Németh Péter
https://microcoin.hu
hello@microcoin.hu

MICROCOIN DOKUMENTÁCIÓ V 1.0

Németh Péter

2018. január 08.

Tartalom

Bevezetés ... 2
Miben más a MicroCoin? ... 2
A MicroCoin számlák egyszerűek ... 2
Nincs szükség mindenhez a blokkláncra ... 2
A tranzakciók teljesen titkosak ... 2
Újrahasznosíthatók a számlák ... 2
Kiemelt tulajdonságok ... 2
A MicroCoin végtelenül skálázható ... 2
Azonnali tranzakciók ... 3
Mikrofizetések - nincs szükség villámgyors hálózatokra, ... 3
Teljes anonimitás ... 3
Számla nevek és típusok ... 3
Pénzügyi és B2B szolgáltatások ... 4
JSON RPC API ... 4
Felhasználási példák ... 4
Fizetés webshopban ... 4
Tartalom megrendelése e-mailben (pl. e-book, kupon) ... 4
Fizetős chat szolgáltatás ... 4
Mobil alkalmazás ... 4
Titkosítás ... 5
Al-Tokenek és Smart Contractok ... 5
Szemléltető példák ... 5
Példa tranzakció összehasonlítva a BitCoinnal ... 5
A módszer előnyei: ... 5
A módszer hátrányai: ... 5
Példa egy tranzakció menetére ... 5
Példa a számla átruházására ... 6
Technikai információk, hogyan működik? ... 6
A SafeBox ... 6
A számla felépítése a SafeBoxban ... 6
Számla blokk ... 7
A Blokklánc felépítése ... 7

Bevezetés

A MicroCoin egy innovatív technológián alapuló kriptovaluta. Bár a működése blokklánc alapú, ha az egész blokkláncot kitöröljük akkor sem vesztjük el a számlákat és az egyenlegeket. Ennek az oka, hogy a SafeBox technológiának köszönhetően a legfontosabb adatok minden csomópontban azonnal megtalálhatóak.

Ebben a dokumentumban leginkább a működése és az előnyei kerülnek bemutatásra. A program használata és a bányászás menete egy másik dokumentumban kap helyet

Miben más a MicroCoin?

A MicroCoin a hagyományos kriptovalutákhoz képest több újdonsággal is szolgál.

- Gyorsabb
- A végtelenségig skálázható
- Biztonságosabb
- Bővíthető

A MicroCoin számlák egyszerűek

A hagyományos kriptovaluta számlák egy hosszú, 26-35 karakteres kulcsot használnak egy számla azonosítására. Ahhoz, hogy utalni tudjunk egy számlára ismernünk kell ezt a hosszú kulcsot. A MicroCoin számlákat két szám azonosítja, ami könnyen megjegyezhető. Az első szám a számla száma, a második az ellenőrzőösszeg, pl. 1-22. Természetesen itt is vannak a háttérben publikus és privát kulcsok, hiszen a számlánkat a privát kulcsunkkal tudjuk megvédeni az illetéktelen használattól.

Nincs szükség mindenhez a blokkláncra

Nem szükséges az egész blokkláncot végig kutatni egy számla egyenlegének a megállapításához. Minden számla egyenlege és a legfontosabb adatai egy kis méretű struktúrában (SafeBox) tárolódnak. A tranzakciók és a számlatörténet természetesen megvan a blokkláncban, de erre csak a SafeBox ellenőrzéséhez van szükség.

A tranzakciók teljesen titkosak

Minden számla publikus kulcsa nyilvánosan elérhető, így lehetőség van arra, hogy egy-egy tranzakciót és a hozzá tartozó adatokat és üzeneteket ezzel a kulccsal titkosítsuk, amit csak a címzett tud dekódolni a saját privát kulcsával.

Újrahasznosíthatók a számlák

Ha egy számla halott (hosszú ideig nem történt aktivitás a privát kulcsával), a számla és az egyenlege újra kiosztásra kerül a bányászok között. Így nem vész el egy MicroCoin sem a szeméttelepeken és a tönkrement lemezeken.

Kiemelt tulajdonságok

A MicroCoin végtelenül skálázható

A MicroCoin végtelenül skálázható. Az oka, hogy nincs szükség a teljes blokkláncra a működéséhez, csupán az utolsó 100 blokkra van szükségünk. Minden 100. blokk után készül egy ellenőrzőpont, ami tárolja a tömörített SafeBoxokat. Így a régebbi blokkokat akár törölhetjük is. Mivel egy

csomópontnak ezzel a technikával maximum 100 blokkot kell tárolnia, sokkal kisebb a hálózati forgalom. **A BitCoin esetében egy csomópont helyszükséglet 6Gb körül van. Elméletileg a MicroCoin fenn tud tartani akár 5,4 Gb-os blokkméretet, ezzel pedig akár 72000 tranzakciót bonyolíthatnánk le másodpercenként.** Ugyancsak ennek a technológiának köszönhetően az adat mérete egy idő után állandó. Körülbelül 6Gb-ban van maximalizálva. Ezt a méretet 2073-ben fogjuk elérni és teljesen mindegy, hogy egy, vagy 100 billió tranzakció fog történni addig, a mérete maximum 6Gb lesz.

Ha ez ilyen jó, akkor a többi kriptodeviza miért nem így működik?

Ennek két oka van. Egyrészt az eredeti elképzelések nem ilyenek voltak és a meglévő blokk adatokat nem lehet már átalakítani erre a sémára. Másrészt ez a technológia csak a Proof-Of-Work alapú kriptovalutákkal működhet. A Proof-Of-Stake nem támogathatja ezt, mert ott mindenképpen szükség van a blokkláncra a munka és az integritás ellenőrzésére.

Azonnali tranzakciók

A MicroCoin lehetővé teszi az azonnali, nulla konfirmációs tranzakciókat. A BitCoin esetén mindenképpen meg kell várni, hogy a tranzakció bekerüljön egy blokkba. Ha ezt nem várjuk meg, a tranzakció egy ellentétes, magasabb költségű tranzakcióval semmissé tehető. A MicroCoin esetében a tranzakció egy kivonás/növelés az egyenleg terhére/javára. Így nem lehetséges visszavonni. Felmerülhet a kérdés, hogy akkor mi véd a dupla tranzakciók (double spending) ellen? A hálózat nem fogad be újra egy olyan tranzakciót, ami már folyamatban van. Így, ha egy tranzakció folyamatban van nem tudunk még egy ugyanolyat indítani, ami az eredeti tranzakció nem lett konfirmálva.

Mikrofizetések - nincs szükség villámgyors hálózatokra,

Az azonnali, nulla konfirmációs tranzakcióknak köszönhetően nincs szükségünk villámgyors hálózatokra a bányászathoz. Mivel a tranzakció azonnal és végérvényesen megtörténik a megerősítő blokk ráér megszületni. Ez ideális lehet mikrofizetésekhez. Míg a BitCoin esetében, ha veszünk egy kávét akár 10 percig is várhatunk amíg sikerül valóban kifizetni, a MicroCoin esetében azonnal a kezünkbe kaphatjuk a kávénkat, gyorsabban, mintha bankkártyával fizetnénk.

Teljes anonimitás

A tranzakciótörténet titkosítva és korlátozottan tárolódik. Amennyiben ez nem elég, lehetőség van komplett számlák átadására is, vagy akár egy második réteg üzemeltetésére, amely különböző tranzakciókkal képest eltüntetni a MicroCoin útját a számlák közt. Mindkettőre olvasható példa a későbbiekben

Számla nevek és típusok

Kiemelkedő funkció, hogy a számlákhoz globálisan egyedi neveket rendelhetünk. Ez hasonló ahhoz, mint a domain nevek és az IP címek kapcsolata. A felhasználók az összes számlát látják a nevükkel együtt, így megoldható, hogy a számlánk száma helyett az e-mail címünket, a webshop domain nevét, vagy akár egy márkanevet használjunk. A tranzakció továbbra is a számlaszámra fog történni, de a számla megkeresése a neve alapján történik.

A számla típusa pedig egy új réteg fejlesztése esetén nyújthat nagy segítséget és alapot. Minden számlának szabadon választhatunk egy saját típust, amelyhez aztán saját funkciókat tudunk rendelni.

Pénzügyi és B2B szolgáltatások

Mivel a tranzakciók azonnal végbe mennek, így lehetőség van a tranzakciókat üzenetekként kezelni. Ezzel a megközelítéssel a számlákat kezelhetjük portokként, amit figyelnek, vagy adatokat küldenek. Az adatokat pedig minden tranzakció mellé meg tudjuk adni. Ezek maximum 256 byte hosszúságúak lehetnek és a tartalmuk tetszőleges. Ez a lehetőség hasonlít a http protokollhoz, azaz adatokat tudunk küldeni és fogadni azzal a különbséggel, hogy itt az üzenetek és az adatok mellett kriptovaluta is vándorol, azaz tranzakció is történik. Ezt nem csak az azonnali, vagy mikrofizetésekre használhatjuk, hanem olyan speciális alkalmazásokat is fejleszthetünk ahol a felhasználó tartalom, vagy egyéb iránti kérése már a fizetett összeget is tartalmazza, így nem kell egy külön folyamatban fizetést indítani. Ugyanakkor a B2B szolgáltatásokat is ki tudunk építeni a későbbiekben leírt módok szerint.

JSON RPC API

A MicroCoin biztosít egy http alapú JSON RPC API-t. Ennek segítségével könnyen és gyorsan tudunk bármilyen programnyelven fejleszteni bármit. A teljes pénztárcánkat vezérelhetjük az API segítségével és bármilyen információhoz hozzá is tudunk jutni. Mind a daemon, mind a Wallett program biztosítja az API-t. Különböző programokkal, webáruházakkal, online tőzsde szoftverekkel kapcsolódhatunk az API-hoz.

Felhasználási példák

Az alábbiak csak példák. Ezeken kívül számos alkalmazás lehetséges, csak a fantázia szab határt a lehetőségeknek.

Fizetés webshopban

A webshop figyeli a saját számlájára érkező tranzakciókat a MicroCoinDaemon programmal. Amikor egy vásárló leadja a rendelést és MicroCoin-nal szeretne fizetni, a vásárló az utalás közleményébe megadja a rendelés számát, majd elutalja a megrendelés árát (Ehhez a Webshop generálhat neki egy QR kódot is például). Az utalás pillanatában a Daemon észleli, hogy beérkezett egy tranzakció és meghívja a WebShopot a tranzakció adatival (összeg, közlemény). A Webshop ellenőrzi majd kifizetetté teszi a rendelést és folytatja a feldolgozást. Mindez pedig rövidebb idő, mint amennyibe került az elolvasása volt. Pár másodperc alatt végbe tud menni az egész folyamat.

Tartalom megrendelése e-mailben (pl. e-book, kupon)

A felhasználó elutalja az e-book árát a megadott számlára és a közleményben (titkosítva) megadja az e-mail címet. A szerver érzékeli az utalást, majd elküldi a megadott e-mail címre a megrendelt e-bookot, vagy a kupon kódot.

Fizetős chat szolgáltatás

A felhasználók kérdéseket tehetnek fel egy szakértőnek amiért fizetniük kell. Kijelölünk egy számlát, mint chat szoba. A felhasználók a kérdéseiket úgy tudják feltenni, ha egyben el is küldik a kérdés árát, és a kérdést a közleményben teszik fel. Ha nem szeretnék, hogy mindenki lássa a kérdést titkosíthatják is azt.

Mobil alkalmazás

Egy mobil alkalmazás, amely a tartalom (pl. hírek, tudományos anyagok, stb.) megnyitásakor már a kérésben küldi a tartalom árát is. A szerver megkapja, majd egyből hozzáférhetővé teszi a kért tartalmat az applikációnak.

Titkosítás

A tranzakció mellé megadott adat tartalmazhat különböző útmutatásokat arra, hogy az összeget milyen számlákra, milyen részletekben és hogyan kell tovább utalni. Így pillanatok alatt több száz, vagy több ezer utalást is létre lehet hozni a két számla között, ezzel pedig az utalt összeget követhetetlenné lehet tenni.

Al-Tokenek és Smart Contractok

Egy második réteggel nagyon egyszerűen le tudjuk fejleszteni az okos szerződéseket, hasonlóan ahogyan a RootStock működik. Etherum Virtuális Gépet is tudunk csatlakoztatni egy MicroCoin számlához, majd az tranzakciós üzeneteket kezeljük az EVM-el. Minden számlához külön EVM-et tudunk rendelni, a kommunikáció pedig megoldható a számlák közötti tranzakciókkal. A sok tranzakció miatt pedig nem szükséges aggódni, a hálózatot nem terhelheti meg a 100 blokkonkénti ellenőrzőpontoknak köszönhetően. Arról viszont a mellékelt láncnak kell gondoskodnia, hogy minden adat rendelkezésre álljon a 100. blokk után is.

Szemléltető példák

Példa tranzakció összehasonlítva a BitCoinnal

Amikor BitCoint szeretnénk utalni ismernünk kell a fogadó számla publikus kulcsát, a saját publikus kulcsunkat és a saját privát kulcsunkat. Ezen kívül pedig szükségünk a küldő számla teljes történetére, hogy meg tudjuk állapítani az egyenlegét. Tehát először le kell tölteni az egész blokkláncot, abban kikeresni a számlatörténetet.

Ha MicroCoint szeretnénk utalni ismernünk kell a cél számla számát (pl. 80-80) illetve itt is szükség van a küldő számla privát kulcsára, azonban a számlatörténetre nincs szükségünk, mert a számla egyenlege megtalálható a SafeBox-ban.

A módszer előnyei:

- Mivel nincs szükség a teljes blokklánc átfésülésére, így a tranzakciók sokkal gyorsabbak.
- A bányászoknak nem szükséges a teljes blokkláncot tárolni, így helyet spórolunk nekik.
- Nem csak a BitCoin által használt secp256k1 privát kulcsok használhatók, ezzel növelve a biztonságot.
- Mivel a publikus kulcsok minden számlához szabadon elérhetőek így bármikor tudunk teljesen titkosított tranzakciókat bonyolítani.

A módszer hátrányai:

- Mivel a számlaszámok egyszerű számok, így a számlák száma véges a BitCoin modelljében viszont végtelen.
- A SafeBox ellenőrző összegét minden blokk után újra kell számolni, ami bár gyors, mégis plusz erőforrást igényel.

Példa egy tranzakció menetére

Sanyi, Zoli és Péter MicroCoin-t használ. Sanyi fizet 10MCC-t a MicroShop-nak. A fizetés pillanatában Sanyi SafeBox-ja módosul, Sanyi egyenlege csökkent 10MCC-vel, a MicroShopé nő 10MCC-vel és a tranzakció bekerül a hálózatra. Ekkor a MicroShop is értesül róla és ő is módosítja a SafeBox egyenlegeket. A tranzakció ekkor már végbement, de még nincs egy blokkban sem.

Péter talál egy blokkot, amelyben szerepelni fog Sanyi tranzakciója. Péter frissíti a SafeBox-ot a blokk alapján, Sanyi egyenlegét csökkenti 10MCC-vel, A MicroWebShop számlaegyenlegét növeli 10MCC-vel és jóváírja az 5 új számlát és a 100MCC-t a blokkért. Zoli megkapja az új blokkot, látja benn, hogy Sanyi költött 10MCC-t így levonja, a MicroShop-nak pedig jóváírja. Hozzáadja az 5 új számlát is a SafeBox-hoz és Péter 100MCC-jét. Sanyi SafeBox-jában már le van vonva a 10MCC és a MicroShopnak is jóvá van írva, így neki csak az új számlákat kell létrehoznia, ugyancsak ez történik a MicroShopnál is. Ekkor a tranzakció már bekerült egy blokkba, azaz meg lett erősítve.

Példa a számla átruházására

Sanyi szeretne Petinek fizetni 100MCC-t, de nem szeretné ezt utalással megoldani. Peti elküldi Sanyinak a publikus kulcsát (nem a privát kulcsot, azt sosem adjuk ki), majd Sanyi választ egyet a számlái közül, amelyen 100MCC az egyenleg. Sanyi beállítja Peti publikus kulcsát a számlához, a csere bekerül a SafeBoxba Petinél és Sanyinál is és bekerül a következő blokkba így a változást az összes csomópont is átvezeti. Ettől a ponttól már Peti rendelkezik a számla felett.

Technikai információk, hogyan működik?

A SafeBox

Ahogyan minden blokklánc alapú kriptovaluta, így a MicroCoin is blokkokat használ a tranzakciók tárolására. (Egy tranzakció alatt azt értjük amikor valamilyen javakat küldünk egy számláról egy másikra.) A blokkok mellett azonban egy másik technológia is rendelkezésre áll, ugyanis a blokkok mellett egy SafeBox is jelen van, amiben az összes számla és azok egyenlege van tárolva. A blokkok mindannyian kapcsolódnak a blokklánchoz. és a bányászok hozzák létre az új blokkokat. Amikor egy bányász létrehoz egy új blokkot az összes csomópont frissíti a nála lévő Safeboxot is. Ekkor a csomópontok frissítik az egyenlegeket a blokkban lévő tranzakciók alapján és létrehozzák az új számlablokkokat.

Az Ősblokk (A Zéró, vagy első blokk)

Az első blokk az indulás pillanatában lett létrehozva. Az első blokkhoz nem tartozik számla, ebben a pillanatban még a SafeBox is üres. Amint az első blokk bányászása megtörtént a hash be lett építve a programba így az mindig jelen van. Ez az első blokk alkotja a blokklánc első elemét, azaz az alappillérét.

A számla felépítése a SafeBoxban

Számlaszám	32 bites előjel nélküli szám	A számla sorszáma.
Publikus kulcs	66-200 byte	A számla publikus kulcsa és a kulcs típusa. A publikus kulcs bármikor megváltoztatható
Egyenleg	64 bites előjel nélküli egész szám	A számla aktuális egyenlege a blokkláncból kalkulálva
Frissítő blokk	64 bites előjel nélküli egész szám	Az utolsó blokk, amely a számlával kapcsolatos tranzakciót tartalmaz
Tranzakciók	Előjel nélküli 32 bites egész szám	Megmutatja, hogy hány tranzakció lett eddig végrehajtva a számlával. Segít

		a tranzakciók sorrendjének meghatározásában és a tranzakciók egyediségének megőrzésében (duplikációk elkerülése)
Név	Karakterlánc	A számla egyedi neve
Típus	Előjel	A számla típusa. Szabadon választható. Egy második réteg implementálásban segítséget nyújthat.

Számla blokk

A számlák blokkokba vannak szervezve. Egy számlablokk öt számlát tartalmaz és egy új blokk bányászásával „jön létre”. A Számla blokk tartalma:

Blokk száma	Előjel nélküli 32 bites szám	A blokk száma a blokkláncban.
Számlák	5 elemű tömb	Az öt számla száma, amely a blokkhoz tartozik
Időbélyeg	Előjel nélküli 32 bites szám	A számla generálásának az időpontja (Unix Timestamp)
Blokk ellenőrző összeg	32 byte	A blokk ellenőrző összege. Minden tranzakció, vagy művelet alkalmával újra kalkulálódik. Ez biztosítja a blokk számláinak integritását.
Blokk fejléc	180 byte	A blokk fejléce. Ennek a segítségével kiszámítható a teljes munka értéke és felépíthető a SafeBox a teljes blokklánc nélkül.

Végül a SafeBox tartalmaz még egy ellenőrző összeget, amelyet az összes blokkellenőrző összegből generálunk. Ez a SafeBox ellenőrző összege

A Blokklánc felépítése

Blokk sorszáma	Előjel nélküli 32 bites szám	A blokk sorszáma
Számla publikus kulcsa	66-200 byte	A blokkhot tartozó 5 számla publikus kulcsa
Jutalom	Előjel nélküli 64 bites szám	A bányászó jutalma
Költség	Előjel nélküli 64 bites szám	A tranzakciók összes költsége
Protokoll verzió	Előjel nélküli 16 bites szám	A protokoll verziója
Elérhető protokoll	Előjel nélküli 16 bites szám	A maximális protokoll, amit a bányászó kliens támogat
Időbélyeg	Előjel nélküli 32 bites szám	UNIX időbélyeg
Cél	Előjel nélküli 32 bites szám	A nehézség (difficulti) amit a bányászoknak el kell érniük

Nonce	Előjel nélküli 32 bites szám	A Nonce az érték, amit a bányászok keresnek. Itt a blokkhoz tartozó megtalált nonce található meg
Előző SafeBox ellenőrzőösszeg	32 byte	Az előző SafeBox ellenőrzőösszege
Tranzakciós ellenőrzőösszeg	32 byte	A tranzakciók ellenőrzőösszege. (Merkle Tree hash)
Proof of Work	32 byte	

A blokk még tartalmazhat egyéb adatokat is, mint pl. a tranzakcióhoz tartozó adatok és üzenetek.