A bitcoin (illetve blokkchain) működése

Mi az a bitcoin, és hogyan működik? Honnan származik az értéke, illetve hogyan lehetséges egy központi autoritás nélküli, decentralizált működésű fizetőeszköz fenntartása? Ezekre a kérdésekre kíván választ nyújtani a jelen ismertető.

Cryptocurrency

A fenti fogalomnak megfeleltethető halmaz egyik első, és mára leginkább elterjedt eleme a bitcoin (vagy BitCoin, BTC. általánosságban azt lehet mondani, hogy a nagybetűs írásmód a konkrét fizetőezközt, míg a kisbetűs a protokollt, szoftvert stb. jelöli, az egyszerűség kedvéért a bitcoin, BitCoin, BTC írásmódot kölcsönösen helyettesíthetőnek tekintem). A cryptocurrency két alapvető kritériummal rendelkezik, nevezetesen, olyan fizetőeszközöket jelöl, melyek titkosítást használnak a, a tranzakciók biztosítására, és b, új egységek létrehozására. Több ilyen eszköz is létezik, melyek más-más elven működhetnek, a bitcoin csupán a legnagyobb karriert befutott a sokaságból.

BitCoin

Wallet & Address

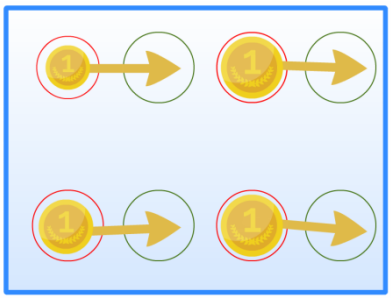
A bitcoin használatához voltaképp egyetlen alapvetődolog szükséges: egy pénztárca (wallet). Ez a bitcoin kliensen keresztül hozható létre. Egy wallet-hez több ún. cím(address) tartozhat, melyek egyfajta hídként szolgálnak a tárca tulajdonosa és a többi használó között. Az addressek mindig egy adott hosszúságú karaktersorozatból állnak, melyek véletlenszerűek, tartalmaznak kis-és nagybetűket, számot (látható tehát, hogy az egyes addresek mögötti személyek kiléténk felfedése pusztán ez alapján nem lehetséges). Továbbá, nemcsak, hogy egy wallethez több address is tartozhat, de technikailag n darab új address is létrehozható, akár minden egyes tranzakcióhoz. Minden ilyen addressnek saját bitcoin egyenlege van, értelemszerűen ezek összege a wallet egyenlege.

Private & Public keys

Ahhoz, hogy egy tranzakció sikeres legyen, szükség van egy kulcspárra, melynek egyik fele ún Private key, míg a másik Public key. (Ezek voltaképp egy-egy addresshez tartoznak, így egy walletet elképzelhetünk kulcscsomóként is) Amikor A személy(cég, alapítvány stb.) küldeni kíván x mennyiségű bitcoint B entitás címére, a kliens az A címéhez tartozó privát kulcsot használja „aláírásként”, majd, és itt az egyik lényeges elem, mivel a public key-ek minden, a hálózaton levő tag számára ismertek, bárki képes validálni, hogy az összeget valóban A küldte (hiszen a kulcsok minden esetben párosával jönnek létre, és egy private key-hez egy és pontosan egy public tartozik, azonban ez többek számára ismert).

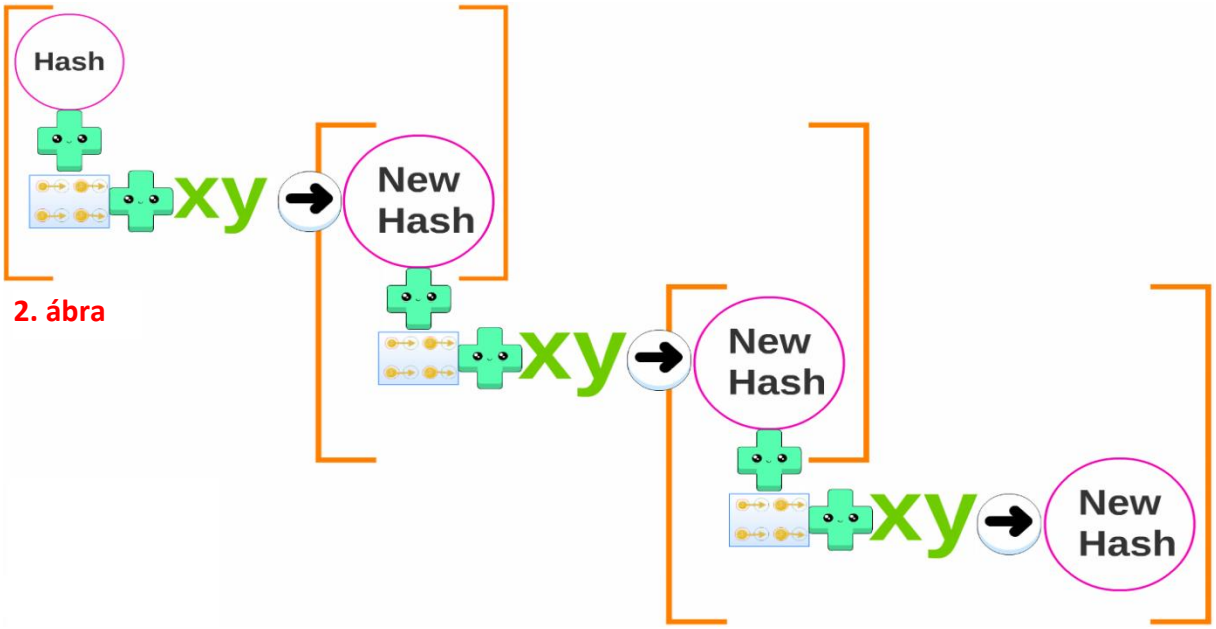
Verification

A tranzakciók érvényesítésének megértéséhez szükséges igazán a szárazabb, technikai leírása a technológiának, ám ebben rejlik a válasz arra a kérdésre, hogyan működhet egy decentralizált digitális fizetőeszköz. A válasz a blockchain, de ez odébb van. Az eddigi két szereplőn (küldő-és fogadó fél, a tranzakció két végpontja) kívül belép egy harmadik is, az ún. bányász (miner). Ők azok, akik számítógépeik (manapság egyéb hardware) számítási kapacitását használják a végbement tranzakciók érvényesítésére, ezt a folyamatot szeretném ismertetni a következőkben.



1. ábra

A bányászatra felállított számítógépek az elmúlt 10 perc tranzakcióit csomagolják össze blokkokba[1], továbbá „cryptographic hash" függvényeket számolnak. Ezek a magyarul hasítófüggvénynek nevezett eljárások tetszőleges n hosszúságú adatból fix, véges hosszal bíró karaktersort képeznek (ez a hash value). A kapott hash value egy véletlenszerű karaktersor, mely számokat és betűket szintúgy tartalmaz, illetve az eredeti adatsorban történő legkisebb módosítás is egy merőben új hash value-t eredményez. A bitcoin esetében ebben a folyamatban szerepet kap egy harmadik szereplő is, az ún. nonce, mely egy véletlenszerűen kreált szám, mely a hash-elés előtt adódik az eredeti adatsorhoz. Az imént leírtakhoz hasonlóan, a nonce megváltoztatása is merőben új



2. ábra

hash value-hoz vezet.

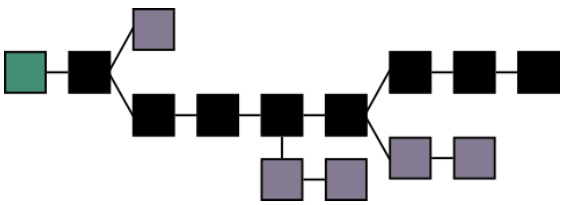
A bányászok számítógépei új hash value-kat számítanak az előző hash value, a tranzakciós blokk, illetve egy nonce kombinálásával[2]. Önmagában ezen új hash value-k létrehozása nem bonyolult, a bitcoin kliens azonban akkor fogadja el érvényesnek, ha egy adott számú nullával kezdődnek. Ezt (mennyi nulla szükségeltetik) a kliens automatikusan állapítja meg

[1] 1. ábra. Ez még nem a konkrét láncon szereplő blokk, helyesebb volna tán a csomag kifejezés.
[2] a folyamatot a 2. ábra szemlélteti. Ezen zölddel kiemelnve a nonce, kisebb méretben az 1. ábra, illetve maguk a blockchainen jelen lévő blokkok láthatók, melyeket a narancs keret(brace) szimbolizál.

egy adott nehézségi szint alapján (difficulty). Komolyabb elmélyedés nélkül azt mondhatjuk, hogy a difficulty minden 2016 létrejött blokk után változik, és aszerint nő vagy csökken, hogy az utolsó 2016 blokk megtalálása több, vagy kevesebb időt vett-e igénybe, mint 2 hét. Ha többet, úgy a difficulty csökken, ha kevesebbet, akkor növekszik.
A bányászoknak nincs módja arra, hogy megjósolják, mely nonce fog érvényes hash value-t létrehozni, így egyfajta brute force módon addig generálják a hash-eket, amíg az egyik nem működik.
Amennyiben ez bekövetkezik, és létrejön az új blokk, a megtalálónak a kliens adott számú bitcoint utal egy frissen létrehozott addressre jutalomként (ez az érték is változik, a korai időkben 50 BTC volt a jutalom, napjainkban 25 BTC).

Blockchain

Az imént említett blokkokból épül föl a blockchain, melyben a fentiek alapján minden blokk tartalmaz információt az őt megelőzőből (hash-t), az az őt megelőzőből, stb. Ez adja a biztonságát a szisztémának, hiszen ahhoz, hogy valaki átírjon egy, a láncba már beépült blokkot, új nonce-al kellene azt ellátnia úgy, hogy az is a megadott számú nullát produkáljon, majd, mivel ezáltal megváltozott az ezen blokkra alapuló hash, a következő blokkal kellene ezt a folyamatot eljátszania addig, míg effektíve minden blokkot újraírt a rendszerben, mindezt úgy, hogy mindeközben a teljes hálózat újakat hoz létre az aktuális láncon. Ekkora számítási kapacitás felhalmozása gyakorlatilag a lehetetlen kategóriájába tartozik. Erre egy érzékletes példa: 2010 december vége táján 1000 KiloHash/s sebességgel egy új blokk létrehozása kb. két évet vett volna igénybe. Összehasonlításképpen, egy mai, újabb szériás Intel i7 processzor nem képes többre, mint 100 KiloHash/s. (Ez vezetett oda, hogy külön cégek alapultak arra a célra, hogy BTC-bányász hardware-t fejlesszenek, melyek ezen kívül másra nem igazán használhatóak, de ebben messze felülmúlják a számítógép hagyományosan bányászatra használt részeit (CPU ill. GPU). Szintén egy példa: nagyjából 40 dollárért online rendelhetőek olyan eszközök, melyek 63 GigaHash/s sebességgel bányásznak, és ezek nem is számítanak felsőkategóriásnak) Maga a blokklánc mindig az ősblokktól (genesis block) számított leghosszabb útvonalat jelenti a teljes fán. Elképzelhetőek árvablokkok, de ezek maximum két lépésig tudnak elágazni normális esetben, ez akkor fordulhat elő, ha nagyon rövid időn belül két blokk is létrejön egy anyablokkból, a kettőből azo fut majd tovább a lánc, amelyre építve előbb létrejön egy új.



A BitCoin jövője

Nehéz biztosat állítani a technológia jövőjéről. Azaz opntosabban, a BTC jövőjéről. Az bizonyos, hogy a maximálisan forgalomba kerülő mennyiség nagyjából 20-21 millió BTC, eztán a blokklétrehozás nem fog újakat adni. Felmerül két kérdés persze, az egyik, hogy lehet 1 BTC-nél olcsóbb dolgokat ezzel vásárolni, illetőleg, mi lesz az ösztönző, ami a rendszer fenntartásában érdekeltté teszi a hálózaton lévőket. Az első kérdésre egyszerű a válasz, egy BTC 8 tizedesjegyik váltható, ezt nevezik 1 Satoshi-nak, a BitCoin kvázi létrehozója után (mint ismeretes, ez egy álnév, nincs konkrét információnk a személy/személyek valódi kilétéről). A rendszer fenntartására vonatkozó kérdésre a technológia támogatói által leggyakrabban elhangzó válasz az ún. transaction fee egyre széleskörűbb alkalmazása, mely idővel akár jövedelmezőbb is lehet, mint a megtalálónak járó puszta jutalom, és már ma is általánosan használt. A transaction fee úgy működik, hogy amikor A vásárolni kíván egy terméket, szolgáltatást stb. B-től, a bitcoin kliensben a tranzakcióhoz hozzárendelhet, önkéntes alapon, plusz díjat, ez a transaction fee. Ez több szempontból módosítja a blokklétrehozást, illetve az arra irányuló motivációt. Elsősorban, a bányászó számítógépek új blokk összeállításakor elsőként azokat a tranzakciókat veszik be a csomagba, amelyeknek a hozzárendelt transaction fee-je a legnagyobb, tehát az eredeti küldő is érdekelt abban, hogy egyáltalán hozzárendeljen egy ilyen összeget a tranzakciójához. Másrészt, az új blokk sikeres létrehozásakor, a blokkban szereplő összes tranzakcióhoz rendelt transaction fee-k összege a megtalálóhoz kerül, az új blokk emgtalálásáért járó jutalomhoz hasonlóan. Látható tehát, hogy a puszta használók is érdekeltek ennek a díjnak a fizetésében, és a bányászók továbbra is érdekeltek a végbemenő tranzakciók verifikálásában. Az, hogy ez valójában elegendő lesz-e a hálózat fennmaradásához, valószínűleg csak akkor derül majd ki, ha már elértük a BTC-k számának felső limitjét.
(Arra a kérdésre, hogy honnan származik a bitcoin értéke, a válasz nagyjából annyi, hogy egyrészt az előállítás nehézsége, a mennyiségének felső limitje (e kettőben hasonlatos az aranyhoz, innen ered a bányászat kifejezés használata a tranzakció-verifikálásra), illetve a használók puszta léte adja, megtámogatva a blockchain megváltozhatatlanságával.)
A blockchain-technológia talán ígéretesebbnek tűnik, mint a rá alapozott fizetőeszköz. Banki, önkormányzati, állami adminisztráció mind szóba kerülhetnek, mint potenciális felhasználási területek (már ma van olyan ember, aki leányának születési anyakönyvi kivonatát a BTC blockchain-be ágyazta). A kérdés mélyebb feltárása a szerző részéről még várat magára, mint ahogyan más, a cryptocurrency halmazába tartozó fizetőeszközök behatóbb ismertetése is.

Összegzés

Noha a bitcoin kibocsátási görbéje napjainkban (2016) túl van a fordulóponton, és az üteme csökkenőben van, a mainstream használata manapság kezd csak igazán elterjedni, főleg Magyarországon. Nem csupán emiatt lehet érdekes megismerkednünk a technológiával, hanem az általa terjedő blokklánc miatt is, melyben talán még nagyobb potenciál rejtőzik, illetve pont a technológia beható ismeretének alacsony aránya miatt, nem kizárható a rossz szándék felszínre kerülése sem. Jelen dolgozat pusztán a fizetőeszköz működését mutatta be a teljesség igénye nélkül, lévén szerzője „kvázi laikus", a fizetőeszköznek a feketekereskedelemmel, motivációs elméletekkel, ideológiákkal, más crypto-fizetőeszközökkel való összevetése nem kis feladat, de legalább ennyire érdekesnek, és ígéretesnek látszik.

Források:

- http://www.coindesk.com/meet-the-dad-who-registered-his-daughters-birth-on-the-blockchain/
- https://en.bitcoin.it/wiki/Controlled_supply
- https://en.bitcoin.it/wiki/Block_chain
- https://www.cryptocoinsnews.com/wp-content/uploads/2013/12/how-bitcoin-works.jpg
- https://en.wikipedia.org/wiki/Cryptographic_hash_function
- https://en.bitcoin.it/wiki/Main_Page
- http://prezi.com/9xi3whaabied/?utm_campaign=share&utm_medium=copy&rc=ex0share