Blockchain technológia

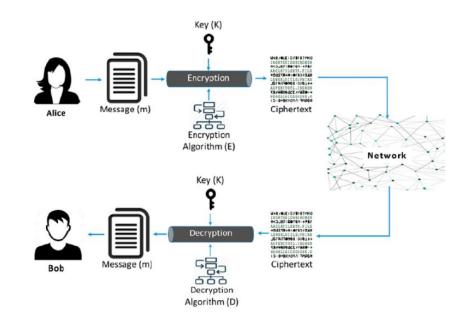
Információ védelmi modellek

Védelmi funkciók céljai:

- adatok titkosítása
- adat integritás védelem
- kliens hitelesítés
- eredeti állapot megőrzése

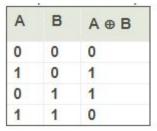
Kódolás és dekódolás

- egykulcsú vagy
- kétkulcsú
- adatfolyam vagy
- blokk kódolás



Egykulcsú védelem

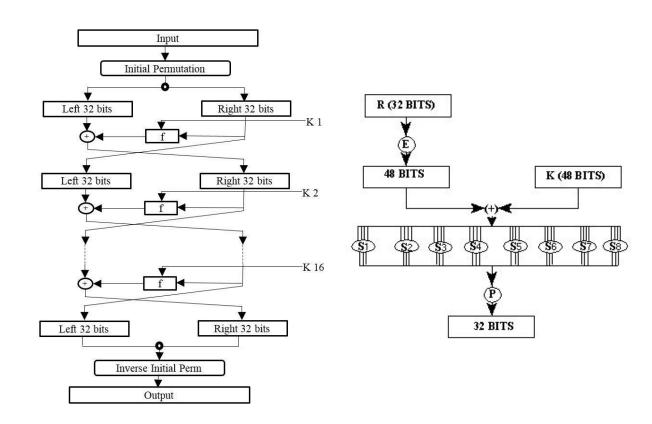
- a kulcs szimmetrikus szerepű (kódolás és dekódolás)
- hatékony algoritmusok
- hardver implementációk
- nagytömegű adatok kódolása
- DES : alap módszer
- XOR alapú
- probléma a kulcs megosztása



Secret N	Nessage
And a	a 64bit Key, that will be us
64bitKe	/
Resu	Iting in a Ciphertext:
0x7bd20	bb5497fd4ee2595dcc6adf0c930

DES titkosítás

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



Kétkulcsú védelem

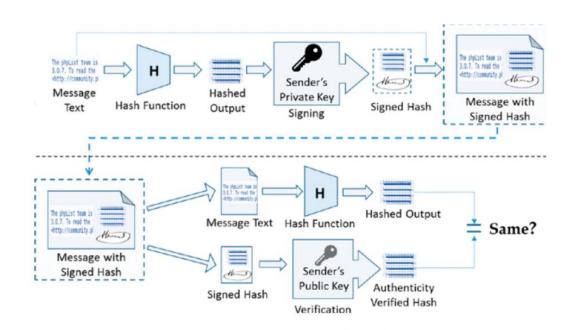
- egy kulcspár él, külön a kódolásra és külön a dekódolásra
- hatékony kódolás
- hardver implementációk
- számolás igényesebb
- kisebb méretű adatok kódolása
- RSA : alap módszer
- hatványozás, prímszám, moduló alapú
- kulcspárok generálása és kezelése

MIGeMA0GCSqGSlb3DQEBAQUAA4GMADCBiAKBqFGxPrv/tYokRmfvhD+15xTfBtBB i1sMi8U++Sn/h7pi9PY42PZdou+a99mvTSCHPZ0x5H1WXmCHPTKmHxRcElaKphfb oZWOdgt4VwxHBu0r3lUmG7lG11UgkXz46TxTYk/MT3jPZxZ8KWsEVXCgpp8kuEc5 a0hPFsbs5imABYSrAgMBAAE= MIICWwlBAAKBgFGxPrv/tYokRmfvhD+15xTfBtBBi1sMi8U++Sn/h7pj9PY42PZd ou+a99mvTSCHPZ0x5H1WXmCHPTKmHxRcElaKphfboZWOdgt4VwxHBu0r3lUmG7lG 11UqkXz46TxTYk/MT3jPZxZ8KWsEVXCqpp8kuEc5a0hPFsbs5imABYSrAqMBAAEC gYADIRxFLk+NwU19HVnVWWrK1YT8+QLdeU1f1wUiPFx9ZgjGC3QoSa7thwQ7fZ6K QKQJErkMbg8xeHzMjdBrGiZ3Uzd/iYdpnLILTS6sPt4o7NLPGYz8aJ2pkmHzTIU8 qdbTwilDdnBtGBjwuv2L9mocT4XnlpCN7Fuuj1QOqfr/cQJBAKD72G5AXSfZl8rQ Random numbe key generator algorithm US2smGVm5Hi72vtP/5GKl9iClpb75DIWSCtEF4FEv3KomK/uVnSHaUqWSkZwYFjT uWsorF8CQCB6LX7otsKimC1uTKtiWGDrzUkuqPrqAN3k9bVLRi/111dfrRAvVCG jxXAgO8aZnLxMjFxZwftyOE7p7owJks1AkAt1WZahYLATKdPIB5stZ4yCKh1425G bRFje6Ud5Hc6q37d79AeWWWjzVIAsBXAyUfeJ4uHy+Bby7TytV0uMEdbAkAhntli O36W1sM6pKhx8wkSrliDbcTP8Px0uQUzfl1YMCk51i3OR3CMsoE9peC7o2lB/CyB ndmWd5Oa/ciY54A1AkEAolgPBAd559n78Efvt6VUxvPTzvazJeWRZcPDaO9gBlKg C3ul6Qv8VSE/t1+FrEhsKZv/kK8XIVOCN+drEehu5w==

generator algorithm

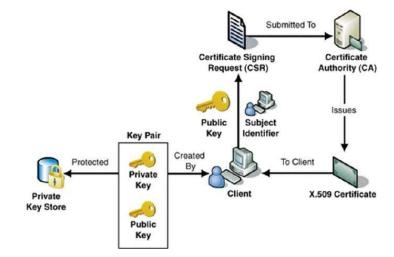
DSA titkosítás

- 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

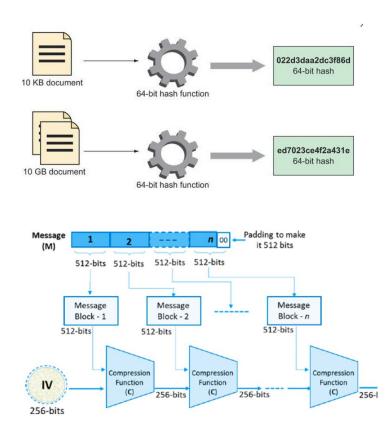
- biztonságos adatkezelés, adatküldés keretrendszere
- hálózati üzenetek titkosítása
- digitális aláírás
- kulcs-szerverek
- ujjlenyomat
- integritás ellenőrzés
- titkosítási primitívek



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

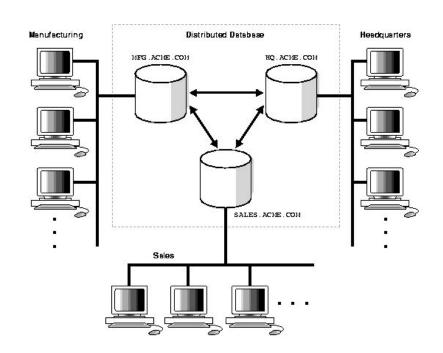
Digitális ujjlenyomat, Hash függvény

- 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



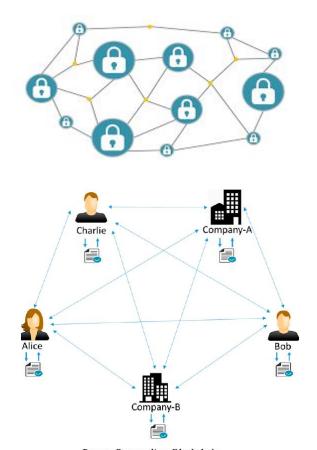
Elosztott DBMS, tranzakció

- 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

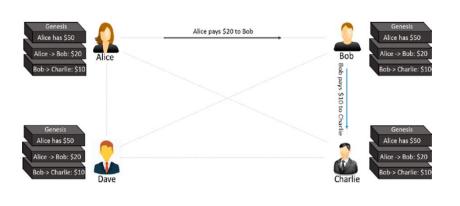
- 2018: Satoshi : "Bitcoin: A Peer-to-Peer Electronic Cash System"
- speciális elosztott adatbázis
- centralizált központi felügyelet kiváltása (nincs központi szerver)
- végrehajtott tranzakciók listája
- peer to peer tranzakciók
- hitelesség, megbízhatóság növelése
- minden tartalom megosztott, látható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

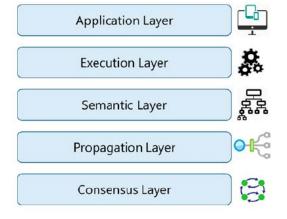


Peer-to-Peer trading: Blockchain

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



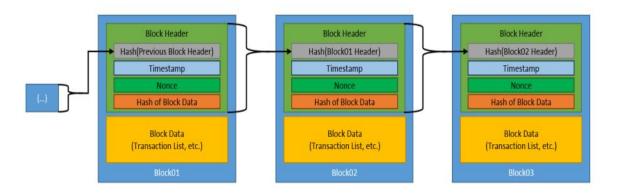


Blockchain adattárolás

- 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)

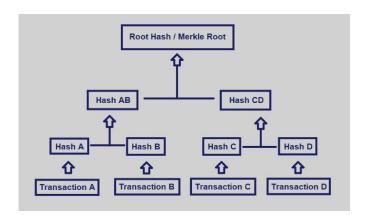
Block number: 234
Timestamp: 56237542657576
Previous block's hash: 9c25b3c178344c1d

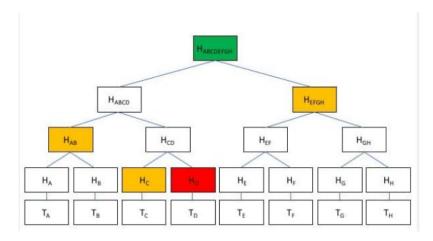
Transaction id:61f42b63-cb5c-48db
Amount: 9899.56
From: aa89c962-d4f8-48b9
To: 4d82b009-0ee1-4c56
Digital signature:e83a3d7539d84ed4



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

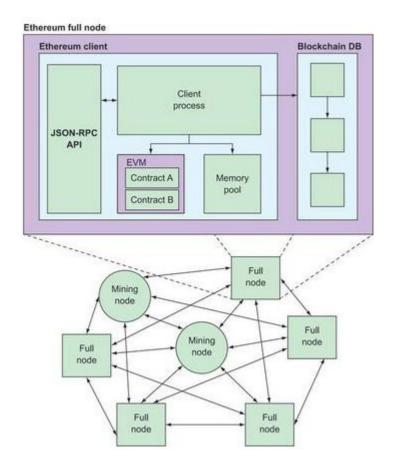




Blockchain csomópont

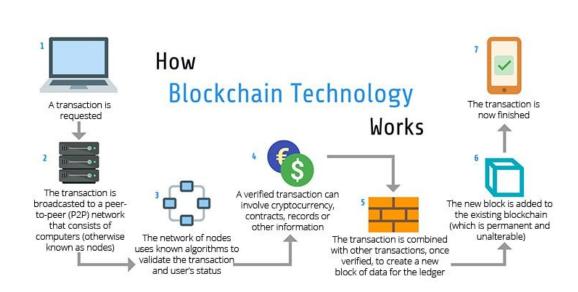
- FULL node:
- MINING node:
- EVM: szerződések kezelése
- Memory pool: vizsgálandó szerződések
- Client process: tranzakciók vizsgálata
- Blockchain DB: tranzakciók helyi másolata
- Mining node: új tranzakciók elfogadása

_



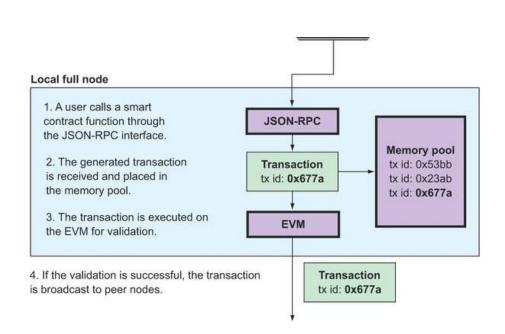
Blockchain tranzakció

- 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



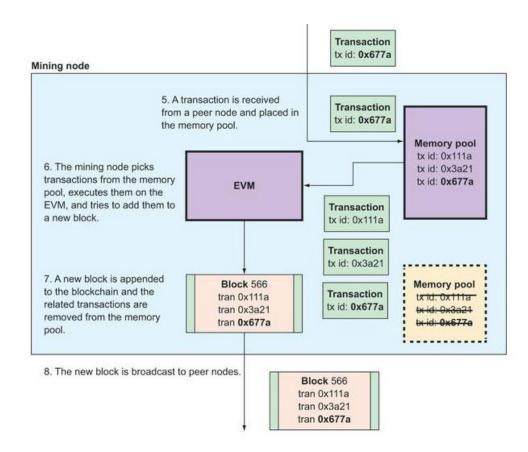
Tranzakciók életciklusa

- 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



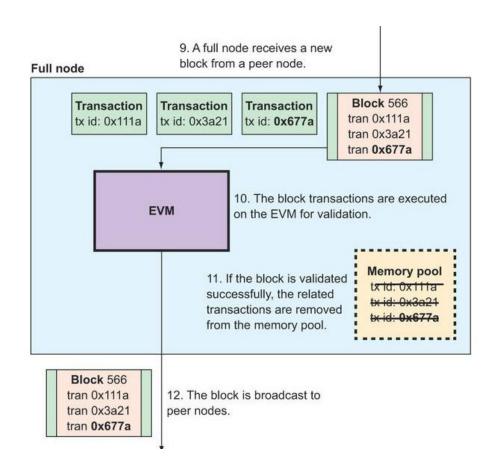
Tranzakciók életciklusa

- 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



1 Bitcoin egyenlő

2 593 746,93

1 N 5 N 1 H 1 É 5 É Max.

magyar forint

nov. 15. 07:10 UTC · Felelősségkizárás

1 Bitcoin

2593746.93

magyar forint

v

2593746.93