzakciók
- hitelesség, megbízhatóság növelése
- minden tartalom megosztott, látható (de titkosított)
- szigorú védelem
- épség validáció
- főleg pénzügyi tranzakciók tárolása
- virtuális pénznem (bitcoin,..)



Peer-to-Peer trading: Blockchain

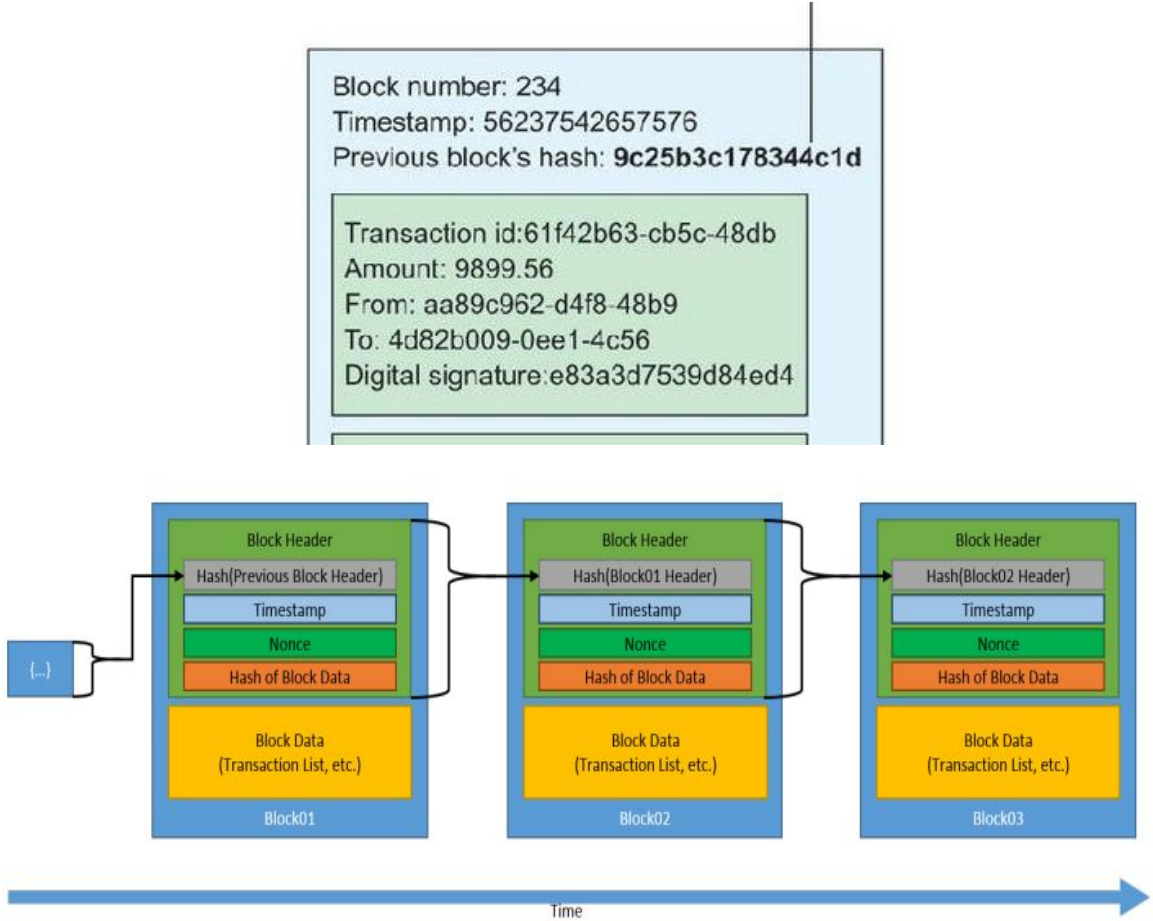
Blockchain hálózat

- Minden csomópontban ugyanazon adatok vannak letárolva
- az adatok nem módosíthatóak
- nincs UPDATE, DELETE csak INSERT
- az új rekord mindenhova elkerül
- az új adatok validáltak
- alkalmazási réteg
- végrehajtási réteg
- validációs réteg
- adattovábbító réteg
- konzisztencia, konszenzus réteg



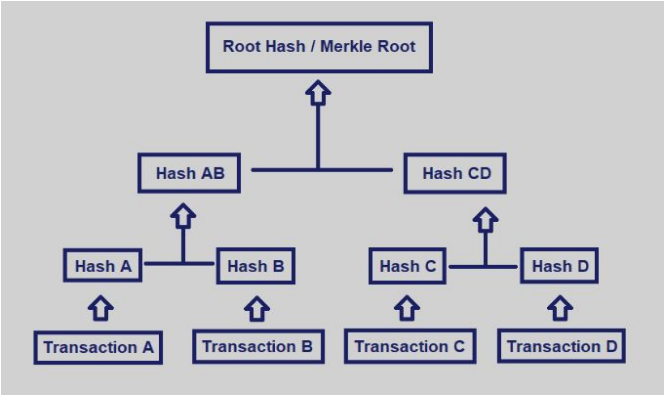
Blockchain adattárolás

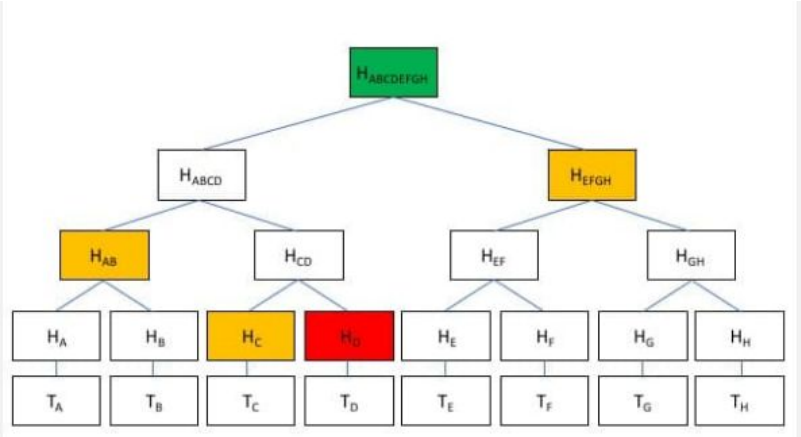
- Az adatok blokkokban árlódnak
- A letárolt adatok nem módosíthatóak
- Egy blokk több tranzakciót tartalmaz
- Adatblokkok láncolata alakul ki
- Genesis blokk
- Blokk header:
  - időbélyeg
  - Merkle tree
  - hash az előző blokkra
- a blokk hash értékét más blokkok is őrzik (nem módosítható titokban)



Merkle-trees

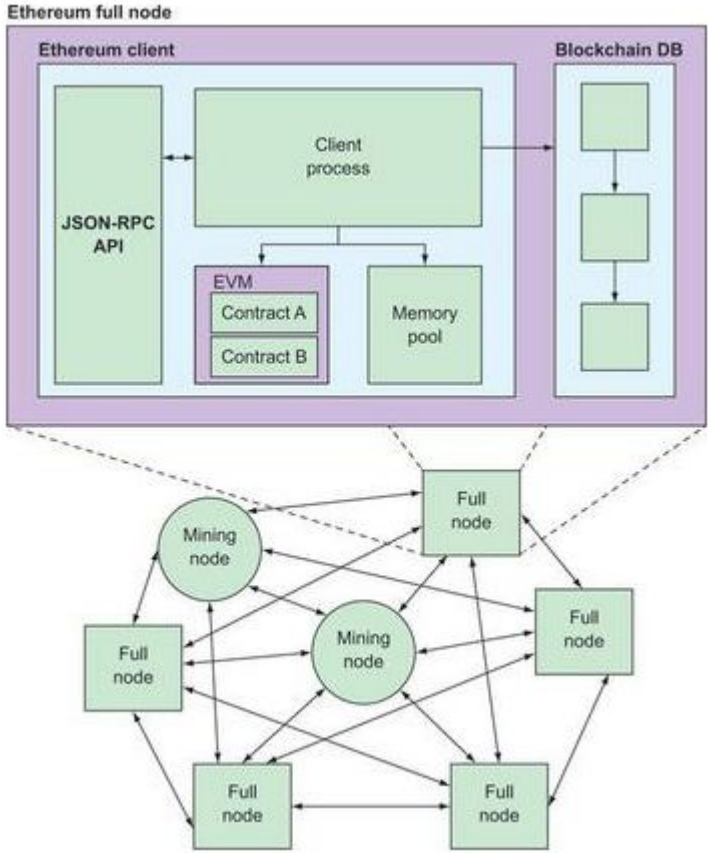
- Adatblokk digitális ujjlenyomata
- Hash értékek hierarchiája
- levelekben az egyes tranzakciók ujjlenyomata
- köztes szint értéke az összesített gyerekeinek a hash értéke
- az adatblokk fejrészében tárolódik
- célja az adatblokk sértetlenségének ellenőrzése
- a módosult tranzakciót gyorsan lehet lokalizálni





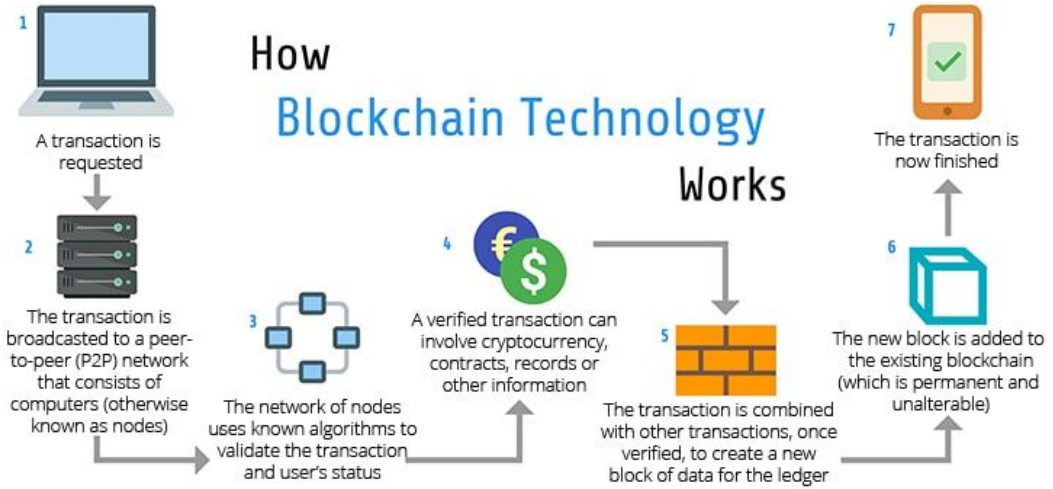
Blockchain csomópont

- FULL node:
- MINING node:
- EVM: szerződések kezelése
- Memory pool: vizsgálandó szerződések
- Client process: tranzakciók vizsgálata
- Blockchain DB: tranzakciók helyi másolata
- Mining node: új tranzakciók elfogadása
-



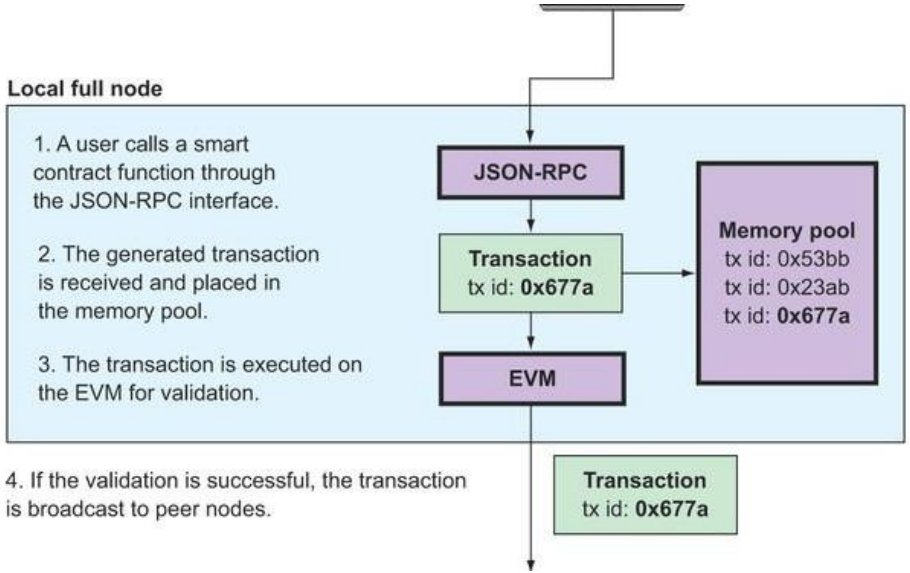
Blockchain tranzakció

- nincs állapot leíró (csak INSERT)
- a tranzakció a korábbi tranzakciókra épül
- validáció: a hivatkozott tranzakciók ellenőrzése
- a validált tranzakció beépül a rendszerbe (titkosítva)
- a rendszeren belül mindenki megkapja



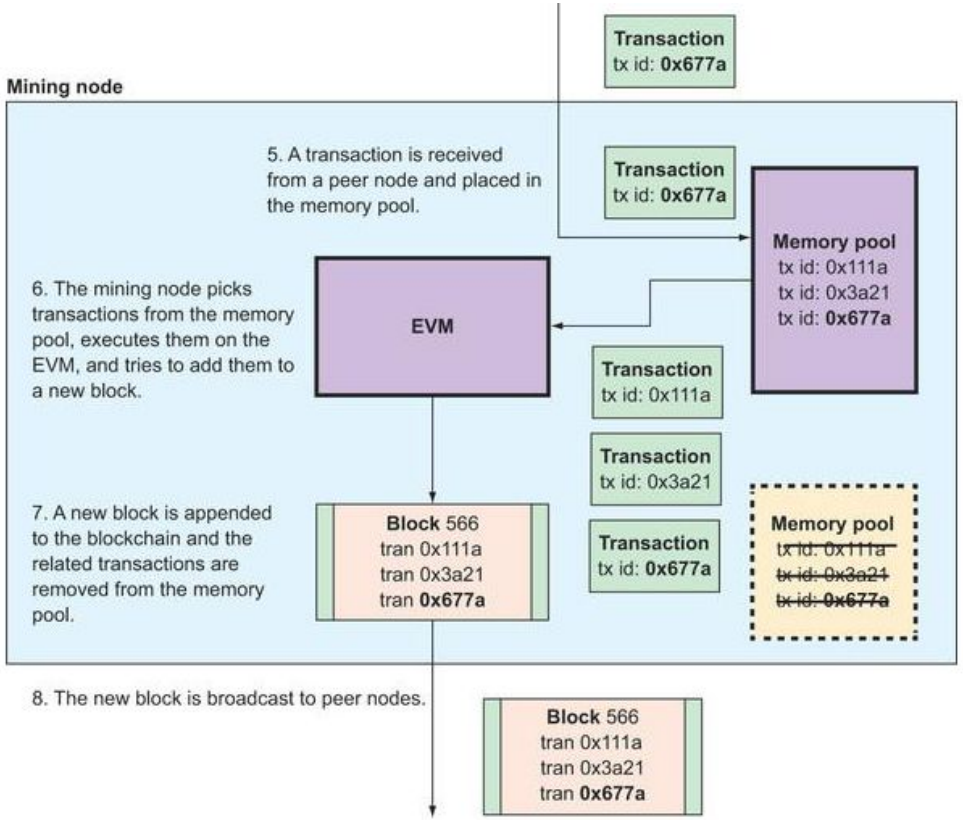
Tranzakciók életciklusa

- a kliens szerződés igénylést küld
- képződik egy tranzakció, amely a várakozósorba kerül
- az EVM kiértékeli a tranzakciót
- ha elfogadott a tranzakció, elküldi többi csomópontnak
- a tranzakció átkerül egy Mining csomópontra



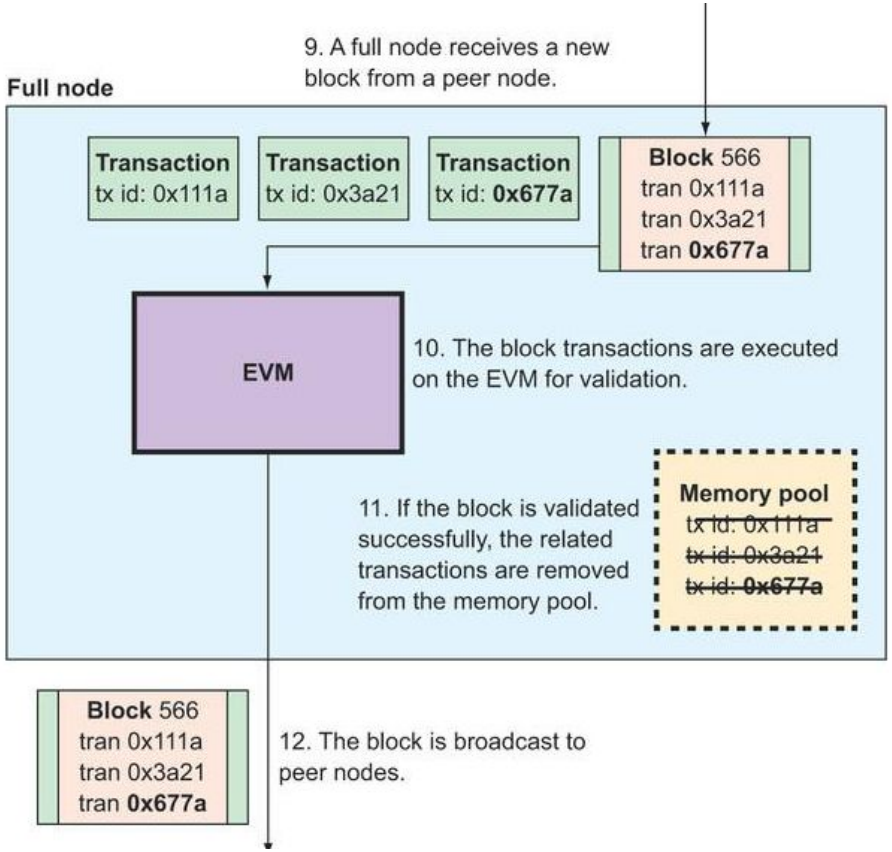
Tranzakciók életciklusa

- a Mining csomóponton a tranzakció bekerül a bufferbe
- az EVM kiválasztja az ígéretes tranzakciókat feldolgozásra
- az EVM végrehajtja a tranzakciót
- a tranzakció beépül egy új blokkba
- a blokk beépül a blokk láncolatba
- a blokk átkerül a többi csomópontra



Tranzakciók életciklusa

- a blokkot fogadja a csomópont
- a blokk minden tranzakciója végrehajtódik / validálódik a helyi EVM-ben
- sikeres validálás esetén a tranzakciók helyi példányai lezáródnak
- a blokk továbbítódik a többi blokk felé



Blockchain működése

A tranzakciók blokkokba kötegelve kerülnek feldolgozásra
- hatékonyság
- egyszerűség

Feldolgozás menete
- tranzakció bekerül, mindenki megkapja
- Egyes csomópontok a tranzakciókat összeállíthatják blokkba
- Kiválasztódik egy csomópont, amely a blokkot beküldheti a rendszerbe ellenőrzésre
- A kiválasztás konszenzus modell alapján történik
- A többi csomópont megkapja a blokkot ellenőrzésre
- Ha a többség elfogadja, bekerül a rendszerbe
- Elfogadásnál a jelölő csomópont nyereségre tesz szert
- Elutasítás esetén a jelölő csomópont veszít
- Az ellenőrzésnél hitelességet és helyességet vizsgálnak

Konszenzus modell : Proof of Work

- csak jelentős munka árán lehet valaki jelölt
- ha elutasítják, felesleges volt a munka
- ne legyen gyakori a nyerés
- sok számolás kell a nyeréshez
- kevés számolás kell az ellenőrzéshez
- Hash alapú kiválasztás
- Adott h()-val dolgozva, olyan x-et kell keresni, melyre h(x) adott értékű
- mining node

Konszenzus modell : Proof of Stake

- csak jelentős munka árán lehet valaki jelölt
- ha elutasítják, felesleges volt a munka
- a csomópontnak fel kell tennie bizonyos összeget, hogy javasolhasson
- a kiválasztás esélye arányos a feltett összeggel
- ha elfogadják a javaslatát, jutalmat kap
- ha elvetik a javaslatát, elveszti a feltett összeget
- gyors algoritmus

Alkalmazási területek

Kriptovaluák
- bitcoin
- ethereum
- tether