Blokklánc technológiák: vízió az elkövetkezendő 10-15 évre

VÁGUJHELYI FERENC

HTE elnök, a Blockchain Koalíció elnöke

Mi a blokklánc (blockchain) és mi hívta életre?

A blokkláncról elmondható, hogy a legtöbb előnyt nem ott fogjuk kiaknázni a technológiából, ahol megalkotói gondolták. Ők ugyanis egy decentralizált rendszerben működő elektronikus pénz megteremtését tűzték ki célul. Ehhez hiteles elektronikus „bankjegyeket" (vagy pénzérméket) kellett létrehozniuk, amihez az aszimmetrikus kulcsú kriptográfián alapuló elektronikus aláírást használták. Mivel az elektronikus jel korlátlanul és tökéletesen másolható, így azt is meg kellett oldani, hogy annak elköltésére csak az utolsó tulajdonos legyen képes, de ő is csak egyszer. Ez már csak egy közösen vezetett nyilvántartással volt megoldható. Fáradozásaikat azért koronázhatta siker, mert olyan konszenzus-protokollt találtak ki, amelyben mindenki a befektetett erőforrások arányában szólhatott bele a működésbe. Aki viszont sokat fektetett be, annak már több hasznot hozott a korrekt működés, mint a csalás, amely a teljes rendszerbe vetett bizalmat romba döntötte volna, így elértéktelenítve korábbi befektetéseit. Az eredmény a Bitcoin, az okosszerződések futtatására képes Ethereum és számos társuk lett. A siker mércéje az, hogy a kriptopiacból 48 százalékkal részesedő Bitcoin piaci kapitalizációja jelenleg (2024.02.24.) ezer milliárd dollár, ami a gazdasági megfontolásokon túl a matematikai és műszaki megoldásba vetett óriási bizalmat is mutatja.

A fejlesztések eredménye megmutatta, hogy az elektronikus aláírásnál használt kulcspár nyilvános tagjának hash-kódja a kvantumszámítógépek által használható információ nélkül képes anonim módon megcímezni a tulajdonost. A kriptográfiai hash algoritmusokra építő, kizárólag a befektetett energiára épülő kiválasztási szabály megakadályozza, hogy valaki arra építsen támadást, hogy a következő blokkokat nagy valószínűséggel ő könyvelheti le. A digitális pénzverés, azaz a monetáris eszköz megteremtése biztonságosan szabályozható egy teljesen nyilvános, bárki által hozzáférhető rendszerben. A bankrendszerben tárolt pénz túlnyomó része ma is elektronikus formában létezik, de ennek biztonságát az adja, hogy a pénzintézet rendszere zárt, és az a feltételezés, hogy meg lehet benne bízni. A blokklánc ezzel ellentétben nyitott, nincs központi döntéshozó, a felhasználók mégis rosszabbul járnak, ha eltérnek a protokolltól. Ezért kívülről úgy tűnik, mintha a szabályrendszer önmagát kényszerítené ki.

A blokklánc technológiák kihívásai és várható előre lépései

„Zöld" konszenzus protokoll

A Bitcoin rendszerben a node-ok gyűjtik a tárcaprogramok által összeállított és aláírt tranzakciókat, ellenőrzik, hogy azok a blokklánc szabályainak megfelelnek-e, és ha igen, összeállítják belőlük a következő blokkot. Ezzel egyszerre sok ezren próbálkoznak és központi döntéshozó nélkül kell egyetértésre jutniuk abban, hogy kinek a blokkjával folytatódjon a lánc. A győztes az, aki a saját blokkjához olyan (sónak is nevezett) adatot talál, amelyet a blokkhoz írva annak SHA256 hash-értéke egy adott értéknél kisebb lesz, például húsz nullával kezdődik. A feladat nehézségét körülbelül kéthetente, 2016 blokkonként határozzák meg a node-ok úgy, hogy a blokkidő tíz perc körül maradjon. Ha a teljes rendszer számítási kapacitása (hash power-je) nő, növelni kell a megoldandó feladat nehézségét, ha csökken, könnyíteni. Mivel a bányászat jövedelmező, így óriási számítógépfarmokat használnak SHA256 értékek kiszámítására különböző véletlenszerűen választott „só" értékekkel. Ez hihetetlen mennyiségű elektromos energiát igényel, így a konszenzust eredményező véletlen kiválasztáshoz egy új, energiatakarékos szabályrendszert kell találnunk. Az elkövetkező évtizedben ilyen megoldásokra fogunk áttérni.

A központ nélküli közösség – a szuverenitás közös és decentralizált gyakorlása

Az elektronikus hitelesség első eszköze az elektronikus aláírás volt. A bizalom jogszabály által meghatározott infrastruktúrán alapult: hatóság által kijelölt gyökértanúsító tanúsítvány kiadók, hatósági eszközökkel azonosított aláírók, és a hardverre és a kriptográfiai algoritmusra vonatkozó műszaki szabályok. Ezzel párhuzamosan, a PGP (Pretty Good Privacy) program megjelenését követően kialakult egy decentralizált közösségként működő rendszer a "Web of Trust", a „bizalom hálója". Ha egy új csatlakozót azonosítani tudott egy régebbi tag, akkor saját aláírásával felülhitelesítette az új tag nyilvános kulcsát, kijelentve, hogy az adott személy hozzá tartozik. Itt a többi tagon múlt, hogy mennyire bízott az alkalmi hitelesítőben. A blokklánc rendszerekben se az állam főhatalmára, se bizalomra nincs szükség a protokoll szerinti működéshez. Ez megteremti a lehetőséget arra, hogy természetes személyek, vállalatok vagy akár országok működjenek együtt közösen létrehozott, de felettük álló központi szervezet nélkül. Az Európai Unió jó példa a hierarchiára épülő együttműködésre: a tagállamok minden olyan kérdésben, ahol közösen akarják gyakorolni szuverenitásuk egy részét, központi szervet hoznak létre. Ezek az Európai Bizottság főigazgatóságai vagy ügynökségei. Ezek létrejöttüket követően önálló életre kelnek, felismerik sajátos szervezeti érdekeiket, ellenőrzik, beperlik, sőt szankcionálják az őket létrehozó tagállamokat. Ugyanakkor a blokklánc rendszerekben is implementálható olyan működési modell, ahol a tagállamok illetékes szervei központi szerv nélkül vannak alávetve a közösen létrehozott protokollnak. Az ezt megsértő működés egyszerűen nem számít döntésnek, a tagállami node-ok nem fogják az ehhez kapcsolódó információt lekönyvelni. Az elkövetkező másfél évtizedben a szuverén közösségek (állami hatóságok, emberek, cégek) fokozatosan ilyen módon fogják kialakítani szakmai együttműködési közösségeiket.

A kvantumszámítógép és a blokklánc

A blokkláncban tárolt adatokon a tárcaprogramokban tárolt privát kulcs segítségével lehet tranzakciókat hitelesíteni. A hitelesítés ellenőrzéséhez szükség van a nyilvános kulcsra, amelynek csak a hash-kódját tárolja a blokklánc, így a tranzakció adataihoz csatolni kell. A tranzakciónak a könyvelő node-oknak történő elküldésének pillanatától kezdve viszont a kvantumszámítógépek megkísérelhetik a hitelesített adat, az aláírás és a nyilvános kulcs birtokában kiszámítani a titkos kulcsot, amellyel saját maguk számára jövedelmező módon megváltoztathatják a tranzakció tartalmát, aláírják, majd ők is igyekeznek minél több node-nak eljuttatni saját verziójukat a tranzakcióról. Ha a blokkidő töredéke alatt képesek a törésre, akkor van rá esélyük, hogy időnként az ő verziójuk kerül be a következő blokkba, azaz hasznot realizálhatnak. A blokkidő lerövidítése csökkenti a törés veszélyét, de mivel nem lehetünk biztosak a támadó tényleges képességeiben, így teljes védelmet nem ad. Így előbb-utóbb a blokklánc rendszerek hitelesítő algoritmusát kvantum-algoritmus álló megoldásra kell cserélni. Ez a kvantumszámítógépek fejlődésével párhuzamosan meg fog történni.

ZK-proof, ZK-SNARK megoldások

Az elkövetkező évtizedben általános lesz, hogy a kereskedelemben és a gazdaságban a személyek és cégek azonosítása digitálisan történik. Ugyanez vonatkozik például egyes jogosultságok igazolására is. Ha például valaki cigarettát akar vásárolni, akkor igazolnia kell, hogy elmúlt 18 éves. Ha ezt hagyományosan, a személyazonosító kártyájának a bemutatásával teszi meg, akkor még az anyja nevét is megismerheti az eladó, de valójában még a nevére sem fog emlékezni, amikor kimegy az üzletből. Ha viszont ezeket az adatokat digitális eszközzel olvassa ki, akkor műszaki értelemben megszerzi azt a képességet, hogy el is tárolja, a fogyasztás jellemzőihez kösse és viselkedés elemzést végezzen rajta. Valójában még a születés időpontjának megismerése sem indokolt, mivel pontosan egy bit adatot kell hitelesen megismerni: nagykorú-e az ügyfél. Erre kiváló kérdezz-felelek alapú, valós idejű, zéró tudásátadással járó interaktív algoritmusok léteznek már ma is. A blokklánc rendszerekben nagyon sokszor ütközünk olyan problémába, hogy egy entitásnak egyetlen attribútumát kell hitelesen igazolni úgy, hogy magának az entitásnak a megismerése nem indokolt. A fizikailag távoli szereplők között, a blokkláncon keresztül megvalósult interaktív bizonyítás – ellentétben a dohányboltban történő vásárlással – sem időtartamát, se költségét tekintve nem ésszerű megoldás. Ezért a következő évtizedben fejlődni fognak a ZK-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) megoldások, ahol a bizonyítást végző és az ellenőrzést végző olyan digitális adatokkal és algoritmussal rendelkezik, amely reális megoldást jelent a blokklánc architektúrában.

Okosszerződések, az orákulumok hitelessége

Az okosszerződések olyan programkódok, amelyeket a blokkláncot könyvelő gépek (nodeok) a tulajdonosok tárcaprogramjai által hitelesítve, összeállított tranzakciók utasítása alapján futtatnak. Ebben óriási lehetőségek és korlátok vannak. Korlát, hogy rendszeren kívüli adatforrást csak körültekintően lehet felhasználni, mert az okosszerződés futtatásának a sok ezer node mindegyikén ugyanazt az eredményt kell adnia. Az ilyen

külső adatforrások sokszor IoT eszközök, a további bizonyítás nélkül hitelesnek tekintett adatforrást pedig orákulumnak nevezzük. Az elkövetkező egy-másfél évtizedben az orákulumokra vonatkozó hitelességi és műszaki szabványok meg fognak születni.

Szervezet a láncban – decentralizált autonóm rendszerek

Az okosszerződések különleges fajtáját képezik a decentralizált autonóm szervezetek (DAOk). Ezek olyan okosszerződések, amelyeknek a programkódja a gazdálkodókhoz hasonló funkciókat valósít meg: letétet kezel, teljesítést igazol vagy vételárat fizet ki. Ha úgy hozzák létre, hogy senki ne legyen képes megváltoztatni a működését, akkor nem lehet addig leállítani (funkciói hívhatóak lesznek) ameddig a node-ok munkáját fedező „gáz”, azaz kriptoeszköz rendelkezésre áll. A decentralizált autonóm szervezeteket vagy akár cégeket (DAC-ok) a jövőben olyan tulajdonságokkal ruházhatják fel, hogy bizonyos események bekövetkezése indítson el folyamatokat. Ilyen esemény lehet az, ha a blokkláncban adott feltételek teljesülnek vagy akár az, ha egy orákulum ad valamilyen információt. Ilyenkor kérdés, hogy a kriptográfiai hitelesítést ki végezze el, mivel az okosszerződés a blokkláncban létezik, ahol viszont problémás lenne a titkos kulcs tárolása. Az elkövetkező évtizedben a problémára ki kell fejleszteni a biztonságos kriptográfiai sémát, például megfelelő többrésztvevős Threshold Signature Scheme megalkotásával.

Okosszerződések és a mesterséges intelligencia

Az okosszerződések akár rendszeren kívüli orákulumként, akár a blokkláncba integráltan mélytanulási módszerek által felismert összefüggéseket is felhasználhatnak paraméterként, illetve az ilyen modellek által kalkulált predikcióktól is függővé tehetik futásuk eredményét. Egy ilyen fejlesztés hihetetlen lehetőséget rejtene magában, ugyanakkor ehhez előbb fel kell oldani azt az ellentmondást, amely abban rejtőzik, hogy a mélytanulási módszerek által alkotott modellek folyamatosan változnak az újabb és újabb tanított adatok feldolgozásával, ugyanakkor az okosszerződés egy-egy funkciójának pontosan ugyanazt az eredményt kell adnia az összes node-on futtatva, legalábbis egy adott blokk lezárása előtt. Az elkövetkező évtized bizonyosan megoldást hoz a kérdésben.

Okosszerződések és a tanútitkosítás (witness encryption)

Tegyük fel, hogy a Nagy-Fermat sejtésre (azóta tétel, mert több, mint 20 éve bebizonyították) a XIX. század közepén egy okosszerződésben letétbe helyezel egy 2 bitcoin-os díjat (tekintsünk el attól, hogy akkor még nem volt se elektronikus számítógép, se blokklánc), és kitalálsz egy olyan kriptográfiai rendszert, ahol a titkos kulcshoz akkor és csak akkor tudsz hozzájutni, hogy átutald magadnak a pénzt, ha ismered a bizonyítást, amiről akkor még azt sem tudod, hogy létezik-e. Ez a witness encryption. Ha sikerülne megkonstruálni, bizalom nélküli szerződéseket lehetne kötni. A kutatások jelenlegi állapota sajnos nem vetíti előre, hogy másfél évtizeden belül itt áttörés érhető el.

Átverés: blokklánccal álcázott centralizáció

Az üzleti célú, zárt (permissioned) blokklánc rendszerekben a szereplők ismerik egymást és bíznak egymásban. Nyilvános kulcsukat megosztják egymással, így a Sybil-támadás ellen védettek. A blokkokat párhuzamosan állítják össze, de bányászat nincs. Többségi szavazás van, vagy egy kitüntetett szereplő dönt, ha erre szükség van. Ezek a zárt rendszerek jelentősen különböznek nyilvános társaiktól. Az első ilyen nagyméretű zárt rendszerű megoldás a kontinenseken átívelő ellátási láncok adatáramlását segítette. Az alapító globális szállítmányozó cég versenytársai egy idő után visszautasították, hogy saját adataikat feltöltsék, sőt azokat az ügyfeleket nem is szolgálták ki, akik használták a rendszert, mivel attól tartottak, hogy versenytársuk ellenük használhatja a blokkláncba feltöltött óriási mennyiségű adatot. A közösségi média vezető cégei esetében is felmerült például kriptovaluta kibocsátása, ahol a könyvelési platform akár nem decentralizált blokklánc rendszer is lehetett volna. Laikusként sokszor nehéz megítélni, hogy egy új blokklánc rendszer vagy egy okosszerződésen alapuló együttműködés valóban decentralizált-e. Az elkövetkező évtizedben várható a centralizáció jeleit kereső szolgáltatások felfutása.