Memeium & Memeium Services

Voidloop

Rátki Barnabás
Felkészítő tanár: Kürtösi Balázs
Árpád Gimnázium, 1034 Budapest, Nagyszombat u. 19.

1. Bevezetés

A Memeium egy blockchain rendszeren működő kriptovaluta és az ehhez tartozó szolgáltatásokat biztosító oldal a Memeium Services. A Memeium egy P2P hálózaton üzemel, mindenki futtathatja a saját teljes értékű szerverét (ún. teljes node- ot). A teljes node applikáció C# -ban megírva, dotnet 2.0 fordítóval lefordítva, hogy minden változtatás nélkül futtatható legyen Windows, Mac és Linux rendszereken. A weboldal ASP.NET Core-ban van elkészítve és jelenleg a Microsoft Azure-on van hosztolva.

2. Probléma megoldásának menete

A kitűzött cél az volt, hogy létrehozzak egy olyan kriptovalutát amit én, és más emberek könnyen tudjunk használni, mint egy digitális token. Nem is volt semmi olyan célja, hogy igazi gazdasági értékkel rendelkezzen, inkább csak jelképes, a felhasználók által nyeri értékét.

Cél volt az is, hogy a token egyszerűen használható legyen és a mozgatása egyik tulajdonostól a másikig relatív kevés időt vegyen igénybe. Másodlagos cél volt, hogy a mai teenagerek világában nagyon elterjedt úgynevezett „meme”-eknek (a „meme” valami vicces kép az interneten) az originalitását díjazni lehessen. Erre készült a szolgáltatások oldal, aminek felhasználói ingyenesen kezelhetik tokenjeiket.

2.1. Memeium protokol

A Memeium protokoll egy elég standard blockchain rendszer. A hálózat P2P, tehát a teljes node-ok egymással közvetlenül kommunikálnak le minden fő adatot. Ezzel is biztosítva, hogy semmilyen fél nem tudja egyoldalúan befolyásolni a rendszert. (Ha egy központi adatbázisban lenne tárolva mindenkinek a tokenjeinek mennyisége, az adatbázis fentartója csak úgy megváltoztathatná azt). A kommunikáció UDP protokollon történik, akármelyik node ha offline állapotba kerül, akkor sem lesz semelyik adat sem elérhetetlen (már persze ha a hálózaton 1-nél több teljes node van). Minden adat minden teljes node-on el van tárolva.

2.2. **Protokol tulajdonságok**

Mint minden blockchain rendszer, a Memeium is egy kizárólagosan írható nyíltan elérhető nyilvántartás („Append only public ledger"), ami csak annyit takar, hogy minden teljes node aki betartja a hálózat „szabályait", olyan adatot tud generálni, amit a többi node a hálózaton igaznak fog elfogadni és senki sem tud törölni semmilyen adatot (csak lokálisan). A blockchain lényege (a neve is innen ered) az, hogy az adatot blokkokra bontjuk le (egy blokkba fogjuk az új tranzakciók adatait) és minden blokk az előtte lévő blokkra épít. Ezeket az adatcsomagokat kell minden node-hoz eljuttatni ahhoz, hogy a hálózaton úgynevezett konszenzus alakuljon ki (egyetértés). Viszont ha mindenki tud generálni újabb adatokat, akkor, hogy döntjük el, hogy mégis kinek írhatja „fel" az általa generált legújabb blokkot a nélkül, hogy kavarodás alakulni ki (egyszerre több node is ugyan arra a blokkra építene egy újabbat). Ennek a megoldására egy általános konszenzus algoritmust alkalmazunk. Aminek az az alapja, hogy az SHA 256 hash algoritmus kimenete pseudo-random, és minden node meg tudja állapítani, mennyi lehet a hálózat össz „teljesítménye" a blokkok kiadásának időközeiből. Ennek a működését elmagyarázni kevés lenne négy oldal. Fontos még megjegyezni, hogy aki sikeresen megnyeri magának az új blokk felírásának lehetőségét, megnyer 4.2 tokent is (1 token = 1 MIM (Memeium) = 100 000 RIP (A legkisebb kifizethető egység 1 RIP)).

2.3. **Kriptográfia**

A Memeium hálózaton minden „pénztárcát" a címe alapján azonosítunk be. A tranzakciók eredetiségét úgy tudjuk bizonyítani, hogy mindenkinek van egy RSA kulcs párja és a privát kulcsával a nyíltan elküldött adatokat még egy példányban aláírva mellékeli a tranzakcióhoz, azzal együtt, hogy megadja a nyílt kulcsát is. Viszont mivel a címe egy tárcának csak a nyílt kulcsának az SHA 256-os hash-e ezért gyakorlatilag csak a cím tulajdonosa tud küldeni tranzakciót, hiszen csak ő ismeri a privát kulcsot. Persze akárki a nyílt kulcs birtokában meg tudja erősíteni, hogy az aláírást csak a nyílt kulcs tulajdonosa készíthette el.

2.4. **Szolgáltatások**

A szolgáltatások oldal (**memeium.ml**) elérhető mindenki számára. Felhasználói rajta tárolhatják biztonságosan a kulcsaikat*. Ezekkel új tranzakciókat hozhatnak létre. Az oldalon lehetőségük van tranzakció kérés létrehozására is. 1. Ábra: a QR- kódot ha eljuttatják a másik félhez és ő beolvassa, majd meglátogatja a benne tárolt linket (akár ezt is el lehet közvetlen küldeni) rögtön a megfelelő címre küldhet egy tranzakciót a kért

összeggel. *(Azt gondolhatnánk, hogy ez elrontja a blockchain lényegét, de valójában a teljes node-ról közvetlen kezelhetjük a címünket és küldhetünk tokeneket, az oldal csak azoknak hasznos akik nem akarják maguk futtatni a node applikációt és megbíznak egy nyílt forráskódú oldalban.)

Még fontos funkció az is, hogy minden nap indul egy verseny, ahova a felhasználók feltölthetik memeeiket és mindenki szavazhat, hogy szerinte melyik a legjobb. A nyertes megnyeri a többi ember által felajánlott token összeget. Persze az oldalon közvetlen adhatunk tokent annak az embernek, akinek a képe elnyerte a tetszésünket.

1. ábra: Tranzakció kérés példa

3. Elért eredmények

A pályamunkám eredetileg nem a pályázatra lett közvetlen fejlesztve, hanem csak saját magam és barátaim szórakoztatására, de azért is, mert nagyon érdekelt az alatta lévő technológia. Az ötlet szerintem elég kreatív de persze más szempontból nem az, mivel nem végeztem új kutatásokat a blockchain technológiával kapcsolatban, inkább csak bevált módszereket ötvöztem. A probléma nélkülöz minden fontosságot hiszen, célja inkább a szórakoztatás. Minden kód fent van githubon: Memeium Github. A teljes node applikáció ~4250 sor. A weboldal ~3440 sor. (Csak a saját kódom számolva.) Megjegyzés: nem mindig van futó teljes node, és olyankor a weboldal minden egyenleget nullának mutat.

Felhasznált könyvtárak és források:

- Bitcoin Wiki
- EmbedIO (Embeded Rest server) * A teljes node-on fut egy REST server de nem ezen keresztül kommunikálnak a node-ok, csak a nyílt REST API megy rajta.
- Newtonsoft.Json

2. ábra: A Memeium logó (Szabó Bianka munkája)