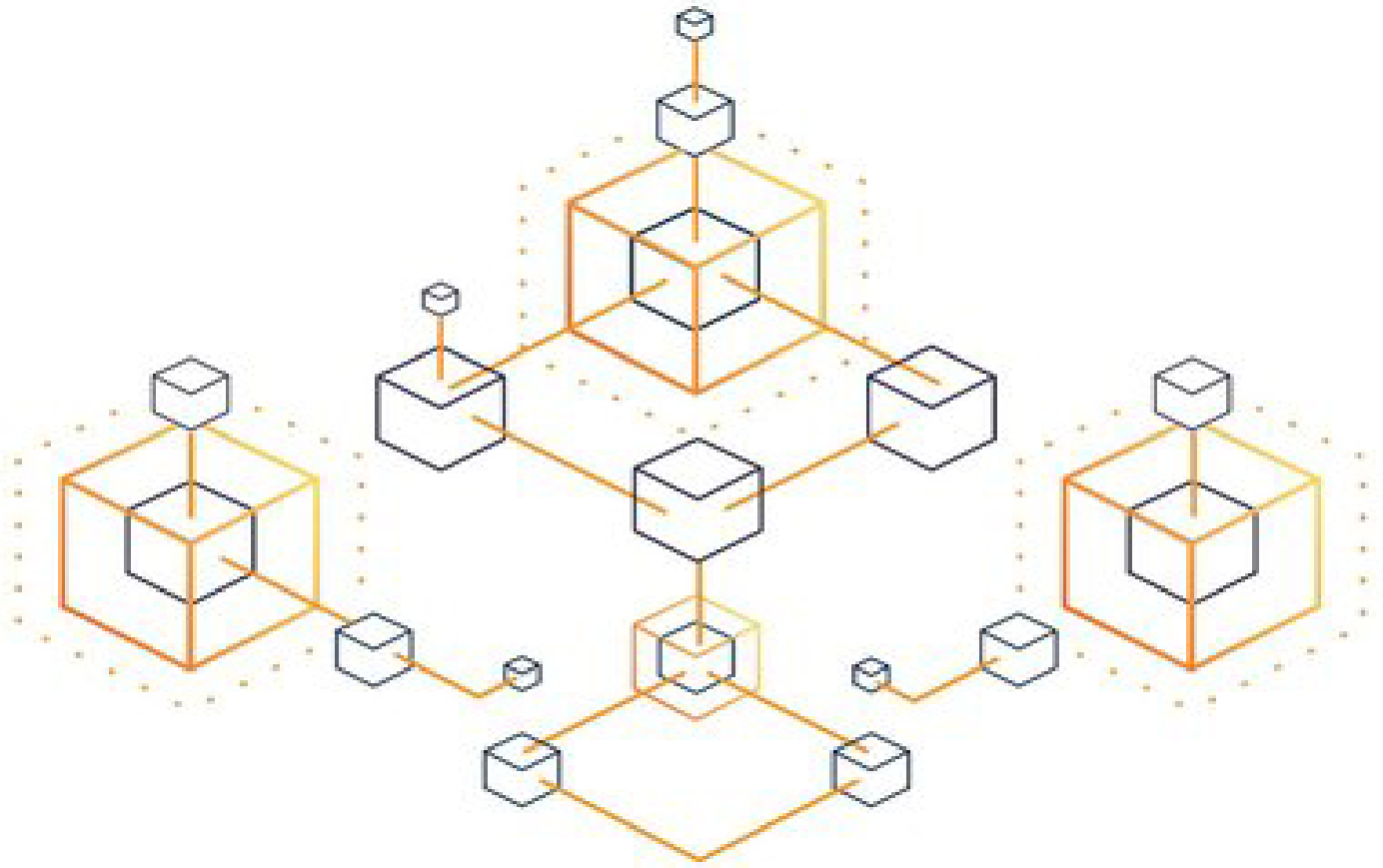
A BITCOIN LÉTREHOZÁSA



A TECHNOLÓGIA A VILÁG ELSŐ, VALÓBAN DECENTRALIZÁLT, LIMITÁLT KÉSZLETŰ PÉNZE MÖGÖTT

Yan Pritzker

YAN PRITZKER

A BITCOIN LÉTREHOZÁSA

A TECHNOLÓGIA A VILÁG ELSŐ, VALÓBAN DECENTRALIZÁLT, LIMITÁLT KÉSZLETŰ PÉNZE MÖGÖTT

A legfrissebb, angol nyelvű verziót az inventingbitcoin.com oldalról töltheted le.

Ajánlom ezt a könyvet Yury és Lana részére, szüleimnek, akik kimenekítették a családunkat a korábbi Szovjetunióból, a diktatorikus szocialista rezsimből, ahol szigorú kontroll alatt tartották a pénzügyeket.
Emellett ajánlom feleségemnek, Jessica-nak is, akinek el kellett viselnie, hogy állandóan a Bitcoinról beszélek, és későig fennmaradok, hogy megírjam ezt a könyvet.

Tartalom

BEVEZETŐ

Mikor a többség először hall a Bitcoinról, sokszor még azelőtt véleményt alkot róla, hogy ténylegesen megismerné. Rengeteg az információ a területtel kapcsolatban, az embert könnyen félre lehet vezetni, hogy mi is a Bitcoin, és hogyan működik. Egészen három évvel ezelőttig én is így voltam. Hogy miért döntöttem ennek a könyvnek a megírása mellett? Az elmúlt húsz év során tech startupokat hoztam létre. Minden egyes nap az új technológiákkal foglalkoztam, és elég jó lettem abba, hogy rájöjjek dolgokra. Még így is öt év telt el az első találkozás után, hogy leüljek, és megpróbáljam megérteni a Bitcoint. Úgy érzem, nem csak nekem lehet hasznos, ha kicsi jobban feltárjuk ennek a világot potenciálisan nagyon megváltoztató innovációnak a hátterét.

Először 2011-ben hallottam a Bitcoinról a slashdot.org-on, egy kockáknak szóló híroldalon. Éppen akkor tetőzött az árfolyam, egy hatalmas növekedéssel egészen 30 dollárig emelkedett. Annyit lehetett tudni az egészről, hogy néhányan az interneten összeálltak, hogy egy újfajta P2P fizetési rendszert hozzanak létre. Anélkül, hogy bármi mást tudtam volna róla, hogy hogyan működik, hogyan jött létre, vagy akár arról, hogy hogyan működik a befektetések világa, és milyen ciklikus a piac, eldöntöttem, hogy vásárolok valamennyit, ha idővel növekedne a fontossága. Egy rettenetesen kinéző weboldalt kellett használnom, amelyet úgy hívtak, hogy Mt.Gox, később erről a dollár-bitcoin közötti váltási lehetőségről a csődje miatt lehetett sokat hallani.

Szép lassan végignéztem, ahogy a kezdeti befektetésem elolvad, mikor az ár 30 dollárról egészen 2 dollárig esett. Egy ponton pedig meg is feledkeztem róla, és éltem tovább az életem a startupokon dolgozva, nem is sejtve, hogy mi a helyzet a coinokkal. Azt hiszem a kulcsok egy régi laptop merevlemezén voltak akkor, amely a kacatok között feküdt.

2013-ban hallottam a Bitcoinról ismét, a médiavisszhangja jóval hangosabb volt, és a vásárlási lehetőségek komoly fejlődést mutattak. Már létezett a Coinbase, és legitim vállalkozásnak látszott. A Mt.Gox-hoz hasonlítva ez

jelentős minőségbeli ugrásnak számított, és úgy tűnt, hogy ebből a Bitcoinból lehet valami.

Biztos, ami biztos alapon, és még mindig semmit sem tudva a dolog hátteréről, ismét bevásároltam a csúcson. Ezután az 1000 dolláros coinjaim lassan egészen 200 dollárig csúsztak. Ekkor úgy döntöttem, hogy ennyi pénzért nem érdemes törnöm magam az eladással, így inkább nem foglalkoztam a dologgal tovább. Minden energiámat az új cégemre, a Reverb.com-ra fordítottam.

A következő négy év során a Reverb nagyot növekedett, az első számú választás lett a zenészek között. Változást hoztam a világba, és a technológiai vezetője voltam egy gyorsan növekvő tech-cégnek. Azzal foglalkoztam, ami a szenvedélyemnek számított, és nem érdekelt az internetes pénz.

Őszintén be kell vallanom, hogy 2016-ban néztem meg az első videót Andreas Antonopoulos előadásában, amelyik megragadta annyira fantáziám, hogy leüljek, és odafigyeljek rá. Elkezdtem feltenni a fontos kérdéseket. Honnan jön a Bitcoin? Ki irányítja? Hogyan működik? Mi az a bányászat? Milyen hatása lesz a világra?
Elkezdtem elolvasni mindent, amihez csak hozzájutottam, a podcast- és videófogyasztásom napi több órányira nőtt, és másfél évig ezt csináltam.

Végül 2018 elején, miután az árfolyam beállította az új rekordot 20000 dolláron, eldöntöttem, hogy otthagyom a Reverb kötelékét, hogy amennyire tőlem telik, segítsem a Bitcoin elterjedését. Miért döntöttem úgy, hogy elhagyom a nagyon is sikeres saját cégemet, hogy a Bitcoinon dolgozzak? Úgy hiszem, a Bitcoin megjelenése az olyan dolgok közé tartozik, amelyek egyszer történnek egy életben, vagy akár még hosszabb idő alatt.

A Bitcoin sikere ahhoz mérhető fontosságú, mint a nyomtatott sajtó megjelenése, amely decentralizálta az információ előállítását. Vagy akár az internet, amely decentralizálta a tartalomfogyasztást és a kommunikációt, de a több pilléren nyugvó, jelenlegi demokratikus társadalmaink is ilyen

dolognak számítanak. Azt remélem, ha megérted, hogy hogyan működik a Bitcoin, meg fogod érteni, hogyan változtathatja meg a világot. A Bitcoin decentralizálja a pénzt, ez pedig olyan új útjait nyitja meg a tömeges együttműködésnek, amelyre az emberiség történelmében még nem volt példa.

A médiában a Bitcoinról főleg az árfolyama kapcsán hallhatsz. Egyik nap egymillió dollárig emelkedhet, aztán másnap egészen nulláig zuhan. Az is lehet, hogy a világ teljes energiatermelését el fogja használni, és 10 éven belül pedig elpusztul miatta a bolygó. Természetesen ezek az állítások nem igazak, ha pedig megérted, hogyan működik a rendszer, remélhetőleg ezt te is belátod. Megérted majd azt is, hogy az árfolyam-lufik miért számítanak a legkevésbé érdekes dolognak a Bitcoinnal kapcsolatban.

Nem célom ezzel a könyvvel, hogy elemezzem a bitcoin, mint értékálló, stabli pénz ökonómiai szerepét, bár futólag szóba kerül ez is majd egy későbbi szakaszban. Nem fogok a bitcoinról befektetési szempontból beszélni, és nem akarok senkit meggyőzni arról, hogy érdemes lenne egy kicsit birtokolni belőle. Ha valakit jobban érdekel ez a téma, akkor ajánlott elolvasni a magyarul is elérhető The Bitcoin Standard című könyvet Saifedean Ammous tollából. Nem fogunk a számítástechnikai részével sem foglalkozni a dolognak, és nem szükséges programozói ismeret, hogy megértsd ezt a könyvet. Ha ez a téma érdekel jobban, akkor az angol nyelvű Mastering Bitcoin Andreas Antonopoulos-tól, illetve a szintén angol nyelvű Programming Bitcoin Jimmy Song-tól lehet a jó választás.

Számomra egyfajta megvilágosodással ért fel, mikor összeállt a kép, hogy a számtalan alkotóelem hogyan formálja a Bitcoin működését. Remélem ezt a tudást sikerül rövid, érthető formában megosztanom veled. Az a célom, hogy felkeltsem a figyelmed, és adjak egy ízelítőt a számítástechnika, a közgazdaságtan, és a játékelmélet hármasából, amelyeknek köszönhetően a Bitcoin talán a jelen korunk legizgalmasabb, legfontosabb találmánya.

Ha megérted, hogyan működik a Bitcoin, rájössz, hogy sokkal többről van szó, mint amennyi elsőre látszik, és lehet, hogy a világ elkövetkező generációinak életére hihetetlen hatással lesz.

Lassan fogunk haladni. Középiskolai szintű matematikai ismereteknél többre nem lesz szükséged, amikor lépésről-lépésre végigmegyünk a Bitcoin létrehozásán. Ez remélhetőleg elég inspirációt fog nyújtani számodra, hogy aztán még mélyebbre merészkedj a nyúl üregébe. Szóval kezdjünk hozzá!

MI A BITCOIN?

A Bitcoin egy P2P, peer-to-peer, azaz közvetlenül a felhasználókat összekapcsoló elektronikus pénz, egy újfajta digitális pénznem, amelyet az emberek vagy a számítógépek közvetítő, például bank nélkül tudnak egymás között küldeni, és amelyik kibocsátását nem egy központi szereplő irányítja.
Gondoljuk át, hogyan működnek a bankjegyek és a pénzérmék. Amikor pénzt adsz egy másik embernek, nem kell, hogy ismerjen téged. Annyit kell csak tudni, hogy az általad átadott pénz nem hamis. Ezt egyszerűen úgy ellenőrzi, hogy megnézi, megvizsgálja a pénzt, nagyobb mennyiség esetén akár valamilyen speciális eszközzel. Ahogy a társadalom egyre inkább digitalizálódik, úgy a pénzmozgás is egyre gyakrabban az interneten keresztül történik, valamilyen közvetítő segítségével. Az ilyen szolgáltatók például a Visa, mint kártyakibocsátó, a PayPal, mint digitális fizetési szolgáltató, de a WeChat Pay, a kínai online közösségi platform fizetési megoldása is így működik.

A digitális fizetés esetén viszont szükség van egy központi szereplőre, hiszen meg kell bízni valakit, aki ellenőrzi, engedélyezi, és igazolja a fizetéseket. Erre azért van szükség, mert a pénz formája megváltozott, már nem egy fizikai, kézzelfogható tárgy, amelyet a saját szemeddel ellenőrizhetsz, amelyet magaddal vihetsz, és átadhatsz másoknak. A pénz most már digitális bitek formájában létezik, adatbázisokban, ezt valakinek tárolnia kell, az átutalásokat pedig adminisztrálni, igazolni.
Mikor feladtuk a fizikai készpénzt a digitális fizetés nyújtotta kényelemért cserébe, ennek árnyoldalaként egy olyan rendszert hoztunk létre, amely különleges hatalmat biztosíthat azok számára, akik ezt rosszra használnák. A digitális fizetési platformok mára a disztopikus autoriter irányítási rendszerek alapjaivá váltak. A kínai kormány esetében például megfigyelik a disszidenseket, de a saját állampolgáraikat is, és aki nem viselkedik az elvárt módon, az egyszerűen nem vehet igénybe bizonyos szolgáltatásokat, nem vásárolhat meg bizonyos termékeket.

A Bitcoin egy alternatívát kínál a központilag irányított digitális pénzek helyett, amely visszaadja nekünk a hétköznapi, emberek közötti készpénzhasználat jellegzetességeit, de immár digitálisan, az alábbi formában:

- Egy digitális pénzeszköz, a bitcoin (kis „b” kezdőbetűvel magát a kriptopénzt jelenti, a Bitcoin nagy „B” betűvel pedig a hálózatot), amelynek a készlete korlátozott, pontosan megállapítható, és megváltoztathatatlan. Ez az ellentéte a bankjegyek és a digitális egyenlegek mögött álló kormányzati, központi banki, úgynevezett fiat pénzeknek, amelyek készletét előrejelezhetetlen, követhetetlen módon tudják megváltoztatni.
- Egy összekapcsolódott számítógépekből álló hálózat, a Bitcoin blokklánc, amelyhez bárki csatlakozhat a megfelelő program futtatásával. Ez a hálózat felel a bitcoin kibocsátásáért, a tulajdonviszonyok felügyeletéért, és ellenőrzi a tranzakciókat anélkül, hogy ehhez bármilyen közvetítő, legyen az bank, fizetési szolgáltató, vagy akár kormányzat, szükséges lenne.
- Egy Bitcoin kliens-program, egy szoftver, amelyet bárki futtathat a saját számítógépén, a hálózat fenntartójává válva. Ez a program nyílt forráskódú, tehát bárki meggyőződhet a működéséről, közreműködhet az új funkciók hozzáadásában, vagy a hibák kijavításában.

A Bitcoin egy számítógép-hálózat, amely a Bitcoin programot futtatja.

A következő szakaszban részletesebben körüljárjuk, hogy mi motiválta a hálózat létrehozását.

Hogyan jött létre?

A Bitcoin feltalálója a magát Satoshi Nakamotoként nevező személy (vagy csoport), 2008 környékén kezdett el dolgozni a Bitcoinon. Senki sem ismeri Satoshi valódi személyazonosságát, és amennyire tudjuk, az eltűnése óta eltelt években semmit sem hallatott magáról.

2009 februárjában egy főleg cypherpunk beállítottságú online fórumon osztotta meg a rendszer első változatát, egy fórumon, ahol a tagok közös érdeklődési körébe tartozott a kriptográfia, valamint az aggodalom a személyes magánszféra, és a szabadság iránt.
Nem ez számít a Bitcoin első, úgymond hivatalos hirdetményének, de nagyon jól összefoglalja Satoshi motivációit, így jó alapot nyújt a rendszer megismeréséhez. El is olvashatod a vonatkozó részt a fórumbejegyzéséből, és bizonyos részek kiemelésével megérthetjük, milyen problémákat azonosított Satoshi a jelenlegi pénzügyi rendszerben, amelyeket a Bitcoin létrehozásával megoldott.

„Létrehoztam egy nyílt forráskódú P2P elektronikus pénzrendszert, amelyet Bitcoinnak neveztem el. Teljesen decentralizált, nincs központi szerver vagy harmadik fél, mivel nem a bizalmon alapul, hanem kriptográfiai eljárásokon.
A hagyományos pénzekkel az a fő probléma, hogy bíznunk kell bennük, hogy működjenek. A központi bankokban is meg kell bíznunk, hogy nem fogják leértékelni a pénzünket, a fiat valuták története viszont tele van példákkal ennek a bizalomnak az elárulásáról.
Meg kell bíznunk a bankokban, hogy tárolják és kezelik a pénzünket, ehelyett a letétek töredékét adják csak a kihelyezett hiteleknek, amelyek hullámokban formálnak buborékokat. Bíznunk kell abban, hogy tiszteletben tartják a magánszféránk, és megakadályozzák, hogy személyiség-tolvajok kiürítsék a számlánkat. A hatalmas járulékos költségek lehetetlenné teszik a mikrofizetéseket.

Egy generációval ezelőtt a többfelhasználós számítógép-rendszerek hasonló problémával küzdöttek. Az erős titkosítási megoldások megjelenése előtt a fájlok biztonságát csak a jelszavak védték. Aztán a titkosítás bárki számára elérhetővé vált, így már nem kellett a jelszavakban megbízni. Az adatok olyan módon lehetnek immár biztosítva, hogy fizikailag nincsen mód rá, hogy illetéktelenül hozzáférjenek, semmilyen okból, semmilyen kifogás mögé bújva, semmilyen esetben.
Eljött az idő, hogy ugyanez a pénzzel is megtörténjen. Legyen egy kriptográfiai eljárásokon alapuló e-pénz, amelyhez nem kell megbízni senkiben, és amelyik könnyen tranzaktálható, biztosítható.
A Bitcoin ezt oldja meg egy P2P hálózat segítségével, amely ellenőrzi a dupla költést. Dióhéjban megfogalmazva egy elosztott időbélyegző-szerverként működik, amelyik meghatározza, hogy mikor lett elköltve egy adott coin. Azt használja ki, hogy az információt természeténél fogva nagyon könnyű terjeszteni, viszont nehéz megállítani.
Ha a részletekre is kíváncsi vagy, hogy hogyan működik, az alábbi címen megtalálod a bővebb kifejtését: http://www.bitcoin.org/bitcoin.pdf"

SATOSHI NAKAMOTO

Milyen problémát old meg?

Nézzük meg Satoshi bejegyzésének egyes szakaszait! A könyv további fejezeteiben végigmegyünk rajtuk, hogy ezek az ötletek hogyan működnek a valóságban. Ne aggódj, ha egyes részek még homályosak maradnak, a későbbiekben részletesebben foglalkozunk mindennel. Most az a lényeg, hogy lássuk Satoshi céljait, és lássuk, hogyan érte el ezeket a Bitcoin létrehozásával.

„Létrehoztam egy nyílt forráskódú P2P elektronikus pénzrendszert…"

A P2P a peer-to-peer rövidítése, a felhasználók közötti közvetlen kapcsolatot jelenti. Az ilyen rendszerben az egyes résztvevők anélkül léphetnek interakcióba, egyenlő félként, hogy ehhez közvetítőre lenne szükség. Az olyan fájlmegosztó technológiák esetén is ilyent használnak, mint amilyen régen a Napster vagy a Kazaa volt, jelenleg pedig a BitTorrent

működik ilyen módon. Ez a megoldás lehetővé teszi, hogy a felhasználók zenéket és filmeket osszanak meg egymással közvetlenül. Satoshi a Bitcoin létrehozásakor ugyanezt a módszert követte, így az emberek ugyanígy tudnak elektronikusan pénzt küldeni egymásnak, közvetítő nélkül.
A szoftver nyílt forráskódú, tehát bárki meggyőződhet róla, hogy hogyan működik, ráadásul közreműködhet a fejlesztésében. Ez azért fontos, mert így arra sincsen szükség, hogy bízzunk Satoshiban. Semmit sem kell elhinnünk abból, amit Satoshi írt a program működéséről, hiszen mi magunk is ellenőrizhetjük a kódot. Még akár jobbá is tehetjük, ha hozzáadjuk a saját fejlesztéseinket.

„Teljesen decentralizált, nincs központi szerver vagy harmadik fél…”

Satoshi kifejezte, hogy a rendszer teljesen decentralizált, világossá téve a különbséget a központi irányítással működő rendszerekkel szemben. Előtte is próbálkoztak már digitális pénz létrehozásával, David Chaum megalkotta a DigiCash-t, de ez egy központi szerver segítségével működött, ez a számítógép felelt a kibocsátásért, a tranzakciók igazolásáért, és egy cég fennhatósága alatt állt.
Az ilyen központosított, magánkibocsátású pénzek elkerülhetetlenül bukásra vannak ítélve. Az emberek nem bíznak meg egy olyan pénzben, amelyik egyik napról a másikra eltűnhet, ha a cég csődbe megy, hackerek támadják meg, összeomlik az informatikai rendszere, vagy a kormányzatok egyszerűen lekapcsoltatják.

A Bitcoin ezzel szemben nem egy központi szereplőtől függ, hanem magánszemélyek és cégek által van fenntartva, akik az egész világon mindenhol ott vannak. Ahhoz, hogy a Bitcoint le lehessen kapcsolni, világszerte több tízezer számítógépet kellene lekapcsolni, ezek közül sokról pedig azt sem tudni, hogy fizikailag hol található. Egyszerűen reménytelen, sziszifuszi munka lenne, ráadásul arra ösztönözné az embereket, hogy újabb és újabb csomópontokat, számítógépeket kapcsoljanak be a hálózatba a leállítottak helyett.

„…nem a bizalmon alapul, hanem kriptográfiai eljárásokon…”

Az internet, ahogy az összes modern számítógép-hálózat, a kriptográfián, a titkosításon alapul. Ez teszi lehetővé, hogy az adatokhoz nem férhet hozzá bárki, kizárólag a címzett tudja dekódolni, és így értelmezni azokat. Hogyan oldja meg a Bitcoin, hogy ne kelljen megbízni senkiben? Egy későbbi fejezetben ezt részletesebben is körüljárjuk, de rövid összefoglalásként elmondhatjuk, hogy kriptográfiával oldja meg. Ahelyett, hogy el kellene hinnünk valakinek, amikor azt mondja, hogy „helló, Alice vagyok, és van 10 dollár a számlámon", matematikai műveletek segítségével tudunk megbizonyosodni ezekről a tényekről. A lényeg, hogy a címzett könnyen ellenőrizni tudja a hitelességet, miközben az információ nem hamisítható meg.
A Bitcoin által használt kriptográfia a matematika segítségével biztosítja, hogy a hálózat résztvevői leellenőrizhetik minden más résztvevő őszinteségét anélkül, hogy ehhez egy megbízható központi szereplőre lenne szükség, aki kezeskedik másokért.

„Bíznunk kell abban, hogy [a bankok] tiszteletben tartják a magánszféránk, és megakadályozzák, hogy személyiség-tolvajok kiürítsék a számlánkat."

A bankszámlákkal, digitális fizetési szolgáltatásokkal, vagy a hitelkártyákkal szemben a Bitcoin segítségével anélkül tranzaktálhat két résztvevő fél, hogy bármiféle személyes információt meg kellene osztaniuk magukról. A bankok, hitelkártya-társaságok, pénzügyi cégek, vagy éppen a kormányzatok által kezelt adatbázisok, tele a fogyasztók, ügyfelek, felhasználók személyes adataival, rendkívül csábító célpontnak számítanak a hackerek számára. Az egyik legjobb példa erre a közelmúltból az Equifax esete 2017-ből, amely során több, mint 140 millió ember adatai kerültek kiberbűnözők kezébe.

A Bitcoin szétválasztja a pénzügyi műveleteket és a való világbeli identitást. Ahogyan a készpénz esetében is, mikor valakinek bankjegyeket adunk, neki nem kell ismernie minket. Nekünk pedig nem kell azon aggódni, hogy olyan információkat szereztek rólunk, amelyek segítségével ellophatják a többi pénzünket. Miért ne várhatnánk el legalább ugyanezt a digitális pénztől is?

„A központi bankokban is meg kell bíznunk, hogy nem fogják leértékelni a pénzünket, a fiat valuták története viszont tele van példákkal ennek a bizalomnak az elárulásáról.”

A fiat mozaikszó a latin nyelvű „legyen így” kifejezésből származik, és valójában rendeleti pénzt takar. Ez azt jelenti, hogy a kormányok és a központi bankok mindenki számára kötelezően betartandó törvényben határozzák meg, hogy az adott pénznem lesz az ország hivatalos pénze. Az emberiség történelme során legtöbbször olyan dolog szolgált pénzként, amelyet nehéz volt előállítani, könnyű ellenőrizni a valódiságát, és szállíthatónak számított. Ilyenek voltak a színes tengeri kagylóhéjak, az üveggyöngyök, az ezüst és az arany. Bármit is használtak pénzként, azonnal jelentkezett a kísértés, hogy valaki még többet hozzon létre belőle. Ha pedig valaki rájött egy jó technológiára, amely segítségével gyorsan lehetett sokat előállítani az adott dologból, az a dolog elvesztette az értékét. Az európai telepesek így tudták megszerezni az afrikai kontinens lakóinak a vagyonát, hiszen a könnyen előállítható üveggyöngyökért cserébe nehezen előállítható emberi munkaerőt, rabszolgákat vehettek. Az arany ezért számított évezredeken keresztül értékálló pénznek, hiszen nagyon nehéz gyorsan, sokat előállítani belőle.[1]
A világgazdaság lassan elkezdett az aranypénzről áttérni a papír bankjegyekre, amelyek eredetileg igazolások voltak a fedezetül szolgáló aranyról, amelyért cserébe azt az aranyat megkaphattuk. Végül aztán a papírpénzt teljesen leválasztották az aranyfedezetről, amikor Nixon elnök 1971-ben megszüntette az USA dollár és az arany közötti átválthatóságot.

Ezzel véget ért az arany-standard, a kormányok és a központi bankok pedig lehetőséget kaptak arra, hogy kedvük szerint növeljék a pénzkészleteiket, lecsökkentve a már forgalomban lévő bankjegyek reálértékét, ezzel elkövetve az úgynevezett pénzrontást. Annak ellenére, hogy a mai korban ezt a kormány által kibocsátott, fedezet nélküli pénzt ismerjük és használjuk nap, mint nap, a világtörténelem skáláján nézve ez egy relatív újdonságnak számít.
Meg kell bíznunk a kormányainkban, hogy nem fogják felelőtlenül használni a pénznyomtatóikat, de nem kell sokáig keresgélnünk, ha példákat szeretnénk találni ennek a bizalomnak az elárulásáról. Az autoriter,

központi tervgazdaságot fenntartó országokban, ahol a kormány saját hatáskörben folyamatosan nyomtatja a pénzt, mint például Venezuelában, a hivatalos pénz szinte teljesen elvesztette az értékét. 2009-ben egy USD 2 bolivárt ért, 2019-re ez 250 ezer bolivárra nőtt. Ennek a könyvnek az írása közben Venezuela az összeomlás felé robog, a kormányzat rettenetes hibái miatt, amelyeket a nemzetgazdaság működtetése során követtek el.

Satoshi a fiat pénzek helyett egy alternatív megoldást akart, amelynek a készlete mindig meghatározható módon növekszik. Hogy elejét vegye az elértéktelenedésnek, Satoshi egy olyan rendszert épített fel, amelyben a készlet véges, a kibocsátási ráta pedig ismert, és megváltoztathatatlan. Maximálisan 21 millió bitcoin fog létezni, bár minden egyes BTC feloszthető 100 millió egységre, amelyeket az alkotó tiszteletére satoshinak nevezünk. Így a 2140-es évekre a forgalomban lévő mennyiség 2,1 kvadrillió satoshi lesz.

A Bitcoin megjelenése előtt nem volt mód rá, hogy a digitális tartalmak sokszorosítását megelőzzük. Egy digitális könyvet, zeneszámot, vagy filmet olcsón és egyszerűen lemásolhatunk, hogy elküldjük egy barátunknak. Ez alól egyedül a közvetítőkön keresztül kapott digitális tartalmak jelentenek kivételt. Például ha az iTunes platformjáról bérelsz egy filmet, csak a saját eszközödön nézheted meg, hiszen a fájl nem nálad van, hanem az iTunes adja neked kölcsön, amíg tart a bérleti időszak. Ehhez hasonlóan a digitálisan létező pénzedet pedig a számlavezető bankod kontrollálja. A banknak az a dolga, hogy nyilvántartsa, mennyi pénzed van, és amikor átutalnál valakinek valamennyit, végrehajtja számodra vagy megtagadja az utalást.
A Bitcoin az első digitális rendszer, amely közvetítő nélkül tudja biztosítani a korlátozott rendelkezésre állást, és ez az első pénzeszköz az emberiség történelmében, amelynek nem lehet megváltoztatni a készletét, a kibocsátási ráta pedig mindenki számára ismert.
Még az arany és a többi nemesfém sem rendelkezik ezzel a tulajdonsággal, hiszen ha nyereségesen meg tudjuk tenni, akkor tudunk belőle többet kitermelni a bányászat során. Képzeljük el mi történik, ha felfedezünk a Naprendszerben egy aszteroidát, amelyik tízszer több aranyat tartalmaz, mint amennyi az egész bolygónkon létezik. Mit okozhat egy ilyen készlet

megjelenése az arany árfolyamában? A Bitcoin immunis az ilyen felfedezésekre, és a készlet manipulációira. Egyszerűen lehetetlen, hogy többet hozzunk létre belőle, a későbbi fejezetekben pedig megnézzük, hogy miért van ez így.

A pénz természete, és a jelenleg létező pénzrendszerünk eléggé komplikált, ebben a könyvben pedig nem fogunk mélységében foglalkozni ezzel. Ha szeretnél többet tudni a pénz fundamentumairól, és, hogy hogyan alkalmazhatók ezek a Bitcoin esetében, ajánlom elolvasásra Saifedean Ammous könyvét, a magyarul is elérhető „The Bitcoin Standard" címűt, jó alapokat nyújthat ebben a témakörben.

„Az adatok olyan módon lehetnek immár biztosítva, hogy fizikailag nincsen mód rá, hogy illetéktelenül hozzáférjenek, semmilyen okból, semmilyen kifogás mögé bújva, semmilyen esetben.
Eljött az idő, hogy ugyanez a pénzzel is megtörténjen."

A biztonság tekintetében jelenleg olyan megoldásokat használunk, hogy például a bankban tartjuk a pénzünket, nem otthon. Ehhez viszont meg kell bíznunk abban, hogy mások elvégzik a munkájukat. Egy ilyen közvetítőben való bizalom azt jelenti, hogy elhisszük, nem fog visszaélni a helyzetével, vagy nem csinál valami ostobaságot. Ezzel együtt pedig abban is bíznunk kell, hogy a kormányzat nem fog nyomást gyakorolni erre a közvetítőre, hogy befagyassza, lefoglalja a javainkat. Mégis, időről időre láthatjuk, hogy a kormányzatok képesek elzárni a lakosságot a pénztől, és ezt meg is teszik, amikor fenyegetve érzik magukat. Az Egyesült Államokban, vagy egy másik nyugati, pénzügyi szabályokkal és törvényekkel alaposan ellátott országban élve hihetetlennek tűnik, hogy egy reggel arra ébredjünk, eltűnt a pénzünk. Mégis állandóan történik ilyesmi. Személy szerint nekem a PayPal fagyasztotta be a fiókom, mivel hónapokig nem használtam. Egy hétig tartott, mire újból hozzáfértem a saját pénzemhez. Szerencsés vagyok, hogy az USA-ban élek, ahol legalább némi jogi segítséget kaphatok, ha a PayPal befagyasztja a számlám, és ahol legalább minimális mértékben, de megbízhatunk abban, hogy a kormány nem akarja ellopni a pénzünket.
Ennél sokkal rosszabb dolgok is történtek, és történnek a kevésbé szabad országokban. Görögországban egyszerűen bezártak a bankok, mikor a

gazdaságuk elkezdett összeomlani, Cipruson úgy oldotta meg a gazdasági mentőcsomagot az állam, hogy lefoglalta a bankbetéttel rendelkezők pénzét, Indiában pedig azonnali hatállyal érvénytelenítettek bizonyos címletű bankjegyeket, értéktelen papírrá változtatva azokat.

A korábbi Szovjetunióban, ahol felnőttem, a kormány teljes irányítást gyakorolt a gazdaság felett, emiatt hatalmas áruhiány alakult ki. Illegálisnak számított külföldi valutát, például dollárt birtokolni. Mikor el akartuk hagyni az országot, fejenként csak meghatározott összeget válhattunk át külföldi valutára. A váltás pedig a hivatalnokok által megszabott árfolyamon történt, amely nagymértékben eltért a valódi piaci árfolyamtól. A kormány tulajdonképpen megfosztott minket a vagyonunktól, bármilyen kicsi is volt az, csak annyi maradt, amennyit egy kézitáskában magunkkal tudtunk vinni.
Az autoriter országok mindig is hajlottak a szigorú gazdasági kontrollra, hogy megakadályozzák az embereket a pénzük kivételére a bankból, így nem tudják kivinni az országból, vagy nem tudják átváltani értékállóbb külföldi valutára. Így a kormányok gyakorlatilag szabadon bevezethetnek bármilyen eszement gazdasági intézkedést, ahogy láthattuk is a Szovjetunió esetében.
A Bitcoin esetében nincsen szükség arra, hogy egy közvetítő, egy harmadik fél felügyelje a pénzed biztonságát. Ehelyett a Bitcoin lehetetlenné teszi, hogy rajtad kívül, a megfelelő privát kulcs birtokosának a hozzájárulása nélkül bárki hozzáférjen a pénzedhez, semmilyen okból, semmilyen indokkal, bármennyire is jó ez az indok. A Bitcoin birtoklásával egy kulcsot birtokolsz a saját pénzügyi szabadságodhoz. A Bitcoin szétválasztja egymástól a pénzt és az államot.

„A Bitcoin ezt oldja meg egy P2P hálózat segítségével, amely ellenőrzi a dupla költést. …egy elosztott időbélyegző-szerverként működik, amelyik meghatározza, hogy mikor lett elköltve egy adott coin.”

A P2P hálózat az egymással kapcsolatban álló számítógépeket jelenti, amelyek közvetlenül tudnak üzenetet, információt küldeni egymás között. Azért elosztott, mert nincsen egy központi felügyelő szereplő, hanem a rendszer résztvevői egyenrangúként működnek együtt a hálózat

koordinálásában, sikeres működtetésében. Egy olyan rendszerben viszont, ahol nincsen központi felügyelet, nagyon fontos tudni, hogy senki sem csal. A dupla költés alatt azt a jelenséget értjük, hogy valaki kétszer költi el ugyanazt a pénzt. A fizikai bankjegyek esetében ez nem probléma, hiszen amikor azokkal fizetsz, kiadod a kezedből. A digitális tranzakciók viszont adatok, ugyanúgy le lehet másolni őket, mint a zenéket vagy a filmeket. Ha egy bankon keresztül utalsz pénzt valakinek, ők gondoskodnak róla, hogy azt az összeget nem költheted el még egyszer. Központi irányítás nélkül viszont meg kell oldanunk valahogy, hogy ne lehessen dupla költést végezni, hiszen az olyan lenne, mint a pénzhamisítás. Satoshi úgy írta le, hogy a Bitcoin hálózat résztvevői együtt dolgoznak azon, hogy a tranzakciókat időbélyegzővel lássák el, meghatározzák a sorrendjüket, így pontosan tudni lehet, hogy melyik történt meg előbb. Így vissza tudjuk utasítani, hogy az egyszer már elköltött pénzt még egyszer elkölthessék. A következő pár fejezetben pontosan ennek a felépítését, megoldását fogjuk részletesen körbejárni. Láthatjuk, hogyan válik lehetővé a hamisítási, csalási próbálkozások észlelése anélkül, hogy központi ellenőrzésre kellene hagyatkoznunk.

***

A Bitcoin nem légüres térben született, Satoshi több fontos próbálkozást is megemlített, amelyek során hasonló rendszert próbáltak létrehozni, például a b-money Wei Dai részéről, vagy Adam Back Hashcash projektje. A Bitcoin így úgymond óriások vállára állva jött létre, de előtte egyik másik esetben sem sikerült az alkotóelemeket a megfelelő módon összerakni, ezért nem született meg a rendszer, amelyik központi szereplő nélkül irányítja egy ténylegesen limitált készletű digitális pénz kibocsátását és kezelését.
Satoshi egy sor érdekes technológiai problémát hozott közös nevezőre, amelyek megoldásával sikerült kijavítani a magánszférát nem tisztelő, a pénzrontást, és a központi irányítást használó jelenlegi pénzügyi rendszer hiányosságait:

- Hogyan hozz létre egy P2P hálózatot, amelyhez bárki önként csatlakozhat, és közreműködhet a fenntartásában?

- Hogyan lehet megoldani, hogy egymást nem ismerő egyének csoportja, akiknek nem is kell felfedniük egymás előtt a személyazonosságukat, és nem kell megbízniuk egymásban, fenn tudjanak tartani egy elosztott pénzügyi főkönyvet, még akkor is, ha van köztük tisztességtelen szándékú?
- Hogyan tudják az emberek létrehozni a saját, hamisíthatatlan pénzüket központi irányítás nélkül, mégis megtartva a készlet korlátjait, és biztosítva, hogy senki sem juthat hozzá ingyen?

Mikor a Bitcoin elindult, alig maroknyian csatlakoztak hozzá, hogy futtassák a programot a számítógépükön, és fenntartsák a hálózatot. A legtöbben egyszerűen azt gondolták akkoriban, hogy az egész csak egy vicc, vagy, hogy olyan végzetes programhibákat fognak találni benne, amelyek miatt nem sokáig fog működni.

Mégis időről időre egyre többen léptek be, csomópontokat futtatva a számítógépeiken, így erősítve a hálózatot. Elkezdték elfogadni más pénzekért cserébe, vagy éppen fizetségként árucikkekért, szolgáltatásokért, így valódi értéket adva neki. Most, egy évtizeddel később több tíz- és százezer számítógépen fut a Bitcoin szoftvere, és világszerte több száz önkéntes és vállalkozás dolgozik a fejlesztésén.
Nézzük meg hát, hogyan épül fel ez a rendszer!

A KÖZVETÍTŐK ELTÁVOLÍTÁSA

Az előző fejezetben elolvashattad, hogy a Bitcoin egy P2P hálózatot működtet pénzügyi műveletekhez. Mielőtt mélyebben is belemennénk, hogy ez hogyan működik a gyakorlatban, nézzük meg, a hagyományos pénzügyi szereplők, a bankok és a fizetési szolgáltatók hogyan csinálják a dolgot!

A bankok nem mások, mint könyvelők

Egy bank, vagy a PayPal hogyan működik? Egyszerűen könyvelést, nyilvántartást vezet arról, hogy ki utalt pénzt kinek, így tudja, hogy kinek mennyi pénz van a számláján.
A bankok elsődleges feladata, hogy a letétbe helyezett pénzt kezelje és vigyázzon rá. De a letétek manapság digitálisan működnek, ritka a fizikai készpénz használata, így az őrzés most az adatbázisok őrzését jelenti elsősorban. Mivel pedig az adat elektronikusan létezik, az őrzés is elektronikusan történik. A bankok programokat használnak, amelyek figyelik, hogy ki fér hozzá a rendszereikhez, folyamatosan biztonsági mentéseket készítenek a fájljaikról, hogy ne veszítsenek el semmilyen információt, külső auditálást, ellenőrzéseket végeztetnek, hogy lássák, a saját belső folyamataik megfelelőek, és biztosításokat kötnek arra az esetre, ha valami rossz dolog történne.

Lássuk, hogyan működnek. Bankot mondunk, de valójában minden pénzügyi szolgáltató ugyanígy csinálja. Kezdésként mondjuk, hogy Alice és Bob a két ügyfelünk, akik pénzt helyeztek letétbe nálunk. Így néz ez ki a bank rendszerében:

Banki főkönyv

Alice egyenlege: 2 dollár bankbetét
Bob egyenlege: 10 dollár bankbetét

Amikor Alice 2 dollárt akar küldeni Bobnak, felhívja a bankját, vagy az interneten keresztül belép az online netbank applikációba, azonosítja

magát jelszó vagy pin-kód segítségével, majd elindítja az utalást. A bank pedig rögzíti ezt a főkönyvében.

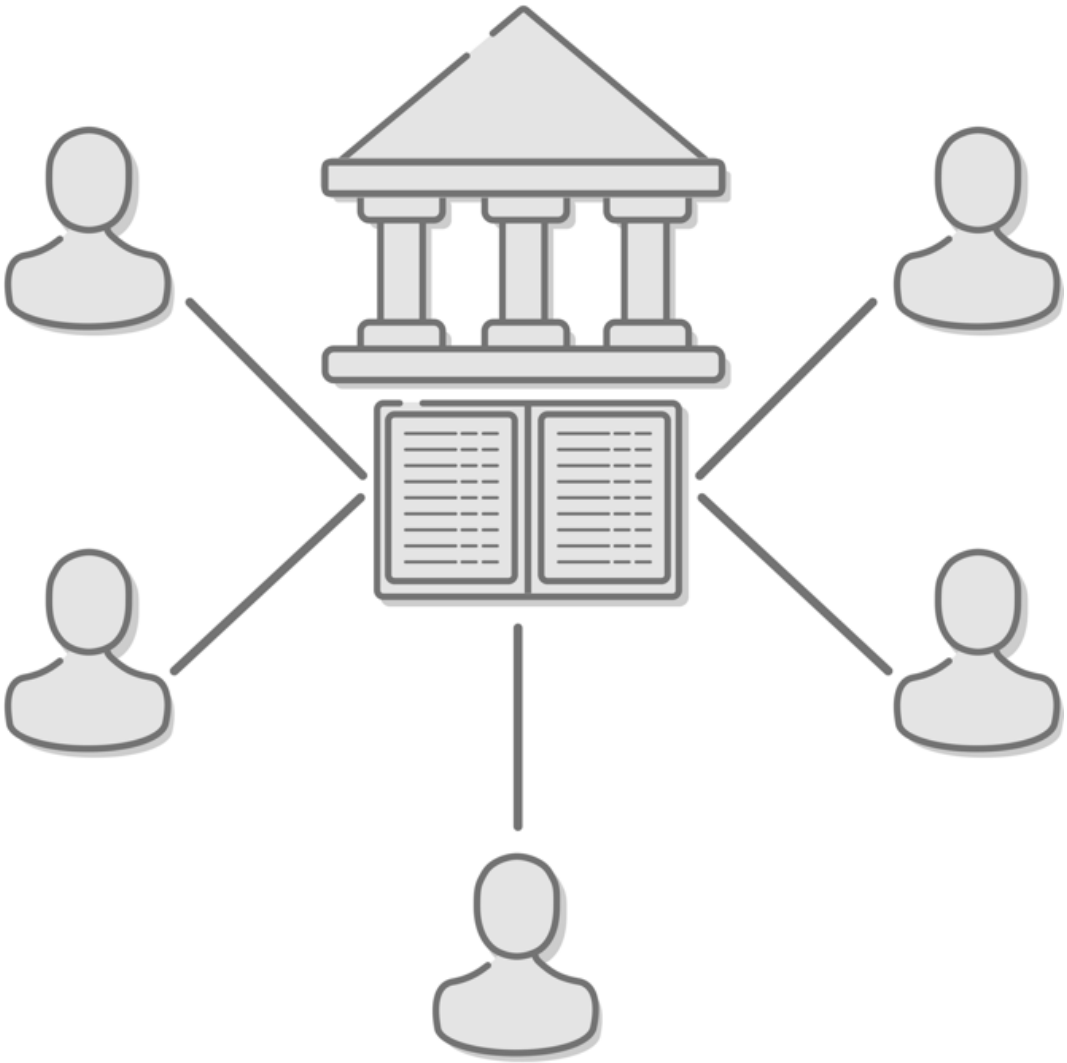
Banki főkönyv

Alice egyenlege: 2 dollár bankbetét
Bob egyenlege: 10 dollár bankbetét
Alice 2 dollár terhelés
Bob 2 dollár jóváírás

A bank tehát elkönyvelte az egyenlegek csökkenését illetve növekedését, így a pénz átutalása megtörtént. Mi történik, ha szembesülünk a dupla költés problémájával?

Tegyük fel, hogy Alice újból el szeretné költeni azt a 2 dollárt, amelyet az egyenlegén tartott. Ez lenne az a bizonyos dupla költés. Átadja a megbízást a banknak, a bank viszont azt mondja, hogy „sajnáljuk, de látjuk a könyvelésünkben, hogy a 2 dollárodat már elküldted Bobnak, nincs már pénz a számládon, nem tudod elkölteni”.

Ha van egy központi szereplőd, például a bank, nagyon könnyen rájön, hogy olyan pénzt szeretnél elkölteni, amelyet egyszer már kiadtál a kezedből. Ez azért van, mert a bank vezeti a saját könyvelését, és csak neki van jogosultsága arra, hogy megváltoztassa a nyilvántartást. Kidolgozott forgatókönyveik vannak, hogy hogyan legyen biztonsági mentés az adataikról, hogyan ellenőrizzék a számítógépeiket, az alkalmazottaikat, és külön szakembereket fizetnek azért, hogy módosításra, manipulációra utaló jeleket keressenek. Ezt centralizált rendszernek nevezzük, hiszen létezik egyetlen központi szereplő, akinek a kezében van az irányítás.

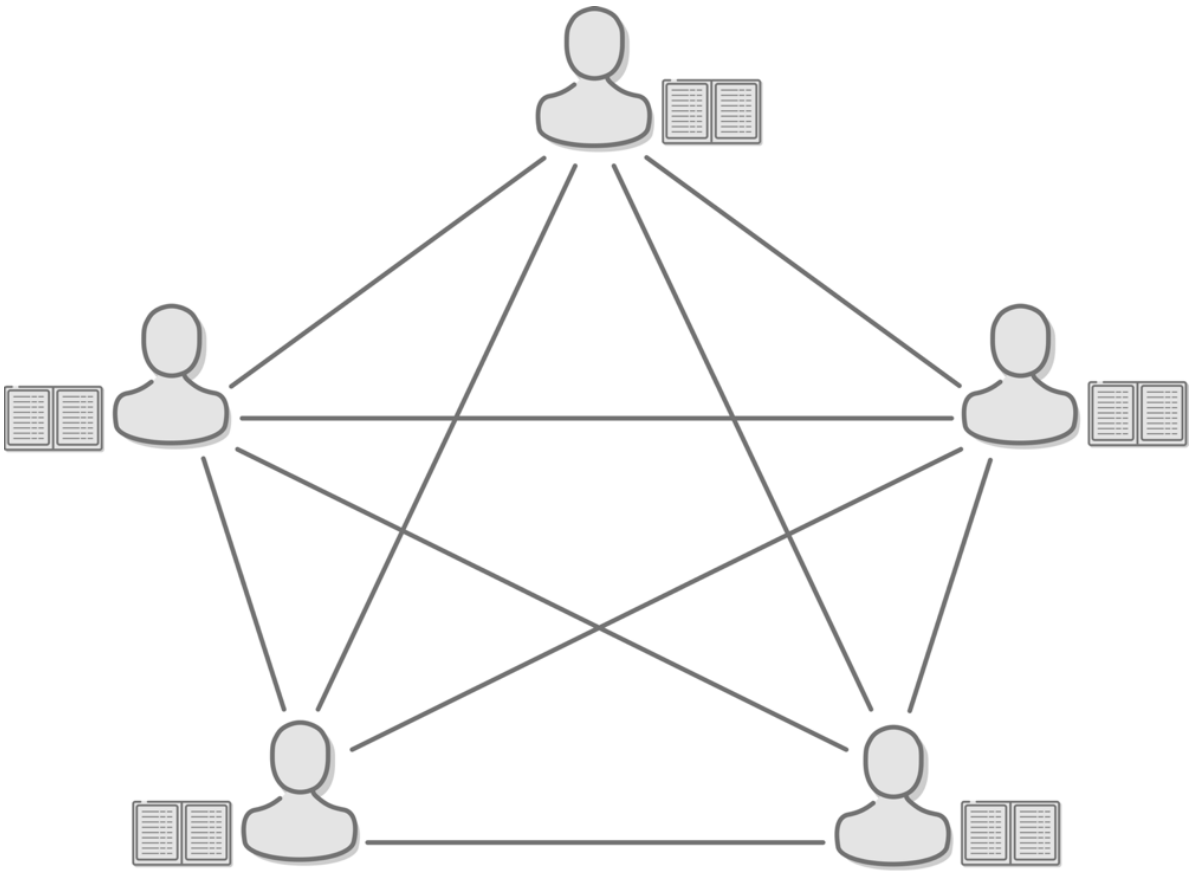


A banki nyilvántartáshoz bárki hozzáférhet, de csak és kizárólag a bankon keresztül.

Elosztott főkönyv

Az első módszer, amellyel a Bitcoin megoldja, hogy ne legyen szükség központi szereplőre, az a P2P hálózat létrehozása. Képzeljük el, hogy eltűnik a bank, és nekünk újból ki kell alakítanunk a pénzrendszerünket. Hogyan tudjuk menedzselni a nyilvántartást központi irányítás nélkül? Ha nincs központ, akkor az embereknek kell azt vezetni. Éljen a forradalom! Lássuk, hogyan oldható meg ez!

Először is társulunk, és létrehozunk egy hálózatot. Ez annyit jelent, hogy valamilyen módon kommunikálni tudunk egymással. Telefonszámot cserélünk, vagy megadjuk egymásnak a Snapchat felhasználónevünket. Mikor Alice pénzt akar küldeni Bobnak, ahelyett, hogy felhívná a bankot, egyszerűen a társulás minden tagjának szól, hogy „küldök 2 dollár Bobnak”. Ezt pedig mindenki hallja, elfogadja, és felírják a saját nyilvántartásukba. Ezt valahogy így érdemes elképzelni:



Mindenki rendelkezik a nyilvántartás másolatával, és közvetlenül hozzá is férhet.

Így, ahelyett, hogy egy bankban tárolnánk az egyetlen példányt a nyilvántartásról, mindenkinél van belőle egy másolat. Mikor valaki költeni akar a pénzéből, egyszerűen szól a többieknek. Mindenki rögzíti a saját könyvelésében a tranzakciót. Mivel ez a könyvelés már nem egyetlen

helyen történik, elosztottnak nevezzük. Mivel pedig nincsen központi irányító a rendszerben, decentralizált is.
Most viszont, hogy nincsen központ, nincsen közvetítő, hogyan tudjuk elejét venni a dupla költésnek? Ki tudja bizonyítani, hogy a pénzt, amelyet valaki el akar költeni, nem lett már egyszer felhasználva? Mivel a nyilvántartás mindenkinél ott van, kénytelenek vagyunk mindenkivel beszélni. Ezt a megoldást konszenzus-alapúnak nevezzük, hiszen azon alapul, hogy minden egyes résztvevő egyetért abban, hogy mi az igazság.
Ha Alice ismét el akarja költeni azt a 2 dollárt, amelyet egyszer már elköltött, a tranzakcióját mindannyian vissza fogják utasítani, mivel ellenőrzik a nyilvántartásukat, és abban azt látják, hogy egyszer már felhasználta a pénzét. Éppen ezért nem fogják feljegyezni a saját nyilvántartásukba Alice újbóli költési kísérletét. Így létrejött egy felhasználók közötti, konszenzuson alapuló hálózat, amely segítségével nyilván tudjuk tartani a tulajdonviszonyokat és a pénzmozgást.

Amíg a hálózathoz való csatlakozáshoz engedély kell, és bízhatunk abban, hogy minden résztvevő becsületes, addig ez a rendszer működik. De ez a fajta felépítés nem alkalmas arra, hogy világszerte egyszerre milliók használják. Az elosztott hálózatok az egyes résztvevőket megbízhatatlanná teszik. Néhányan alkalmanként offline lesznek, lekapcsolódnak a hálózatról. Így nem hallják, amikor mi megosztjuk a saját tranzakciónkról szóló információt. Mások esetleg szándékosan be akarnak csapni minket, és azt mondják, hogy adott tranzakció megtörtént, vagy éppen nem történt meg. Az újonnan csatlakozó tagok esetleg a nyilvántartás egy hibás, vagy hiányos változatát töltik le. Nézzük meg, milyen módszerrel próbálkozhat, aki csalni szeretne!

Dupla költés a gyakorlatban

Ha én lennék Alice, esetleg összebeszélhetnék néhány más résztvevővel, és azt mondanám, „figyeljetek, mikor használom a pénzem, azt ne jegyezzétek fel a nyilvántartásba, csináljunk úgy, mintha sosem történt volna meg”. Nézzük meg lépésről lépésre, hogy ezután mi történik! Az induló 2 dolláros egyenleggel, Alice a következőket teszi:

- Elküldi a 2 dollárt Bob számlájára, hogy így vásároljon egy csokit tőle. Ezután Alice egyenlege nulla kellene, hogy legyen.
- David, Eve és Farrah viszont megegyeztek Alice-szel, és nem jegyzik fel ezt az utalást Alice számlájáról Bob számlájára. Az ő nyilvántartásukban Alice sosem költötte el a pénzét, és még mindig 2 dollár az egyenlege.
- Charlotte egy becsületes résztvevő. Feljegyzi a nyilvántartásba, hogy Alice küldött Bobnak 2 dollárt. Nála Alice egyenlege nulla.
- Henry éppen nyaralt, offline volt, és nem hallott a tranzakcióról. Újra csatlakozik a hálózathoz, és megkéri a többieket, hogy küldjék el neki a friss nyilvántartást.
- Henry kap 4 darab hamisított nyilvántartást Alice, David, Eve és Farrah részéről, és kap egy valódit, amelyet Charlotte küld el neki. De hogyan tudja eldönteni, hogy melyik a valódi? Mivel nincsen jobb módszere, megbízik a többség állításában, és így a hamis nyilvántartást fogadja el valódiként.
- Alice vásárol egy csokit Henrytől is, és ad érte 2 dollárt, amellyel valójában nem rendelkezik. Henry viszont elfogadja, mivel az ő nyilvántartásában, amelyet a többségtől kapott, Alice számláján ott szerepel a 2 dollár.
- Alice így már két csokival rendelkezik, a tranzakció meghamisításával pedig a 2 dollár helyett a rendszerben már 4 dollár létezik. Alice fizetségként megosztja a csokit a többiekkel, és ezt együtt mindig újra elkövetik, amikor valaki újonnan csatlakozik a hálózathoz.
- A végén Alice birtokolja az összes csokit, mindenki másnál csak egy rakás értéktelen hamis pénz van.
- Mikor pedig valaki el akarja költeni azt a pénzt, amelyről azt feltételezi, hogy Alice elküldte neki, a többséget kontrolláló Alice, David, Eve és Farrah visszautasítják a tranzakciót, hiszen tudják, hogy a pénz a kezdetektől hamis.

Ezt nevezik a konszenzus bukásának. A hálózat résztvevői nem tudnak megegyezni, hogy mi a pontos valóság. Mivel nincs jobb megoldás, a többség szavára adnak, ez pedig ahhoz vezet, hogy a nem becsületes

résztvevők megszerzik a hálózat feletti irányítást, és olyan pénzt költenek el, amellyel nem is rendelkeznek.
Ha egy olyan rendszert akarunk használni, amelyhez bárki szabadon csatlakozhat, meg kell oldani, hogy a nem becsületes résztvevők tevékenységét semlegesíteni lehessen.

Hogyan oldjuk meg az elosztott konszenzus problémáját?

Elértünk a számítástechnika-tudomány egyik legnagyobb problémájához, amelyet meg kell oldani. Egy elosztott hálózaton hogyan jutunk konszenzusra, ha néhány résztvevő nem őszinte vagy nem megbízható? Ez az úgynevezett Byzantine Generals Problem néven ismert jelenség, és ez volt a kulcsmomentum, amely megoldásával Satoshi létre tudta hozni a Bitcoint. Szükségünk van a résztvevőkre, akik egyetértenek abban, hogy mit is tartalmaz a nyilvántartás, anélkül, hogy tudnánk, melyik résztvevő végezte becsületesen a nyilvántartás vezetését, és melyikük próbált csalni, kihagyni vagy hozzáadni tranzakciókat.

Az egyik, naívnak tekinthető megoldás, hogy megbízható résztvevőket választunk. Ahelyett, hogy bárki beleírhatna bármit a nyilvántartásba, kiválasztjuk egy maroknyi barátunkat, akik vezetik a könyvelést. Charlotte, Gary, Frank és Zoe lesznek a kiválasztottak, mert ők nem szoktak hazudni, és mindenki tudja, hogy még bulizni sem járnak hétvégente.
Minden alkalommal, mikor tranzakciót kezdeményeznénk, egyszerűen felhívjuk Charlotte és a többiek figyelmét erre, ahelyett, hogy elmondanánk mindenkinek a hálózaton. Egy jelképes összegű munkadíjért cserébe ők nagyon szívesen beleírják a nyilvántartásba, hogy mi pénzt küldtünk valakinek, ezután pedig nyilvánosan is megosztják a hálózattal, hogy friss bejegyzést könyveltek el, mindenki mentse le magának a nyilvántartás legújabb változatát.

Ez a rendszer remekül működik, ám egy nap megjelennek a hatóságok, és körbeérdeklődnek, hogy ki működteti ezt az illegális pénzügyi rendszert? Ezután Charlotte és a többiek csuklójára bilincs kerül, az elosztott nyilvántartás pedig használhatatlanná válik. A nálunk lévő másolatok nem

megbízhatók, nem bízhatunk meg egymásban sem, és nem tudjuk, hogy kinek a változatát kellene használnunk az újraindításhoz.

A teljes lekapcsolás helyett a kormány azt is megteheti, hogy börtönbüntetéssel fenyegeti meg a nyilvántartást vezetőket, ha rögzítik az Alice számára küldött tranzakciókat, hiszen róla feltételezhető, hogy drogokkal kereskedik. Mi történik viszont, ha megpróbálkozunk a demokráciával? Találjunk 50 őszinte résztvevőt, és minden nap szavazással döntjük el, hogy közülük ki könyvelheti az aznapi tranzakciókat. A hálózat minden résztvevője kaphat egy szavazatot. Ez is jól működhet, egészen addig, amíg fel nem tűnnek a színen olyanok, akik erőszakot, vagy pénzügyi ösztönzést használnak, hogy a már ismert végkimeneteleket idézzék elő:

- Kényszeríteni próbálják a szavazókat, hogy az általuk kívánt jelöltre szavazzanak.
- Ezután kényszerítik a megválasztottakat, hogy hamis bejegyzéseket írjanak bele a nyilvántartásba, vagy ne igazoljanak vissza bizonyos tranzakciókat.

Látható tehát, hogy komoly problémába ütköztünk. Bármikor, ha meghatározott résztvevőket választunk ki a nyilvántartás vezetésére, meg kell bíznunk abban, hogy őszinték, és becsületesen végzik a dolgukat. Emellett viszont semmilyen módunk sincsen arra, hogy megvédjük őket a zsarolástól, ha valaki tönkre akarná tenni a nyilvántartásunkat.

Hamis személyazonosságok

Eddig már két módszert is találtunk, amely nem tudja biztosítani a hitelességet: az egyik, hogy pontosan ismert résztvevőket bízunk meg a nyilvántartás vezetésével, a másik pedig a könyvelést végzők közötti körforgás alkalmazása. Mindkettő esetben amiatt bukik meg a rendszer, hogy a megbízhatóságot a résztvevők valódi személyazonosságához rendeljük hozzá. Pontosan tudnunk kell, hogy ténylegesen kik felelősek a nyilvántartás vezetéséért. Viszont minden esetben, ha személyazonossághoz kötjük a megbízhatóságot, felmerül az úgynevezett Sybil Attack jelensége, amely valójában csak egy divatos elnevezése a

megszemélyesítésnek, a személyazonosság-lopásnak. Volt már rá példa, hogy furcsa üzenetet kaptál valamelyik barátodtól, és később kiderült, hogy ellopták, vagy elvesztette a telefonját? Ha a történetben pénz is szerepel, millió vagy billió dollár akár, az emberek bármilyen erőszakot képesek jogosként megmagyarázni, csak ellophassák azt a telefont, és elküldhessék azt az üzenetet. Látható tehát, mennyire fontos a nyilvántartásunk kezelőit bármi áron megvédeni a kényszerítéstől. De hogyan tehetjük meg ezt?

Használjunk lottóhúzást!

Ha nem akarjuk lehetővé tenni, hogy erőszakkal vagy lefizetéssel kompromittálódhassanak a könyvelést végző résztvevők, egy olyan rendszer kell, amelyben túl sokan vannak, hogy zsarolni lehessen őket. Még jobb a helyzet, ha egyáltalán nem is ismerjük a valódi személyazonosságukat. Úgy kell intézni, hogy ténylegesen bárki csatlakozhasson a hálózathoz, részt vehessen a fenntartásában, de ehhez nincs szükségünk szavazásra, amely amúgy is manipulálható kényszerítéssel vagy szavazatvásárlással. Mi van akkor, ha egyfajta lottóhúzásként minden alkalommal, amikor új bejegyzést könyvelnénk a nyilvántartásunkba, véletlenszerűen választanánk ki valakit a résztvevők közül, hogy ezt megtegye? Nézzünk meg egy vázlatot erről, hogyan is nézne ki a gyakorlatban!

- A világon bárki csatlakozhatna. Akár tízezrek is beszállhatnának a nagy nyilvántartás-lottóba.
- Ha pénzt akarunk küldeni valakinek, ahogyan eddig is, most is elmondjuk a hálózat összes résztvevőjének ezt.
- Ahelyett, hogy mindenki feljegyezné ezt a tranzakciót, sorshúzással döntjük el, hogy ki írhatja bele a nyilvántartásba.
- Amikor megvan a nyertes, ő a mi tranzakciónk mellett az összes többi új tranzakciót is feljegyzi, amelyeket adott időszakban hallott.
- Ha a nyertes érvényes tranzakciókat jegyez fel, olyanokat, amelyek megfelelnek a hálózat, a résztvevők által felállított szabályoknak, megkapja a jutalmat a munkájáért.

- Mindenki frissíti a saját másolatát, beleírva a nyilvántartásba ugyanazt, amit a nyertes is beleírt a sajátjába.
- Várunk egy kicsit, hogy mindenkinek legyen elegendő ideje frissíteni a saját nyilvántartását a legújabb tranzakciókkal, ezután pedig újból szervezünk egy lottóhúzást.

Ez a módszer már határozottan működőképesnek tűnik. Gyakorlatilag nem nagyon lehet kompromittálni a résztvevőket, hiszen egyrészt nem is tudjuk, hogy pontosan kik a résztvevők, másrészt nem lehet előre tudni, hogy ki fogja nyerni a sorsolást. Mindenesetre nem tudjuk, hogyan csináljuk ezt az egész lottóhúzás dolgot felsőbb irányítás nélkül, és nem tudjuk, hogy megbízhatunk-e abban, hogy a nyertes végül becsületesen viselkedik majd a nyilvántartás frissítésekor. A következő fejezet ennek a megoldásáról fog szólni.

PROOF OF WORK

Ez a lottóhúzásos módszer, amelyet felvázoltunk, két nagy hátulütővel jár. Egyrészt ha semmilyen központi szereplő nincsen a rendszerben, ki fogja eladni a szelvényeket, és kiválasztani a nyertes számokat? Másrészt hogyan lehetünk biztosak abban, hogy a nyertes becsületes lesz, és nem akar mindannyiunkat becsapni?
Ha egy olyan hálózatot szeretnénk, amelyhez bárki szabadon csatlakozhat, akkor meg kell oldanunk, hogy ne kelljen megbíznunk egymásban. Egy olyan rendszert kell kiépítenünk, amely a következő tulajdonságokkal rendelkezik:

- Mindenki számára biztosítani kell, hogy létrehozhassa a saját lottószelvényét, hiszen nem tudja azokat megvásárolni a nem létező központi irányítótól. A centralizált lottókat, mint amilyen például az Ötöslottó, cégek futtatják, amelyek létrehozzák a szelvényeket, és kisorsolják a számokat. Mivel a mi hálózatunkon nincsen központi szereplő, mindenkinek meg kell engednünk, hogy létrehozza a saját szelvényét.
- Gondoskodni kell arról, hogy a részvétel pénzbe kerüljön, így el tudjuk kerülni, hogy valaki hatalmas mennyiségű szelvényt hozzon létre magának ingyen. De ha nincs kitől megvásárolni, mivel magunknak hozzuk létre, hogyan oldható meg, hogy mégis pénzbe kerüljön? Hívjuk segítségül a fizika törvényeit, és a szelvények létrehozásához legyen szükség elektromos energiára, egy erőforrásra, amely pénzbe kerül!
- A hálózat többi résztvevőjének könnyen ellenőriznie kell, mégpedig kizárólag a szelvény segítségével, hogy tényleg mi nyertünk. Az Ötöslottónál a cég húzza ki a nyerőszámokat. A mi decentralizált rendszerünkben nincsen cég, így a résztvevőknek kell megegyezniük abban, hogy a nyertes számnak egy bizonyos tartományba kell esnie, például 1 és 10 közé. Ha az általad generált szelvény száma 1 és 10 közé esik, nyertél. Ahhoz pedig, hogy létrehozzuk a saját szelvényünket, egy kriptográfiai módszert, az úgynevezett hash funkciót fogjuk használni.

Proof of Work: energiaigényes, aszimmetrikus kirakózás

Mindhárom szükséges tulajdonságot biztosítani tudjuk egy elegáns megoldás, az úgynevezett Proof of Work használatával. Ezt jóval a Bitcoin születése előtt, már 1993-ban kitalálták. A Bitcoin működésének a megértésében valószínűleg ennek a sorshúzásos módszernek a megértése a legnehezebb, így a következő pár fejezetet a mélyebb, alaposabb kifejtésnek fogjuk szentelni.

Biztosítanunk kell, hogy a szelvények létrehozása sokba kerüljön, különben az emberek végtelen mennyiségűt generálnának maguknak, ingyen. Mi lehet az, ami garantáltan sokba kerül, de nem egy centralizált központi szereplőnek köszönhetjük?
Itt találkozik a Bitcoin rendszere a fizikával. A termodinamika első törvénye kimondja, hogy az energiát nem lehet sem létrehozni, sem megsemmisíteni. Más szavakkal fogalmazva, ha az energiáról beszélünk, nincs ingyen ebéd. Az elektromosság mindig drága, mert meg kell vásárolnod a szolgáltatótól, vagy saját energiatermelő egységet üzemeltetned. Az elektromosság mindkét esetben sokba kerül.
A Proof of Work mögötti koncepció az, hogy egy véletlenszerű folyamatban veszel részt, hasonlóan ahhoz, mintha egy dobókockát dobálnál újra és újra. Ez a kocka viszont nem hatoldalú, hanem annyi oldala van, amennyi atom létezik az univerzumban. Ezzel a kockadobással hozol létre magadnak egy lottószelvényt, egészen pontosan generálsz egy számot. Ahhoz, hogy ezt megtedd, a számítógépednek dolgoznia kell, ahhoz pedig áramra van szükség, és az áram pénzbe kerül.

Ahhoz, hogy nyerjél a lottón, egy olyan számra van szükséged, amelyet matematikailag le lehet vezetni a nyilvántartásba írandó tranzakciókból, valamint egy véletlenszerűen kiválasztott számból, és ezt a számot kaphatod meg a kockadobással. De ahhoz, hogy a megfelelő számot megtaláld, milliószor, billiószor, vagy akár kvadrilliószor is dobnod kell a kockával. Ennek a számnak kisebbnek kell lennie az úgynevezett célszámnál, amelyet a hálózat határoz meg bizonyos időközönként. A célszámról a későbbiekben beszélünk még. Ez megdolgoztatja a

számítógéped, és drága elektromos áramot használ hozzá, akár sok ezer dollárnyi értékben. Mivel a folyamat a véletlenszerűségen alapul, bárki számára lehetőség nyílik arra, hogy létrehozza a saját lottószelvényeit. Ehhez mindössze egy véletlenszerű számokat próbálgató számítógépre van szüksége, és a nyilvántartásba felvezetendő tranzakciók listájára. Ahhoz, hogy megtaláld a megfelelő számot, rengeteg energiára van szükséged. A hálózat többi résztvevőjének ezzel ellentétben nagyon egyszerű dolga van, ha le akarják ellenőrizni, tényleg te nyertél-e, mindössze három dolgot kell megvizsgálniuk:

- Az általad generált szám tényleg kisebb az előre meghatározott célszámnál?
- Az általad generált szám matematikailag tényleg levezethető azokból a tranzakciókból, amelyeket kiválasztottál, hogy bekerüljenek a nyilvántartásba?
- Ezek a tranzakciók megfelelnek a hálózat általános szabályainak? Nincs köztük dupla költés vagy ütemterven kívüli coin-generálás?

A Proof of Work véletlenszerű folyamata rengeteg próbálkozást igényel, hogy rátaláljunk a nyertes számra. Ennek a leellenőrzésére viszont elegendő egyetlen egy dolgot megtenni. Kicsit úgy kell elképzelni, mint egy sudoku-táblát, vagy éppen egy sok darabból álló kirakót. Nagyon sokáig tarthat megoldani, kirakni, viszont elég egyetlen pillantás, hogy lássuk, készen van-e vagy sem. A Proof of Work ezért számít aszimmetrikusnak. Nehéz a játékosoknak, de könnyű annak, aki ellenőrizni szeretné.

A folyamat során elhasznált energia és pénz miatt értelemszerű az igény, hogy mindenki elfogadja az általad generált nyerőszámot. Ez pedig nagy motiváció, hogy az ember rendesen viselkedjen, betartsa a szabályokat, és csak érvényes tranzakciókat rögzítsen.
Ha például úgy döntesz, hogy dupla költést végeznél, és olyan pénzt használnál, amellyel nem rendelkezel, a hálózat többi tagja vissza fogja utasítani a próbálkozásodat, így a rengeteg energia, amelyet a találgatásra fordítottál, kárba vész, az erre költött pénzeddel együtt. Viszont ha szabályos tranzakciókat rögzítesz a nyilvántartásba, és becsületesen végzed

a munkád, bitcoint kapsz jutalmul, amellyel kifizetheted a villanyszámládat, és még nyereséged is lesz belőle.

A Proof of Work így rendelkezik egy nagyon fontos tulajdonsággal, hiszen a fizikai világban is kézzel fogható költsége van a használatának. Emiatt tehát ha valaki erőszakkal, kényszerítéssel szeretné manipulálni a hálózatot valamelyik résztvevőn keresztül, nem elegendő megtalálni és eltéríteni a számítógépét. Ki kell fizetni a villanyszámláját is.

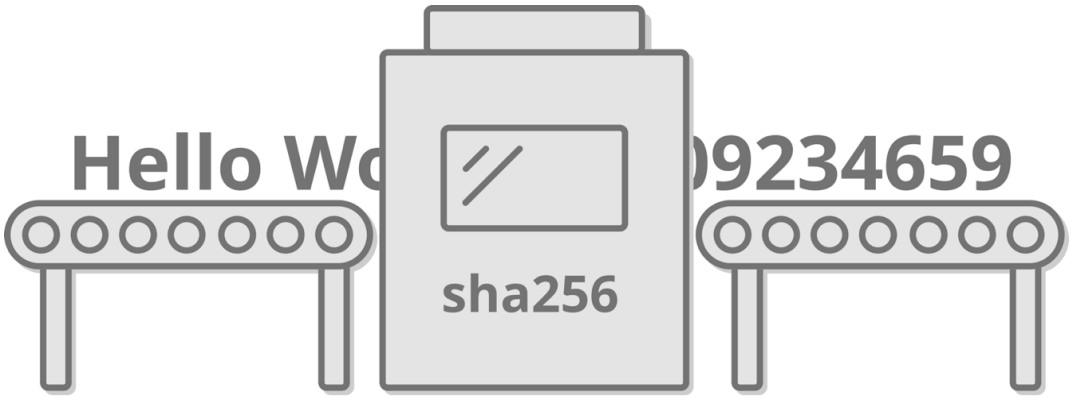
De hogyan tudjuk bizonyítani a többi résztvevő számára, hogy mi tényleg elégettük az adott mennyiségű energiát? Ehhez szükségünk lesz egy rövid kitérőre a számítástechnika-tudományba, amely során megnézünk két fogalmat, a hashelés és a bitek dolgát.

Hashelés

A Bitcoin aszimmetrikus Proof of Work kirakósa az úgynevezett hash funkció segítségével működik. Matematikórán megtanultuk, hogy a funkció az egy valamilyen folyamat, amely során x inputból f(x) output lesz. Például ha ez a funkció az f(x)=2x, akkor tudjuk, hogy ez egyszerűen megduplázza az x értékét. Ha az x-re azt mondjuk, hogy 2, akkor az f(x) 4-gyel lesz egyenlő.
A hash funkció azt csinálja, hogy az inputból, betűkből, számokból, vagy bármilyen más adatból, például a „Hello world” kifejezésből egy hosszú, véletlenszerűnek tűnő számot generál, amely így néz ki:

869913660443924676617831651669733090238
071816480247187783135263898928609948 42

Az a hash funkció, amellyel ezt a számot létrehoztuk, az úgynevezett sha256 algoritmus, és ezt használja a Bitcoin is.



Adat megy be, egy hosszú, megjósolhatatlan szám jön ki

Az sha256 hash funkció rendelkezik néhány kifejezetten hasznos tulajdonsággal:

- Az output determinisztikus, azaz előre meghatározott. Ugyanabból az inputból mindig ugyanaz az output származik.
- Az output nem megjósolható. Egyetlen betű cseréje, de akár egy szóköz hozzáadása is jelentősen megváltoztatja az outputot, egyszerűen nem fedezhető fel a kapcsolat az eredeti inputtal.
- Bármekkora méretű inputból gyorsan lehet hashelni.
- Nem lehetséges, hogy két különböző bemenetből egyforma output jöjjön.
- Az output birtokában sem lehet visszafejteni, hogy mi volt az eredeti input. Ezt egyirányú hash funkciónak is nevezik.
- Az output mérete meghatározott, az sha256 esetén 256 bit.

Mi a helyzet a bitekkel?

Az általunk, emberek által használt számrendszer a tizes, mivel a 0 és 9 közötti skála tíz számjegyet tartalmaz. A számítógépek viszont nem ezt a számrendszert használják, hanem azt, ahol csak egyesek és nullák vannak. Ezek szimbolizálják az elektromos impulzus állapotát, amely vagy van, vagy nincs. Ezt a rendszert binárisnak nevezzük.

A tizes számrendszerben tíz darab számjeggyel írjuk le az összes számot. Ha egyetlen számjegyet használunk, az 10 különböző változat lehet. Ha két

számjeggyel dolgozunk, akkor már 10 x 10, tehát 100 különböző szám jöhet létre, 0-tól 99-ig. Három számjegy esetén pedig 10 x 10 x 10, tehát ezer lehetséges szám létezik.

Ebből már látható, hogy ez hogyan folytatódhat. Ha arra vagyunk kíváncsiak, hogy mekkora számot tudunk „N" darab számjeggyel leírni, egyszerűen csak annyiszor összeszorozzuk a tizet, amennyi az N értéke. Azaz 10 az N-ediken, tehát 10^N.

A bináris rendszer ugyanígy működik. Az egyetlen különbség az, hogy kevesebb számjeggyel dolgozhatunk. A tizes számrendszerben 10 szám áll rendelkezésünkre, de a bináris esetén csak kettőből választhatunk, az 1-es és a nulla közül.

Ha azt mondjuk, hogy 1 bit, akkor annak az értéke kétféle lehet, 0 vagy 1. Ha 2 bitről beszélünk, akkor 2 x 2, tehát négy különöző számot hozhatunk létre: 00, 01, 10, 11. Ezt a sort tovább folytathatjuk, ha mindig megszorozzuk kettővel, hiszen a bit értéke csak kétféle lehet.

Három bit már 2 x 2 x 2, azaz 2^3, tehát összesen 8 féle különböző szám lehet, mégpedig a 000, 001, 010, 011, 100, 101, 110, és a 111.

Egy N számjegyből álló bináris szám olyan hosszú, amennyi az N értéke, és úgy tudjuk kiszámolni, hogy 2^N. Ha tehát megnézzük, az sha256 hash funkciója 256 bites, tehát a szám, amelyet generál, 2^{256} féle lehet. Ez egy elképzelhetetlenül nagy szám, egészen pontosan 78 számjegy hosszúságú a tizes számrendszerben. Több, mint amennyi atom létezik az ismert univerzumban. Így néz ki:

2^{256} = 115.792.089.237.316.195.423.570.985.008.687.907.853.
269.984.665.640.564.039.457.584.007.913.129.639.936

Ha bármilyen inputból az sha256 segítségével szeretnél hashelni, ennyi féle lehetséges output származhat belőle. Ezért mondjuk, hogy gyakorlatilag megjósolhatatlan a kimenetele. Nincs rá mód, hogy előre megmondjuk, adott inputból milyen output fog származni. Ez azzal lenne egyenlő, ha

előre pontosan megmondanánk, hogy 256 érmefeldobásból milyen sorrendben lesz fej vagy írás, és melyik hányszor fog bekövetkezni.

Ezt a számot nem fogjuk még egyszer leírni, csak a 2^{256} formájában hivatkozunk majd rá, de remélhetőleg segített elképzelni, hogy valójában mennyi is a lehetséges kimenetelek száma.

Hasheljünk valamit!

Próbáljuk ki egy konkrét példán, hogy hogyan is néz ki ez a gyakorlatban! Itt a könyvben hagyományos, tizes számrendszerbeli számként írjuk le, de természetesen a számítógépek binárisként számolják és kezelik ezeket.
A lényeg, hogy bemutassuk, egyetlen apró változtatás mekkora eltéréshez vezet az output esetén. Azonnal láthatod, hogy tényleg nem lehet megjósolni, kikövetkeztetni a kimenetet, bármennyire is hasonló a bemenet:

“Hello world!”
86991366044392467661783165166973309023807181648024718778313526389892860994842

“Hello world!!”
84940227720695898955447627108840424364390283616735576803008868844073193772558

Egyértelmű, hogy mindössze egyetlen felkiáltójel különbség a két input között teljesen más outputhoz vezet.
Egyszerűen nincsen rá mód, még számítógép segítségével sem, hogy a kimenetként kapott véletlenszerű szám visszafejtésével meghatározhassuk, hogy mi volt az input. Ha te magad is kísérleteznél, játszanál egy kicsit az sha256 képességeivel, egy jelszógenerátorral kedvedre próbálgathatod az alábbi oldalon:
https://passwordsgenerator.net/sha256-hash-generator

Proof of Work lottózás a hashelés segítségével

Most már tudjuk az alapokat, hogy rátérhessünk a valódi varázslatra a Bitcoin működésében. Beszéltünk róla, hogy az sha-256 esetében a kimenetelek száma 2^{256} lehet. Ez túl nagy szám, az egyszerűség kedvéért most tegyük fel, hogy mindössze 1000 variáció létezik.
A lottó rendszere az alábbiak szerint működik:

- Alice kihirdeti, hogy 2 dollár küldene Bob részére.
- Mindenki nekiáll lottószámokat generálni, az „Alice küld Bobnak 2 dollárt" tartalmú tranzakcióval, és ehhez hozzáadnak egy véletlenszerű számot, amelyet nonce (number using only once, azaz mindössze egyszer használt szám) néven ismerünk. Ez biztosítja, hogy nem használnak két egyforma inputot, így egyszerűbb megtalálni a nyerőszámot. A cél nem az, hogy mindenki ugyanazokat a számokat próbálgassa, hanem, hogy találjanak egy darab megfelelő nyerőszámot.
- Ha valakinél a nyerőszám kisebb, mint a célszám (ezt már említettük korábban, a következő fejezetben részletesebben is beszélünk róla), akkor megvan a nyertes.
- Ha a kapott szám nagyobb, mint a nyerőszám, a résztvevők újból próbálkoznak, egy másik nonce értékkel. „Alice küld Bobnak 2 dollárt, nonce = 12345", aztán „Alice küld Bobnak 2 dollárt, nonce = 67890", aztán „Alice küld Bobnak 2 dollárt, nonce = 918273645", és így tovább, egészen addig, míg a kapott szám végre kisebb lesz a célszámnál.

A célszámnál kisebb megoldás megtalálása nagyon-nagyon sokáig tarthat. Az esélyeket pedig azzal tudjuk befolyásolni, hogy mekkora mértékű célszámot állítunk be. Ha a fent említett 1000 lehetséges megoldás létezik, a célszámot pedig 100-ra állítjuk, akkor alapfokú matematikával kiszámolható, hogy a próbálkozások 10%-a lesz sikeres. Ha tehát egy olyan algoritmussal hashelsz, amellyel a lehetséges megoldások száma 1000, akkor 100-as célszámnál minden tizedik próbálkozásod fog sikerülni.

Tehát a lottó tulajdonképpen így működik. Meghatározzuk a célszámot, amelyet mindenki elfogad, ezután fogjuk a függőben lévő tranzakciók listáját, hozzáadjuk a nonce-ot, egy véletlenszerűen kiválasztott számot, és

indulhat a hashelés. Amint valaki talál egy olyan hasht, amely értéke kisebb a célszámnál, már ki is hirdeti a résztvevők között:

Helló mindenki!

- Ezeket a tranzakciókat hasheltem: Alice küld 2 dollárt Bobnak, Charlotte küld 5 dollárt Alicenek.
- Hozzáadtam a nonce-ot, amely a 32895-ös szám.
- Az output hash értéke 42 lett, ez kisebb, mint a célszám, hiszen az 100.
- Proof of Work: a tranzakciók adatai, az általam használt nonce, és a hash, amely ebből az inputból lett.

Lehet, hogy egymilliárdszor kellett próbálkozni, sok ezer dollárnyi áram elhasználásával, mire meglett a megfelelő hash, de mivel megosztom a résztvevőkkel, hogy mit használtam inputként, ők mindössze egyetlen próbálkozással ellenőrizni tudják, hogy tényleg megtaláltam a jó megoldást, meglett a nyertes szám. Ehhez elegendő ugyanezt az inputot használni, az outputot pedig összehasonlítani azzal, amelyet én küldök. Ha a kettő egyezik, az bizonyítja, hogy tényleg elvégeztem a munkát.

Ahogy már írtuk, a hashelés folyamatát fel lehet fogni kockadobálásként, ahol a lehetséges változatok száma annyi, mint ahány atom van az univerzumban. De csak a célszám alatti eredmény nyer, és meg kell mutatnod mindenkinek, hogy hogyan jött ki az a szám.

Hogyan tudjuk biztosítani, hogy ehhez tényleg sok energiára legyen szükség? Újból elmondhatjuk, a lehetséges kimenetelek száma több, mint amennyi atom létezik az ismert univerzumban. Ha elég alacsony célszámot

határozunk meg, akkor a hash értékeknek csak egy apró töredéke fog érvényesnek számítani. Így hát bárki, aki érvényes hasht szeretne találni, rengeteg próbálkozásnak néz elébe, rengeteg számítási kapacitást kell elhasználnia, ez pedig rengeteg energiát igényel, mert csak sokára fog a célszámnál alacsonyabb számot találni.

Minél kisebb a célszám, annál több próbálkozást igényel a nyertes hash megtalálása. Ha a célszám nagyobb, akkor pedig értelemszerűen könnyebb dolgunk van. Ha tudni lehet, hogy a célszám alá menni mindössze 1 a millióhoz az esélyünk, a nyertes szám megtalálása egyben azt is bizonyítja, hogy elvégeztük az egymillió próbálkozást, elvégeztük a munkát.

BÁNYÁSZAT

A Proof of Work lottózás folyamata, amely során elnyerhetjük a jogot, hogy a Bitcoin elosztott főkönyvébe, a nyilvántartásba feljegyezhessük a várakozó tranzakciókat, bányászat néven ismert. Lássuk, hogyan is működik:

- Bárki részt vehet, ehhez csak csatlakoznia kell a hálózathoz, futtatnia a Bitcoin szoftverét, és figyelni a tranzakciókra.
- Alice bejelenti, hogy 2 dollárt küld Bobnak. A hálózat gépei elterjesztik ezt az információt egymás között, amíg mindenkihez el nem jut.
- Mindenki, aki szeretne részt venni a lottóban, elkezdi a hashelést a tranzakciókkal és a nonce hozzáadásával az sha256 hash funkciója segítségével.
- Átlagosan 10 percenként egy számítógép talál egy számot, amely alacsonyabb a célszámnál, így megnyeri a lottót.
- Ez a gép ezután bejelenti a résztvevők számára a nyertes számot, hogy milyen inputot használt ehhez (tranzakciók plusz a nonce értéke). Lehet, hogy idáig eljutni órákig tart, de lehet, hogy csak pár másodperc. Ezek az információk, a tranzakciók adata, a nonce, és a megfelelő hash együtt, egy blokkot alkotnak.
- A hálózat többi résztvevője ellenőrzi a blokkot az adatok alapján. Ugyanabból az inputból megkapják ugyanazt a hasht outputként, és látják, hogy tényleg alacsonyabb a célszámnál, nincs érvénytelen tranzakció a listán, nincs összeütközés az előző blokkok adataival.
- Mindenki bemásolja a blokkot a saját nyilvántartásába, ez a blokk sorban következik az előtte lévők után, így egy blokkláncot alkotnak.

Tulajdonképpen ennyi az egész. Létrehoztuk az első blokkunkat, az első bejegyzésünket a nyilvántartásba, a Bitcoin főkönyvébe.

A médiában már olvashattad, hogy a Bitcoin bányászata során „komplex, nehéz kriptográfiai feladványokat, egyenleteket” kell megoldania a számítógépnek. Most már látod, hogy ez egyáltalán nem igaz. Feladványok megoldása helyett nem kell mást tenni, csak próbálkozni a kockadobálással, ugyanazt az egyszerű hashelést ismételgetni újra és újra, amíg nem találunk egy megfelelő számot. Egyszerű játék az esélyekkel, amelyhez el kell használni bizonyos mennyiségű energiát.

Hogyan jön létre új bitcoin?

Eddig úgy mondtuk, hogy Alice 2 dollárt küld Bobnak. Ezentúl viszont nem fogunk dollárról beszélni, mivel a Bitcoin semmit sem tud a dollárról. A bitcoin, mint digitális egység maga jelenti az értéket a Bitcoin hálózatán.

Hogy újrafogalmazzuk a példánkat, amikor Alice azt mondja, hogy 2 bitcoint küld Bobnak, akkor valójában azt hirdeti ki, hogy az adott bitcoin, amely az ő egyenlegén van, átkerül Bobhoz. Ezután valaki megnyeri a Proof of Work lottót, a tranzakció pedig bekerül egy blokkba.
De honnan van Alice egyenlegén az a 2 bitcoin? Hogyan indult a Bitcoin, és hogyan tudtak coinokat vásárolni az emberek, amikor még nem léteztek tőzsdék és váltók, ahol fiat pénzért, például dollárért hozzá lehetett jutni?

Mikor Satoshi létrehozta a Bitcoint, megtehette volna, hogy az adatbázisban saját maga számára elkönyveli mind a 21 millió bitcoint, és a többi embernek meg kellett volna vásárolnia tőle. Mindenesetre elég kevés indok van arra, hogy valaki egy olyan hálózathoz csatlakozzon, ahol az összes vagyon egyetlen kézben összpontosul. Megtehette volna, hogy egyfajta várólistát vezet be, amelyre fel lehet iratkozni, és egy email címmel esélyünk lehet valamennyi bitcoin megnyerésére. Ez viszont Sybil Attack, megszemélyesítés áldozatául eshetett volna, hiszen szinte ingyen hozhatunk létre bármennyi email címet.

Így hát maga a bányászat, a Proof of Work lottó, amely során hozzáférést kapunk a nyilvántartáshoz, az új blokk bejegyzéséhez, az szolgál az új bitcoinok létrehozására. Mikor érvényes blokkot hozol létre a hashelés folyamatával, miután elhasználtál nagy mennyiségű energiát a lottó

megnyeréséhez, akkor az általad hallott tranzakciókat mind felvezeted a főkönyvbe. De ezek mellett egy nagyon különleges tranzakciót is beleírsz, amelyet coinbase tranzakció néven ismerünk. Ez pedig azt mondja, hogy „12,5 BTC létre lett hozva, és Mary, a bányász részére elküldve, hogy kompenzáljuk ennek a blokknak a létrehozására fordított energia-felhasználását".

Pontosan ez a módja az új bitcoinok létrejöttének. Ez a folyamat a világon ténylegesen bárki számára lehetővé teszi, hogy létrehozza a saját bitcoinját bármiféle központi irányító nélkül, anélkül, hogy nyilvánosságra kellene hoznia a személyazonosságát. Mindössze ki kell fizetni az ehhez szükséges energia áramszámláját. Ez teszi ellenállóvá a bitcoin létrehozását a Sybil Attack módszerrel szemben. Ha coinokat akarsz, nincs más mód, el kell használnod a megfelelő mennyiségű energiát, és annak ki kell fizetni az árát, így tudod kibányászni a coinokat.

A blokkjutalom

Az a személy, aki megnyeri a Proof of Work lottót, saját magának is „ad" coinokat. De miért pont 12,5-öt, miért nem mondjuk ezret? Miért nem lehet csalni a rendszerben, és bármennyi coint adni magunknak?
A Bitcoin egy elosztott konszenzuson alapuló rendszer. Ez azt jelenti, hogy mindenkinek egyet kell értenie abban, hogy mi számít érvényesnek, mi az igazság. Ezt úgy lehet megvalósítani, hogy mindenki ugyanazt a szoftvert futtatja a saját gépén, amely ellenőrzi, hogy mindenki betartja-e ugyanazokat a pontosan meghatározott szabályokat, amelyeket összefoglalóan a Bitcoin konszenzus szabályainak hívunk. Minden egyes blokk, amelyet a bányászok létrehoznak, végigmegy ezen az ellenőrzésen. Ha megfelel a szabályoknak, mindenki beleírja a saját főkönyvébe, és mindenki elfogadja, hogy érvényes. Ha nem felel meg, akkor visszautasítják, nem kerül bele a nyilvántartásba.
A teljesség igénye nélkül lássunk néhány szabályt, amelynek meg kell felelni:

- Az érvényes blokk új bitcoin létrehozását is tartalmazza, ennek a mértéke pedig a programban meghatározott kibocsátási rátától

függ, annál nem több.
- A tranzakcióknak rendelkeznie kell a megfelelő digitális aláírással, amely bizonyítja, hogy az adott coinokat tényleg a tulajdonosuk akarja elkölteni.
- A blokkban nincs olyan tranzakció, amely ebben, vagy egy előző blokkban már egyszer elköltött coinokat akar újból elkölteni.
- A blokkban lévő adatok mennyisége nem haladhat meg egy bizonyos mértéket.
- A blokkhoz tartozó Proof of Work hash értéke kisebb a célszámnál, ez bizonyítja, hogy a véletlenszerű találgatás során el lett használva a megfelelő mennyiségű energia.

Ha Mary a bányászat során úgy dönt, hogy létrehoz magának egy kis mellékes jövedelmet, a többi résztvevő számítógépe vissza fogja utasítani a blokkját, mivel az érvénytelen lesz. Ez azért történik így, mert a Bitcoin programkódjában, amelyet mindenki a saját gépén futtat, van egy olyan kódrészlet, amely kimondja, „a jelenlegi blokkjutalom pontosan 12,5 BTC, ha látsz egy blokkot, amelyik ennél többet tartalmaz, az érvénytelen, utasítsd el”.

Ha Mary csalni próbál, és érvénytelen blokkot hozna létre, ez a blokk nem kerül bele a többiek főkönyvébe, ehelyett a létrehozására fordított rengeteg energia mind kárba vész, hiszen olyan dologra fordítódott, amit senki sem akar, a pénzhamisításra. Emiatt a bitcoin hamisítása gyakorlatilag megfizethetetlen, ahogyan erre Nick Szabo is rávilágított a Shelling out című értekezésében. Azt mindenki tudja, hogy egy pénz, amelyet könnyű hamisítani, nem a legjobb választás. A bitcoint ezzel szemben lehetetlen hamisítani, hiszen egy egyszerű matematikai ellenőrzéssel észre lehet venni a csalást.

Satoshi a Bitcoin első blokkjában, a Genesis blokkban bányászta ki az első bitcoinokat. A program nyílt forráskódú, ez pedig azt jelenti, hogy bárki szabadon belenézhet, megnézheti, hogyan működik, és ellenőrizheti, hogy semmiféle kétes dolog sincs a motorháztető alatt. Még maga Satoshi is részt kellett, hogy vegyen a Proof of Work lottóban, és milliónyi próbálkozást végrehajtania, hogy létrehozhassa az első blokkokat. Ő hozta

létre az egész rendszert, de még ő sem tudta meghamisítani az energiafelhasználás bizonyítékát, nem tudta megkerülni a szabályokat.

Bárki, aki őutána csatlakozott a hálózathoz, gyakorlatilag azonnal ellenőrizhette az összes blokkját, a generált hash értékét a szükséges célszámmal együtt, és megbizonyosodhatott arról, hogy ő is elhasználta a megfelelő mennyiségű energiát, hogy megtalálja a statisztikailag nehezen megtalálható nyerőszámot. Most képzeljük el, hogy a jelenlegi, bankok által irányított fiat pénzrendszerben mekkora esély van egy ilyen precíz, valós idejű auditra a pénznyomtatással kapcsolatban.

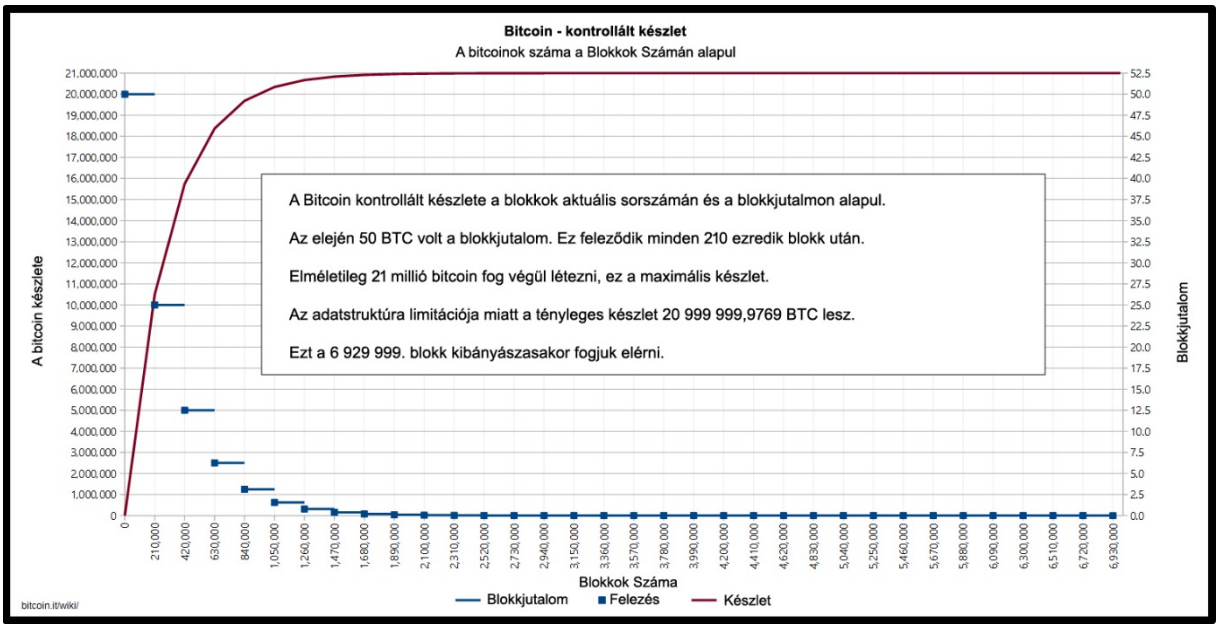
A felezés

A bányászat segítségével jön létre új bitcoin a hálózaton. De Satoshi olyan rendszert akart létrehozni, amelyben nem lehetséges a pénzrontás. Nem akarta, hogy a pénzkészlet folyamatosan, vég nélkül növekedjen. Ehelyett egy kibocsátási ütemtervet talált ki, amely először gyors iramban, majd az évek múlásával egyre lassulva hozza létre az új coinokat, egészen addig, míg évente már egyetlen új bitcoin sem kerül kibányászásra.

Kezdetben a blokkjutalom 50 bitcoin volt, Satoshi is ennyit kapott az első blokkokért, ugyanúgy, ahogyan a rendszerhez akkoriban csatlakozó új résztvevők is, amikor kibányászták a blokkjaikat.
A Bitcoin programja tartalmazza a blokkjutalom felezésének a kódját is, amely nagyjából négy évente megfelezi a blokkokért járó BTC mennyiségét. Nem is igazából az idő múlását követi, hanem a létrehozott blokkok számát, mivel átlagosan 10 percenként jön létre egy új blokk, és négy évente éri el a felezési értéket a blokkok száma.

2008-ban 50 bitcoin járt a bányászoknak, 2012 után 25, 2016-ban ez lement 12,5-re, és 2020 májusa után a blokkokért 6,25 bitcoin jutalmat ír jóvá a rendszer. A könyv írásakor, 2019 júniusában még a 12,5 fél bitcoinnak örülhetnek a bányászok, de kicsivel több, mint 50000 blokk múlva ez ismét a felére csökken, és az éves kibocsátási ráta már csak 1,8% lesz.

Tizenkét év múlva pedig, újabb három felezés után a bitcoin teljes 21 milliós készletének a 99%-a már forgalomban lesz, és blokkonként kevesebb, mint 1 BTC jár majd a bányászoknak. A bitcoinblockhalf.com oldalon te magad is megnézheted, hogy milyen ütemterv alapján kerül kibányászásra a bitcoin.



Végül nagyjából a 2140-es évek környékén a blokkjutalom nullára csökken, a bányászok számára pedig a tranzakciós jutalékok jelentik majd a bevételt, és a hálózat fenntartásáért járó jutalmat.

A kibocsátási ráta és a blokkjutalom mértéke rögzítve van a programban, amely teljesen nyílt forráskódú, így bárki meggyőződhet erről a saját szemével is. Így attól függetlenül, hogy mennyire megyünk előre a Bitcoin történetében, azok a blokkok, amelyek megszegnék ezeket a szabályokat, elutasításra kerülnek a többiek részéről, hiszen nem fognak megfelelni a közösen futtatott program követelményeinek, amennyiben ezek nem változnak.

A kibocsátás és a bányászat kontrollja

A bányászat számítógépeket és elektromosságot igényel, és minél több áll a rendelkezésedre ezekből, annál jobb esélyekkel indulsz a nyertes lottószám

megtalálására. Például, ha van 100 egyforma teljesítményű számítógép a hálózaton, és ebből 10 a tiéd, átlagosan az idő 10%-ában a tiéd lesz a nyertes szám. Mindenesetre a bányászat az esélyek és a véletlen összjátékán alapul, így lehetséges, hogy órákig, vagy akár napokig nem találsz új blokkot.

Az előző fejezetből már tudjuk, hogy a bányászok nem írhatnak jóvá maguknak csak úgy egy kis plusz jutalmat, mert ha megteszik, a többi résztvevő elutasítja a blokkjukat. De mi történik akkor, ha hajlandóak és képesek hatalmas mennyiségű plusz energia felhasználására, és ezzel felgyorsítják a blokkok generálását, egy csomó bitcoinhoz jutva, és egyben felborítva a kibocsátási ütemtervben meghatározott rátát?

Térjünk vissza a már használt példánkhoz, és mondjuk, hogy a hashelés során 1000 lehetséges output jöhet létre, a célszámot pedig 100-ra állítjuk. Ez alapján elmondhatjuk, hogy a próbálkozások 10%-a lesz kisebb a célszámnál, és ennyi esetben tudunk blokkot generálni.

Mondjuk, hogy minden egyes hash létrehozása 1 másodpercet vesz igénybe. Ha minden másodpercben megtesszük ezt, és a nyerő találatra 10% az esélyünk, akkor átlagosan 10 másodpercenként fogunk új blokkot találni.

De mi történik, ha nem egy, hanem kettő számítógép teszi ugyanezt? Kétszer olyan gyorsan tudják a hashelést csinálni, így nagyjából 5 másodpercenként jönne új blokk. Ha pedig 10 számítógépet használunk, akkor minden egyes másodpercben lesz egy nyerő találat.

Ez pedig baj: ha több ember bányászik, túl gyorsan jönnek létre az új blokkok. Ennek két következménye is lehet, és mi egyiket sem szeretnénk:

- Nem lehet tartani az előre meghatározott kibocsátási ütemet. Azt akarjuk, hogy nagyjából ugyanannyi bitcoin jöjjön létre óránként, hogy a teljes készlet 2140-re kerüljön forgalomba, ne pedig előbb.
- Problémát okozhat a hálózaton belül is, hiszen ha túl gyorsan jönnek egymás után a blokkok, akkor lesznek számítógépek,

amelyekhez nem jut el időben a legfrissebb blokk, mielőtt legenerálnák a következőt. Így nem lehet konszenzusra jutni, hogy lineárisan hogyan fest a főkönyv aktuális helyzete, ráadásul több bányász is blokkba foglalhatná ugyanazokat a tranzakciókat. Így a blokkok érvénytelenné válnak, mert a többiek azt látnák, hogy több blokkban is ugyanaz a bitcoin kerülne elköltésre.

Ha pedig túl kevés ember bányászik, az pont az ellentétes problémákhoz vezet:

- Túl lassan kerülnek forgalomba az új coinok, szintén felborítva a kibocsátási ütemtervet.
- Használhatatlanná válna a rendszer, hiszen órákat, napokat, vagy még hosszabb időt kellene várakozással tölteni a felhasználóknak, hogy a tranzakciókat blokkba foglalják a bányászok.

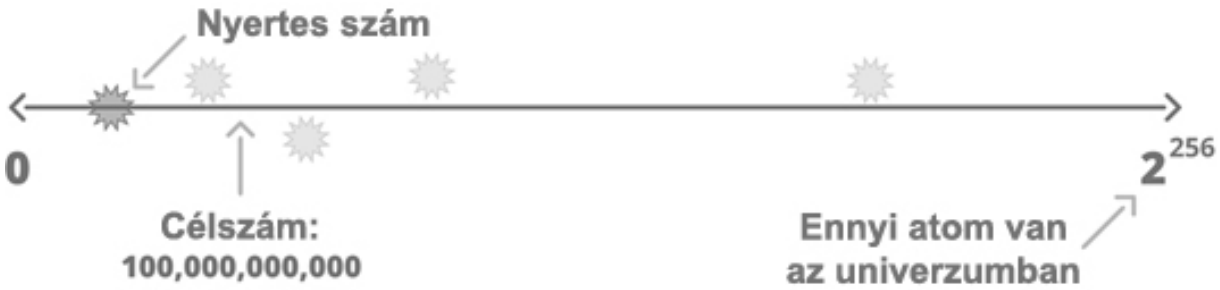
A hálózaton résztvevő összes számítógép másodpercenkénti hashelési kapacitását hashrátának nevezzük.

A blokkok közötti időtartam attól függően változik, hogy a hashráta növekszik vagy csökken, de persze a véletlen is szerepet játszik benne.

Nehézségi igazítás: határozzuk meg közösen a célszámot

A Bitcoin hálózatához bárki bármikor önkéntesen csatlakozhat, nincs főnök, aki irányítana, így természetesen a hashráta is nagy változatosságot mutat. Ki kellett találni valamit, hogy meghatározott ütemben jöjjenek a blokkok egymás után, ne gyorsuljon fel a kibocsátás, ha egy új bányász csatlakozik, és ne lassuljon, ha valaki kilép a rendszerből.

Hogyan tudjuk biztosítani, hogy nehezebb legyen megtalálni a nyerőszámot, ha sokan csatlakoznak újonnan, és könnyebbé váljon, ha sok a kilépő? Ahogyan már szóba került, a bitcoin bányászata nem más, mint egyfajta lottózás, ahol meg kell találnuk a nyerőszámot, amelynek kisebbnek kell lennie a célszámnál:



Egy ilyen kicsi célterületre kell eljutnunk. A lehetséges kimenetelek száma elképesztően hatalmas, így nagyon sokáig tart, mire a megfelelő értéket dobjuk a kockával.

A Bitcoin ezt a problémát az úgynevezett nehézségi igazítással oldja meg. Mindenki ugyanazt a programot futtatja, amely ugyanazokat a szabályokat várja el mindenkitől, és mindenkinek megvan az összes eddigi blokkot tartalmazó főkönyv másolata, mindenki ki tudja számolni, hogy milyen gyorsan jönnek egymás után a blokkok.

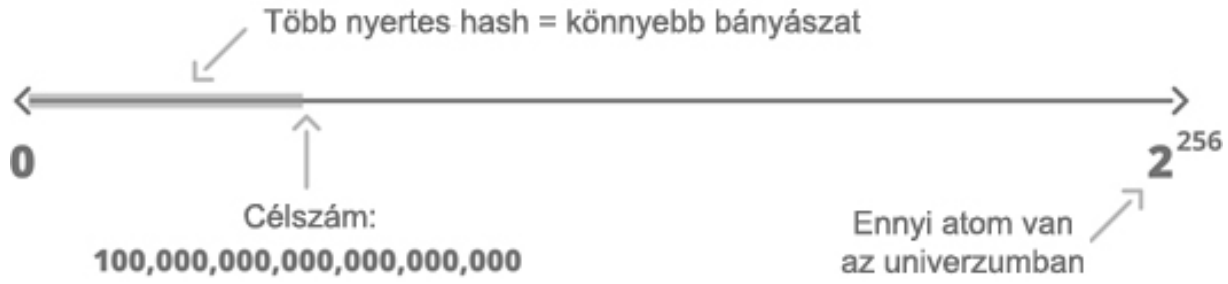
Minden alkalommal, amikor létrehoztunk 2016 új blokkot, ez nagyjából két hét[2] alatt megvan, megnézzük, hogy mennyi ideig tartott eljutni idáig, és ez alapján megváltoztatjuk a célszámunkat, hogy gyorsítsunk vagy lassítsunk a blokkok létrehozásán.

Mindenki megnézi, hogy ezt a 2016 blokkot átlagosan mennyi idő alatt sikerült létrehozni. 10 percnél sűrűbben jönnek a blokkok? Akkor túl

gyorsak vagyunk. 10 percnél ritkábban? Akkor viszont túl lassúak.

Ez alapján módosítani tudjuk a célszámot, így az alacsonyabb vagy magasabb lesz, attól függően, hogy a kódban meghatározott 10 perces blokkidőhöz gyorsítanunk vagy lassítanunk kell.

Meg tudjuk növelni a célszámot, így több nyerő lehetőséget biztosítunk a bányászok számára, ezzel együtt csökkentjük a felhasználandó energia mennyiségét. Ezt úgy nevezzük, hogy a nehézség csökkentése.



Ha megnöveljük a tartományt, amelyet el kell találniuk a bányászoknak, akkor kevesebb próbálkozással is meglesz a nyerőszám, olcsóbb lesz a blokk generálása.

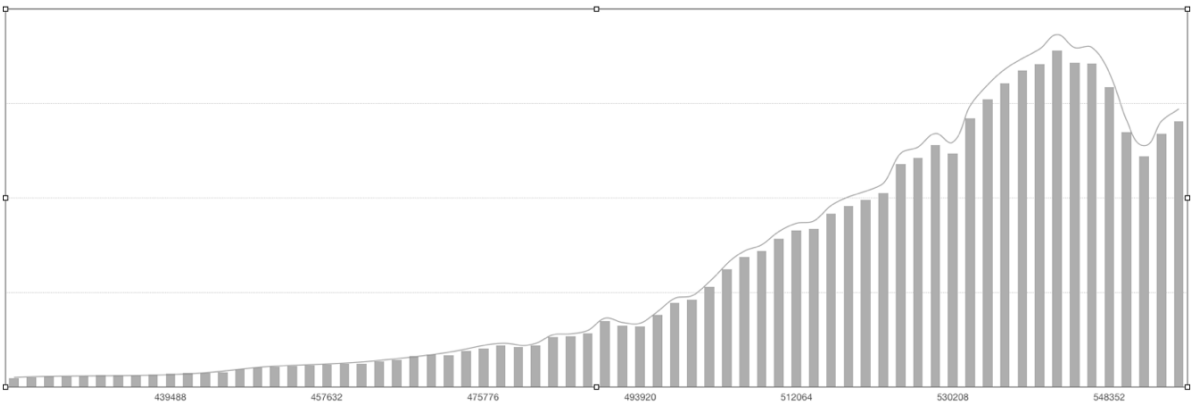
Ugyanígy csökkenteni is tudunk a célszámon, szűkíteni az érvényes hashek arányát, így a bányászoknak több energiát kell a nyertes szám megtalálására fordítani. Ekkor azt mondjuk, hogy növekszik a nehézség.

Ez alapján elmondhatjuk, hogy minden egyes 2016 blokkot tartalmazó intervallumban pontosan ismerjük a célszám értékét. Pontosan tudjuk, hogy melyik az a mágikus határ, amely a nyertes lottószámot jelenti, amelyet el kell érnünk a Proof of Work hashelése során minden egyes blokk létrehozásához.

A nehézségi igazítás, és a célszám meghatározása valószínűleg a Bitcoin innovációjának a legfontosabb eleme. Ez teszi lehetővé, hogy mindenki, másoktól függetlenül ellenőrizni tudja a nyertes lottószámot a másoktól függetlenül, de pontosan ugyanolyan módon kiszámolt célszám

ismeretében. Emiatt tudunk részt venni a lottózásban anélkül, hogy bárkinek el kellene mondania nekünk a nyertes számokat.

Az alábbiakban láthatsz egy grafikont, a vonal a hashráta értékét mutatja, az oszlopok pedig a nehézséget. A nehézség nem véletlen néz ki lépcsősornak, ez azért van, mert a rendszer lépésenként, minden 2016 blokk után tudja növelni az értékét. Láthatod, hogy minden esetben, amikor a hashráta nagyot növekedett, nem sokkal utána a nehézség is emelkedett, hogy lépést tudjon tartani a hashrátával. Amikor a hashráta viszont esik, mint ahogyan például 2018 októbere és decembere között láthattuk, a nehézség szintén fokozatosan csökken.



Hashráta és nehézség

A nehézség így 2016 blokk „lemaradással” követi a hashrátát. Emiatt viszont lehetséges, hogy ezen a 2016 blokkos perióduson belül nagy kilengés történjen a hashrátában, felfelé, vagy lefelé. Ezzel gyorsítani vagy lassítani lehet a bitcoin kibocsátási ütemét, kismértékben megsértve a kibocsátási ráta szabályait.

A hashráta növekedése viszont a legtöbbször azt jelenti, hogy nagy mennyiségű új bányászhardvert állított csatasorba valaki, ez pedig elég ritka, így a nagy kiugrások is elég ritkák, és nincs is túlságosan nagy hatásuk az összképre. Minden egyes kilengés csak abban a 2016 blokkos időintervallumban tud hatást kifejteni, amelyikben megjelenik, hiszen az utána következő nehézségi igazítás máris megváltoztatja a célszámot,

alkalmazkodva az új körülményekhez, a megváltozott hashrátához. Így vissza is térünk az átlagosan 10 percenként létrejövő blokkokhoz.

A hashráta és a BTC árfolyama

A Bitcoin automatikusan alkalmazkodik a hálózatán lottózók összesített hashelési kapacitásához, és hozzáigazítja a nehézséget. Ezzel a bányászok által a hálózaton elhasznált energiára reagál a rendszer. Ezen a ponton ér össze a digitális és a fizikai világ. A BTC árfolyama, a bányászhardverek és az áram költsége, valamint a nehézséget adó célszám egyfajta visszacsatolási hurkot hoznak létre.

- A spekulánsok bitcoint vásárolnak, mivel áremelkedésre számítanak, így az ár X dollárral növekszik.
- A bányászok X dollárral többet költenek az áramra és a hardverekre, hogy még több bitcoint tudjanak kibányászni.
- A nagyobb vásárlói igény áremelkedést okoz, így még több bányász csatlakozik, hiszen csinos profit érhető el a bányászaton.
- A több bányász nagyobb hashrátát jelent, ez pedig több energia felhasználását a bitcoin bányászata során, ezzel pedig még biztonságosabbá válik a hálózat. A vásárlók újból megnyugodnak, hogy a hálózati biztonság növekszik, ez pedig sokszor önmagában is újból felfelé hajtja az árat.
- 2016 blokk múlva az újonnan jelen lévő plusz hashráta emelkedést okoz a nehézségben.
- A magasabb nehézség miatt kisebb lesz a célszám, a bányászok kisebb eséllyel dobnak alá, és néhányan több, mint X dollárt költenek el a bányászatra.
- Ezek a bányászok így már nem tudnak profitot termelni, hiszen többet költenek áramra, mint amennyi pénzt a BTC értékesítéséért kapnak. Így kikapcsolják a gépeiket, az összesített hashráta pedig emiatt leesik.
- Újabb 2016 blokk múlva a nehézségi igazítással a célszám nagyobb lesz, könnyebbé válik a bányászat, hiszen kevesebben maradnak versenyben.

- A kisebb nehézség miatt a korábban nem nyereséges bányászok vissza tudnak térni a hálózatra, és még akár új bányászok is csatlakoznak.
- Újrakezdődik az egész, előről.

Egy medvepiacon, egy csökkenő árfolyamokat hozó trend esetén a ciklus pont az ellenkező módon működik, a felhasználók szabadulnak a coinjaiktól, ez áresést generál, a bányászok pedig ezért nem tudnak nyereségesen működni.

A nehézségi igazítás biztosítja, hogy az árfolyam és a hálózaton aktív hashráta között mindig lesz egyfajta egyensúly. Még ha az árfolyam hirtelen és drasztikusan le is zuhan valamiért, és ezzel például kiüti a nyeregből a bányászok felét, az utána következő igazítással ismét nyereségessé válik a részvétel.

A nehézségi igazítás alapvetően nagy segítség, hogy a kevésbé hatékony bányászokat kirostálja a rendszerből. Ezzel egyidőben azoknak kedvez, akik a lehető legolcsóbb áramot használják, és a lehető legalacsonyabb összköltség mellett tudnak bányászni. Idővel ez ahhoz vezethet, hogy a bányászok a világ távoli részeire is elmerészkednek, hogy feleslegben lévő, vagy akár teljesen kihasználatlan energiaforrásokat tudjanak hasznosítani. A CoinShares egyik 2019-es jelentése[3] alapján a bányászat energiaigényének közel 75%-a megújuló energiából származik.

Az elmúlt pár év során az árfolyam viszonylag gyors ütemben emelkedett, és ugyanez vonatkozik a hashrátára is. Minél nagyobb a hashráta, annál nehezebb megtámadni a hálózatot, hiszen az aktuális blokk megváltoztatásához is legalább az 51%-át kell irányítani a rendszernek. Azaz az eszközállomány több, mint a felét, így a hashráta több, mint a felét, ehhez pedig az elhasznált energiának több, mint a felét szintén a támadónak kellene biztosítania. Ez az energiafelhasználás pedig mára egy közepes méretű ország energiafogyasztásával egyenértékű.

A blokkjutalom vége és a jutalékok

Mikor évek múlva elérünk az utolsó kibányászott bitcoinhoz, és már nem lesz blokkjutalom, hogyan vesszük rá a bányászokat, hogy továbbra is fenntartsák a hálózatot? Miért égetnék el továbbra is az energiát, hogy biztosítsák a főkönyvünk használhatóságát? A Bitcoin válasza erre a tranzakciós jutalékok rendszere. Ezek nem csak, hogy helyettesíteni fogják a blokkjutalmat, de általános ösztönzőt is jelentenek a bányászok számára, hogy blokkba foglalják a tranzakciókat, ne csak a jutalomért generálják az üres blokkokat.

A jutalékok piaci alapon működnek. A felhasználók licitálnak a korlátozottan rendelkezésre álló tárhelyre a blokkokon belül. Tranzakció-indításkor megadjuk, hogy mennyit vagyunk hajlandóak fizetni a feldolgozásért, a bányászok pedig ezt az összeget látva eldöntik, hogy megcsinálják-e ennyiért vagy sem. Amikor kevés tranzakció várakozik a következő blokkra, a jutalékok alacsonyak, hiszen nincs verseny, mindenkinek jut hely. Amikor viszont megtelik az adott blokk, akkor egyes felhasználók rálicitálnak a jutalék, a fee mértékére, hogy biztosan bekerüljenek a következő blokkba, hogy gyorsan lekönyveljék a tranzakciójukat. Akik nem akarnak sokat fizetni, azok beállíthatnak kisebb összeget is, de ilyenkor tovább kell várni, hogy elég hely szabaduljon fel a blokkokban.

A hagyományos pénzügyi rendszerben a jutalék mértéke általában százalékos, tehát a tranzakcióval feldolgozott összeg bizonyos hányada. A Bitcoin esetében a továbbított érték nem számít. A jutalék ehelyett a felhasznált tárhely mértékével arányos. A jutalékot satoshiban határozzák meg, mégpedig az alapján, hogy a tranzakcióhoz mennyi hely kell, hány bájtot foglal el a benne foglalt adat. Például ha valaki egymillió bitcoint akar küldeni egy másik felhasználónak, az a tranzakció kevesebbe kerül, mintha 1 bitcoint 10 címzett között osztanánk fel. Ez utóbbi esetben lényegesen több adatot kell rögzítenünk, több tárhelyet igényel a tranzakció, több jutalékot kell fizetnünk.

A múltban előfordult, hogy nagy igény jelentkezett a Bitcoinra, ilyen volt például a 2017-es év végi őrületes bullrun is. Akkor a jutalékok mértéke extrém magasságokba ért. Azóta már kapott néhány fejlesztést a hálózat, amelyek csökkentik az ilyen irányú terhelést.

Az egyik a Segregated Witness, SegWit néven ismert megoldás, amely a blokkokban lévő adatot rendezi át különböző okos trükkök segítségével. Az így küldött tranzakciók, bár belefférnek a limitbe, tényleges formájukban akár nagyobb helyet is foglalhatnak, mint az eredeti blokkok által meghatározott 1 MB. Mindenesetre ebbe jobban most nem megyünk bele, ez kívül esik ennek a könyvnek a fő csapásirányán.

Egy másik jó módszer a kötegelés. Tőzsdék, vagy más, nagy volument bonyolító résztvevők elkezdték kombinálni a tranzakciókat több felhasználó között, és ezeket egyetlen közös tranzakcióba összehozni. A hagyományos bankszámlák közötti utalásnál, vagy a PayPal esetében egy küldő van, és egy címzett. A Bitcoin viszont lehetővé teszi, hogy az input és az output is nagyszámú legyen. Így például egy tőzsde, ha 100 ember számára hajtana végre kiutalást, ezt egyetlen tranzakcióban megteheti. Ez sokkal hatékonyabb módja a blokk-tárhely kihasználásának, és a másodpercenkénti néhány tranzakció helyett másodpercenként több ezer kifizetést tesz lehetővé.

A SegWit és a kötegelés már most nagyon jó hatást gyakorolt a blokk-tárhely iránti igény csökkentésére. Emellett viszont további fejlesztések is úton vannak, amelyek még hatékonyabb helykihasználást tesznek majd lehetővé. Mindezek mellett is el fog jönni viszont az az idő újra, amikor a hatalmas igény miatt a helykínálat szűkössé válik, a blokkok megtelnek és a jutalékok ismét magasak lesznek.

Mostanra szinte már teljesen kialakult a Bitcoin rendszere:

- A központi bankot lecseréltük egy elosztott főkönyvre.
- Kitaláltunk egy lottósorsolást, amellyel eldöntjük, ki írhat bele a főkönyvbe.
- A lottóban résztvevőket arra kényszerítjük, hogy valódi energiát használjanak el a részvételhez; ezzel párhuzamosan könnyűvé tettük, hogy bárki leellenőrizhesse a hashelés során kapott nyertes számot, a bárkitől függetlenül kiszámolható célszám birtokában.

- Elmondtuk a résztvevőknek, hogy ha nem tartják be a szabályokat, akkor a blokkjaikat el fogjuk utasítani, és nem kapják meg a blokkjutalmat sem. Így a csalás pézügyi veszteséggel jár, a becsületes viselkedés pedig jutalmat kap.
- Irányítjuk a kibocsátás sebességét, és a célszám meghatározását, mivel a programkódban meghatározott szabályok alapján az előző 2016 blokk adataiból bárki kikalkulálhatja, hogy mennyinek kell lennie az aktális célszámnak.
- Biztosítjuk, hogy az előre betervezett kibocsátási ráta megmaradjon, ezért a nehézséget időszakosan hozzáigazítjuk a hashráta csökkenő vagy emelkedő mértékéhez.
- Nyílt forráskóddal dolgozunk, hogy bárki szabadon leellenőrizhesse, hogy mindenkire ugyanazok a szabályok vonatkoznak a tranzakciók igazolása, a blokkjutalom, és a nehézség kiszámolása során is.

Nincs többé központi szereplő. Egy teljesen elosztott, decentralizált rendszerünk van. Már majdnem a teljes képet látjuk. Mindössze egyetlen probléma maradt: amikor valaki újonnan csatlakozik a hálózathoz, és elkéri a többiektől a főkönyv másolatát, lehet, hogy a különböző csomópontoktól különböző változatokban kapja meg. Hogyan tudjuk biztosítani, hogy egyetlen valódi, folytonos tranzakciós történet létezzen, és, hogy a bányászok ne tudják újraírni a múltat?

MEGBÍZHATÓ FŐKÖNYV

Mostanra már tudjuk, hogy hogyan lehet fenntartani egy elosztott főkönyvet, és hogyan tudjuk frissíteni, új adatokat rögzíteni anélkül, hogy korrupció, vagy kényszerítés léphetne fel, köszönhetően a lottó-szerű rendszernek, és a konszenzusnak.

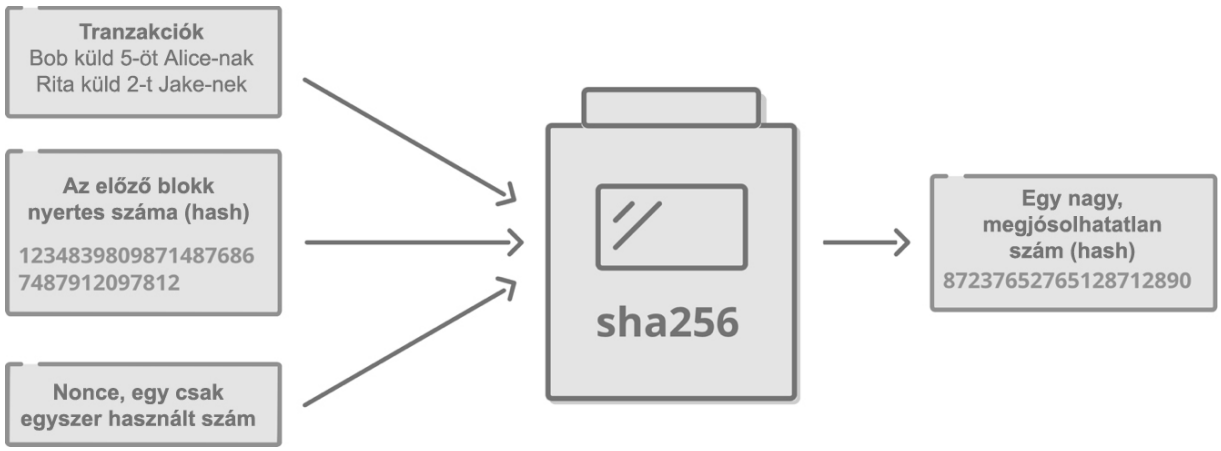
De mi történik, ha a lottónyertes az, aki becstelen lépésre szánja el magát? Képes egy bányász arra, hogy a főkönyv előző bejegyzéseit visszamenőleg megváltoztassa? Ha összeesküvést szőnek, Eve, Dave és Farrah képesek lehetnek átírni a nyilvántartásban a tranzakciókat, esetleg megváltoztatni az egyenlegeket, és plusz coinokat jóváírni maguknak?

Itt jön be a képbe a blokklánc, mint fogalom. A blokklánc valójában csak egy iparági marketing kifejezés, amely arra utal, hogy a blokkok lánc-szerűen vannak összefűzve, úgy követik egymást adott időközönként, linkekkel összekötve. Ennek a segítségével lehet létrehozni a tranzakciós történet folytonos, lineáris nyilvántartását, a coinok létrehozását és elköltését rögzítő főkönyvet, egészen a 2009-es Satoshi-féle Genesis blokktól a mai napig.

Az előző fejezetekben nem említettünk meg egy fontos dolgot, mert az egyszerűségre, érthetőségre törekedtünk. Mikor a hasheléssel foglalkozunk a Proof of Work lottózás folyamatában, tehát bányászunk, az input nem csak a tranzakciókból és a nonce értékéből áll. Hozzáadjuk még a hasht is az előző blokkból, így az általunk létrehozott, legfrissebb blokk közvetlenül összekapcsolódik az előző blokk adataival.

Tudjuk, hogy a hash funkció teljesen véletlenszerű számokat generál, de mindig attól függ, hogy milyen inputtal dolgozunk. Most tehát három különböző input kerül a blokkba:

- Az aktuális, függőben lévő tranzakciók.
- A nonce, egy véletlenszerűen kiválasztott szám.
- Az előző blokkból generált hash.



A nyertes lottószámot jelentő hash tartalmazza az előző blokkhoz szükséges nyerőszámot is, így közvetlenül egymáshoz kapcsolja a két blokkot.

Ezzel lehetőség nyílik arra, hogy egy historikus nyilvántartást vezethessünk, ahol minden egyes blokk egészen a legelső Genesis blokkig visszavezethető. Mikor új blokkot generálunk, és beleírnánk egy tranzakciót a főkönyvbe, meg kell győződnünk róla, hogy az abban szereplő coinok nem lettek már korábban elköltve.

Ha megváltoznak az adatok, amelyekből a hash outputja származik, akkor maga a hash is megváltozik, mégpedig megjósolhatatlan módon, de drasztikus mértékben. Ha bármely blokk adatait módosítani akarjuk, azzal megváltozik az adott blokk hash értéke. Viszont ez a hash szerepet játszott az utána következő blokk hash-értékének a megállapításában, tehát ha megváltoztatod, az utána következők is megváltoznak. Minden blokk hash értéke hozzá van kötve az összes megelőző blokkhoz, ezt akár elképzelhetjük pillanatképként is, amely a teljes eddigi tranzakciós történetet, az összes bejegyzést egyszerre tartalmazza.

Mindenki ki tudja számolni, hogy a szükséges célszám eléréséhez mennyi energiára van szükség, hogy megtaláljuk a megfelelő hasht, így a Proof of Work használata esetén nincs mód csalásra. Ha valaki egy régebbi blokk adatait akarná módosítani, újra kellene számolnia az ahhoz tartozó hasht, elhasználva ugyanannyi energiát, mint a blokk létrehozásakor, emellett ugyanezt kellene tennie az összes utána következő blokk esetében is. Nem

csak, hogy bizonyítható lenne a módosítás ténye, de extrém mennyiségű energiába, így rengeteg pénzbe kerülne ez a próbálkozás.

Gyakorlatilag a Bitcoin hálózatán minden egyes új blokk növeli a rendszer biztonságát, hiszen plusz mennyiségű energiát igényelne minden egyes új blokk újraszámolása a Proof of Work hash létrehozásához. A legtöbb felhasználó azon a nézeten van, hogy azok a tranzakciók, amelyek blokkja után már legalább hat újabb blokk létrejött, véglegesnek minősülnek. A mai hashráta ismeretében elképesztő mennyiségű energiát igényelne a legutolsó hat blokk újraszámolása egy esetleges támadás esetén. Ha pedig valaki 100 blokkra visszamenőleg szeretné módosítani az adatokat? Felejtsd el.

Mikor csatlakozol a hálózathoz, és letöltöd a blokkláncot, a főkönyvet a saját gépedre, minden egyes tranzakció minden egyes blokkban teljesen transzparens. Le tudod ellenőrizni te magad is a Proof of Work hash értékeit, hogy a személy, aki elküldte neked, hiteles másolatot küldött, semmit nem módosított rajta.

Amikor két blokk összeér

Van még valami a konszenzus esetén, amelyet figyelembe kell vennünk: hogyan tudjuk biztosítani, hogy mindenkinél ugyanaz a lineáris tranzakciós történet legyen meg, ha két bányász egyszerre, ugyanabban az időpillanatban tud blokkot létrehozni, és ezeket elküldeni a hálózat többi résztvevőjének?

Egy világméretű hálózatról beszélünk. Az Egyesült Államokban ugyanúgy vannak bányászok, mint Kelet-Ázsiában, és mindenki ugyanazt a Proof of Work lottót játsza, egyszerre.
Valaki Chicagoban blokkot talál, azaz a kapott hash értéke a célszám alá esik. Kihirdeti a hálózaton, és a többi résztvevő Amerika-szerte elkezdi bemásolni a saját főkönyvébe.
Pár másodperc különbséggel viszont Sanghajban is blokkot talál egy bányász. A fizikailag, földrajzilag hozzá közelebb lévő csomópontok még

nem értesültek az amerikai blokkról, így ők először a kínai blokkot vezetik fel a saját nyilvántartásukba.

Mindkét blokkban szerepel, hogy Alice 1 dollárt küld Bobnak. Bob viszont ahogy megkapja a pénzt, azonnal tovább is küldi Charlie számára. Az időzítési különbségek miatt az újabb amerikai blokk ezt a tranzakciót is előbb hallja, és feljegyzi, hogy Bob végső egyenlege 0 dollár. Kínába viszont még nem érkezett meg ez az információ, így anélkül jön létre a blokk, hogy tartalmazná Bob költését, így a kínai változatban Bob még mindig 1 dollárral rendelkezik.

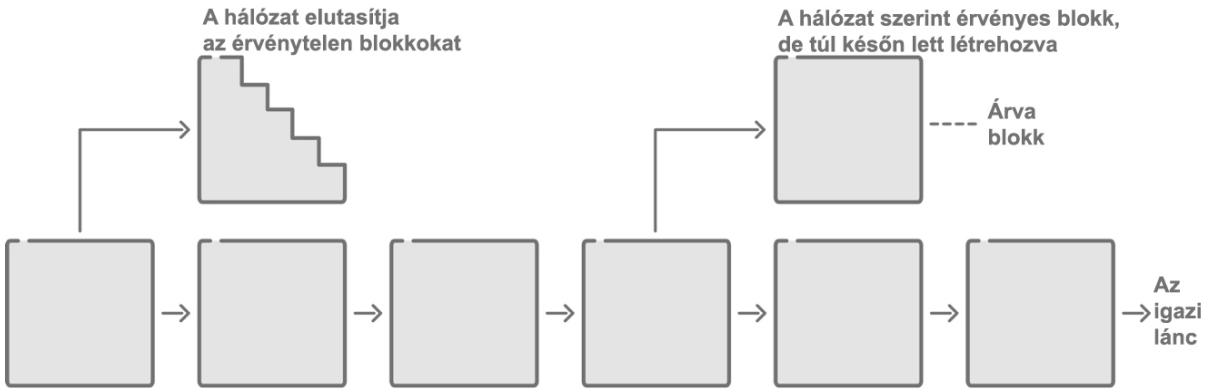
A hálózat így megosztottá válik, hogy melyik főkönyv a helyes, valódi példány. A probléma az, hogy mindkét blokk érvényes, hiszen mindkettő érvényes tranzakciókat tartalmaz, és mindkettő az előző blokkok tranzakciós történetének a megfelelő folytatása. Mindkettőhöz bizonyíthatóan el lett használva a megfelelő mennyiségű energia a Proof of Work során. Ezt lánc-elágazódásnak hívják, a blokklánc kettéválik, két egyformán érvényesnek tűnő lánccá, de nincsen központi szereplő, aki megmondaná, hogy melyik az érvényes. Mit lehet ilyenkor tenni?

A Bitcoin megoldása egyszerű. Dőljünk hátra, és várjunk. A bányászok szabadon eldönthetik, hogy melyik blokkot fogadják el érvényesnek, melyikkel folytatják tovább a láncot. Az amerikaiak az általuk hallott blokkot folytatják, a kínaiak pedig az ő blokkjukat veszik alapul.

A következő, nagyjából 10 perces intervallumban létrejön az újabb blokk. A Bitcoin kódjában meg van határozva, hogy elágazódás esetén az a lánc nyer, az lesz érvényesnek tekintve, amely több energiát használt el a Proof of Work során. Ez egy nagyon fontos szabály a Bitcoin működésében, a rendszer összesíti, hogy mennyi munka lett belefektetve a lánc továbbvitelébe, és a nagyobb értékűt választja érvényesnek. Ezt a szabályt Satoshi tiszteletére a számítástechnika-tudományokban Nakamoto-konszenzusnak nevezik.

Mondjuk, hogy a kínaiak előbb bányásszák ki a következő blokkot. Így az ő láncuk most egy blokk előnnyel rendelkezik az amerikai lánchoz képest, és

több munkát is végeztek, több a Proof of Work értéke. Mikor ezt az új blokkot kihirdetik a hálózaton, az amerikai csomópontok felismerik, hogy a kínai csomópontok által futtatott lánc értékesebb, több energiát, több munkát fektettek bele, így újraszervezik a saját láncukat. Ez azt jelenti, hogy az ő legfrissebb blokkjukat lecserélik a kínaiak által bányászott két új blokkra.



Az elágazódás természetes folyamat, akkor következik be, ha két bányász egyszerre talál blokkot. Az a lánc lesz az érvényes, amely több befektetett munkát tartalmaz, a másik nem folytatódik, úgymond árva lesz.

Az amerikai blokk most már árva blokknak számít. Mivel a hálózat elutasítja, a bányász nem kapja meg érte a blokkjutalmat, a belefoglalt tranzakciókat pedig nem jegyzik fel a főkönyvbe. Ezek a tranzakciók természetesen nem vesznek el. Néhány amúgy is benne van a másik, a kínai blokkban, és amelyik nem, az is belekerül valamelyik következőbe.

A bányászok minden tranzakciót az úgynevezett mempool-ban tárolnak addig, amíg blokkba nem kerülnek. Az elutasított blokkokból ide kerülnek vissza a tranzakciók. Amennyiben érvényes tranzakciók, és nem kerülnek összetűzésbe a rendszer eddigi nyilvántartásával, úgy egy későbbi blokkba kerülnek bele.

Ebben a példában amerikai és kínai blokkról, csomópontokról beszélünk, mivel fizikailag elég messze vannak egymástól, hogy számítson az a pár másodperces különbség az adatátvitelben. A valóságban azonban a csomópontok semmit sem tudnak egymás személyazonosságáról, vagy a

földrajzi helyzetükről. Az egyetlen információ, amelyre szükségük van, az a Proof of Work során elhasznált energia bizonyítása, hogy kiderüljön, melyik lánc értékesebb, és az, hogy a blokkba foglalandó tranzakciók érvényesek, nem számítanak például dupla költésnek.

Ezek a fajta lánc-elágazódások normálisak, és időről időre megtörténnek a Bitcoin hálózatán. Szinte kivétel nélkül megoldódnak a következő blokk létrejöttekor. Az internet-hálózati kapcsolatok sebességének a növekedése, és a blokkok terjedésének a javulása egyre ritkábbá teszik majd ezt a fajta problémát. Ma, és valószínűleg a belátható közeljövőben is a Bitcoin továbbra is szigorúan meghatározza, hogy mennyi adatot lehet beletenni egy blokkba. Ennek, és a 10 perces blokkidőnek is köszönhető, hogy az árva blokkok elég ritkának számítanak, hiszen kevés adatot kell megosztani a többi résztvevővel, és elég hosszú idő áll ehhez rendelkezésre.

A bányászat a véletlenen alapul. Néha pontosan 10 perc telik el a blokkok között, de néha előfordul, hogy csak néhány másodperc. Ha másodpercenként hozzuk létre az új blokkokat, vagy túl sok adatot zsúfolunk bele, nagy a valószínűsége, hogy az amerikai és a kínai csomópontok össze fognak ütközni. Földrajzilag messze vannak egymástól, és hosszabb ideig tart az adatátvitel. Ha az árva blokkok túl gyakoriak, a blokklánc széteshet. Árva blokkok következhetnek árva blokkok után, a csomópontok pedig nem tudják kiválasztani, hogy melyik az érvényes, mert közben már érkezik is a következő.

Nagyon fontos, hogy a blokkok viszonylag kicsik maradjanak, hogy a hálózat összes résztvevője megkapja a friss adatokat még a következő blokk létrehozása előtt. Egy másik, szintén fontos oka is van a kis blokkok használatának. A csomópontok futtatásához szükséges hardveres követelmények így alacsonyak maradhatnak, ezzel ösztönözni lehet a további csomópontok, bányászok részvételét a decentralizált hálózat fenntartásában. A nagy blokkok arra ösztönöznék a bányászokat, hogy adatközpontokba telepítsék a tevékenységeiket, sokszor ugyanabba a földrajzi régióba „összeköltözve”, így megakadályozva a nyereségességet csökkentő árva blokkok előfordulását.

Az egyetlen valódi lánc

Menjünk vissza ahhoz a részhez az egyik korábbi fejezetben, hogy Henry újonnan csatlakozik a hálózathoz.
Az általa futtatott csomópont csatlakozik néhány másik csomóponthoz, és megkéri azokat, hogy ajánljanak számára további csomópontokat, amelyekhez szintén csatlakozhat. Ezt nevezik csomópont-felfedezésnek.

A csomópontok közül néhány azonban nem játszik tisztességesen, és a főkönyv manipulált változatát adják oda Henrynek, érvénytelen tranzakciókkal, vagy hamis egyenlegekkel, amelyek nem rendelkeznek érvényes Proof of Work hash értékkel. Ezeket a csomópontokat a Henry által futtatott szoftver azonnal elutasítja, és megakadályozza, hogy a továbbiakban Henry gépéhez csatlakozzanak[4].

A többi csomópont becsületes, viszont az általuk küldött főkönyvek nem egyeznek meg. Néhány esetleg offline volt egy ideig, és egy vagy két blokk hátrányban van a többiekhez képest. Ha Henry több különböző változatot tölt le a nyilvántartásból, amelyek egyformán érvényesnek számítanak, a program a Nakamoto-konszenzus segítségével dönti el, hogy melyik az érvényes. Összeveti az egyes másolatok által elvégzett munkát a Proof of Work használatával, és amelyik a többet éri, az lesz az egyetlen valódi lánc.

A csomópontok folyamatosan kommunikálnak egymással, hogy biztosan mindenkinél ott legyen a legújabb blokk is. Mivel minden csomópont az értékesebb láncot fogadja el érvényesnek, ebből származik a megegyezés, a konszenzus, hogy mi a főkönyv aktuális állapota. Henry nincs rákényszerülve, hogy a többség szavára hallgasson, amelyet el lehet téríteni egyszerűen azáltal, hogy a csalásra sikerül rávenni a többséget.

Ha Henry több tucatnyi rosszindulatú csomóponthoz csatlakozik, és csak egyetlen becsületeshez, a gépén futtatott Bitcoin programja akkor is tudni fogja, hogy melyik változat az érvényes, mivel az fogja a nagyobb Proof of Work értéket tartalmazni, és visszavezethető egészen a Genesis blokkig. Ennek a fontosságát nem lehet eléggé hangsúlyozni. Nem kell megbízni senkiben, hogy a kapott adatok hitelesek, mivel a saját csomópont

segítségével minden egyes hash értéket le tud ellenőrizni, így tudhatja, hogy a valódi, érvényes blokklánc van nála.

Éppen emiatt rendkívül nehéz egy rosszindulatú hackernek, hogy hamis másolatot juttasson el egy csomópontba. Hogy ez sikerüljön, biztosítani kell, hogy az új csomópont semmilyen más, becsületes csomóponthoz nem csatlakozik, csak azokhoz a módosítottakhoz, amelyeket a támadó eltérített.

A tranzakciók visszavonása

A láncok kettéágazására van ugyan esély, de ha ilyen történik, az hamar megoldódik. Mindenesetre, ha valaki meg akarna támadni egy hálózatot, akkor kihasználhatja a Nakamoto-konszenzust, ha irányítani tudja a hashráta több, mint 50%-át. A támadó ilyenkor több munkát fektethet bele a hamis lánc létrehozásába, amely tartalmazza az általa kívánt tranzakciókat, ha hajlandó az ehhez szükséges energiát elhasználni, nagyobb Proof of Work értéket adva neki. Mikor pedig megosztja a hálózattal ezt a láncot, a csomópontok ezt fogadnák el egyetlen valódi láncként. Ezt 51%-os támadásnak nevezzük, mert az elkövetéséhez szükség van a hashráta több, mint a felének az irányítására.

A Bitcoin tranzakciók esetén fontos megérteni, hogy teljes véglegesség nem létezik, mivel mindig van matematikai esély az 51%-os támadásra, és árva blokkok is képződhetnek. Emiatt a tranzakciók címzettjei általában megvárnak néhány új blokkot, hogy véglegesnek tekintsék a történteket. Több blokk esetén már annyira sok energia kellene a manipulációhoz, hogy nem valószínű annak a bekövetkezte.

A blokkok bányászatakor az előző blokk hash-értékét is mindig az inputok közé teszik a bányászok, ebből származik az úgynevezett konfirmáció. Ha azt hallod, hogy egy tranzakciónak hat konfirmációja van, az azt jelenti, hogy a tranzakciót tartalmazó blokk után már hat újabb blokkot is létrehoztak. Ha digitális könyveket adsz el a webshopodban, amelynek nincsen sok plusz költsége, esetleg 1 konfirmációval is megelégedhetsz, vagy éppen azonnal teljesítettnek fogadod el a tranzakciót, és amint látod a

mempoolban a bejegyzést, már küldöd is a letöltő-linket a vásárlónak. Viszont ha egy lakóházat adsz el, akkor esetleg 12 konfirmációt, két órát is hajlandó vagy kivárni. Minél több konfirmációt akarsz, minél tovább vársz, annál több Proof of Work kerül bele a blokkokba, annál több energiát használnak el a bányászok a valódi, fizikai világban, annál drágább lenne a manipulációs kísérlet, a tranzakció visszafordítása. Manapság az az elterjedt nézet, hogy hat konfirmáció után már biztosan megtörténtnek vehetjük a tranzakciókat.

Ha a Bitcoin hashrátája jelentős mértékben lecsökkenne valamiért, tehát kevesebb energia kellene a blokkok létrehozásához, akkor módunk van rá, hogy növeljük a szükségesnek tartott konfirmációk számát. Első ránézésre nem hangzik túl jól, hogy várni kell a tranzakciók véglegesítésére, de ehhez érdemes figyelembe venni, hogy a bankkártyás tranzakciókat akár 120 nap múltán is vissza tudják fordítani.

A Bitcoin tranzakciók ezzel szemben mindössze néhány blokkig tekinthetők elméletben visszafordíthatónak. A kereskedők szemszögéből nézve a véglegesség és a visszafordíthatóság tekintetében így a Bitcoin hatalmas előrelépést jelent a hagyományos digitális fizetési, pénzügyi megoldásokhoz képest.

Léteznek becslések, amelyekből kiderül, hogy ha egy egész ország energiatermelését irányítanád is, és nálad lenne az összes létező Bitcoin-bányászgép, akkor is több, mint egy évig tartana, mire a teljes lánc-történetet újra tudnád írni. Ha több adatra vagy kíváncsi ezzel kapcsolatban, a http://bitcoin.sipa.be oldalon kedvedre nézelődhetsz.

HARD FORKOK ÉS 51%-OS TÁMADÁSOK

A kezdetekben Satoshi az első bitcoinokat a saját számítógépe processzorával, a CPU-val bányászta ki. A bányászati nehézség ekkor még alacsony volt, így nem került túlságosan sokba, hogy a számítógépével kibányászhassa ezeket a coinokat.

Az idő múlásával a hozzáértő felhasználók elkezdtek belenyúlni a bányász-programba, hogy minél hatékonyabbá tegyék. Nemsokára megjelent az első szoftver, amely már használni tudta a gépek videókártyáit, a GPU-kat is, amelyeket elsősorban a játékok futtatására terveztek.

A videókártyák segítségével a bányászat pedig nagyságrendekkel hatékonyabbá vált a CPU bányászathoz képest. A nehézség gyorsan emelkedett, ahogy egyre több hashráta érkezett a hálózatra az újonnan rendszerbe álló videókártyák részéről. Ez volt az a pont, ahol a kizárólag processzorral bányászóknak már nem volt nyereséges a további részvétel, így lekapcsolták a gépeiket.

A GPU bányászat egy új versenyző megjelenése miatt került bajba: az Applikáció-specifikus Integrált Áramkörök, azaz az ASIC-csipek megalkotásával. Az ASIC bányászgépek speciális csipeket tartalmaznak, amelyek kizárólag egyetlen dologra jók, a Bitcoin sha256 hash funkciójának a futtatására. Mivel pedig csak ezt csinálják, a GPU bányászathoz képest ismét nagyságrendet lépett a hatékonyság. A nehézség újból emelkedésnek indult, az ASIC miatt pedig a GPU-bányászat elvesztette a nyereségességét, ahogy a videókártyák miatt ugyanez történt a processzoros bányászattal is. Mostanra oda jutottunk, hogy pár évente megjelenik egy új változat az ASIC gépekből, amely elavulttá teszi a régebbi modelleket, annyival jobb a hatékonysága.

Az első bányászok mindössze centeket költöttek a hasheléshez szükséges elektromosságra. Ahogyan a bitcoin ára emelkedett, egyre több bányász csatlakozott, a hashráta növekedett, és növekedett a nehézség is. Emiatt egyre drágább lett a bányászat. Mára, 2019-ben az árfolyam 8000 dollár

környékén jár, az emberek pedig több ezer dollárnyi áramot használnak el egyetlen coin létrehozásához is.

Bányászpoolok

A bányászattal az a fő probléma, hogy véletlenszerű, mint a kockadobálás. Emiatt lehetséges, hogy rengeteg energiát elhasználsz, rengeteg hashelést végzel, de mégsem találsz egyetlen érvényes blokkot sem.

2010-ben ennek a megoldásaként jelent meg egy innováció, az úgynevezett bányászpool, hogy megoldja a problémát, amely során a bányászok energiát használnak el, de nem kapnak jutalmat. A poolok a biztosítótársaságokhoz hasonlóan a kockázatokat osztják meg a résztvevők között.

A bányászok a pool keretein belül végzik a tevékenységüket, így a hálózat szempontjából egyetlen nagy résztvevőnek számítanak. Ha bárki blokkot talál, az érte kapott jutalmat a poolba beadott egyéni hashrátájuk arányában osztják szét. Ezzel a módszerrel a kisebb bányászok is bitcoinhoz juthatnak, még ha összességében nagyon kevés hashrátát is tudnak csak a bányászatra fordítani. A pool üzemeltetője pedig bizonyos százalékot magának is megtart a jutalomból, cserébe az együttműködés koordinálásáért, a pool fenntartásáért.

A poolok valamekkora fokú centralizációt jelentenek, hiszen a felhasználók hajlamosak a nagyobb poolokhoz csatlakozni. Mindenesetre észben kell tartani, hogy a poolok nem birtokolják az általuk kezelt hashrátát, az a felhasználóktól jön. Ők pedig időről időre poolt váltanak, önként.

Történelmi precedens is van erre. 2014-ben a Ghash.io számított a legnagyobb poolnak, és már majdnem elérte a hálózat hashrátájának a felét. A bányászok viszont látták, hogy ezzel túlságosan is nagy a centralizáció kockázata, és önként elkezdtek átpártolni más poolokhoz, hogy helyreálljon az egyensúly.

A valamilyen szinten centralizált poolok ma is jelentős szereplők a hálózaton, de folyamatosan azon dolgoznak a fejlesztők, hogy ezen

változtassanak. A bányászat technológiai fejlődése olyan kezdeményezéseket hozott, mint például a BetterHash, amely lehetővé teszi a felhasználók számára a nagyobb kontrollt, és csökkenti a centralizált poolokra való ráutaltságot.

51%-os támadás

A bányászpoolok centralizációja felerősítette azokat az aggodalmakat, amelyek szerint a legnagyobb bányászok esetleg összebeszélhetnek, hogy 51%-os támadást indítsanak a hálózat ellen. Ma az öt legnagyobb ismert pool több, mint a hashráta felét adja. Nézzük meg, hogyan történne egy ilyen támadás, és milyen következményekkel járna!

Ha te irányítod a hashráta több, mint a felét, eldöntheted, hogy mit jegyzel fel a főkönyvbe, hiszen a Proof of Work segítségével több energiát elhasználó, értékesebb láncot hozhatsz létre, mint a többiek. A Nakamoto-konszenzus miatt pedig a csomópontok az értékesebb láncot fogják valódiként elfogadni.

Nézzük meg egy példán keresztül, hogyan történik egy egyszerű 51%-os támadás:

- Tegyük fel, hogy a hálózati hashráta 1000 hash másodpercenként.
- Vásárolsz egy nagy rakás bányászgépet, és be is üzemeled mindet, így 2000 hash per másodperc teljesítményel tudsz dolgozni. 3000 hash/másodperc a teljes hashráta, ebből 2000 a tiéd, így tiéd a hálózat 66%-a.
- Elkezdesz teljesen üres blokkokat bányászni, hiszen blokkot anélkül is generálhatsz, hogy tranzakció kerülne bele.
- Két hét elteltével nyilvánosságra hozod az üres blokkokat tartalmazó láncod. Mivel nagyjából kétszer olyan gyorsan tudsz bányászni, mint a többiek, a te láncod kétszer annyi Proof of Work során elhasznált energiát tartalmaz. A csomópontok így újraszervezik a láncot, ezzel pedig elveszik az előző két hét minden tranzakciója.

Az üres blokkok bányászata használhatatlanná teszi a láncot, de emellett még dupla költést is végezhetsz:

- Bitcoint küldesz egy tőzsdére.
- Átváltod dollárra, ezt a pénzt pedig kiutaltatod a bankszámládra.
- Valamivel később megosztod a titokban létrehozott üres láncod, amely viszont nem tartalmazza a tőzsdére küldés tranzakcióját.
- Újraírtad a tranzakciós történetet, és most nálad van a bitcoin, és az érte kapott dollár is.

A Bitcoin hashrátája annyi áramot fogyaszt, mint nagyjából egy közepes méretű ország energiaigénye. Ennyi hardver és elektromosság megvásárlása rendkívül drága mulatság. A becslések alapján a hálózat 51%-os támadással való eltérítéséhez most nagyjából óránként 700 ezer dollár kellene, ez az összeg pedig folyamatosan növekszik. Ez a becslés viszont nem számol a többi bányász reakciójával, amely valószínűleg az újabb és újabb gépek bekapcsolása lenne, még jobban megdrágítva a műveletet. Ha kíváncsi vagy, mennyibe kerülne a különböző kriptopénzek megtámadása, a https://www.crypto51.app oldalon kedvedre nézelődhetsz.

Az sem könnyű, hogy egy dupla költés után nyomtalanul el tudjon tűnni az elkövető. A hátrahagyott nyomokból ki lehetne következtetni, hogy ki is állt a háttérben. A végén oda lyukadunk ki, hogy el kell használni annyi áramot, amennyi egy egész országnak is elegendő, sokmillió dollárnyi bányászfelszerelést kell megvásárolnunk, emellett egy ilyen támadás kivitelezéséhez szintén sokmilliónyi pénzt kell beküldenünk a tőzsdékre.

De mondjuk, hogy egy rengeteg pénzzel rendelkező entitás, például egy kormány elszánja magát, megindít egy ilyen támadást, és sikerrel is jár. A hálózat ekkor elméletileg megteheti, hogy átáll egy másik Proof of Work hash funkcióra, tehát nem az sha256 algoritmust használja, hanem egy másikat. Ez a lépés ócskavassá változtatja a támadó által használt összes bányászgépet, mivel azok kifejezetten az sha256-ra lettek tervezve.
Az algoritmus megváltoztatása mindenesetre a nukleáris válaszcsapás digitális megfelelője, és a hálózat becsületes résztvevőit ugyanúgy a

padlóra küldi, mint a támadót. A hálózat maga viszont túlél, és feltámadhat a hamvakból.

Amellett, hogy egy ilyen támadás vélhetően nem jár sikerrel, a hashráta nagyjának az irányításával sem tudod megváltoztatni a két legfontosabb dolgot:

- Nem hozhatsz létre coinokat úgy, hogy nem tartod be a kibocsátási rátát. Ezzel megsértenéd a blokkjutalom konszenzusát, a blokkjaidat pedig elutasítaná a hálózat, hiába van nálad a több Proof of Work.
- Nem költhetsz el olyan coinokat, amelyek nem a tieid. Nem tudsz érvényes digitális aláírást rendelni mások coinjaihoz, ez pedig szintén sérti a szabályokat.

Azok a csomópontok, amelyek elfogadják fizetségként a bitcoint, képesek tisztán tartani a hálózatot még akkor is, ha a rosszindulatú bányászok kerülnének többségbe. Még velük is betartatnák a Bitcoin szabályait, amelyek rögzítve vannak a programkódban. Ilyen szempontból nézve, az 51%-os támadás inkább elméleti lehetőség, semmint biztonsági kockázat. A legvalószínűbb negatív forgatókönyv ténylegesen egy feneketlen zsebű állami szereplő megjelenése, aki használhatatlanná tudná tenni a Bitcoint. Egy ilyen támadás viszont nem tartható fent örökké. Mikor véget ér, és a Bitcoin hálózata visszarendeződik az eredeti állapotába, azzal is csak a strapabíróságát bizonyítja, és még jobban megnehezíti a további próbálkozók dolgát.

A Bitcoin még sosem esett áldozatául ilyen támadásnak, de több más blokklánc esetében már megtörtént ez. A kifejezetten alacsony hashrátával rendelkező blokkláncokat többször is eltérítették. Ezekben az esetekben a tőzsdék sok pénzt veszítettek dupla költés miatt, olyan alacsony biztonságú kriptopénzekkel végrehajtva, amelyeket eleve listázniuk sem szabadott volna.

SZÁMLANYITÁS SZEMÉLYAZONOSSÁG NÉLKÜL

Létrehoztunk egy központi irányítás nélküli elosztott főkönyvet. Egy lottószerűen működő bányászati rendszert, amellyel eldöntjük, ki írhat bele. Egy hálózatot, amely megbünteti a csalókat és jutalmazza a becsületes játékosokat. Egy módszert, amellyel hozzáigazíthatjuk az erőforrásokhoz a követelményeket, hogy megmaradjon a kibocsátási ráta. Végül egy szabályrendszert, amely alapján a Proof of Work energiafelhasználása és a tranzakciós történet alapján meghatározhatjuk a lánc hitelességét, valódiságát.

Nem került viszont még szóba a személyazonosság kérdése. A bankok esetében úgy tudod használni a pénzedet, hogy először azonosítod magad a bank előtt. Az ATM-hez kell a kártyád és a pin-kódod, a banki appokhoz pedig a felhasználóneved és a jelszavad. A bank megbizonyosodik arról, hogy tényleg te, és nem másvalaki használja a személyazonosságodat.

A mi esetünkben nincsen központi szereplő, aki nyilvántartaná a felhasználókat, hogyan hozhatunk létre így számlákat a Bitcoin-alapú pénzügyi rendszerünkben? Hogyan lehetne elérni Satoshi célját, hogy legyen különválasztva az identitásunk és a pénzügyeink, hogy így kerüljük el a személyazonosság-lopást, és a harmadik felek hozzáférését a személyes adatainkhoz? Hogyan tudunk megbizonyosodni arról, hogy amikor Alice kihirdeti a 2 dolláros átutalását Bobnak, akkor tényleg Alice beszél, és tényleg joga van átutalni azt a pénzt?

Hogyan hozzunk létre egy Bitcoin-számlát?

Nincs központi szereplő, aki kézben tartaná a felhasználói regisztrációkat, így nem bízhatjuk rá senkire ezt a munkát. Mi lenne, ha lehetővé tennénk, hogy bárki regisztrálja a saját felhasználónevét, és jelszavát? A bank megnézné, hogy az adott felhasználónév foglalt-e már, vagy szabad, de ez itt nem működik, mert nincs bank, nincs központi szereplő. Olyasmire van szükségünk, ami nagyobb, erősebb, és sokkal egyedibb, mint egy egyszerű

felhasználónév, jelszó kombináció. Az előző fejezetekből már sejthetjük, mi is ez. Egy jó hosszú, véletlenszerű számra van szükségünk.

Ahogyan lehetővé tettük, hogy mindenki létrehozza a saját lottószelvényeit, ugyanezzel a módszerrel létre lehet hozni a számlákat is. Egy Bitcoin-számla, vagy ahogyan sokszor hivatkoznak rá, egy Bitcoin-cím létrehozásához először generálunk egy 256 bites, matematikailag összekapcsolódó szám-párt, ezt pedig a legtöbbször publikus és privát kulcsnak nevezzük. Azt már tudjuk, hogy egy 256 bites szám olyan nagy, mint ahány atom van az univerzumban, így szinte lehetetlen, hogy két ember véletlenül ugyanazt a számot generálja le magának. A címünket pedig megadhatjuk bárkinek, aki pénzt akar küldeni nekünk. De hogyan működik ez a gyakorlatban?

A titkosítás az a folyamat, amikor bizonyos adatokat speciális módszerekkel lekódolunk, így csak az tudja elolvasni, aki rendelkezik a megoldókulccsal. Gyerekként akár találkozhattunk is különböző kódoló/dekódoló játékokkal, amelyek halandzsává változtatták a szöveget, majd vissza, olvasható formába. Ez az úgynevezett szimmetrikus titkosítás, hiszen ugyanaz a kulcs kell a kódoláshoz és a megfejtéshez is. A publikus/privát kulcspár technikája aszimmetrikus, mivel az egyik kulcs a kódoláshoz kell, a másik pedig a dekódoláshoz.

A publikus kulcsodat bátran megoszthatod bárkivel. Aki küldeni szeretne neked valamit, ennek a segítségével le tudja kódolni. Mivel pedig a privát kulcs nálad van, kizárólag te tudod elolvasni, hogy mit küldtek neked.

Lássuk, Alice hogyan tudja elküldeni a coinjait Bobnak. Hogy Bob megkaphassa a pénzét, létrehoz egy kulcs-párt, a privát kulcsát pedig titokban tartja. Ezután generál egy bitcoin-címet, egy hosszú karaktersort, amelyet a publikus kulcsa hashelésével kap meg. Ezt a bitcoin-címet elküldi Alice számára.

A bitcoin-címeket elképzelhetjük akár postafiókként is, csak éppen levelek helyett ide bitcoint lehet küldeni. Elolvasni, megnyitni pedig csak az tudja,

aki rendelkezik a privát kulccsal, így a bitcoint is csak ez a személy tudja elkölteni.

Mikor egy bankon keresztül mozgatsz pénzt, megadod a felhasználóneved és a jelszavad. Mikor megírsz egy csekket, elismervényt, aláírod, ezzel bizonyítod, hogy te írtad. Mikor bitcoint akarsz küldeni, akkor be kell bizonyítanod, hogy nálad van a coinokat tartalmazó cím privát kulcsa.

Alice be kell, hogy bizonyítsa, a fiókjához tartozó publikus cím privát fele, a privát kulcs is nála van. De nem akarja ezt senkinek megmutatni, nehogy rossz kezekbe kerüljön, és esetleg feltörjék a fiókját, hogy ellopják a bitcoinjait.

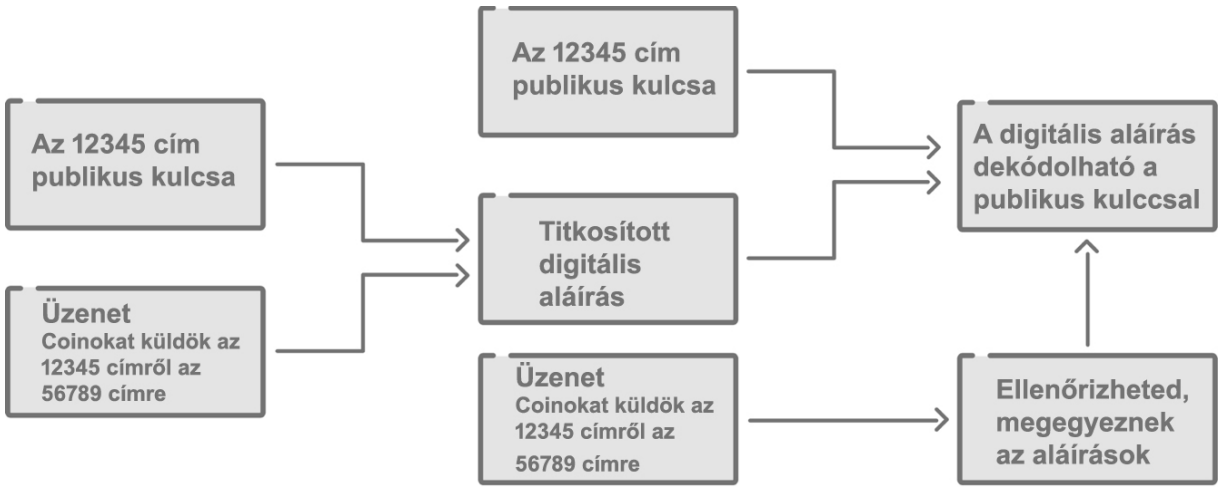
A kulcs birtoklását egy úgynevezett digitális aláírással lehet bizonyítani. Amikor Alice elindít egy tranzakciót, az egy rakás adatot jelent, és valahogy így néz ki:

Az 12345 bitcoin-cím, amelyen 2,5 BTC egyenleg
van, elküld 2 bitcoint az 56789 címre,
és vissza 0,5 bitcoint az 12345 címre.

A valóságban a bitcoin-címek hosszú, 160 bites számok. Miután megvan a tranzakció szövege, fogja ezeket az adatokat, és a privát kulcsa segítségével titkosítja, létrehozva a digitális aláírást.

Mikor kihirdeti a hálózaton az utalását, megmutatja a publikus kulcsát, és a privát kulcsával titkosított digitális aláírást. Ez a gyakorlatban így néz ki:

- Coinokat küldök az 12345 bitcoin-címről.
- Itt van az 12345 bitcoin-címhez tartozó publikus kulcs, ezt le tudod ellenőrizni, mivel ha hasheled a kulcsot, megkapod ugyanezt a címet.
- Itt van a tranzakcióhoz tartozó digitális aláírás, amelyet a publikus kulcshoz tartozó privát kulccsal titkosítottam. Ezt is le tudod ellenőrizni, hiszen a publikus kulccsal vissza tudod fejteni, és láthatod, hogy tényleg ezt a tranzakciót hitelesíti.



A tranzakció adata a privát kulccsal van titkosítva, egy digitális aláírás létrehozásával. Vissza lehet fejteni a publikus kulccsal, amelyet mindenki ismer.

Mindenki ismeri Alice publikus kulcsát, így könnyen dekódolható a digitális aláírása. Márpedig ahhoz, hogy Alice publikus kulcsával dekódolni tudjuk az üzenetet, ahhoz Alice a privát kulcsával kellett, hogy titkosítsa azt. Ha nem így tett volna, nem lehetne visszafejteni a kódolást, hiszen ez a fajta titkosítás csak és kizárólag akkor működik, ha a megfelelő privát kulcs, publikus kulcs párral van létrehozva. Emiatt nincs szükség arra, hogy Alice mindenkinek megmutassa a privát kulcsát. Mindenki tudja, hogy nála van, különben nem tudta volna kódolni a digitális aláírását.

A csekkeken lévő aláírásoddal, vagy a banki felhasználónév, jelszó kombinációval ellentétben a Bitcoin esetében használt digitális aláírásod kifejezetten csak az adott tranzakcióra vonatkozik. Ezért nem lehet ellopni, és egy másik tranzakcióhoz felhasználni. Minden egyes tranzakció új, a többitől különböző aláírást kap, még akkor is, ha ugyanarról a címről küldöd, ugyanarról a privát kulcsról. Ez azért van így, mert a tranzakció egyedi, új adatokat is tartalmaz, például az időpontot, és minden egyes új adat, új input megváltoztatja az outputot, a hasht.

Ki tudunk találni egy privát kulcsot?

Rá tudunk-e jönni találgatással egy adott címhez tartozó privát kulcsra, hogy így elkölthessük a rajta lévő coinokat? Milyen esélyeink vannak? Már említettük, hogy a kulcsok 256 bites számok. Minden bit két értéket vehet fel, nulla, vagy egyes. Minden bitet elképzelhetünk érmefeldobásként, vagy fej, vagy írás. Ha 1-bites kulcsunk van, akkor kétesélyes a játék, kettőből egyszer ki fogjuk találni.

Egy kis alapfokú matematika van a történetben, ebből tudjuk, hogy egy adott esemény többszöri ismétlődésének az esélye az egyedi megtörténések szorzata. Ha tehát az érmedobásnál ½ az esélyünk, hogy fej lesz, akkor az egymás után kétszer fej esélye ½ szorozva ½, tehát ¼, máshogyan megfogalmazva 1 a 4-hez.

Ha nyolcszor egymás után szeretnénk fejet dobni, akkor annak az esélye 2^8, tehát 1 a 256-hoz.

Egy rendszámtábla hat karakterből áll, betűkből és számokból. Van 26 betű és 10 szám, öszesen 36 karakter. Mivel pedig hat kell, ezért 36^6 különböző változat lehetséges, így az esélyed, hogy kitaláld az én kocsim rendszámát, 1 a két milliárdhoz.

Egy bankkártya-szám 16 számból áll. Mindegyik 10 különböző számjegy lehet, tehát 10^{16} változatból tudnád kitalálni az én kártyaszámomat. Ez 1 a 10 kvadrillióhoz esélyt jelent.

A Föld bolygón 10^{50} atom van. Ha én kiválasztom az egyiket, hasraütés-szerűen, az esélyed, hogy kitaláld, melyikre gondolok, 1 a 1.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000-hoz.

A privát kulcsok 256 bitesek, ez 2^{256} vagy nagyjából 10^{77}, tehát az 1 után még 77 nulla. Ekkora esélyeid vannak, ha az egész univerzumban szeretnél megtalálni egyetlen egy atomot, vagy megnyerni a lottó fődíját, kilencszer egymás után. Az esély 1 a majdnem végtelenhez.

Mi a helyzet akkor, ha van egy szuperszámítógépünk? Annak könnyebb dolga lenne? Erről egy Reddit bejegyzésben értekezett valaki, főleg technikai szempontból megközelítve, de az utolsó bekezdése nagyjából segít elképzelni, mennyire lenne könnyű dolga:

„Szóval, ha szó szerint az egész Föld bolygót használhatnád számítógépes winchesterként, atomonként 1 bájt adatot tárolva, csillagokat használva energiaforrásként, és nagyjából másodpercenként egy billió kulcsot lejegyezve, 37 kvadrilliárd, 10^{27} darab Földre lenne szükséged, amelyhez 237 milliárd Nap energiája kellene, és még így is 3,6717 nonilliárd, 10^{57} évig tartana leírni az összes lehetséges kulcsot.”

U/PSBLAKE az R/BITCOIN subredditen

Gyakorlatilag lehetetlen kitalálni valakinek a privát kulcsát. Ráadásul a lehetséges bitcoin-címek száma annyira nagy, hogy a javaslatok szerint érdemes minden egyes tranzakcióhoz új címet generálnunk magunknak. Ez olyan, mintha egyetlen bankszámla helyett több ezer, vagy akár több millió bankszámlád lenne, minden, valaha fogadott vagy indított tranzakciódhoz egy új.

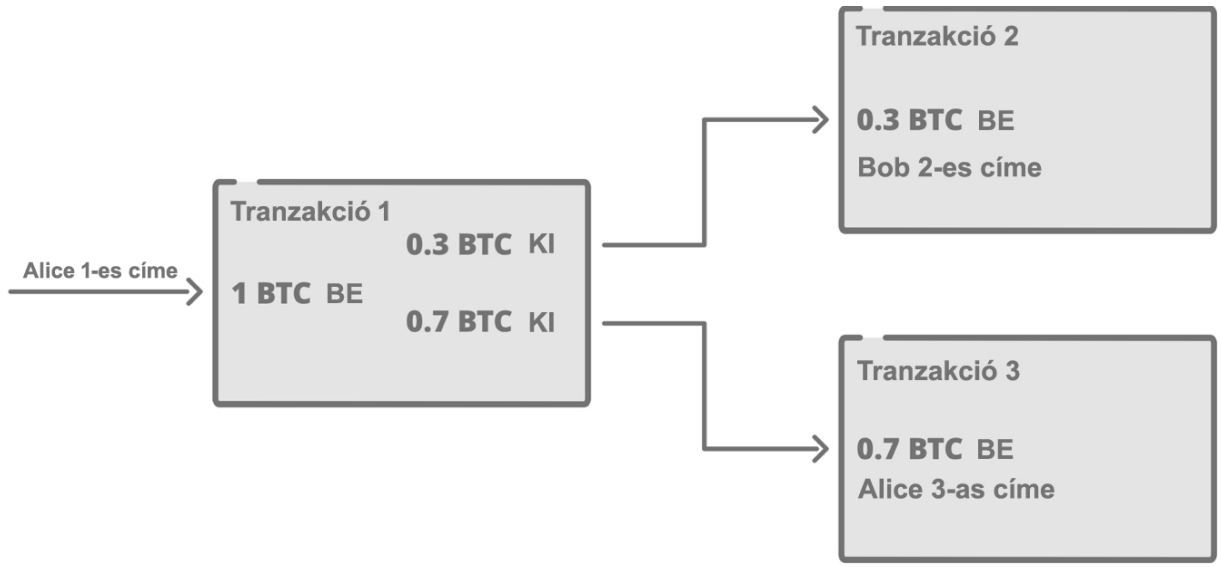
Elsőre zavarónak gondolhatod, hogy a privát kulcsokat csak a nagy számok törvénye védi. De ahogyan az előbb olvashattad, azok a számok tényleg nagyok, és sokkal nagyobb biztonságot nyújtanak, mint a bankok által egy központi szerveren tárolt felhasználónevek és jelszavak, a hackerek számára kiszolgáltatva.

Az egyenlegek követése

Van még egy dolog, amelyet eddig nem tisztáztunk le az előző fejezetekben. A főkönyvünkben valójában nincsenek egyenlegek. A Bitcoin ehelyett az UTXO, Unspent Transaction Outputs, azaz nagyjából az „elköltetlen tranzakció-kimeneteket” jelentő módszert használja. A tranzakció-kimenet azokat a coinokat jelenti, amelyeket megkaptál, függetlenül attól, hogy másvalaki utalta neked, vagy te bányásztad, és a coinbase tranzakcióval kerültek hozzád.

A hagyományos pénzekkel ellentétben, amelyek meghatározott címletekben, például 10 cent, negyed dollár, és hasonló formában léteznek, a bitcoin százmillió alegységre bontható, ezeket az alkotó tiszteletére satoshinak nevezzük. Emiatt attól függően, hogy mekkora összeget kaptál, fel kell osztanod az egyenleged, ha kevesebbet küldenél valakinek, vagy össze kell vonnod más címmel, ha többet akarsz utalni. Ugyanez pénzérmékkel úgy nézne ki, mintha a nagyobb összeg küldéséhez összeolvasztanád a fém érméket, és úgy adnád oda valakinek. Ezeket a technikai részleteket a tárcaprogramok automatikusan kezelik a háttérben, így felhasználóként nekünk csak annyi a dolgunk, hogy megadjuk a küldeni kívánt mennyiséget.

Mondjuk, hogy Alice címén 1 bitcoin van. 0,3 bitcoint akar elküldeni Bobnak. Létrehoz egy tranzakciót, amely megmutatja, hogy a saját címe 1 bitcoin UTXO-t tartalmaz, mint input, és ehhez jön két output, az egyik egy új bitcoin UTXO 0,3 bitcoinról, Bob címére, a második pedig egy másik, szintén új bitcoin UTXO 0,7 bitcoinról, vissza a saját címére. Ez a 0,7 bitcoin „visszajáró” mehet a saját, eredeti címére, de biztonsági okokból egy teljesen új címre is küldheti, amelyet a tárcája hozott létre, automatikusan, menet közben.



Ha nem a pontos küldendő mennyiséget tartalmazza az UTXO, akkor a tárca szétbontja az egyenleget, hogy a megfelelő UTXO küldhető legyen. Ugyanígy, több UTXO is kombinálható egyetlen nagyobb, új UTXO-ban.

Nincs rá mód, hogy a láncon beazonosítsuk, hogy kihez melyik cím tartozik. Ehhez ismerni kell a címhez tartozó privát kulcsot, és azt hozzá kell rendelni egy valós személyhez. Az UTXO megoldás egy kiváló módját jelenti a magánszféra védelmének, mivel minden alkalommal, mikor a coinok mozognak, új címet generálhatunk. Emiatt előfordulhat, hogy ha valaki sokszor végez tranzakciót, több száz, vagy akár több ezer bitcoin-címmel is rendelkezhet. Ezeket a tárcaprogramok kezelik nekünk, így nem kell foglalkoznunk a technikai részletekkel.

Ha meg szeretnénk nézni egy adott bitcoin-cím egyenlegét, akkor össze kell adnunk minden ahhoz tartozó UTXO-t. Az UTXO-k mennyisége növekszik, ha az emberek egy címről küldenek többre, és csökken, ha több címről gyűjtik össze egyetlenre a coinokat.

Az UTXO nagy segítség a dupla költés ellenőrzésében is, hiszen minden UTXO kizárólag egyszer használható fel. Nem kell ismernünk az adott bitcoin-cím teljes tranzakciós történetét, elég csak a küldendő UTXO adatait megvizsgálni.

Az UTXO-kat tömegesen létre is tudjuk hozni, illetve elhasználni, ha olyan komplex tranzakciókat indítunk, amelyek különböző inputokat és outputokat kombinálják. Ez teszi lehetővé a CoinJoin[5] működését, amely egy coin-mixer, ahol több résztvevő működik együtt, hogy egyetlen közös bitcoin-tranzakcióban tömörítsenek számos inputot és outputot, elrejtve ezzel az eredeti UTXO-k tranzakciós történetét. Ezeknek a megoldásoknak a népszerűsége egyre növekszik, és fontosak is a magánszféra védelmében, valamint a felcserélhetőség, angolul fungibility miatt. Ez utóbbi fogalom arra vonatkozik, hogy egy bitcoin egyenlő egy másik bitcoinnal, egymással felcserélhetők. Így lehet megoldani, hogy adott bitcoinok nem lesznek véglegesen „piszkosként” megbélyegezve csak azért, mert egyszer valamikor törvénytelen célra használták fel azokat.

Tárcák

Egy Bitcoin-számla létrehozása nem több, mint egy 256 bites kulcspár létrehozása. Mivel több ezer, vagy akár több millió számlát is létrehozhatunk, érdemes valahogy menedzselni ezeket. A Bitcoin esetében ezek az úgynevezett tárcák, ezek kezelik a kulcsainkat. Ez lehet egy darab papír is akár, de lehet egy kifejezetten erre szolgáló hardver is.

A Bitcoin első változata, amelyet Satoshi publikált, egy szoftvertárcát is tartalmazott. Ez tárolja a kulcsaid, címeket generál neked, és küldésnél a megfelelő UTXO-kat választja ki, hogy a kívánt mennyiséget utalhasd.

A bankod által kiadott opciókkal ellentétben, amely lehet egy webes vagy mobilos app, közvetlenül a banktól, a Bitcoin egy teljesen nyílt rendszer. Emiatt több tucatnyi különböző tárca létezik már, ezek nagy része nyílt forráskódú, emellett számos hardvertárca közül választhatunk. A jövőben pedig még több ilyen lesz. Bárki, aki ért a programozáshoz, létrehozhatja a saját tárcaprogramját, vagy belenézhet a nyílt forráskódú tárcák kódjába, hogy ellenőrizze, semmiféle kétes dolog nem rejtőzik a motorháztető alatt.

A coinjaid elköltéséhez egyedül a privát kulcsodra van szükség, így ajánlott nagyon vigyázni rá. Ha ellopják vagy elveszted a bankkártyádat, felhívhatod a bankod, hogy letiltsák, az esetleges költést pedig vissza lehet fordítani. A Bitcoin esetében nincs kit felhívni, nincs központi irányító. Ha valaki megszerzi a privát kulcsod, akkor a coinjaidat is megszerezte. De a kulcsok el is veszhetnek. Ha a számítógépeden tartod a tárcád, és tönkremegy, gondban vagy. Ha pedig követed az ajánlásokat, és minden tranzakcióhoz új címet hozol létre, azt a sok kulcsot fárasztó lesz kezelni.

Egy idő után, köszönhetően a Bitcoin fejlődésének, ennek a problémának is több megoldása született. 2012-ben a BIP32 (Bitcoin Improvement Proposal, azaz Bitcoin Fejlesztési Javaslat, a különböző új dolgok bevezetésének a módszere, hogy hogyan javítsunk a rendszeren) létrehozta az úgynevezett hierarchikusan meghatározott tárcákat. Ez az ötlet azon alapult, hogy egyetlen univerzális számmal, amelyet seed-nek nevezünk, létre tudunk hozni tetszőleges számú kulcspárt, amelyek bitcoin-címeket, és a hozzájuk tartozó privát kulcsokat jelképezik.

Azóta, ha a szélesebb körben elterjedt tárcákat használod, neked csak a mesterkulcsot kell elmentened, a tárca automatikusan új címeket és kulcsokat generál neked minden egyes tranzakcióhoz.

2013-ban a BIP39 a biztonsági mentést még egyszerűbbé tette. Ahelyett, hogy egy hosszú, véletlenszerű számot kellett volna elmenteni, a kulcsokat hétköznapi szavakból is le lehet generálni, ezeket a szavakat pedig mi, emberek is egyszerűen elolvashatjuk és akár meg is jegyezhetjük.

Ez például így is kinézhet, egy 12 szavas seed:

witch collapse practice feed shame open
despair creek road again ice least

Ezzel a módszerrel a kulcsok biztonságban tartása nagyon egyszerű. Leírod egy darab papírra, azt pedig beteszed egy széfbe. Meg is tanulhatod, memorizálhatod. Így megoldható, hogy egy összeomlóban lévő országból, például Venezuelából üres kézzel kisétálj, a teljes vagyonodat a fejedben szállítva.

Van arra is mód, hogy egy bitcoin-címhez több kulcsot hozzárendelj, és mindegyik szükséges legyen a hozzáféréshez. Ezek az úgynevezett multisig, multialáírásos címek. Például megosztozhatsz valakivel ugyanazon a címen, egy 1 / 2 multisig segítségével. Ez azt jelenti, hogy közösen használjátok ugyanazt a címet, és mindketten költhettek belőle. Létezik 2 / 2 multisig is, ez azt jelenti, hogy csak akkor lehet felhasználni a címen lévő coinokat, ha mindkét kulcs megvan hozzá. Ezzel a módszerrel számos biztonsági megoldást lehet bevezetni a kulcsok kezelésének a területére, hiszen megakadályozható, hogy egyetlen személy a hatalmába kerítse az adott címet, ez üzlettársak, vállalkozások esetén lehet aktuális kérdés.

Létrehozhatsz egy közvetítői rendszert is, egy 2 / 3 multisig segítségével. Egyik kulcs a vásárlónál, másik az eladónál, a harmadik pedig egy közvetítőnél. A közvetítő akkor lép színre, ha az eladó és a vevő vitás helyzetbe kerülnek. Ha megegyeznek, ketten fel tudják oldani a zárolást, de ha nem, akkor második kulcsnak jön a közvetítő, ekkor végre lehet hajtani a tranzakciót.

3 / 5 multisig sémát is használhatsz, ekkor az 5-ből két kulcs akár el is veszhet, még mindig hozzá lehet férni a javakhoz. Az egyiket tárolhatod egy barátodnál, más kulcsokat különböző helyeken. Valamelyiket rá is bízhatod egy speciális letétkezelőre, mint amilyen például a BitGo, amelyek társaláírást biztosítanak a tranzakcióidhoz, így nagyon megnehezítik, hogy bárki ellopja a coinjaidat, amellett, hogy a kulcsok elvesztése ellen is védenek.

Ennél is tovább lehet menni, és olyan zárolást alkalmazni, amely csak bizonyos feltételek teljesülésekor kerül feloldásra, hasonlóan, mint ahogyan a számítógép-programokat létrehozzuk. „Ha ez van, akkor az történik.” Még az is lehet, hogy egy címen 10 évre lekötsz coinokat, és még te, a létrehozó sem képes ennél előbb hozzáférni, akkor sem, ha közben meggondolnád magad.

Egyre több félig-meddig letétkezelői szolgáltatás jön létre az olyan cégek jóvoltából, mint amilyen például a Casa vagy az Unchained Capital, amelyek segítenek biztonságosan tárolni a kulcsaidat. Ellentétben a bankkokkal, amelyek bármikor befagyaszthatják a bankszámlád, ezek a részleges letétkezelők biztonsági mentésként működnek, vagy társaláíróként, de sehogyan sem tudnak hozzáférni a javaidhoz a te kulcsaid nélkül. A tárcaprogramok a banki appokkal ellentétben folyamatosan fejlődnek, mivel senkitől sem kell engedélyt kérni a fejlesztéshez. Emiatt az idő múlásával egyre többen lépnek be a területre, és egyre több innovációt fogunk látni.

Ez a dolog alaposan meg fogja változtatni a világot. Sosem volt még ennyire egyszerű magaddal vinni, és egyben megvédeni a személyes vagyont az ellopástól vagy az elkobzástól.

KI HOZZA A SZABÁLYOKAT?

Mostanra összeállt az elosztott, működő rendszerünk, amellyel nyilván tudjuk tartani és kezelni a pénzmozgásokat. Nézzük sorban, mit is hoztunk létre eddig:

- Egy elosztott főkönyvet, amelyről minden résztvevő rendelkezik egy másolattal.
- Egy lottóhoz hasonló megoldást, amely a Proof of Work és a nehézségi igazítás segítségével megvédi a hálózatot a manipulációtól, és fenntartja a meghatározott kibocsátási rátát.
- Egy konszenzusos módszert, amely lehetővé teszi, hogy a hálózat minden egyes résztvevője önállóan ellenőrizni tudja a tranzakciós történet hitelességét, egy nyílt forráskódú szoftverrel, a Bitcoin klienssel.
- Egy azonosító megoldást digitális aláírással, ezzel lehetővé téve, hogy központi szereplők irányítása nélkül hozzunk létre saját bankszámla-szerű fiókokat, amelyekre utalást fogadhatunk.

Nézzük hát meg az egyik legérdekesebb dolgot a Bitcoinnal kapcsolatban! Honnan jönnek a szabályok, ki hozta létre őket, miért kell betartani, és hogyan lehet változtatni rajtuk?

A Bitcoin program

Az előző fejezetekben végigvettük, hogy a hálózat résztvevői mind ugyanazokat a szabályokat követik, és tartatják be. Nem engedik a dupla költést. Figyelnek, hogy megfelelő mennyiségű munka legyen a Proof of Work mögött. Minden blokk hozzá van kötve az előtte lévő blokkhoz, egyfajta láncot alkotva. Megbizonyosodnak arról, hogy a tranzakciók megkapták a helyes aláírást, így tudni lehet, hogy a coinokat a jogos tulajdonosuk mozgatná. Ezen kívül pedig van még néhány pont, amelyet az idők folyamán felvettek a listára.

Azt is mondtuk, hogy a Bitcoin szoftvere nyílt forráskódú. Ezt azt jelenti, hogy bárki belenézhet a kódba, és a saját példányába tetszés szerint

beleírhat bármit. De hogyan lehet változtatni a Bitcoinon?

A Bitcoin egy protokoll. A számítógép-programok világában ez azt jelenti, hogy a program bizonyos szabályokat követve működik. Amíg ugyanezeket a szabályokat változatlanul hagyod, addig bármit módosíthatsz, kedved szerint. Mikor azt mondjuk, hogy valaki Bitcoin csomópontot futtat, valójában azt mondjuk, hogy van egy programja, amelyik követi a Bitcoin szabályait. Ez a program kommunikálni tud más csomópontokkal, tranzakciókat hirdethet ki, vagy akár saját részről blokkolhatja az azokról szóló kihirdetéseket, kereshet más csomópontokat, amelyekhez csatlakozna, és így tovább.

A tényleges részletek, hogy ki hogyan implementálja a Bitcoin protokollt, egyéni döntés kérdése. Sokféle változata létezik. Az egyik legnépszerűbb az eredeti, Satoshi Nakamoto által létrehozott Bitcoin Core. Természetesen vannak más változatok is, mások által fenntartva, akár más programnyelven megírva. Mivel a Bitcoin esetében kritikus fontosságú a konszenzus, tehát minden egyes csomópontnak egyet kell érteni abban, hogy mely blokkok érvényesek vagy érvénytelenek, a csomópontok döntő többsége a Bitcoin Core programot használja, hogy elejét vegyék az esetleges programhibák előfordulásának. Valójában az új Bitcoin kliensprogramok legegyszerűbben úgy hozhatók létre, ha elolvasod az eredeti Bitcoin Core kódját, és mindent úgy csinálsz a saját változatodban is, ahogy abban meg van határozva. Még akkor is, ha esetleg hiba van benne.

Ki hozza a szabályokat?

A Bitcoin szabályai bele vannak írva a Bitcoin Core kódjába. De ki dönt ezekről a szabályokról? Miért mondjuk, hogy a BTC készlete véges, ha egyszerűen beleírhatjuk a kódba, hogy ne 21 millió legyen, hanem mondjuk 42 millió?

Egy elosztott rendszerben minden csomópontnak egyet kell érteni a szabályok kérdésében. Ha bányászol, és eldöntöd, hogy átírod a programot, hogy ezentúl neked dupla mennyiségű blokkjutalom járjon, akkor a hálózat összes csomópontja vissza fogja utasítani a blokkjaidat. Rendkívül nehéz

megváltoztatni a szabályokat, mert sok ezernyi csomópont futtatja ugyanazt a Bitcoin hálózatot szerte a világon, és mindegyik ugyanazokat a szabályokat tartatja be a többiekkel.

A Bitcoin irányítási, kormányzati modellje nem tűnik logikusnak, főleg azok számára, akik nyugati típusú demokráciában élnek. Az ilyen helyeken szavazatokkal kormányoznak. A többség eldönti, hogy melyek legyenek a szabályok, ezeket törvénybe foglalják, és ezt bármely kisebbségre rákényszerítik. A Bitcoin „kormányzata" viszont sokkal közelebb áll az anarchiához, mint a demokráciához.

Minden egyes ember, aki pénzként elfogadja a bitcoint, eldöntheti, hogy mit tekint bitcoinnak. Ha valaki azt a programot futtatja, amely kimondja, hogy a végső készlet 21 millió, te pedig a saját, házilag írt programodból küldenél neki coinokat, arról a láncról, ahol átírtad a készletet 42 millióra, a coinjaid hamisnak lesznek értékelve, és nem fog megtörténni az utalásod.

Milyen szereplők vannak a Bitcoin hálózatán, és ők milyen viszonyban állnak egymással?

Csomópontok: a hálózat minden egyes résztvevője egyben egy csomópontot is jelent. A legtöbben a Bitcoin Core programot használják, amelyet Satoshi indított, és amelyet mostanra világszerte több száz önkéntes fejlesztő és vállalat gondoz. Ha egy programváltozat rosszindulatúvá válna, és olyan újdonságokat vezetne be, mint például az infláció, akkor azt a programot senki sem használná. Csomópontot bárki futtathat, és futtat is. Kereskedők, tőzsdék, tárcaszolgáltatók, és átlagemberek is, akik arra használják a Bitcoint, amire csak szeretnék.

Bányászok: sokan közülük egyben csomópontok is, részt vesznek a bitcoinok létrehozásában, könyvelik a tranzakciókat, és eközben nagyon drágává teszik, hogy bárki módosíthassa a főkönyvet. Mivel egyedül a bányászok írhatnak bele a főkönyvbe, a blokkokba, akár azt is hihetnénk, hogy ők irányítják a rendszert, pedig valójában nem. Ők egyszerűen csak követik a szabályokat, amelyeket a csomópontok hoznak. Ha egy bányász olyan blokkot hozna létre, amely többlet jutalmat adna neki, a

csomópontok ezt visszautasítanák, az adott coinok pedig értéktelenné válnának. Éppen emiatt a csomópontok egyfajta anarchikus kormányzást biztosítanak a Bitcoin számára. Eldöntik, hogy a Bitcoin hálózatán lévő valódi coinoknak milyen szabályoknak kell megfelelnie, és amelyik nem ilyen, azt törvénytelenként elutasítják.

Felhasználók, befektetők: olyan emberek, akik csomópontokat futtatnak, vagy egyszerűen csak pénzként használják a bitcoint. A legtöbb felhasználó nem futtat saját csomópontot, hanem rábízza magát a tárcaszolgáltatója csomópontjára, amely egyfajta képviselőként, megbízottként a felhasználók igényeit követi. A kereslet és a kínálat egyensúlyának beállításával a felhasználók döntik el, hogy mennyi a bitcoin piaci ára. Még ha a bányászok és a tőzsdék össze is beszélnének, hogy egy új dolgot, mondjuk inflációt vezessenek be a rendszerben, a felhasználók egyszerűen megválnának ezektől a coinoktól, az érintett cégek pedig vélhetően eltűnnének a süllyesztőben. Egy elkötelezett kisebbség is életben tudja tartani az eredeti verziójú Bitcoint, amely az eredeti szabályok szerint működik.

Fejlesztők: a Bitcoin Core szoftvere a legnépszerűbb Bitcoin kliens. A legjobb fejlesztők és cégek százainak a figyelmét keltette fel. Mint program, a Core kifejezetten konzervatívnak számít, mostanra pedig 100 milliárd dolláros (2019-ben) hálózatot kezel. Minden nagyobb változásnak egy Bitcoin Improvement Proposal[6] keretein belül kell megtörténnie, és minden ötletet alaposan megvizsgálnak. Az egész folyamat transzparens, a beadványtól a véleményezésen át az elbírálásig. Bárki csatlakozhat, hozzászólhat, még kódot is írhat hozzá. Mindenesetre, ha a fejlesztők olyan dolgot fogadnának el, amelyet a felhasználók nem akarnak, akkor a felhasználók egyszerűen nem frissítik a szoftvereiket a nem kívánt módosításokkal. Lehet, hogy egy régebbi verziónál akarnak maradni, vagy éppen egy teljesen újat használnának. Emiatt a fejlesztők jobban teszik, ha olyan dolgokat fejlesztenek, amelyeket általánosságban a felhasználók szeretnének, különben elveszítenék a státuszukat, népszerűségüket, és a programjukat sem futtatná senki.

A szabályok megváltoztatása, lánc-elágazódással

Remélhetőleg mostanra látod, hogyan tartatja be a Bitcoin szoftvere a szabályokat, amelyeket az emberek elvárnak tőle, és láthatod, hogyan tudjuk az általunk futtatott program kiválasztásával kikényszeríteni ezeket a szabályokat, amelyeket fontosnak tartunk.

A bányászok eldönthetik, milyen szabályok szerint dolgoznak, amikor blokkot hoznak létre, de jobban teszik, ha ezek a szabályok egybeesnek az emberek kívánságaival, különben a blokkjaik elutasítását, a blokkjutalom elvesztését kockáztatják.

Tudjuk, hogy a Bitcoin programja a legértékesebb Proof of Work láncot fogja elfogadni egyetlen valódi láncként, és a különböző elágazódások időről időre természetes módon is előfordulnak, mivel van esély az egyidejű blokktalálatra.

Mivel a hálózat szereplői elképesztő sokféleséget képviselnek, a fő szabályok a kezdetektől fogva szinte kőbe vannak vésve. Eddig kizárólag olyan fejlesztéseket vezettek be a Bitcoin esetében, amelyek visszamenőlegesen is kompatibilisek, hogy megőrizzék a konszenzust azokkal a csomópontokkal is, amelyek nem frissítik a programjukat.

Szóval akkor, hogyan lehet megváltoztatni a szabályokat? A szándékos lánc-elágazódás, a fork akkor jön létre, ha egyes szereplők, felhasználók, bányászok eldöntik, hogy nem értenek egyet a jelenlegi szabályokkal, és azokat meg kell változtatni. Ilyenkor két fajta változás következhet be, a szoft fork akkor történik meg, ha a változás visszamenőlegesen is kompatibilis, a hard fork pedig akkor, amikor ez a kompatibilitás nem biztosított. Először vegyük át, hogy elméletben hogyan történik ez, utána pedig beszéljünk a valóságban is megtörtént esetekről[7]!

A szoft forkok visszamenőleges kompatibilitása olyan változást jelent a konszenzusban, amely tulajdonképpen szigorítja a szabályokat. Tehát ha te egy régi csomópontot futtatsz, amelyik nem frissít az új verziókra, a csomópontod attól függetlenül még működni fog, és érvényesként látja az új szabályok alapján létrehozott blokkokat is. Egy példa segítségével ez könnyebben elképzelhető.

2010 szeptember 12-én egy új szabályt vezettek be, a blokkoknak legfeljebb 1 MB lehetett a mérete. Ez a spam-tranzakciók miatt vált szükségessé. Előtte bármekkora méretű blokk érvényesnek számított. Az új szabályok esetében már csak az 1 MB-ot meg nem haladó blokkok lettek érvényesek, így a szabályok szigorodtak. Ha te egy régebbi csomópontot futtattál, és nem frissítettél, a kisebb blokkok akkor is ugyanúgy érvényesnek számítottak a te szabályaid alapján, így téged nem érintett a fejlesztés.

A szoft fork egy kezelhető módja a fejlesztéseknek, mivel lehetővé teszi, hogy a csomópontok futtatói önként, fokozatosan frissítsenek az új verzióra, de ha nem teszik ezt meg, akkor is ugyanúgy működőképesek maradnak, ahogyan előtte is. Kizárólag a bányászoknak kell frissíteni, hogy az új szabályoknak megfelelő blokkokat tudjanak generálni. Miután ők végrehajtották a frissítést, attól kezdve minden blokk maximum 1 MB-os lett.

Hard fork esetén olyan változás történik, amely visszamenőlegesen nem kompatibilis. Ez a szabályok lazítását jelenti, tehát olyan blokkok is érvényesnek számíthatnak ezután, amelyek eddig nem voltak azok. A régi csomópontok frissítés nélkül már nem képesek követni a blokkokat, mivel az ő régi szabályaik szerint azok nem számítanak érvényesnek. Emiatt a régi láncon maradnak addig, amíg nem frissítenek.

Hard fork esetén a csomópontoknak egyhangúan egyet kell érteniük a frissítésben, és végrehajtani azt a lehető leggyorsabban. Ha néhányan lemaradnak a többiektől, nem fognak értesülni az új blokkokról, a szoftverük nem fog működni, és rá lesznek kényszerítve a frissítésre.

A gyakorlatban a hard forkok nem mennek zökkenőmentesen. Egy valódi, decentralizált, anarchikus rendszerben egyszerűen nem tudsz kényszeríteni senkit, hogy elfogadja az új szabályokat. 2017 nyarán néhány ember nem örült túlságosan, hogy a bitcoin egyre kevésbé használható olcsó fizetési módként. Eldöntötték, hogy létrehoznak egy forkot, amely nagyobb blokkmérettel dolgozik. A Bitcoin egyik 2010-es szoft forkja óta a

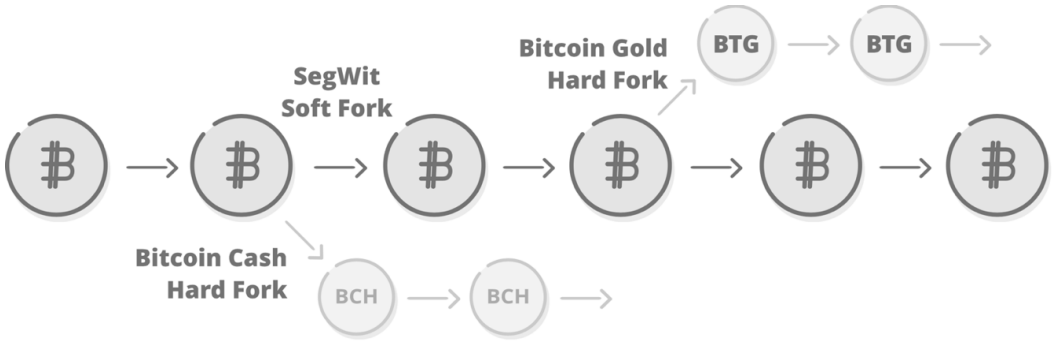
blokkméret 1 MB lehet. Néhányan viszont egy új láncot akartak, nagyobb blokkokkal. Ez a fork lett végül az, amelyet Bitcoin Cash néven ismerünk.

A konszenzus nélküli forkok, mint amilyen a Bitcoin Cash is, nem élvezik minden bányász és csomópont támogatását, emiatt új blokklánc jön létre. Ez a lánc egészen a szétválás pillanatáig megőrzi az eredeti hálózat adatait, az UTXO-kat, így az egyenlegeket is. Mindenesetre ezt követően az új láncon létrejövő coinok már nem számítanak bitcoinnak, hiszen az eredeti lánc csomópontjai nem tekintik annak azokat.

A téma, hogy mi, illetve mi nem számít bitcoinnak, évekig tartó vitát eredményezett a Bitcoin Cash létrejötte után. Néhányan a Bitcoin Cash támogatói közül úgy vélték, hogy a Bitcoint az alapján kellene meghatároznunk, ahogyan azt Satoshi a white paperben leírta, tíz évvel ezelőtt. Ennek alátámasztásához kiválasztottak néhányat az eredeti dokumentumokban lévő szavak közül, és ezekkel érveltek. De a konszenzussal működő hálózatokat nem lehet felsőbb erővel irányítani. Az ilyen rendszerek a közösség és az egyének lépésein keresztül működnek, ezek a lépések pedig többek között azok, hogy kiválasztjuk, melyik szoftvert futtatjuk, és melyik coint adjuk-vesszük a szabad piacon.

Ennek a forknak az esetén, a csomópontokat futtatók döntő többsége, ide értve a tárcaszolgáltatókat, tőzsdéket, kereskedőket is az átlagemberek mellett, nem akarta megváltoztatni a szoftverét egy olyanra, amelyet sokkal kevesebb fejlesztő kezel, akik kevésbé tapasztaltak, és amelyik láncot lényegesen kisebb hashráta tart biztonságban. A résztvevők nem érezték úgy, hogy egy ilyen „fejlesztés” megéri, hogy felforgassuk érte a teljes ökoszisztémát. A hard forkokkal pedig az a baj, hogy csak akkor működnek, ha mindenki egyetért. Ha ez nem így van, akkor két blokklánc lesz, két coinnal. Emiatt a Bitcoin továbbra is Bitcoin maradt, a Bitcoin Cash pedig egy teljesen különálló coin lett. Mindenki, aki a fork pillanata előtt rendelkezett bitcoinnal, ugyanannyi coint kapott az új láncon, gyakorlatilag ingyen. Sokan pedig tényleg ingyenpénzként tekintettek erre, és azonnal eladták, amely miatt az árfolyam csökkenő pályára állt.

Mára több tucatnyi Bitcoin-fork létezik, mint amilyenek a Bitcoin SV (önmagában is a Bitcoin Cash forkja), Bitcoin Gold, Bitcoin Diamond, és a Bitcoin Private. Mindegyiket nagyon alacsony hashráta biztosítja, kicsi a fejlesztői aktivitás, a láncon mérhető aktivitás és a tőzsdei likviditás pedig szinte nem is létezik. Emiatt a likviditás-hiány miatt kiváló célpontot nyújtanak a különböző pump&dump sémák számára, rakétaszerűen emelkedő árral, majd ezt követően elkeserítő mértékű zuhanással. Közülük számos áldozatul esett a tárcák meghekkelésének, 51%-os támadásnak, és más katasztrófáknak. Néhány egyértelműen csalás, vagy egyszerűen csak egyfajta szerencsejáték a spekulánsok számára. A legtöbb kifejezetten centralizáltnak számít bizonyos mérőszámok esetén. A forkdrop.io weboldal jelenleg, 2019-ben 74 forkot tart nyilván.



A szoft forkok után még mindig elfogadják a coinokat a régebbi csomópontok is. A hard forkok viszont olyan UTXO-kat hoznak létre, amelyek visszamenőlegesen nem működnek, mert nem felelnek meg a szabályoknak.

Több más kriptopénz működik hasonló kódkészlettel, de a főkönyvüket a nulláról indították, a Bitcoin UTXO-i nélkül, ilyen például a Litecoin vagy a Dogecoin. Ezeket nem is tekintjük a Bitcoin forkjainak, még akkor sem, ha ugyanaz a kódjuk, hiszen nem osztoznak a tranzakciós történeten.

A Bitcoin forkjai nem befolyásolják a bitcoin 21 milliós készletét. Képzeld el, hogy a világ összes aranyát egy szuperbiztonságos erődben, Fort Knoxban őrzöd, fegyveres őrökkel. Építesz egy kicsi, rozoga viskót, az lesz a neve, hogy Fort Knox Lite, és egyetlen őr fog vigyázni rá. Aranyszínűre festesz néhány követ, és elhelyezed a viskóban. Ezután bejelented, hogy forkoltad

az aranyat, és mindenki az általa birtokolt arany mennyiségében jogosult ingyen kőre, amelyet nálad lehet átvenni.

A Bitcoint rengeteg bányász „őrzi”, így nehéz és drága egy 51%-os támadást megindítani. Egy fork, amely mögött csak pár bányász van, könnyen megtámadható, mint az egyetlen őrrel védett viskók. A forráskód vélhetően szerkezetileg sem túl stabil, kevésbé tapasztalt fejlesztők által lett megépítve, és alig lett átnézve, ugyanúgy, ahogy a házilag tákolt viskó is gyenge. A forkolt coinokat nem fogadják el a csomópontok, mivel nem felelnek meg a Bitcoin szabályainak. Ugyanúgy, ahogyan a köveket sem tekinti aranynak senki, akkor sem, ha aranyszínűre vannak festve, főleg, ha kémiailag is letesztelik. A forkolt coinok, és a színesre festett kövek létrehozási költsége nagyjából nulla, hiszen a tulajdonosok ingyen kapják meg. Emiatt nincs túl nagy piaci igény az ilyen forkokra.

Ha figyelembe vesszük, hogy mostanra ezernyi klónja létezik a Bitcoinnak, és egyiknek sincs túl jelentős piaci értéke, egy paradoxonnal találjuk szembe magunkat. A Bitcoin forkjait és másolatait könnyen, ingyen létrehozhatjuk. Magát a Bitcoint, a szabályokat, az új bitcoinok létrehozásának a módját viszont egyáltalán nem könnyű megváltoztatni. Ha megkérdezik, hogy miért olyan különleges a Bitcoin a többi coinnal összehasonlítva, ez a jó válasz.

A Bitcoin hálózatának a decentralizált természete kiváló példája a status quo-nak. A nagy változások hónapokat vagy akár éveket vesznek igénybe, hiszen konszenzusra kell jutni, meg kell beszélni, és át kell nézni a bevezetés előtt. Ez jó dolog, és pontosan ezt kell biztosítania a rendszernek, amelyik globális pénzként akar működni. A Bitcoin egy sosem lassuló tánc az ezernyi résztvevő között, sokuk pedig csak a saját érdekét nézi, akár versenyezve is másokkal. Egy valódi szabadpiaci, anarchikus rendszer, ahol senki sem irányít.

HOGYAN TOVÁBB?

A Bitcoin a kriptovilág MySpace-e?

Miért írtam könyvet a Bitcoinról, mikor írhattam volna az egész kriptoszféráról, összefoglalóan? Hiszen sok ezernyi más coin létezik. Mitől olyan különleges a Bitcoin, amellett, hogy ez volt az első decentralizált kriptopénz? Hiszen lassabb és kevesebb funkcióval rendelkezik, mint az újabb versenytársai.

Ezeket a kérdéseket gyakran felteszik az újoncok. Miután megértik az alapokat, a következő kérdés logikusan valami hasonló szokott lenni:
„Ez a blokklánc-technológia érdekesnek tűnik. De honnan tudjuk, hogy nem fog jönni egy fejlettebb projekt, és a Bitcoin nem jut a MySpace sorsára?”

Ha egy cég versenyelőnyt akar a többi piaci résztvevővel szemben, valahogyan el kell sáncolnia magát, így az új belépőknek nehéz dolga lesz. A MySpace esetén ez a sánc a kiterjedt szociális kapcsolatrendszer volt, a baráti kapcsolatok a rengeteg felhasználó között. Az emberek nem használnak olyan közösségi szolgáltatást, ahol nem tudnak a barátaikkal lenni. De amilyen nagy volt a felhasználó-szám, és amilyen sűrű a kapcsolati háló, ez sem akadályozta meg a Facebook-ot abban, hogy alig pár év alatt elhódítsa a MySpace részesedését.

A Bitcoin sáncai sokkal-sokkal nagyobbak, mint amekkora a MySpace körül épült. Ezt úgy tudjuk könnyen megérteni, ha végigvesszük, mire is van szüksége a versenytársaknak, hogy letaszítsák a trónról a Bitcoint.

Még likvidebb pénzeszköznek kell lenni

A Facebook vs MySpace összehasonlítással kapcsolatban az első dolog, amit meg kell érteni, az az, hogy ez egy hibás összehasonlítás, mivel bárkinek lehet regisztrációja egyszerre mindkét platformon, ingyen. A Facebook megjelenésekor pontosan ez történt, rengeteg ember mind a két

oldalra regisztrált. Mikor pedig már elegen voltak a Facebook-on, elérték a kritikus többséget, egyszerűen abbahagyták a MySpace használatát.

A pénz viszont nem így működik. Ha van egy dollárnyi bitcoinod, az azt jelenti, hogy egy dollárnyi másmilyen kriptopénzed viszont nincsen. Tudatosan el kell döntened, hogy azt az egy dollárt melyik kriptopénzre költöd. Nem tudod ugyanazt a pénzt egyszerre mindkettőben tartani. Az emberek pedig felteszik maguknak a kérdést: miért tartanék bármi mást, mint a leginkább likvid, a legszélesebb körben elfogadott kriptopénzt? Ennek csak spekuláció lehet az oka. Ha az adott kriptopénzt nem kezdi el a teljes társadalom és a gazdaság használni körülötted, gyakorlatilag esélytelen, hogy dominánssá váljon.

A BTC likviditása messze megelőzi minden versenytársáét. Most, 2019-ben a piaci kapitalizációja 160 milliárd dollár a Messari adatai szerint, a második helyezett Ethereumé pedig 30 milliárd. Ez a kapitalizációs érték pedig nem is számol a vételi, eladási megbízások mértékével a tőzsdéken, amelyeket teljesíteni kell, hogy az árfolyam jelentősen elmozduljon.

A likviditás hógolyóként viselkedik. Ha a leglikvidebb eszközzel rendelkezel, számíthatsz rá, hogy a likviditás még jobban növekszik, ahogy egyre többen szintén birtokolni akarják. Ha nem a legnagyobb likviditású kriptopénzt tartod, akkor tulajdonképpen magadat bünteted, amíg azt várod, hogy mások is ugyanazt válasszák, mint te. Márpedig a likviditás mértéke a versenytársak között nem szokott egyik napról a másikra megfordulni.

100 milliárd dolláros biztonság, 10 év alatt

A Bitcoin számára adott volt a lehetőség, hogy egy értéktelen, számítógép-rajongó kockák által elkezdett kísérletként, egy 10000 bitcoinos pizza-vásárlástól 2017-re a közel 20 ezer dolláros rekord-árig jusson. Ezt pedig viszonylag csendesen hozta össze, anélkül, hogy bárkit magára haragított volna. Ez alatt az idő alatt elsőrangú immunrendszert fejlesztett ki a támadások kivédésére, és a világ legnagyobb hashrátájával rendelkező hálózatává vált. 10 év alatt közel 100 milliárd dollárt vonzott be a rendszerébe, és gyakorlatilag lehetetlenné vált a meghekkelése.

Ma szinte esélytelen csendben elindítani egy kriptopénzt. A szellem kibújt a palackból, és minden trükköt ismerünk már. Nézzük meg például az egyik altcoin, az EOS blokkláncát, amely nagyjából 10 milliárd dollárt ért az indulásakor, ma pedig alig a felét. Két nappal a start után az egész rendszer leállt, mert hibát találtak a kódban. A hiba órákon belül ki lett javítva, mégpedig különösebb utólagos ellenőrzés nélkül. Egy ilyen hálózaton akarsz 100 milliárd dollárt tárolni? Lehet, hogy az EOS létezni fog 10 év múlva, de addigra a Bitcoin már 20 éves lesz, több billió dollárral maga mögött.

A támadások kivédése

Sok ezernyi új coin létezik, ráadásul tucatnyi különböző hashelési algoritmust használnak. Az indulásuk pillanatától fogva ki vannak téve az 51%-os támadásoknak. Ahogy olvashattad korábban, történt már ilyen, nem is egyszer, például a Bitcoin Gold esetében is.

Az új versenyzőnek túl kell élni a jelenlegi hashráta ellen, vagy pedig olyan algoritmust használni, amelyre nincsen ASIC gép. Ha nincsen ASIC, akkor viszont támadási kockázatként jelentkezik a bérelhető GPU-kapacitás, amely széles körűen elérhető. Természetesen megoldható, hogy az első pillanattól kezdve nagy mennyiségű pénzt tudnak a biztonságra fordítani, ahogyan az EOS is tette, de ez egy elég biztos út a centralizált berendezkedés felé. Ha nem tudnak befektetői tőkét gyűjteni, ehelyett fair indulásra vannak kényszerítve, hasonlóan a Bitcoinhoz, akkor lassan kell felépíteniük a biztonsági szintjüket, a kezelt pénz mennyiségével együtt. De ha lassan építkeznek, nem fogják tudni utolérni a Bitcoint, egyszerűen az eltelt idő miatt.

Decentralizáció

A Bitcoin által nyújtott biztonság nagy része a magas fokú decentralizáltságnak köszönhető. A protokollt nagyon nehéz megváltoztatni, így bízhatunk abban, hogy a kódban rögzített tulajdonságok, például a véges készlet, megmaradnak. Ez a jelleg élesben is bebizonyosodott, amikor sok bányász, és néhány nagyobb cég összefogott,

hogy megváltoztassák a blokkméretet, és egy általuk elképzelt irányba tereljék a protokollt[8]. A próbálkozásuk csúfos kudarcba fulladt, az általuk létrehozott forkot elutasította a közösség.

Egy ténylegesen decentralizált versenytárs hamar kirekeszti az ismert személyekből álló cégeket, csapatokat, mivel az ilyenek részvétele hibalehetőséget jelent, és egy sebezhető pontot, amely kényszerítés áldozatává válhat. A decentralizáció a „csináld gyorsan, nem baj, ha elrontasz közben valamit" típusú coinokat is megtizedeli, mivel ez csak akkor működik, ha egy projekt centralizált. Ha egy versenytárs gyorsan fejlődik, akkor centralizált, ha pedig lassan, akkor nem tudja utolérni a Bitcoint.

Keltse fel a legjobb fejlesztők figyelmét

Ahogyan a Linux örvényként vonzza a fejlesztői aktivitást a versenytársak kárára, ugyanezt teszi a Bitcoin is. A közösség minden egyes nappal növekszik, és egyre több vállalkozás épít rá a Bitcoin rendszerére valamilyen szolgáltatást. A versenytársaknak ezek fejlesztőit kell magukhoz átcsábítani, egy exponenciálisan fejlődő területről, több tucatnyi vállalat, oktatási szervezet, és saját konferenciák mellől.

Világméretű pénzügyi hálózat építése

A Bitcoin világszerte sok száz tőzsde által van támogatva, emellett határidős és derivatíva kereskedők részéről is, akik között olyan nagy neveket találhatunk, mint a Chicago Mercantile Exchange. Több száz befektetési alap és kereskedőcég, emellett emberek millióinak a hálózata, akik a világ bukott valutái, például a venezuelai bolivár helyett használják a bitcoint, mint pénzt. Amelyik kriptopénz versenyezni akar a Bitcoinnal, ugyanezt fel kell mutatnia.

A Chicago Mercantile Exchange, ahogyan a többi hasonló intézmény sem, nem fog minden új coint listázni, hacsak nincsen mögötte hatalmas tőzsdei kereskedési forgalom, amely indokolná ezt. Meg kell győzni a vállalatokat, hogy a Bitcoin helyett ezt az új versenyzőt támogassák inkább. Egy új

versenyzőt, amely valószínűleg kevésbé biztonságos, kevésbé likvid, kevésbé hozzáértő fejlesztői vannak, és kevésbé van elterjedve a világon. Ez bizony egy elég meredek hegy, amelyet meg kell mászni.

Még stabilabb pénz

Van egy nagy félreértés a Bitcoinnal kapcsolatban, amely szerint gyors és olcsó pénzküldési módszernek kellene lennie. Egyértelműen nem képes erre az alapvető tulajdonságai miatt, kezdve a világszerte, elosztottan tárolt főkönyvével. A Bitcoin tényleges felhasználási módja viszont, mint cenzúra-ellenálló stabil pénz, egyre több figyelmet kap.

Minden más dolog, például a határokon átnyúló pénzküldés olcsóbbá és gyorsabbá tétele, tulajdonképpen csak a cseresznye a tejszínhab tetején. A Bitcoin legtöbb versenytársa mégis a mai napig azt hiszi, hogy a gyors és olcsó pénzküldést kell megoldania, holott azt már több tucatnyi centralizált vállalat megoldotta, tulajdonképpen egész jól. Sőt, a Bitcoinra épülő, és gyorsan növekvő Lightning Network szintén megoldotta.

A stabil pénz terén folytatott verseny mindenek előtt azt igényli, hogy valódi decentralizáció legyen, és a rendszer tulajdonságait nehéz legyen megváltoztatni. A coinok, amelyek ebben a mezőnyben versenyeznek, valójában nem tudnak labdába rúgni, mivel centralizált szervezetek, csoportok építik őket, profitszerzés céljából. Ez messze van attól a lassan növekedő ökoszisztémától, amelyet a cypherpunk mozgalom tagjai alapoztak meg annak idején.

A Bitcoin jövője

Mostanra elértünk a protokoll megszületéséhez. Nézzük meg, mit tartogathat számunkra a jövő, és mi az, amely már akár rövid távon valósággá válhat!

A Bitcoin egy programozható pénz, amelyre rengeteg szolgáltatás ráépülhet. Egy teljesen új, eddig még nem létező koncepció, és valójában még csak a felszínét kapargatjuk a lehetőségeinknek.

Lightning Network

A Bitcoin esetében a jutalékok mértéke problémás lehet, amikor megnő az igény a blokkok tárhelyére, azaz több lesz a tranzakció. A mai állás alapján a Bitcoin másodpercenként 3-7 tranzakciót tud rögzíteni, ennyi fér bele az 1 MB-os blokkméretbe, de ahogyan már korábban említettük, a kötegelés miatt egy tranzakció akár több száz kifizetést is összesíthet. De még így sem elég a kapacitása, hogy globális fizetési platformmá váljon.

Az egyszerű megoldás erre a blokkméret növelése lenne, ahogyan számos versenytárs, köztük a Bitcoin Cash meg is tette ezt. A Bitcoin számára ez nem járható út, mivel a blokkméret növelése negatív hatással lenne a decentralizációra. Kevesebben tudnának csomópontot futtatni, és ők is földrajzilag közelebb településnének egymáshoz. Ha a hardverek folyamatos fejlődésének köszönhetően megoldhatóvá is válna a blokkméret növelése, a Bitcoin továbbra is decentralizált rendszerként viselkedne, rengeteg vita és visszásság övezné az egész próbálkozást, amely valószínűleg csak egy újabb forkban, egy újabb, különálló coin létrejöttében végződne.

Ráadásul a blokkméret növelése sem változtatná a Bitcoint világszerte jól használható fizetési platformmá. Egyszerűen nem lehet annyira megnövelni a blokkok méretét. Itt jön a képbe a Lightning Network. Ez egy másik protokoll, amely off-chain, láncon kívüli tranzakciókat kezel, és ezeket adott időközönként rögzíti a Bitcoin hálózatán. A Lightning Network önmagában megérne egy teljes könyvet, de mi most csak érintőlegesen foglalkozunk vele.

A Lightning abból az alapfeltevésből indul ki, hogy nem szükséges minden tranzakciót rögzíteni a blokkláncon. Például ha te meg én leülünk egy bárba sörözni, elég a végén rendezni a fogyasztásunkat. Semmi értelme minden egyes kör után a pulthoz sétálnunk, és kifizetni az italokat, ez időpazarlás. A Bitcoin esetében tényleg arra kell elhasználnunk egy ország fogyasztásával megegyező energiamennyiséget, hogy rögzítsük a főkönyvben a sör- vagy a kávévásárlásunkat, és ennek a tranzakciós történetét a világon több ezer számítógép tárolja? Ez nem túl jó módszer, és a privát szféránkra nézve sem bölcs dolog.

A Lightning Network a Bitcoin számos hátrányát ki tudja küszöbölni:

- Gyakorlatilag korlátlan tranzakciós forgalmat tud kezelni. Egyetlen végső, a Bitcoin blokkláncra beküldött adatcsomagban több százezer mikrotranzakciót tud összesíteni.
- Azonnali konfirmáció, nem kell megvárni a blokk-generálást.
- Cent-töredékekkel egyenértékű jutalékok, így lehetővé válnak a szó szerinti mikrotranzakciók, például ha pár centet fizetsz egy blogbejegyzés elolvasásáért.
- Magánszféra. Kizárólag a résztvevők tudnak az adott tranzakcióról, szemben a Bitcoin hálózatán rögzítettekkel, amelyek az egész világ számára nyilvánosak.

A Lightning az úgynevezett fizetési csatornákat használja, amelyek hagyományos on-chain tranzakcióknak felelnek meg, és amelyekkel le tudunk kötni valamennyi bitcoint. Ezt az összeget aztán a Lightning Network rendszerén belül azonnali, szuperolcsó fizetésre használhatjuk fel. A Lightning most, 2019-ben még a korai fázisban jár, de nagyon is ígéretesnek tűnik. A https://yalls.org/ oldal már használja a cikkeihez a Lightning Networköt, mint fizetési modellt.

Bitcoin az űrben

A bitcoin kiválóan ellátja a feladatát, mint cenzúra-ellenálló pénzeszköz, ráadásul lefoglalni, elkobozni sem könnyű, hiszen memorizálhatjuk, és a fejünkben vihetjük magunkkal a szükséges információt. A cenzúra elkerüléséhez elegendő egyetlen becsületes bányászt találni, aki rögzíti a tranzakciódat a főkönyvben. Ez pedig te magad is lehetsz, hiszen bárki beállhat bányásznak.

A Bitcoin viszont az internet segítségével működik, így infrastruktúrális szinten cenzúrázható. Az autoriter rezsimek az internet megfigyelésével megakadályozhatják, hogy a bitcoin-forgalom beérkezzen az országukba, vagy elhagyja azt.

A Blockstream műhold-hálózata az első próbálkozás, amely ezt az állami szintű cenzúrát akarja kivédeni, emellett elviszi a Bitcoint azokra a távoli helyekre, ahol esetleg nincs is internet. Ez a műhold-hálózat lehetővé teszi, hogy egy tányérantennával, és viszonylag olcsó eszközökkel kapcsolódhassunk a Bitcoin hálózatához, akkor is, ha nincs internetünk. Hamarosan pedig már nem csak letölteni tudunk adatot a blokkláncról, hanem rögzíteni is rá, tehát tranzakciót indítani. Vannak más kezdeményezések is, mint amilyen például a TxTenna, amely kommunikációs vonalak nélkül, úgynevezett mesh-hálózat segítségével biztosítja az adatforgalmat. Ha ezt kombináljuk a műholdas technikával, ez a fajta rendszer majdnem megállíthatatlan.

További olvasnivaló

A végére értünk hát a Bitcoin létrehozásának. Remélhetőleg még jobban belenéznél a varázsgömbbe, hogy még több ismeretet szerezz. De merre indulj tovább? Ajánlok neked néhány olvasnivalót, angol nyelven.

Ha többet szeretnél tudni a Bitcoin mögötti gazdaságtanról:

- A Bitcoin Standard Saifedean Ammous-tól, ez már magyarul is megjelent
- Bitcoin Investment Theses Pierre Rochard-tól
- Vijay Boyapati: The Bullish Case for Bitcoin
- Gyerekeknek pedig a Bitcoin Money című könyv Michael Caras tollából

Ha a számítástechnikai rész érdekel jobban:

- A Bitcoin White paper Satoshi Nakamoto-tól
- Mastering Bitcoin Andreas Antonopoulos-tól
- Programming Bitcoin Jimmy Song-tól, és az ő szemináriumai a saját oldalán

Ha érdekel a Bitcoin történelme és filozófiája:

- Planting Bitcoin, Dan Held értekezése

- Pierre Rochard: Bitcoin Governance
- Bitcoin Past and Future, Murad Mahmudov
- Andreas Antonopoulos összes videója, főleg a Currency Wars és a The Monumentum of Immutability című̋ek a Youtube-csatornáján

A Bitcoin ökoszisztéma nagy része a Twitteren is aktív. A https://bitcoinerlist.com oldalon megtalálod azok listáját, akiket érdemes követni. Kezdd el itt, és innen tudsz tovább menni.

Az én cikkeimből többet is olvashatsz a https://yanpritzker.com weblapomon. Találkozunk a túlsó oldalon.

KÖSZÖNETNYILVÁNÍTÁS

Számos embernek mondhatok köszönetet, akik a könyv írása során támogattak a visszajelzéseikkel: Joe Levering, Phil Geiger, Yury Pritzker, Jonathan Wheeler, Walter Rosenberg, Michael Santosuosso, és David Harding.
Jimmy Songnak köszönöm a Programming Blockchain tanfolyamot, az adta meg a végső lökést, hogy nekilássak ennek a könyvnek a megírásához.

A SZERZŐRŐL

Yan Pritzker fejlesztőként és vállalkozóként startupok építésével töltötte az elmúlt húsz évet. A legutóbbi években a saját alapítású Reverb.com berkein belül időzött, ahol a technológiai, infrastruktúrális folyamatokat irányította 2012 és 2018 között, CTO-ként.
Társalapítója és technológiai vezetője a Swan Bitcoin váltónak, amely az új felhasználók szerzésére, és a Bitcoinnal kapcsolatos oktatásra fókuszál.

Yan a Bitcoinnal és a kapcsolódó témákkal foglalkozó cikkeket, írásokat publikál a https://yanpritzker.com weboldalon.
Twitteren is követheted: @skwp

Megjegyzések

[←1]

Nick Szabo írt egy kiváló értekezést a pénzrendszer történelméről, az alábbi linken angolul elolvasható: https://nakamotoinstitute.org/shelling-out/

[←2]

A 2016-os blokk-intervallum azért lett kiválasztva, mert így oldható meg a nagyjából 10 perces blokkidő. 2016 blokk, átlagosan 10 percenként az két hetet jelent. A 10 perces blokkidőre azért van szükség, mert ez elég hosszú ahhoz, hogy a csomópontok többsége szinkronizálni tudja a legfrissebb adatokat, a legújabb blokkot. A két hét pedig azért fontos, mert ezzel megelőzhető, hogy valaki a hashráta hirtelen, jelentős mértékű megváltoztatásával ki tudja játszani a rendszert.

[←3]
https://coinshares.co.uk/bitcoinmining-cost-june-2019

[←4]

Angol nyelven olvashatsz erről egy nagyon jó értekezést az alábbi címen:
https://hackernoon.com/bitcoin-miners-beware-invalid-blocks-need-not-apply-51c293ee278b

[←5]
https://en.bitcoin.it/wiki/CoinJoin

[←6]

Angolul olvashatsz erről bővebben Jameson Lopp tollából, a „Who Cotrols Bitcoin Core?” című bjegyzésben.

[←7]

A BitMEX tőzsde blogján egy jó összefoglalót olvashatsz a forkokról az alábbi címen: https://blog.bitmex.com/bitcoins-consensus-forks/

[←8]

Ez volt az úgynevezett SegWit2X fork, amelyet privát megbeszéléseken terveztek meg. A történetről angol nyelven itt olvashatsz bővebben: https://bitcoinmagazine.com/articles/now-segwit2x-hard-fork-has-really-failed-activate