BUDAPESTI GAZDASÁGI EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

Blockchain

A kriptovaluták és az okos szerződések világa

Belső konzulens: Dr. Gubán Miklós

Külső konzulens: Hári Gergő

Budai Gergő
Nappali tagozat
Gazdaságinformatikus
Logisztikai informatikus

2018

BUDAPESTI GAZDASÁGI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME

BGE

GAZDÁLKODÁSI KAR ZALAEGERSZEG

NYILATKOZAT

a szakdolgozat digitális formátumának benyújtásáról

A hallgató neve: Budai Gergő
Szak/szakirány: Gazdaságinformatikus / Logisztikai informatikus

Neptun kód: FSR5FI * A szakdolgozat védésének éve: 2019.
A szakdolgozat címe: Blockchain – A kriptovaluták és az okos szerződések világa

Belső (operatív) konzulens neve: Dr. Gubán Miklós
Külső (szakmai) konzulens neve: Hári Gergő
Legalább 5 kulcsszó a dolgozat tartalmára vonatkozóan: blockchain, kriptovaluta, okos szerződés, Bitcoin, UX

Benyújtott szakdolgozatom **nem titkosított / titkosított**.
(Kérjük a megfelelőt aláhúzni! Titkosított dolgozat esetén a kérelem digitális másolatának a szakdolgozat digitális formátumában szerepelnie kell.)

Hozzájárulok / nem járulok hozzá, hogy nem titkosított szakdolgozatomat az egyetem könyvtára az interneten a nyilvánosság számára közzétegye. (*Kérjük a megfelelőt aláhúzni!*) Hozzájárulásom - szerzői jogaim maradéktalan tiszteletben tartása mellett –nem kizárólagos és időtartamra nem korlátozott felhasználási engedély.

Felelősségem tudatában kijelentem, hogy szakdolgozatom digitális adatállománya mindenben eleget tesz a vonatkozó és hatályos intézményi előírásoknak, tartalma megegyezik nyomtatott formában benyújtott szakdolgozatommal.

Dátum: 2019.01.03. .....
hallgató aláírása

A digitális szakdolgozat könyvtári benyújtását és átvételét igazolom.

Dátum: 2019 JAN. 03 .....
könyvtári munkatárs

Budapesti Gazdasági Egyetem
Gazdálkodási Kar Zalaegerszeg
Könyvtár
8900 Zalaegerszeg
Gasparich u. 18/a
Adószám: 15329822-2-41

P.H.

Tartalomjegyzék

1. Bevezetés

Egyetemi tanulmányaim során több gazdasági területtel is megismerkedtem, de az informatikai tárgyak már a középiskolában is közelebb álltak hozzám. Manapság véleményem szerint ez a leggyorsabban fejlődő iparág. Választásom ezen a területen belül is egy viszonylag újnak mondható technológiára esett.

A blockchain, vagy magyarul blokklánc (továbbiakban blokklánc) vitathatatlanul az elmúlt évek legnagyobb technológiai újítása lehet. A feltételes mód azonban indokolt ezzel a témakörrel kapcsolatban, hiszen napról napra új hírek érkeznek a technológia felhasználásáról, illetve magáról a technológiáról is.

Dolgozatom során több, az egyetemi éveim alatt tanult, hallgatott tárgyat is érintek a témával kapcsolatosan. Néhány ezek közül például az ellátási lánc menedzsment és ügyfélkapcsolati menedzsment, a logisztikai szakirányhoz kapcsolódó tárgyak illetve a dolgozatom egy pontján a Matematikai alapok I. tárgynál tanult ismereteimet is tudtam hasznosítani.

Kutatásom során főleg internetes forrásokból tájékozódtam: weblapokról, blogokról, különböző videókból. Ezek közül is szeretném kiemelni a https://kriptoakademia.com/ oldalt, ahol naponta jelennek meg új hírek gyakorlatilag mindenről, ami a blokklánc technológiával kapcsolatos. Videókat, elemzéseket, részletes leírásokat tesznek közzé, hiteles forrásokból. Nyomtatott forrásom Pásztor Dávid könyve a UX design-ról, amely részletes leírást, betekintést ad a UX szemléletbe.

Dolgozatomban arra keresem a választ, hogy milyen területeken lehet felhasználni ezt a technológiát, mi az oka annak, hogy szinte lehetetlen sikeres hacker támadást végrehajtani egy működő, egyre több felhasználóval rendelkező blokklánc ellen. Továbbá azokra a feltevésekre, hogy hogyan dönthetik össze az ügyvédek munkáját a blokklánc technológiát használó okos szerződések.

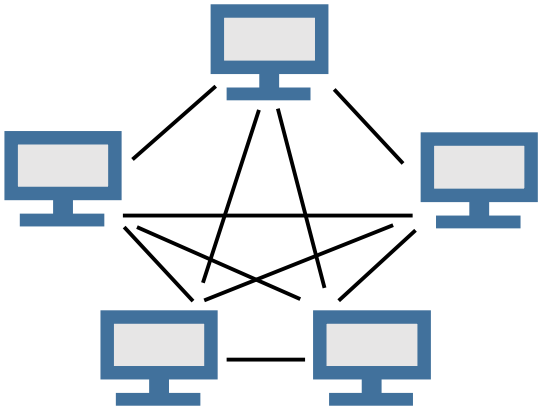
Ezek mellett keresem a választ olyan kérdésekre, is hogy milyen UX problémák találhatóak meg a jelenleg még kiforratlan technológia alkalmazásában illetve arra, hogy ezekre milyen megoldásokat lehetne találni.

Azokra a felvetésekre szeretnék választ találni, hogy az egyes kriptovaluták árfolyama mennyiben tudja befolyásolni a blokklánc világszintű elterjedésének folyamatát, illetve, hogy az emberek az egyes trendek alapján, hogyan viszonyulnak jelenleg ehhez a technológiához.

A szakdolgozat elkészítésében nagy segítségemre szolgált a duális gyakorlati helyemtől, a Zalaszám Informatika Kft-től kapott segítség a három és fél év során. Ezalatt értem a duális mentoromtól, a rendszerszervezési osztály vezetőjétől, a külső konzulensemtől illetve a fejlesztő csapat tagjaitól kapott segítséget. Továbbá a különböző oktatásokat, amikben részt vehettem a cégnél, különösen kiemelve a UX oktatást.

2. Előzmények – Nick Szabo, Satoshi Nakamoto

Meglepő, de ebben a témában az első olyan leírás, ötlet, amely ha csak közvetetten is, de kapcsolódik a blokklánc mai formájához, az okos szerződésekről szólt. Nick Szabo, kriptográfus 1996-ban fektette le az okos szerződések alapjait. Az volt az elképzelése, hogy létrehozzon a kibertérben egy olyan rendszert, amiben az emberek a kriptográfia segítségével gyorsan, kötetlenül kereskedni tudjanak egymással. Szabo szeretett volna ehhez a rendszerhez létrehozni egy virtuális pénzt. Az alapvető probléma, amit ki akart küszöbölni az volt, hogy a kriptovaluták megjelenése előtt csak úgy tudott a pénzünk gazdát cserélni, hogy megbíztunk egy közvetítő, „harmadik személyben", amely ebben az esetben a bank. Ezt a harmadik személyt a szaknyelv gyakran csak Middleman-ként emlegeti. Ennek a virtuális pénznek az elméleti alapjait, amelyet egy peer-to-peer hálózaton gondolt megvalósítani két évvel később, 1998-ban írta le. A peer-to-peer hálózat lényege, hogy nincs egy központi számítógép, szerver vagy kliens, hanem az eszközök közvetlenül egymással kommunikálnak. A virtuális pénzt Szabo Bit Goldnak nevezte el és csak 2005-ben hozta teljes mértékben nyilvánosságra. A proof of work („a munka bizonyítéka") rendszert és a hash-eket akarta használni a mining-hoz (bányászat). Ezekről a fogalmakról a későbbiek során lesz szó részletesebben. Később Szabo a saját blogján keresett társakat, akik segítenek neki megvalósítani a Bit Goldot. Sosem fogjuk megtudni, hogy miként működött volna a gyakorlatban Nick Szabo kriptovalutája, ugyanis sosem lett létrehozva. Ahogyan arra sem tudjuk a választ, hogy érkezett-e megkeresés Szabonál az üggyel kapcsolatban. [1]



1. ábra: Peer-to-Peer (P2P) hálózat, Saját szerkesztés

Satoshi Nakamoto

Ez a név, álnév vagy fantázianév valószínűleg örökre fenn fog maradni egyfajta lenyomatként az utókor számára a kriptovalutákkal, okos szerződésekkel illetve a blokklánc technológiával kapcsolatban. A név - amelynek egy külön sort szántam a dolgozatomban - 2008-ban a gazdasági világválság évében vált ismertté a világ számára, ugyanis ebben az évben november 1.-jén hozta nyilvánosságra a Bitcoin „white paper"-jét, leírását. [2]

Satoshi 2009-ben elindította a Bitcoin első verzióját, majd egy levelezőlistán együtt dolgozott egy fejlesztőcsapattal a tökéletesítésén. Mindvégig nagyon figyelt arra, hogy semmi olyan dolog ne derüljön ki róla, ami által beazonosítható lenne a személye. Akik vele dolgoztak, azt mondták, hogy szinte hiba nélkül, minimális teszteléssel programozott, egyszerű, rövid válaszokat adott. A mai napig nem tudjuk, hogy kicsoda Satoshi Nakamoto. Nincsenek róla információk, hogy nő, férfi vagy esetleg egy szervezet lenne. [3]

Joshua Davis a „The New Yorker" újság egyik írója sokáig kutatta a személyét, egy ismerősével átnézette a Bitcoin programkódját is, azt remélve, hogy talál benne valami információt, ami a segítségére lehet. Azt írja, hogy több olyan helyet is talált a kódban, ami egy lehetséges hibája lehetne a rendszernek első ránézésre, de ezeknél a részeknél kivétel nélkül talált egy megjegyzést is Satoshi-tól, hogy az tényleg egy hibája lehetne a rendszernek, de már ki lett javítva. Satoshi 2011 tavaszán írt utoljára a fejlesztőcsapatnak, az e-mail a tőle megszokott rövidséggel és határozottsággal csak annyit tartalmazott, hogy már továbblépett a témától, mással foglalkozik, és jó kezekben lesz a fejlesztőcsapatnál a Bitcoin. Azóta számos személyre, kriptográfusra próbálták rábizonyítani – köztük Nick Szabora és Elon Muskra (a Tesla vezérigazgatója) is -, hogy ő volt Satoshi Nakamoto, de ezek az egyének egytől egyig visszautasították a feltételezéseket. Satoshi nagyon ügyelt arra, hogy ne derüljön ki a személye, valószínűleg ezzel az volt a célja, hogy a figyelem ne rá, hanem sokkal inkább az általa megvalósított technológiára irányuljon. [3,4]

3. Blokklánc

A blokklánc egy elosztott, decentralizált, nyilvános adatbázis. Elosztott azért, mert minden tranzakciót minden egyes blokkláncban szereplő fél ellenőriz valós időben, decentralizált, mert nincs egy központi számítógép, eszköz, ami irányítaná a folyamatot, és nyilvános, mert a benne történő tranzakciók minden csomópont részére elérhetőek, láthatóak. A legtöbb weboldalon, blogon vagy konferenciákon általában úgy emlegetik a blokklánc technológiát, mint az internet új korát, vagy mint az új internetet. Eredetileg a kriptovaluták használatához lett kitalálva, és a Bitcoinnal kezdődött meg a használata, de számos felhasználási területe van és lehet még a jövőben ennek a technológiának. [5,6]

A legtöbb ember manapság azt kérdezi, mi is az a blokklánc, mi ez a technológia, hogyan működik, mire lehet használni? A kérdések nagy részére valószínűleg nem fogják megkapni az emberek a választ, vagy ha meg is kapják, nem fogja őket érdekelni, amennyiben valóban széles körben elterjed majd a blokklánc a jövőben és számos területen használni fogja az emberiség. Akárcsak az internet esetében, annak sem tudják az emberek a működését, a hátterét, a technológiai részleteit, de mégis használják.

Manapság a hétköznapi emberek nagy része szereti a megszokott dolgokat és az új, innovatív dolgok iránt nem érdeklődnek annyira, egészen addig, amíg egy terméknek, szolgáltatásnak vagy technológiának nem lesz egészen nagy felhasználói közössége, nem írnak róla véleményeket vagy tartanak a hétköznapi ember számára is érthető előadásokat. Egy szóval az emberek bizalmatlanok, szkeptikusak az új dolgokra, amiknek nem ismerik a technológiai hátterét, sokszor féltik az adataikat, féltik megadni a számla és bankkártya vagy éppen más személyes adataikat.

A dolog érdekessége, hogy ez a technológia pont a bizalmatlanság ellen megoldás. Amikor böngésszük az interneten a különféle szállásközvetítő, fuvarozó oldalakat vagy akár az internetes piacokat, a legelső, amit az oldalon megnézünk, hogy az adott szállásadó, fuvarozó vagy termékkínáló cég vagy magánszemély milyen értékeléssel rendelkezik. Milyen kommenteket írtak róla, vagy az általa kínált termékekről, szolgáltatásokról. A blokklánc technológia lehetőséget nyújt az ilyen bizalmi kérdések elkerülésére, mellőzésére. A korábban említett kérdéseim közül a legfontosabb valószínűleg az utolsó, az, hogy mire is lehet felhasználni ezt a technológiát. Erről a későbbiek során részletesebben fogok írni. [7]

A következő alpontok a technológia hátteréről, a működési elvéről fognak szólni.

3.1. Elosztott adatbázis, node-ok, blokkok

A legjobb példa annak az elmagyarázására, megértésére, hogy hogyan is működik egy ilyen elosztott adatbázis, az a Google dokumentum. Korábban, amennyiben egy dokumentumot, például egy szakdolgozatot véleményeztetni szerettünk volna a konzulensünkkel, akkor elküldtünk neki e-mailben, vagy odaadtuk neki pendrive-on és az így képződött másolatot véleményezte a konzulensünk majd később visszaküldte. Így a dokumentumunkból már kettő verzió volt, és akárhányszor egy ilyen folyamat lezajlott mindig egyre több verzió készült a dokumentumból és egy idő után nehéz volt követni a verziószámokat, gyakran össze lehetett keverni őket. [5,8]

Amennyiben egy Google dokumentumban dolgozunk, akkor elég az elérési útját tudni mindkét vagy akár több félnek, és a módosítások valós időben történnek egyetlen dokumentumon. Így nem veszünk el a verziószámok és a dokumentumok sokasága között. Nagyjából így működik a blokklánc elosztott adatbázisa is, mindenki számára valós időben elérhető a teljes blokklánc.

A blokklánc decentralizált hálózatának egyes csomópontjain lévő számítógépeket, eszközöket node-oknak nevezzük. A node-ok hitelesítik a blokkláncon történő tranzakciókat és mindegyik node számára letöltésre kerül az aktuális blokklánc, amikor csatlakozik a hálózathoz. Minden egyes node „adminisztrátor" a blokkláncon, nincsen közöttük kitüntetett szereppel rendelkező, továbbá mindegyik node önként, saját szándékából csatlakozik a blokklánchoz. Ezért is mondhatjuk azt, hogy ez egy decentralizált hálózat. [5,8]

Ezek a csomópontok egymás között elkezdenek kereskedni, tranzakciók zajlanak le közöttük. Ahhoz hogy egy blokklánc létrejöjjön, minimum három tagjának kell lennie. Megtörténik az első tranzakció, az egyik tag – hívjuk őt Bettinek – utal 5 kriptovalutát egy másik tagnak – hívjuk őt Dávidnak. Ezt a tranzakciót minden egyes, a blokkláncban szereplő node ellenőrzi és feljegyzi magának. Ellenőrzik, hogy Bettinek van-e elegendő mennyiségű pénz a tárcájában, majd amennyiben megbizonyosodtak róla, feljegyzik. Majd ezt követik további tranzakciók és egy bizonyos mennyiségnél betelik egy blokk. Ekkor ezt a blokkot le kell zárni, hitelesíteni kell. Ez úgy történik, hogy ez a blokk kap egy hitelesítési kódot az egyik tag által, majd az összeg többi tag megvizsgálja ezt a kódot, és amennyiben érvényesnek találják, akkor bekerül a blokk a blokklánc végére. [5,8]

Itt több kérdés is felmerülhet, mi alapján készül egy hitelesítési kód, mi alapján fogadják azt el a többiek, vagy, hogy mi történik akkor, ha egy tagnál nem stimmel a hitelesítési kód. Az egyszerűség kedvéért a fentiekben a hitelesítési kód szót használtam a probléma átláthatósága érdekében. Ezt a hitelesítési kódot a Proof of Work (PoW) mechanizmussal (a munka bizonyítéka), és egy hash-függvénnyel lehet előállítani. [5,8]

A hash folyamatát a későbbiek során mélyebben kifejtem, a probléma megértéséhez egyelőre elegendő annyi, hogy ez egy kód, amit egy bonyolult függvénnyel lehet előállítani. Ezt a hitelesítési kódot tehát az összes tagnak el kell fogadnia, amennyiben egy node-nál nem stimmel, akkor vagy rosszul jegyezte fel az egyik tranzakciót vagy szándékosan csalni szeretne a rendszerben. Mivel a többiek mind elfogadták a hitelesítési kódot, így neki két lehetősége van:

- Ő is átírja a kódját arra, ami a többiek által az elfogadott
- Nem változtatja meg a hitelesítési kódját, ebben az esetben ő kiesik a blokkláncból, nem maradhat a tagja. [5,8]

Itt el is érkeztem a rendszer egyetlen kiaknázható hibájára. Amennyiben a blokklánc hálózatához tartozó közösségünk tagjainak a száma például 20 fő és ebből 11-en „csalni" akarnak, vagyis megváltoztatni egy hitelesítési kódot, vagy átírni egy korábbi tranzakciót - ami szintén a hitelesítési kód megváltoztatásával járna – akkor a rendszer működése felborul, és a hacker-csapat sikert arat. Ezt a szaknyelv 51% Attack néven emlegeti. Ez a probléma kicsit összetettebb, de ahhoz, hogy ezt érthető legyen, szükség van arra, hogy világos legyen számunkra a hash folyamata is. Erre a témára is később fogok kitérni a dolgozatomban. [5,8]

Van még egy fontos dolog, ami szükséges ahhoz, hogy a blokklánc probléma nélkül működhessen. Ahogy korábban írtam, a hitelesítési kódot előállítja egy node és a többiek ezután ellenőrzik, majd ők is „lepecsételik" ezzel a blokkot. Ezt a folyamatot – a hitelesítési szám előállítását – nevezik bányászásnak (mining). Itt felmerül a kérdés, hogy amennyiben valaki „megkeresi" helyettünk a hitelesítési számot, akkor miért nem várjuk meg mindig, hogy valaki más megkeresse, és mi csak elfogadjuk? [5,8]

Így jönnek létre a kriptovaluták, mert aki a leggyorsabban megtalálja ezt a hitelesítési kódot, ő jutalomban részesül, kap érte egy adott számú kriptovalutát például bitcoint. Így már kicsit érthetőbb, hogy miért hívják ezt a folyamatot bányászásnak, hasonlíthatjuk például az arany bányászásához, csak itt a bányászáshoz nem csákányt kell használnunk, hanem egy erős számítógépet.

3.2. Hash-ek, megváltoztathatatlanság, biztonság

A hash függvény egy stringet ad eredményül minden esetben. A string számok és betűk sorozata. Ez a függvény változó számú karakter befogadására képes, de meghatározott számú karaktert ad eredményül. Amennyiben a bemeneti oldalon megváltoztatunk akár csak egyetlen karaktert is, a kimeneti oldalon a hash értéke teljesen más lesz. Az alábbi példában egy online hash generátor segítségével fogom bemutatni ennek a működését:

Beviteli oldal	Kimeneti oldal (Hash)
Betti 8 bitcoint ad Dávidnak	9E68D4B7AE95C966A22185346FDBA1CD17AE0D907F760F0893071FB6A16D0F3C
Betti 6 bitcoint ad Dávidnak	536ED0CACC57618C3EF1B2907A801EBA73D945C1D6353F3F81A8B56C4994860A
Betti 6 bitcoint ad Dávidna	91F484922742B4025BE95BC903D9DACDA3A719BC9C20AB6B5AA667705AF8A1C8

1. táblázat: Hash-függvény
Letöltés időpontja: 2018.09.27. Hozzáférés (URL): https://passwordsgenerator.net/sha256-hash-generator/

Látható, hogy valóban elég egyetlen karakter módosítása és teljesen más hash-t kapunk a kimeneti oldalon. Ennek a hash generátornak a neve SHA256, ezt használja a Bitcoin is. Az előző pontban említettek szerint, amikor egy blokk elkészül, akkor kap egy hitelesítési kódot, amit úgy bányásznak ki a tagok.

Tegyük fel, hogy egy blokk tartalmazza a fent említett példámban az első tranzakciót. Legyen ez az első blokkunk a láncon. Ebből generálni egy kimeneti stringet a hash függvénnyel nem igényel nagy energiát, hiszen ez pillanatok alatt elő tud állni. Ezért is van meghatározva, hogy a kimeneti hash-nek ez bizonyos része hogyan kell, hogy kinézzen. A Bitcoin esetén egy bizonyos számú nullával kell kezdődni ezeknek a hash-eknek. Ezt úgy tudja elérni egy bányász, hogy a bemeneti oldalon lévő adatokhoz hozzáír egy számot. Ekkor a kimeneti oldalon megváltozik az egész hash. [5,8]

Mivel a hash kimenetele nagyon bonyolult, ezért a bányásznak próbálkozni kell, hogy mi az a szám – a szaknyelv ezt úgy hívja, hogy nonce - amit, ha hozzáír a bemeneti adatokhoz, egy olyan hash-t eredményez, ami egy meghatározott számú nullával kezdődik. Amint az egyik bányász megtalálja ezt a számot, elkészül az új blokk hitelesítése és hozzáadódik a lánc végéhez. Felvetődik a korábbi kérdés, hogy mi történik, ha valaki át akar írni valamit az egyik tranzakcióban? Erre az esetre van egy csavar a blokkok hitelesítésében. Ugyanis amint a következő blokk hitelesítésére kerül sor, a tranzakciós lista mellett a bemeneti adatokhoz hozzátevődik az előző blokk hash-e. Így tehát három dologból tevődnek össze a bemeneti oldalon lévő adatok:

- a tranzakciók listája
- az előző blokk hash-e
- és a megkeresendő nonce érték [5,8]

Ezzel biztosítva van a felülírhatatlanság, hiszen amennyiben valaki az egyik blokkban egy tranzakciót módosítani szeretne, akkor az összes többi blokk hash-ét is meg kellene változtatnia, a blokklánc növekedésével viszont erre egyre kisebb és kisebb esélye van egy esetleges támadó csapatnak. [5,8]

3.3. Felhasználása, lehetőségek

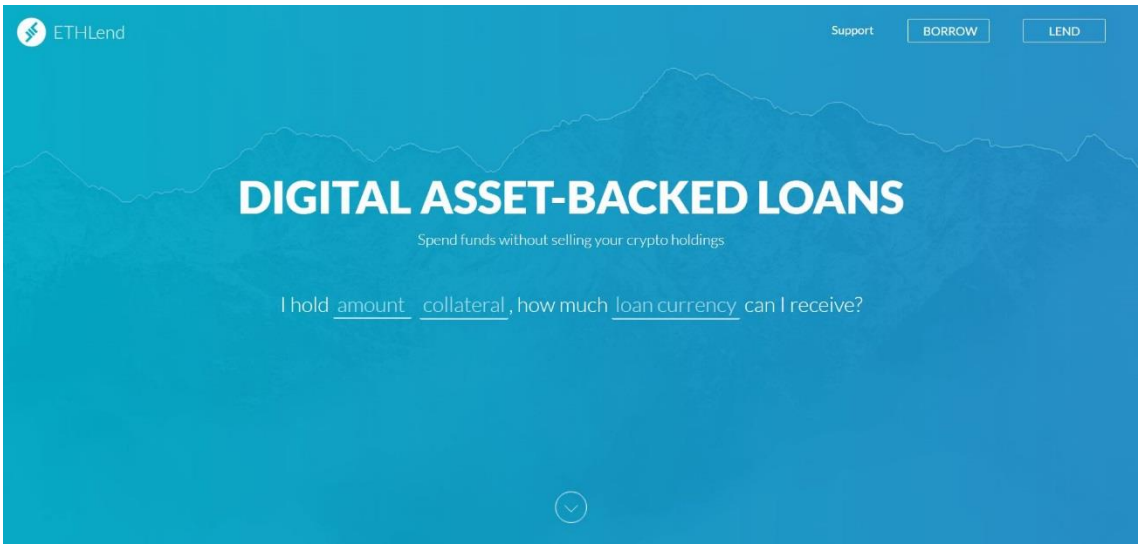
Tény, hogy 2018-ban az elsődleges felhasználási területe a kriptovalutáknál van. A második leghíresebb ága az okos szerződések hátterében való működés. A kriptovalutáknál elsősorban a Bitcoin, az okos szerződéseknél pedig az Ethereum, ami elsőre eszünkbe juthat. Ezt a két témát dolgozatom során részletesebben ki fogom fejteni. Egy másik érdekes lehetőség ehhez a technológiához kapcsolódva a közösségi finanszírozás (Crowdfunding).

A közösségi finanszírozás lényegében azt jelenti, hogy az emberek tőkét fektetnek be bizonyos cégek megalapításába, termékek vagy szolgáltatások megvalósításába. Ilyen cég volt 2016-ban, az Ethereum által „szponzorált" The DAO. Ennél a cégnél a részvényeseknek a tőkéjükért cserébe tokeneket[1] adtak, amik a cégben való részvényüket fejezték ki. Későbbiek során ennek a cégnek az életútját az Ethereumhoz kapcsolódóan írom le.

[1] A token egyfajta részesedést jelent egy decentralizált cégben vagy egy használati jogot egy ilyen applikációhoz. Egy tokennek van egy kezdeti értéke, illetve a későbbiek során el lehet adni, üzletelni lehet vele.

A blokklánc technológia felhasználását kétféleképpen csoportosíthatjuk. Egyrészt kategorizálhatjuk a felépítésük, architektúrájuk szerint, másrészt a felhasználási körük szerint. Felépítésük szerint a Bitcoin egy komplett rendszert jelent, nem csak egy applikációt, magába foglalja a blokkláncot és a teljes szerkezetet. A Bitcoin után megjelenő felületek sokkal inkább már csak az infrastruktúrát valósítják meg. Az újonnan megjelenő alkalmazások pedig nem rendelkeznek saját blokklánccal, hanem az imént említett keretrendszerekhez kapcsolódnak. [13]

Az előbbire jó példa az Ethereum az utóbbira pedig például az ETHLend. Az ETHLend egy decentralizált hitelezési applikáció, ami az Ethereum hálózatán, blokkláncán működik. A biztonságért pedig peer-to-peer alapú okos szerződés(ek) felelnek. Az ETHLend célja az, hogy biztonságos hitelezési lehetőséget biztosítson a nagy bankok és pénzügyi intézetek (harmadik fél) kihagyásával. [14]



2. ábra: ETHLend honlap kezdőképernyő [képernyőkép]. Letöltés időpontja: 2018.10.30. Hozzáférés (URL): https://ethlend.io/#/main

A decentralizáció a jelenlegi hitelfelvételi rendszerekhez kapcsolódó számos problémát megoldhatja. A három legnagyobb ok a hitelek decentralizálása céljából:

- Megbízhatóság: A decentralizáció teljesen megszünteti a bizalmi kérdéseket a hitelszolgáltatók illetve a partnerek felé. Ebben az esetben a hitelezések harmadik, köztes fél nélkül zajlanak, a hitelbiztosítékokat okos szerződésekben lehet rögzíteni és zárolni, amelyeket a nyilvános blokklánc rendszeren tárolnak.

- Átláthatóság: Az Ethereum blokklánc hálózata könnyen átlátható könyvelést biztosít, ami - mivel nyílt blokkláncon történik - bárki számára ellenőrizhető. Minden egyes tranzakció, ami a hálózaton történik, rögzítésre kerül és ezután áttekinthető. Ez a könyvelés megszüntet egy újabb bizalmi kérdést a különböző bankintézmények között.
- Hozzáférés: A hitel felvételéhez, vagy a hitel nyújtásához nem kell közvetlenül bemennünk egy hitelintézethez vagy egy bankhoz. Az elérhetősége a világ bármely pontjáról nyitott a hitelfelvevők illetve a hitelnyújtók számára. A hitelezések száma, illetve azok nagysága pedig korlátlan, mind a hitelezők, mind a hitelfelvevők hozzá tudnak férni ezáltal egy sokkal szélesebb körű hitelezési rendszerhez. [14]

Ahhoz hogy érthető legyen ez a hitelezési lehetőség, szükség van egy fogalom ismertetésére, ami nem más, mint az ERC20 token. Egy példát szeretnék megemlíteni a könnyebb megértés érdekében. Tegyük fel, hogy egy adott személy vásárol egy koncertjegyet, amihez kapcsolódik úgynevezett voucher (utalvány) amivel egy doboz tejre jogosult az említett személy az egyik nagy áruházláncban. Amennyiben elmegy beváltani az utalványát akkor a koncertjegy volt számára a token amiért valami értéket/vagyoni értékű jogot kapott, illetve a pénz, amivel kifizette a koncertjegyet, az volt az adott kriptovaluta. Annak érdekében, hogy a korábban említett témánál (ETHLend) maradjak, legyen ez a kriptovaluta az ether. Az ERC az Ethereum Request for Comments rövidítése, ami egy szabvány, egy hivatalos protokoll. [15]

Ez a protokoll 6 követelményt tartalmaz.

```
contract ERC20 {
  function totalSupply() constant returns (uint totalSupply);
  function balanceOf(address _owner) constant returns (uint balance);
  function transfer(address _to, uint _value) returns (bool success);
  function transferFrom(address _from, address _to, uint _value) returns (bool success);
  function approve(address _spender, uint _value) returns (bool success);
  function allowance(address _owner, address _spender) constant returns (uint remaining);

  event Transfer(address indexed _from, address indexed _to, uint _value);
  event Approval(address indexed _owner, address indexed _spender, uint _value);
}
```

3. ábra: ERC20 token szabvány. Letöltés dátuma: 2018.11.08. Hozzáférés (URL): https://medium.com/envienta-magyarorsz%C3%A1g/nyomjunk-saj%C3%A1t-p%C3%A9nzt-avagy-az-erc20-as-tokenek-rejtelmei-1-r%C3%A9sz-ethereumtudas-190b72e21115

Nézzük sorban ezeket a szabályokat:

„*function totalSupply() constant returns (uint totalSupply);*

Ez a metódus azt adja meg, hogy összesen hány darab létezik az adott tokenből.

function balanceOf(address _owner) constant returns (uint balance);

Ez a metódus megmondja, hogy a megadott Ethereum cím tulajdonosának hány darab tokenje van.

function transfer(address _to, uint _value) returns (bool success);

Ezzel a metódussal tudunk a megadott ethereum címre megadott mennyiségű tokent küldeni.

function approve(address _spender, uint _value) returns (bool success);

Ezzel a metódussal engedélyezhetjük a megadott ethereum cím tulajdonosának, hogy a megadott értékig tokent vonjon tőlünk le. Ez olyasmi, mint bankoknál a csoportos beszedési megbízás engedélyezése mondjuk a biztosító számára, hogy havonta levonja az életbiztosításunk díját.

function allowance(address _owner, address _spender) constant returns (uint remaining);

Ezzel a metódussal lehet lekérdezni, hogy a megadott ethereum cím tulajdonosának számlájáról a megadott másik cím tulajdonosa még mekkora összeget tud levonni.

function transferFrom(address _from, address _to, uint _value) returns (bool success);

Ezzel a metódussal indítható utalás az approve metódusban megadott egyenleg terhére. Tehát ezt kell hívnia pl. a biztosító társaságnak, hogy levonja a biztosítási díjat.

A végére maradt két esemény, amin keresztül az okos szerződés értesítheti a pénztárcát (walletet), hogy utalás (mi indítottuk), vagy levonás (másik fél indította a számára engedélyezett mennyiség terhére) történt:

event Transfer(address indexed _from, address indexed _to, uint _value);

event Approval(address indexed _owner, address indexed _spender, uint _value);

Ezen kívül meg kell adnunk 3 publikus változó értékét, ami a token elnevezését, szimbólumát, és a kezelt tizedes jegyek számát tartalmazza. Vagyis azt, hogy az adott token hányfelé osztható (ez az érték általában 18).

string public constant name = "Token Name";
string public constant symbol = "SYM";
uint8 public constant decimals = 18;„[2]
Az ETHLenden a hitelfelvevőnek ilyen ERC20 szabványú tokent kell lekötnie a szerződésben arra az esetre, ha nem fizetné vissza a hitelt. A hitelkérelem beadásához néhány adatot meg kell határozni:

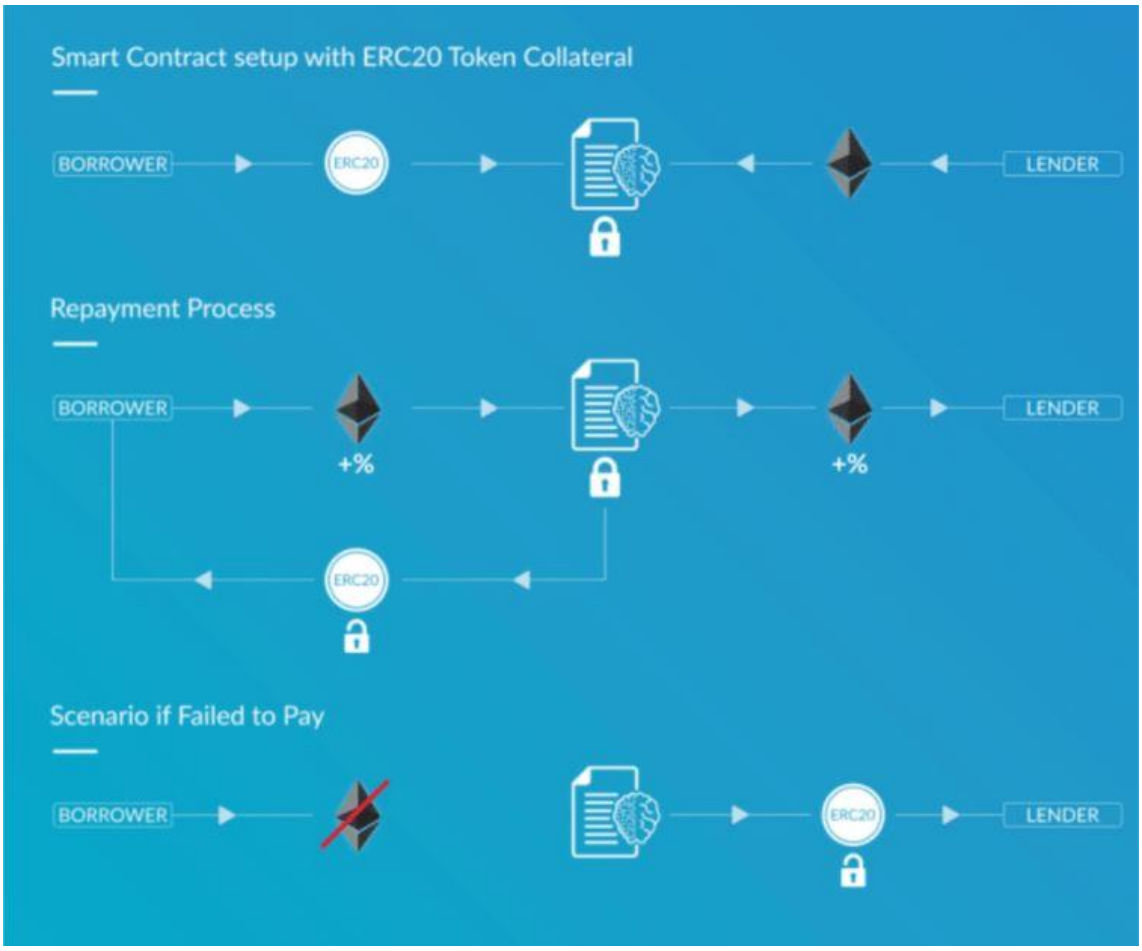
- a hitel hossza (lejárati ideje)
- a hitel nagysága
- a kamat mértéke
- illetve a szükséges tokenek mennyisége/összege [14]

Amennyiben a hitelező beleegyezik a feltételekbe, létrejön a hitelszerződés. Ennek a szerződésnek kettő kimenetele lehet:

- A hitelfelvevő probléma nélkül visszafizeti hitelösszegét a meghatározott kamatokkal együtt.
- A hitelfelvevő nem fizeti vissza a hitelt, ezután a hitelező megkapja a hitelfelvevő által fizetett biztosítékot (token). [14]

[2] Fazekas László: Nyomjunk saját pénzt, avagy az ERC20-as tokenek rejtelmei (1.rész) [online]. Letöltés dátuma: 2018.11.08. Hozzáférés (URL): https://medium.com/envienta-magyarorsz%C3%A1g/nyomjunk-saj%C3%A1t-p%C3%A9nzt-avagy-az-erc20-as-tokenek-rejtelmei-1-r%C3%A9sz-ethereumtudas-190b72e21115

Az alábbi ábra ennek a szerződésnek a kimeneteleit szemlélteti:



4. ábra: ETHLend hitelszerződés menete. Letöltés időpontja: 2018.11.09. Hozzáférés (URL): https://coincentral.com/ethlend-beginner-guide/

Jól látható tehát, hogy az ETHLend nem működtet saját blokkláncot, hanem az Ethereum blokkláncát használja, és ők csak egy alkalmazást biztosítanak a hitelszerződések létrehozásához.

A keretrendszerek, illetve az applikációk között megjelent egy harmadik réteg is. Ezt a réteget a szaknyelv middleware névvel illeti/jellemzi. Itt olyan szolgáltatásokról beszélhetünk, amelyek például az integrációt valósítják meg a meglévő rendszerekhez. Ugyanakkor ide sorolhatóak azok a middleware-ek is, amelyek különféle kriptovaluták közötti átváltási lehetőségeket biztosítják. Ilyenre példa a Kraken. [13]

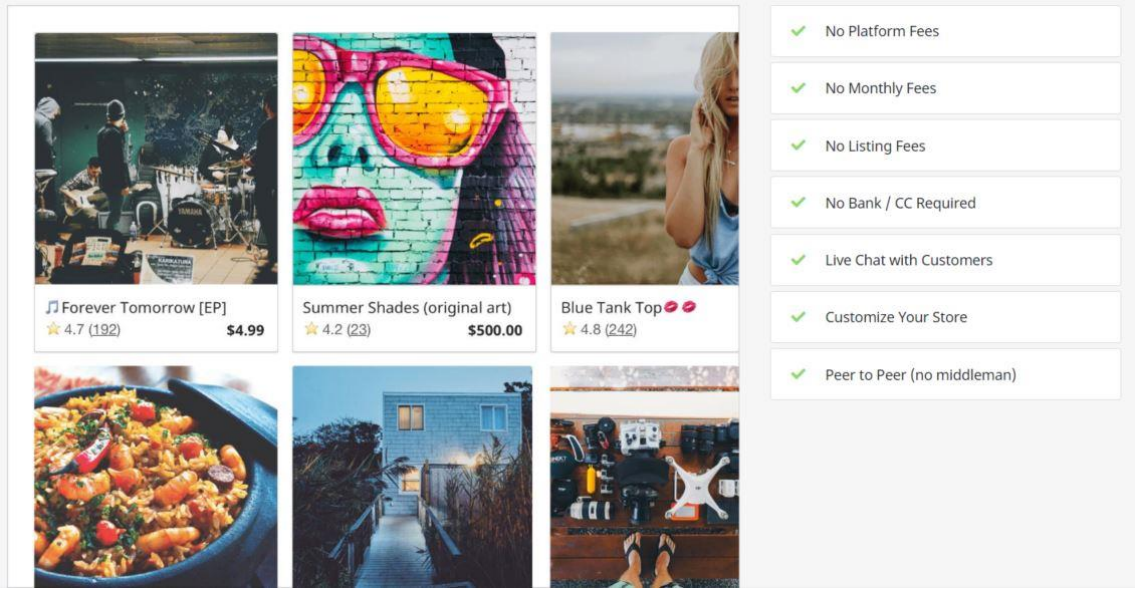
A következőkben bemutatok pár területet (felhasználási kör szerinti csoportosítás), ahol hasznosítani lehetne a technológiát, illetve említek rá példát, amelyik részben vagy egészében az előtte lévő felvetést valósítja meg.

- Okos szerződések

A blokklánc technológia lehetővé teszi, hogy szerződéseket kódoljunk rajta, amelyek harmadik fél nélkül jönnek létre, működnek és zárulnak le. Erre ad lehetőséget az Ethereum. Az okos szerződésekkel illetve az Ethereummal dolgozatom során a későbbiekben részletesen foglalkozom.

- Gazdaság

Az Uber és az AirBnB bebizonyította, hogy a gazdaság ezen megosztott formájának sikere van és lesz a jövőben. Az Uber a szállítás, közlekedés terén, az AirBnB pedig a szálláskiadás, szállásfoglalás terén. Ugyanakkor ezek nem mondhatók decentralizált hálózatnak, mivel mindkét szolgáltatásnál található middleman. Egy jó példa erre az OpenBazaar. Ezt az alkalmazást úgy kell elképzelni, mint egy peer-to-peer alapú virtuális piactér. [16]



5. ábra: Openbazaar honlap [képernyőkép]. Letöltés időpontja: 2018.11.13. Hozzáférés (URL): https://openbazaar.org/

A honlapjuk kezdőképernyőjén felsorolják, hogy mivel jobbak, mivel többek, mint egy egyszerű virtuális piactér:

- Nincsenek platform díjak
- Nincsenek havi díjak
- Nincs listázási költség
- Nincs szükség bankra

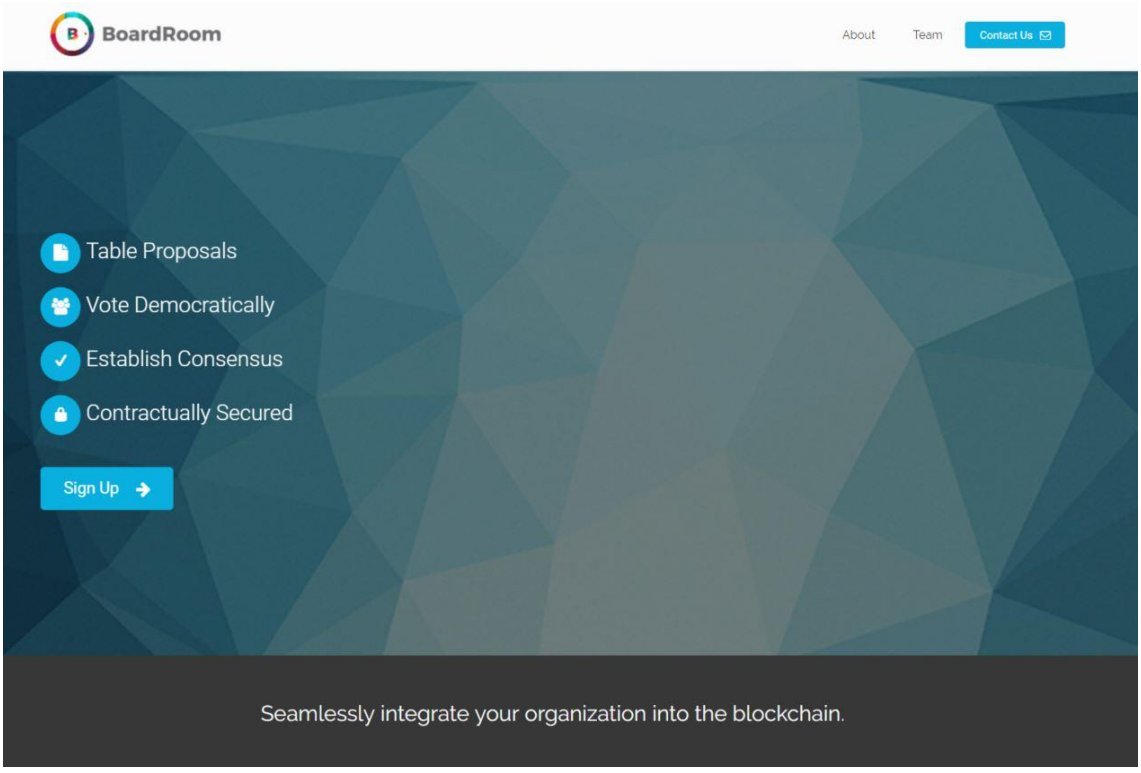
- Az alkalmazásban valós időben lehet kommunikálni az ügyfelekkel
- Testreszabhatóság
- Peer-to-peer hálózat, tehát nincs szükség harmadik, köztes félre. [17]

- Közösségi finanszírozás

A közösségi finanszírozás egy előrelépési lehetőség a peer-to-peer alkalmazásokat fejlesztők számára. Amennyiben közösségi finanszírozást szeretnénk indítani, a legismertebb lehetőségek erre a Kickstarter vagy a Gofundme. Ahogy a korábbiakban már említettem, egy ilyen közösségi finanszírozáson alapú kísérlet volt a The DAO is. A későbbiek során részletesen foglalkozom a cég életútjával. [16]

- Kormányzás

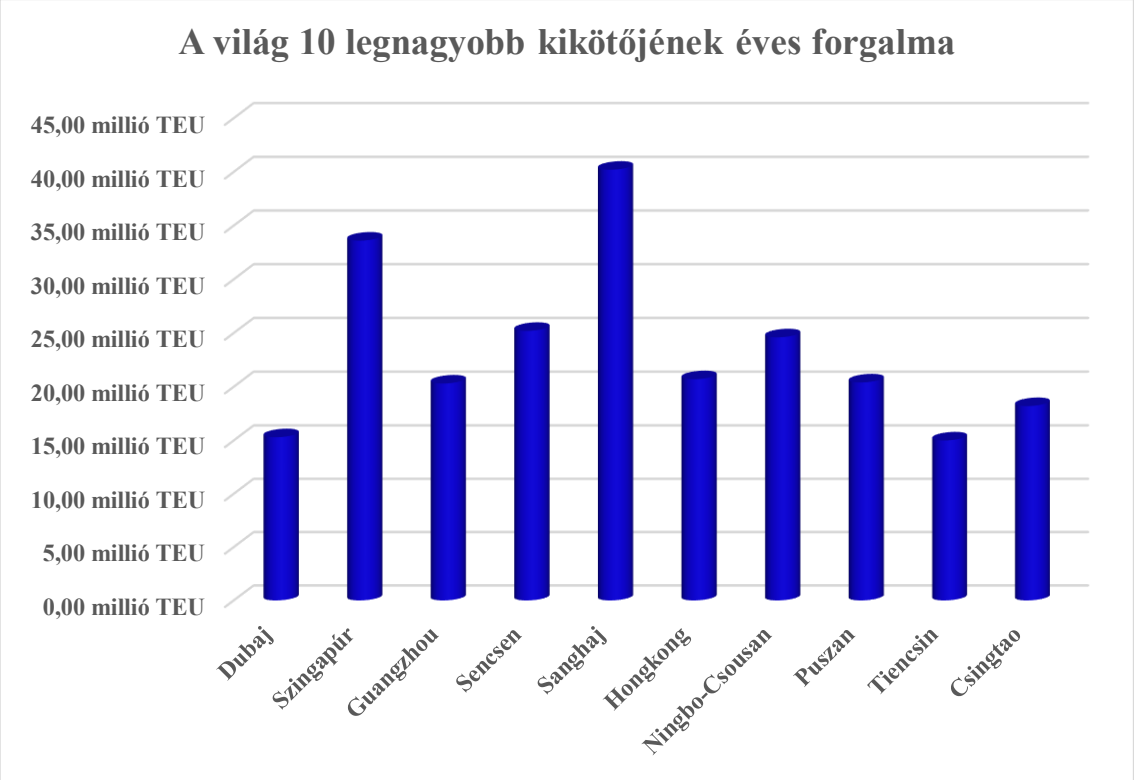
A blokklánc technológia megkönnyítheti a szavazások, választások menetét. Segítheti a szavazások átláthatóságát, felgyorsíthatja a folyamatot és kizárja a csalások lehetőségét. Ennek a lehetőségét próbálja megvalósítani a BoardRoom nevű applikáció. A BoardRoom egy, az Ethereum blokklánc hálózatán működő okos szerződésekkel vezérelt kormányzati keretrendszer egyének és cégek számára egyaránt. [16,17]



6. ábra: Boardroom honlap kezdőképernyő [képernyőkép]. Letöltés időpontja: 2018.11.22. Hozzáférés (URL): http://boardroom.to/

- Ellátási lánc

Manapság az emberek szeretnék tudni, hogy a termék, amit megvásárolnak az üzletekben, honnan is származik valójában, honnan indult el, milyen csomópontokon ment keresztül és mennyi idő alatt ért el az otthonukba. Amennyiben az ellátási láncot a blokklánc technológiával kezelnék a résztvevői, akkor nem csak a résztvevők és a fogyasztók (akik az ellátási lánc utolsó résztvevői) láthatnák át az egész folyamatot, de fel is gyorsíthatnák, egyszerűsíthetnék.



7. ábra: Saját szerkesztés a Forbes 2018. októberi számának 64. oldalán található adatai alapján.

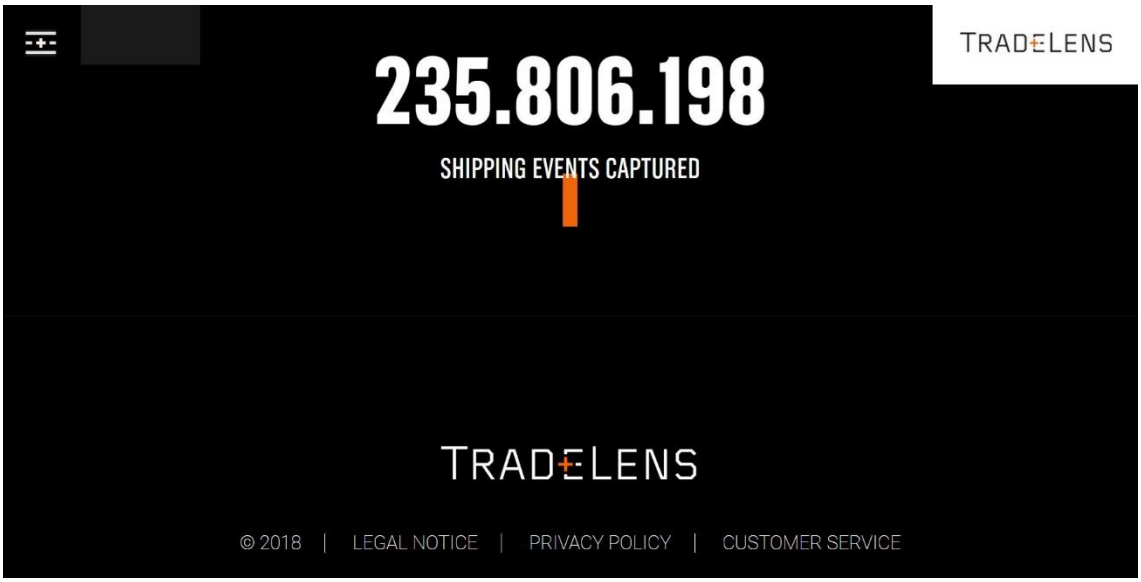
A világ 10 legnagyobb kikötőjéből 7 Kínában található és ezek éves forgalmából 40,2 millió TEU[3]-t Sanghaj tesz ki. Elképzelni is nehéz ezt a mennyiséget. Ekkora mennyiség megközelítőleg 92 milliárd kilónyi üres(!) konténert jelent. [18]

[3] Twenty-foot equivalent unit magyarul húsz láb – megközelítőleg 6 méter - hosszú konténert jelent.

„Az IBM kimutatása szerint egy konténernyi virág útnak indításához egy hónapnyi szervezés, harmincnál is több szervezet közös munkája és kétszáz különböző kapcsolatfelvétel kell. Ahhoz pedig, hogy a gyorsan romló szállítmány ne kerüljön hajóra, elég, ha egyetlen irat elkallódik vagy elkésik. És ez a piac 105 milliárd dollárt mozgat meg évente.”[4]

Látszik, hogy nemhogy a fogyasztónak, a részvevőknek is szinte lehetetlen átlátni az ellátási láncot. 2017 óta az IBM elkezdett együttműködni a világ legnagyobb konténerszállító cégével, a Maerskkel. Egy blokklánc alapú applikációt fejlesztenek, aminek a neve TradeLens, ezzel a céljuk az, hogy megszüntessék a papírt - mint tényezőt - a folyamatban, illetve, hogy követhetőbb legyen az ellátási lánc. [18]

2018. októberi adatok szerint 94 helyen alkalmazzák a TradeLens alkalmazást. 2018. november 20.-án megközelítőleg 236 millió eseményt rögzítettek a blokkláncon. [18]



8. ábra: TradeLens honlap [képernyőkép]. Letöltés dátuma: 2018.11.20. Hozzáférés (URL): https://www.tradelens.com/

A TradeLens az ellátási lánc minden résztvevőjénél minden felmerülő információt, változást dokumentál. [18]

[4] Szedlák Ádám: Az adat az új adat. In: Forbes 2018.10., p. 64.

„A blokklánc, ha eléggé leegyszerűsítve nézzük, nem különbözik jelentősen egy adatbázistól. Ez az adatbázis azoknak a leltárkönyveknek és főkönyveknek a digitális megjelenési formája, amelyeket a szállítmányozás a hajózás feltalálása óta használ. A különbséget az adja, hogy míg egy főkönyvbe az ír, akinek az a főkönyv a birtokában van, és nincs védve hamisítás ellen, addig a blokkláncon dolgozó gépek mindegyike, kriptográfiai módszerek használatával, közösen hitelesíti az összes felvitt tranzakciót.

Azt az adatot, amit a rendszer egyszer hitelesnek fogadott el, később nem lehet megváltoztatni. A TradeLenshez hasonló privát blokkláncoknál meg lehet határozni, hogy milyen szereplők milyen adatokat vihetnek fel, még azt is, hogy melyik szereplő milyen adatot láthat. A felépítésnek köszönhetően nem egy nagy, közös, üzleti titkokkal teli adatbázison dolgoznak a résztvevők."[5]

- Előrejelzési piacok

Nagy valószínűséggel egy esemény kimenetelének a valószínűségét úgy a legkönnyebb megállapítani, hogy megfigyeljük, hogy az emberek többsége mit gondol róla. Nagy mennyiségű minta figyelembevételével kiküszöbölhetünk különböző elfogultsági, döntés befolyásoló tényezőket.

Ha mindehhez hozzátesszük még azt, hogy azok a személyek, akik egy eseménynek eltalálják a kimenetelét, jutalomban részesülnek, még egy fokkal biztosabbak lehetünk az esemény kimenetelében. Az ilyen applikációkat nevezzük előrejelzési piacoknak, vagy ahogy a szaknyelv említi, prediction markets. [16]

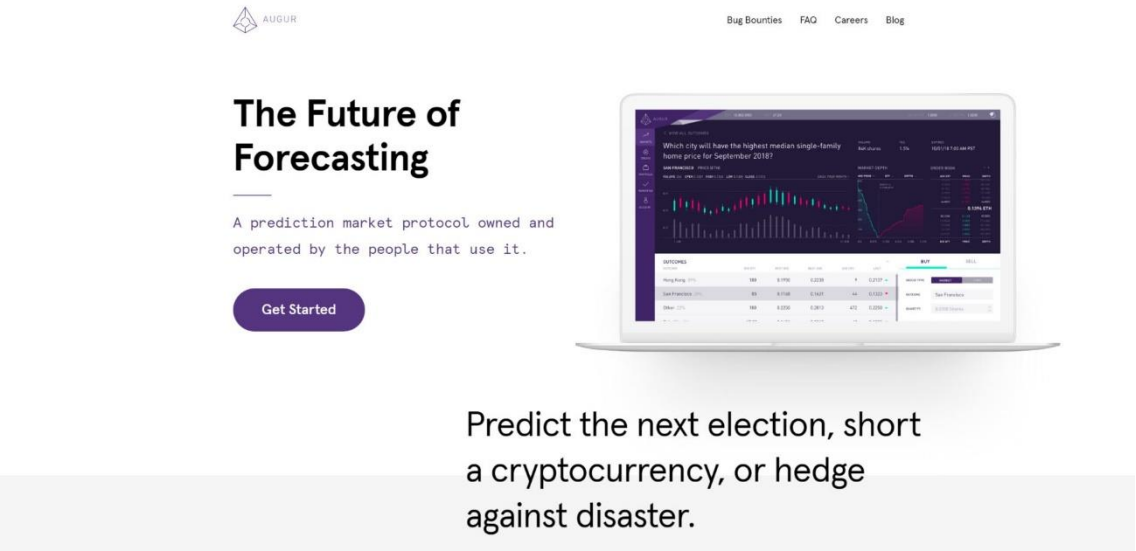
Bár egy ilyen alkalmazásnak nem feltétele, hogy jutalomban részesítse a felhasználókat, de az Augur[6] megvalósításánál ez is egy szempont volt. Az Augur egy decentralizált, az Ethereum hálózatán indított ICO. [16]

[5] Szedlák Ádám: Az adat az új adat. In: Forbes 2018.10., p. 66.
[6] Az ókori rómában az augur azt jelentette, hogy madárjós. Feladatuk az volt, hogy a madarakon figyeltek meg különféle jeleket.

„Az ICO az Initial Coin Offering vagy Initial Public Coin Offering angol kifejezés rövidítése. Legegyszerűbben úgy magyarázhatnánk, a crowdfunding és a nyilvános tőzsdei kibocsátás (röviden: IPO) különleges ötvözete. A célja, hogy a kibocsátó a kriptovaluta kibocsátásával szerezzen tőkét projektjének, cégépítésének finanszírozásához."[7]

Az alkalmazásban bárki hozhat létre eseményt, amire ezután bárki fogadhat. Lehetőség van például létrehozni egy eseményt, hogy holnap sütni fog-e a nap. Az emberek megteszik a tétjeiket, majd egy okos szerződés (amibe belefoglalták a kimeneteleket) szétosztja a nyereményeket azok között, akik eltalálták a kimenetelt. A nyeremény értelemszerűen az emberek által felrakott tét összege.

Az Auguron csak akkor tudunk létrehozni eseményt illetve fogadni rá, amennyiben rendelkezünk Ethereum wallettal. Ebből kifolyólag, csak kriptovalutával tudunk fizetni a fogadásokért. A kriptovalutákhoz kapcsolódó walletokról (pénztárcákról) a későbbiek során részletesebben írok. [19]



9. ábra: Augur honlap kezdőképernyő [képernyőkép]. Letöltés időpontja: 2018.11.22. Hozzáférés (URL): https://www.augur.net/

[7] Németh Mónika: A bitcoin után itt az adrenalin-függők új játéka: ICO [online]. Letöltés időpontja: 2018.11.22. Hozzáférés (URL): https://fintechzone.hu/mi-az-ico-bitcoin-utani-kripto-vilag/

Az előrejelzési piacokkal kapcsolatban - beleértve az Augurt - felmerülnek erkölcsi kérdések is. Mivel bárki szabadon létrehozhat eseményeket, illetve annak a kimeneteleit, így létrehozhatnak az emberek olyan fogadásokat, amiket képesek lehetnek befolyásolni. Amennyiben komoly függőség alakul ki a „játék" iránt, az emberek nem csak erkölcsi normákat, de törvényeket is megszeghetnek adott esetben.

Az egyik legjobb példa erre az, hogy az alkalmazás még csak 2018 augusztusában indult, de már többen is adtak le rajta olyan fogadásokat, amik a jelenlegi amerikai elnök Donald Trump meggyilkolására irányulnak. Mondani sem kell, hogy milyen veszélyekkel járhatnak az ilyen fogadások. [19,21]

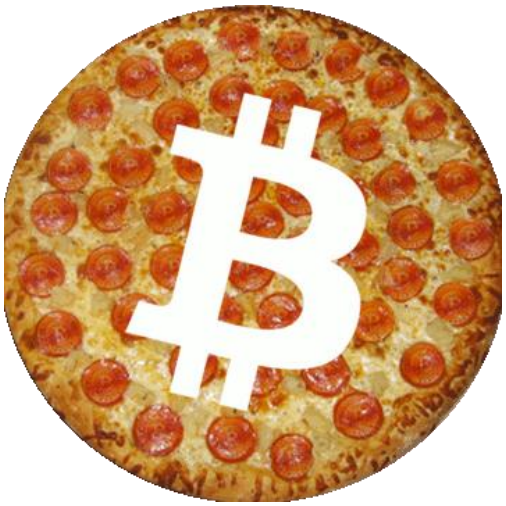
Azt, hogy mennyire kiforrott dAppról van szó, igazolja az is, hogy közel három éven keresztül fejlesztették az programot. Amikor elkezdték a munkálatokat az ether értéke még az 1 dollárt sem érte el, ez a mai napon (2018.11.22.) az elmúlt hetek nagy árfolyamesései után is nagyjából 132 dollár környékén mozog. [21]

4. Kriptovaluták

4.1. Általánosan

Napjaink legismertebb és legelterjedtebb kriptovalutája egyértelműen a bitcoin. A Satoshi Nakamoto által kitalál majd megvalósított kriptovaluta azóta hatalmas sikereket illetve kudarcokat is megélt. A média által köztudottá vált, hogy az első kriptovalutás fizetést Jacksonville-ban hajtották végre, amikor is egy feltehetőleg magyar származással rendelkező lakos, Laszlo Hanyecz 10 000 bitcoint adott kettő pizzáért.

Ez a vásárlás 2010-ben történt, az akkori árfolyamon ez az összeg 25 dollárnak felelt meg, magyar forintban ez nagyjából 5400 forintot jelentett akkoriban. 2017. december 17.-én éjfélkor egy darab bitcoin értékét a tőzsdék nagyságrendileg 19 357 dollárra becsülték (ez az eddigi legmagasabb érték). Ez tehát azt jelenti, hogy az a bizonyos kettő Jacksonville-i pizza 7 és fél évvel később 193 570 000 dollárt, 51 102 480 000 forintot ért. Valószínűleg maga Satoshi sem gondolta, hogy a kriptovalutáját valaha is ekkora értékűre becsülik.



10. ábra: Bitcoin pizza.
Letöltés időpontja: 2018.11.23.
Hozzáférés (URL):
https://twitter.com/bitcoin_pizza

Egy biztos, nagyon sok embert foglalkoztat a téma gazdasági és politikai körökből is. Ezeket az embereket két részre csoportosíthatjuk: akik elutasítóak illetve akik hisznek a technológia fejlődésében és a mindennapokba való bekerülésében.

Akik a 2010-es évek elején bitcoinba vagy szinte bármilyen más kriptovalutába fektettek és türelemmel vártak, akkor az évek során pár ezer forintnak megfelelő összegből válhattak milliomossá, milliárdossá. Bár a szakdolgozatom írásának jelenlegi időintervallumában (2018 novemberének vége) hatalmas csökkenésnek indultak a kriptovaluták - köztük található olyan, ami közel 250%-ot veszített az értékéből pár nap alatt - nem mondható biztosra, hogy a 2017-es év végi állapot volt a csúcsa a kriptovalutáknak.

Miután Satoshi elindította a Bitcoint, sorra jelentek meg a különféle kriptovaluták, vagy a különféle alkalmazások, megvalósítások, amik saját kriptovalutát foglaltak magukba.

Ennek az alapvető koncepciója, a miértje az volt, hogy szerették volna kiütni a harmadik köztes szereplőt, a kriptovaluták esetében a bankokat. A legnagyobb előnye ezeknek a kriptovalutáknak pont az előbb említett tény, hogy nem kell különféle pénzintézeteken keresztül mennie a valutánknak ahhoz, hogy célba érjen. A blokklánc technológiát használva megszűnnek a bizalmi kérdések a bankok és a köztes szervezetek felé, és a pénzünk közvetlenül a fogadó félhez kerül.

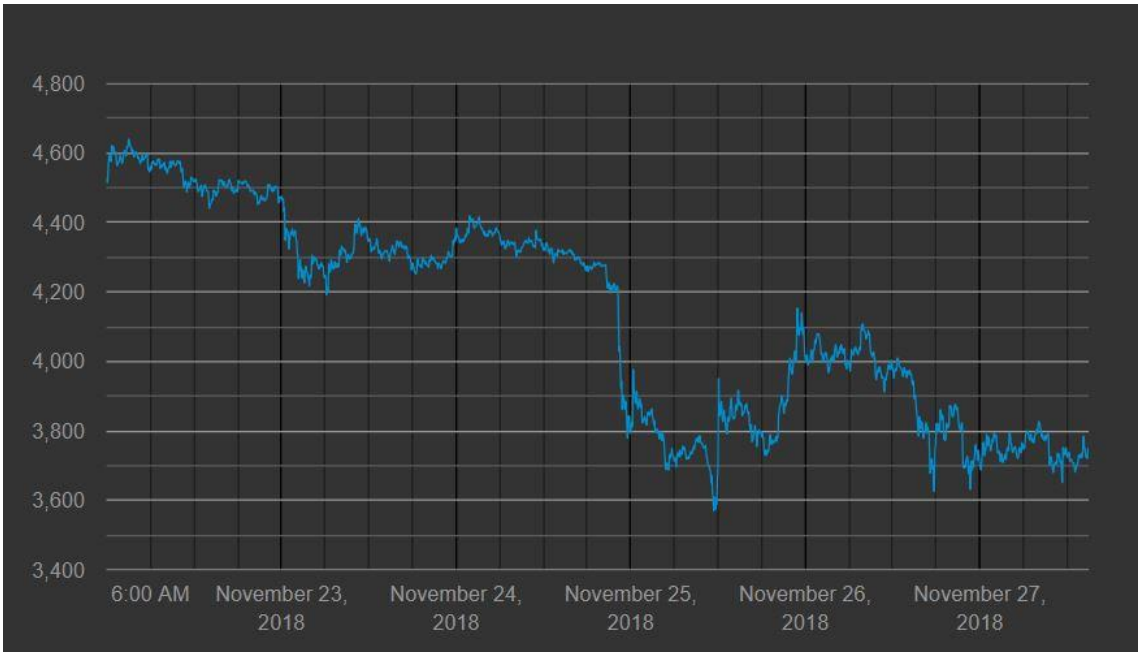
A kriptovaluták legnagyobb előnye az, ahogy a nevéből is ered, kriptográfiai, titkosítási módszerekkel van megoldva az, hogy nem lehet meghamisítani, illetve nem lehet kétszer elkölteni.

2018.11.27.-én a https://coinmarketcap.com/ oldal 2071 a bitcointól különböző kriptovalutát jegyzett. Ezeket a kriptovalutákat a szaknyelv altcoinnak nevezi. Minden a bitcointól különböző kriptovalutát altcoinnak nevezünk.

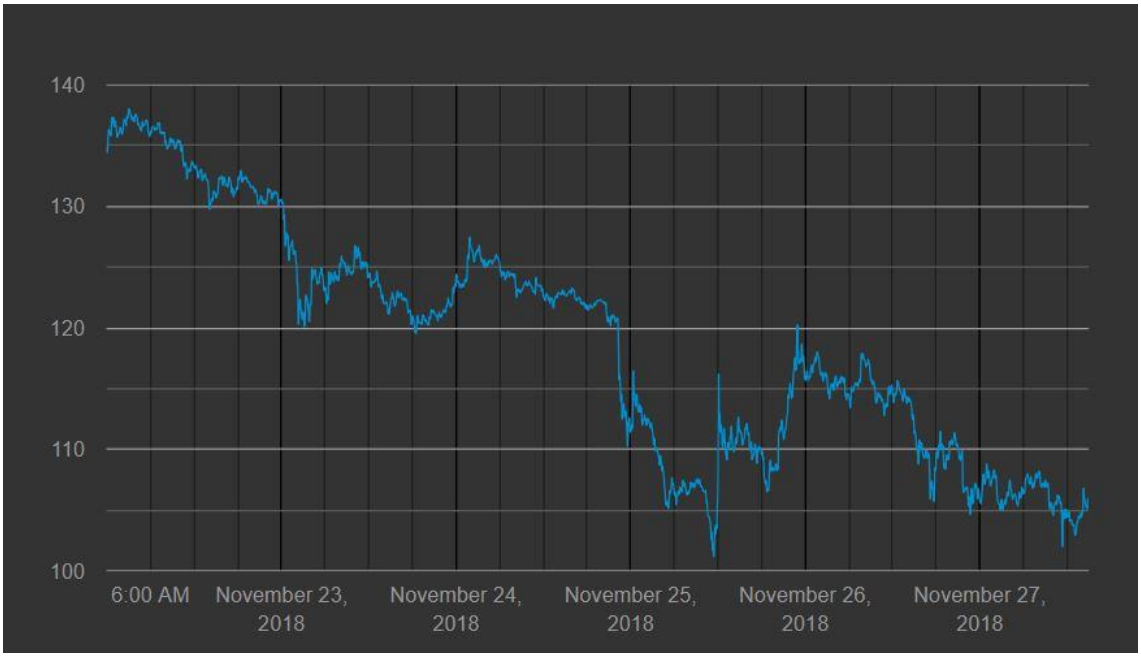
#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$65 232 611 533	$3 749,80	$6 570 705 510	17 396 275 BTC	-3,76%	
2	XRP	$14 092 047 963	$0,349442	$786 675 945	40 327 341 704 XRP *	-4,03%	
3	Ethereum	$10 964 603 253	$105,98	$2 268 708 847	103 456 959 ETH	-5,26%	
4	Bitcoin Cash	$3 086 903 898	$176,60	$192 808 483	17 479 988 BCH	-8,39%	
5	Stellar	$2 692 904 694	$0,140612	$90 366 006	19 151 289 939 XLM *	-5,49%	
6	EOS	$2 692 530 915	$2,97	$1 013 023 490	906 245 118 EOS *	-8,76%	
7	Tether	$1 822 389 303	$0,981668	$4 722 311 755	1 856 421 736 USDT *	-0,16%	
8	Litecoin	$1 766 686 812	$29,78	$534 842 602	59 328 663 LTC	-1,42%	
9	Bitcoin SV	$1 742 419 235	$99,69	$431 423 308	17 477 861 BSV *	-9,23%	
10	Cardano	$909 535 815	$0,035081	$23 870 529	25 927 070 538 ADA *	-4,25%	
11	Monero	$888 625 643	$53,53	$19 878 250	16 602 030 XMR	-3,41%	

11. ábra: A 10 legnagyobb altcoin a piaci kapitalizációjuk szerint [képernyőkép]. Letöltés időpontja: 2018.11.27. Hozzáférés (URL): https://coinmarketcap.com/

A legtöbb altcoin árfolyama nem független a bitcointól. Ez azt jelenti, hogy amennyiben a bitcoin árfolyama emelkedik vagy csökken, ezek a kriptovaluták is ugyanúgy hasonló arányban változnak. A következő ábrákon az elmúlt napokból az Ethereum illetve a Bitcoin kriptovalutájának a mozgását szemléltetem, a tőzsdén bejegyzett rövidítéseket használva mely szerint a bitcoin BTC, az ether pedig ETH.



12. ábra: BTC árfolyam [képernyőkép]. Letöltés időpontja: 2018.11.27. Hozzáférés (URL): http://napiarfolyam.hu/%C3%A1rfolyam/Bitcoin/coin/



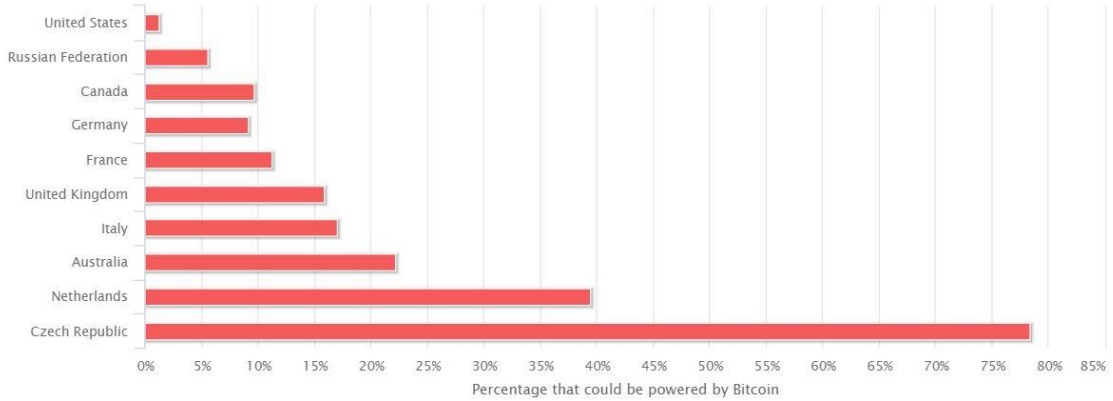
13. ábra: ETH árfolyam [képernyőkép]. Letöltés időpontja: 2018.11.27. Hozzáférés (URL): http://napiarfolyam.hu/%C3%A1rfolyam/Ethereum/coin/

Jól látható az ábrákon, hogy a két árfolyam a mozgása arányaiban megegyezik. Persze ez alól mindig vannak kivételek. Történnek olyan esetek, amik néhány olyan altcoinra nem hatnak, vagy épp ellenkezőleg hatnak. Ilyen lehet például egy fork (a későbbiek során részletesebben foglalkozom ezzel a fogalommal), vagy olyan események, amelyek azért hatnak másként bizonyos altcoinokra mert más technológiai megvalósításokat alkalmaznak, mint a Bitcoin.

4.2. Bányászat

A bányászat vagy, ahogy a szaknyelvben szerepel a mining lényege, hogy a blokkláncban résztvevő csomópontok matematikai feladványokat oldjanak meg a blokklánchoz csatlakozott eszközükkel. A legtöbb kriptovaluta a már korábban általam említett Proof of Work mechanizmust használja a bányászáshoz. Ez a mechanizmus jelenti a bányászást, azt hogy valamekkora energia felhasználásra van szükség ahhoz, hogy előállításra kerüljenek a kriptovaluták. Azt, hogy mekkora energia felhasználása szükséges ehhez a mechanizmushoz, kettő diagrammal szemléltetem az alábbiakban:

14. ábra: A Bitcoin 1 évre jutó energia felhasználása [képernyőkép]. Letöltés időpontja: 2018.11.30. Hozzáférés (URL): https://digiconomist.net/bitcoin-energy-consumption



15. ábra: Egyes országokhoz viszonyítva a Bitcoin éves energia felhasználása [képernyőkép]. Letöltés időpontja: 2018.11.30. Hozzáférés (URL): https://digiconomist.net/bitcoin-energy-consumption

A 14. ábra azt szemlélteti, hogy a legismertebb kriptovaluta éves energia felhasználása az adott napi forgalom alapján mekkora. 2018. november végén ez nagyjából 50 terawattórát jelent. A terawattóra mértékegység értelmezése nem lényeges a diagramok elemzése és megértése végett. Amennyiben a következő diagramra tekintünk, láthatjuk, hogy a Bitcoin éves energia felhasználása közel 80%-át teszi ki Csehország éves energiafelhasználásának és több mint 15%-át az Egyesült Királyságának.

Ezek a számok azért tudnak ilyen hihetetlenül magasak lenni, mivel a Proof of Work mechanizmussal a kriptovaluták bányászása a növekvő felhasználók és az egyre több kibányászott kriptovalutával arányosan nehezedik, ezzel együtt nő az energiafelhasználás is.

Visszatérve a matematikai problémának a kiszámítására, erre ad megoldást a hash függvény. A hash függvényt a blokklánccal kapcsolatban részletesen kifejtettem, lényege a „helyes" szám megtalálása. Ezekre a matematikai műveletekre a Bitcoin esetében körülbelül 10 percenként adnak választ a bányászok. Ez azt jelenti, hogy 10 percenként készül egy új blokk és kapcsolódik hozzá az előzőhöz.

Ezek a számítások alapvetően lassítják a rendszer működését, mivel mi hiába hajtunk végre egy tranzakciót, az először bekerül egy blokkba, majd meg kell várnunk, amíg valaki hitelesíti azt. Miután megtörtént a hitelesítése egy blokknak, a többi résztvevő már pillanatok alatt tudja azonosítani az eredményt, és ellenőrzik, hogy helyes-e a megoldás.

Nem hivatalos adatok alapján bloggerek, weblapszerkesztők nagyjából 3000-3500 dollárra becsülik egyetlen bitcoin előállítását manapság. Jelenleg (2018.11.30.) egy bitcoin értéke körülbelül 4200 dollár. Ha az eszköz vásárlását, tárolását és az egyéb dolgokat nem vesszük számításba, csak az üzemeltetését, akkor ez 700 dolláros profitot jelenthet minden egyes bitcoin után.

Ez természetesen országonként eltérő, és manapság már nem jellemző, hogy egyéni felhasználók kriptovalutát bányásszanak, főleg a nagyobb kriptovalutáknál. Felhasználói csoportokat hoznak létre, „egyesítik" az erőforrásaikat és úgynevezett bányász-farmokat hoznak létre.

Ami a hardveres oldalát illeti a bányászatnak eleinte az emberek a saját számítógépjük processzorát használták a kriptovaluták előállítására. Egy idő után rájöttek, hogy a számítógép videókártyájával sokkal gyorsabban és hatékonyabbak megoldhatók ezek a műveletek. Azonban ezzel egyidejűleg, illetve a kriptovaluták elterjedésével és fejlődésével a videó kártyák egyre drágábbak lettek.

Így történhettek meg olyan esetek (természetesen csak nagyobb teljesítményű, több százezer forintos kártyáknál), hogy ha az ember vásárolt egy videó kártyát x forintért, pár hónappal később használtan ugyanazt a videó kártyát jóval drágábban tudta eladni, mint amennyiért korábban vásárolta.

Később aztán elkezdődött a konkrétan a bányászatra alkalmas eszközök gyártása. Ezeknek az eszközöknek a fejlesztésénél kettő célja van a gyártóknak, az egyik, hogy a lehető legalacsonyabb energia felhasználással működjenek, illetve a lehető leggyorsabban tudják végezni a számításokat.

16. ábra: Bitcoin bánya. Letöltés dátuma: 2018.11.30.
Hozzáférés (URL): https://www.bitcoinbazis.hu/bitcoin-banyasz-tarsasagok/

A legtöbb bányászfarm, a legnagyobb bányászattal foglalkozó egyesületek székhelye Kínában található. Kínán belül is a hegyvidéki tájakon, ahol a levegő viszonylag hűvösebb a mélyebben található területeknél. Ennek az az előnye, hogy kevesebb energiát kell fordítani az eszközök hűtésére.

Ahhoz, hogy akár a kibányászott, akár a vásárolt kriptovalutáinkat biztonságosan tárolni tudjuk, szükségünk van egy wallet-ra. A wallet egy digitális pénztárca, amely lehet offline vagy online. Utóbbi esetben webes felületről, mobilos alkalmazásról beszélünk. Előbbi esetben egy hardveres pénztárcáról beszélünk.

A pénztárca lényegében csak a privát kulcsunkat, kulcsainkat tárolja az adott kriptovaluta címünkhöz kapcsolódóan. Ezek a technológiák folyamatosan frissülnek és fejlődnek a biztonság érdekében. Többször lehetett olyan esetet hallani, hogy online tárcákból eltűntek a kriptovaluták, ezért is sokkal biztonságosabb egy offline eszköz vásárlása, ugyanakkor ez egy drágább megoldás is, hiszen meg kell vásárolnunk az eszközt.

Van egy harmadik lehetőség is, amikor egyszerűen kinyomtatjuk a privát kulcsunkat és megőrizzük egy biztonságos helyen. Ennek is van veszélye, hogyha elveszítjük a papírt, akkor, akinek a birtokába jut, szabadon hozzáférhet a kriptovalutáinkhoz amennyiben tudja, milyen címhez tartozik.

Lehetőségünk van ugyanakkor ezt a kódot kinyomtatni például QR kód formájában, így megkönnyítve a hozzáférést coinjainkhoz. Ez a megoldás sokall időigényesebb, mint más offline vagy online megoldások, viszont ha hosszú távú befektetést szeretnénk csinálni, és nem használni a valutáinkat, akkor valószínűleg jelenleg ez a legbiztonságosabb megoldás.

4.3. Bitcoin

Fontos tisztázni az elején, hogy a Bitcoin nagybetűvel magára a technológiára utal, az egész rendszerre, ami a kriptovaluta mögött áll. Amennyiben kisbetűvel találkozunk vele, akkor pedig magáról a kriptovalutáról van szó.

Ahogy már a korábbiakban említettem, a Bitcoint a 2008-as gazdasági világválság idején egy Satoshi Nakamoto nevű személy vagy csoport találta ki. Satoshi legnagyobb feladata az volt a rendszerben, hogy valamilyen módon megoldja a kétszer-költés problémáját. A korábbiakban ez egy gyakori probléma volt a különböző digitális pénzeknél. A fiat pénzeknél ez a probléma nem léphet fel, hiszen egy kézzel fogható érmét vagy papírpénzt nem tudunk kétszer elkölteni.

Viszont, amennyiben valamilyen hiba csúszott a digitális pénzeknél a rendszerbe, könnyen fellépett a kétszer-költés problémája. A későbbiek során egy hasonló problémát szemléltetek az okos szerződésekkel kapcsolatban. A kétszer-költés problémájára javasolta Satoshi a peer-to-peer hálózatot, amiben a hashelés folyamatával a proof of work metódust használva hitelesítésre kerülnek a blokkok. Ahogy a korábbiakban írtam ez egészen addig megváltoztathatatlan és biztonságos, amíg a nodeok többsége nem áll össze, hogy befolyásolják a rendszert. Ez pedig a blokklánc és a nodeok növekedésével egyre inkább lehetetlen feladatnak tűnik.

A bitcoin árfolyamát szinte lehetetlen megjósolni, sokszor olyan dolgok, amikről azt gondolná az ember, hogy csökkenteni fogják az árfolyamát éppen a másik irányba mozgatják el. Nehéz megmondani, hogy valaha a bitcoin vagy valamely másik kriptovaluta (esetleg több) le fogja-e váltani teljes mértékben a jelenlegi fiat pénzeket. Az biztos, hogy jelenleg úgy tűnik, hogy ha valakinek vagy valamelyik kriptovalutának lehetősége lesz erre, az a bitcoin lesz. Egyre több helyen van lehetőség a világban arra, hogy bitcoinnal fizessük adott szolgáltatásért vagy termékért.

Több repülőtársaság illetve egyes országokban például már dohányboltokban is elfogadják a bitcoint mint hivatalos fizetőeszközt. Egyre több és több helyen, többek között már Budapesten is található Bitcoin automata. Ezt úgy kell elképzelni, mint egy hagyományos ATM-et, csak itt bitcoin eladására, vagy vásárlására van lehetőségünk. Mivel a Bitcoin hitelesítési rendszere korlátozva van, tehát 10 percenként jöhet létre egy új blokk, ezáltal a bitcoinok forgalomba helyezése is szabályozva van. A bitcoin indulásakor az első 4 évben az első 210 000 blokk kibányászásáért blokkonként 50 BTC-t kaptak a bányászok. A következő 4 évben már csak 25 BTC-t és az idő előrehaladtával ugyanígy folytatódik a számsor.

Satoshi és a fejlesztőcsapat úgy tervezték meg a rendszert, hogy véges számú bitcoin legyen forgalomban ezért 2140-ben (ha addig működik a rendszer) fogják az utolsó olyan blokkot hitelesíteni, amiből BTC származik jutalmul. Innentől kezdve a forgalomban lévő bitcoinok száma nem fog változni. Egy viszonylag egyszerű matematikai számítással (mértani sor összege) megkaphatjuk, hogy ez az összeg valamivel több, mint 21 000 000 BTC. Hivatalosan ez az összeg 2140-ben viszont kicsit kevesebb, mint 21 000 000 BTC lesz.

Az eltérést ebben az esetben az jelenti, hogy 2009-ben az induláskor még nem volt szabályozva 10 percenként a blokklétrehozás, így megtörténhetett az is hogy a két blokk között eltelt idő 1-2 perc volt, illetve az is, hogy ez az idő egy fél nap volt. Jelenleg (2018.12.03.) a forgalomban lévő bitcoinok száma a https://www.blockchain.com adatai alapján 17 405 450 BTC. Ezzel a megoldással Satoshi az inflációt szerette volna kikerülni. Ennek a miértjét egyszerű megérteni, hiszen ha idővel csak a bitcoin lesz, mint fizető eszköz, akkor nem igazán tudna romlani az értéke, hiszen nem lehet belőle többet előállítani, mint az egyes ma forgalomban lévő fiat pénzekből. Satoshi gondolkodása ezen a téren is hihetetlenül előrehaladottnak látszik.

5. Okos szerződések

5.1. Technológiája

Az okos szerződés, vagy, ahogy a szaknyelv nevezi smart contract célja, hogy egy blokkláncba írt/programozott szerződés teljesítését ellenőrizze vagy hajtsa végre. Az okos szerződések legnagyobb előnye, hogy nem szükséges köztes, harmadik fél ahhoz, hogy megkössünk egy szerződést. Nincsen szükség ügyvédekre, sem a szerződés megkötésekor, sem az utólagos bírálatokkor.

17. ábra: Okos szerződés. Letöltés időpontja: 2018.12.13.
Hozzáférés (URL): http://bertazsolt.com/mi-az-az-okos-szerzodes-smart-contract/

Egy okos szerződésnél minden tranzakció, minden művelet nyomon követhető, utólag megtekinthető. Amennyiben egy ilyen szerződésnél teljesülnek az előre leírt feltételek, a szerződés azonnal, önállóan teljesíti a következményeket. Az okos szerződésekről, mint ahogy a bevezetőben is írtam Nick Szabo írt először a ’90-es évek végén. Ugyanakkor ebben az időben, még nem volt meg a megfelelő technológia a megvalósításához.

Aztán 2008-ban jött Satoshi és megteremtette a lehetőségét annak, hogy a későbbiek során létrehozzanak egy olyan blokkláncot, ami okos szerződések megkötésére alkalmas. Így jött létre az Ethereum.

Az okos szerződések alapvető működési funkciója olyan, mint egy csokoládé automatáé. Csak azokat az utasításokat hajtja végre, amiket beleprogramoztunk. Hogy a példánál maradjanak a csokoládé kiválasztása, illetve a pénz bedobása, majd a gomb megnyomása lesznek a feltételek a szerződés teljesüléséhez. Ezeket a feltételeket a szaknyelv triggernek hívja. Miután ezek a triggerek bekövetkeztek, a szerződés végrehajtja a következményeket. Ebben a példában ez lesz az, amikor az automata kiadja a csokoládé és adott esetben a visszajárót.

Egy okos szerződés létrehozásához négy dologra van szükség. Először is, mint minden hagyományos szerződésnek, ennek is kell, hogy legyen egy tárgya, amiről a szerződés szól. Továbbá tartalmaznia kell a feltételeket, ez szintén hasonlóság a hagyományos szerződésekkel. Ezeket a feltételeket és a szerződés tárgyát minden a szerződésben résztvevő félnek hitelesítenie kell. Ez a valóságban egy aláírással történik. Az okos szerződések esetén digitális aláírásról beszélünk. A digitális aláírással a következő pontban részletesebben foglalkozom. Ezeken felül pedig szükség van még egy decentralizált környezetre, egy blokkláncra ahol a szerződés létrejön.

Az okos szerződések előnyei:

- Garantálják a biztonságot a szerződések digitális aláírásával. Később nem tudják módosítani a szerződést a másik fél beleegyezése nélkül.
- Biztosítja, hogy a lehető leggyorsabban teljesítődjenek a szerződések, hiszen nem kell köztes fél ahhoz, hogy megállapítsák kérdéses helyzetekben a szerződés hatályát.
- Manapság egyre több és több ilyen szerződés születik, ezért vannak már forgalomban sablonok, amiket szinte bárki könnyen alkalmazhat egy kis változtatással is.

Az okos szerződések hátrányai:

- Az emberi tényezőt nem tudjuk elkerülni ezzel a folyamattal sem. Hiszen a programot emberek írják, amik alapján működni fognak ezek a szerződések. Erre fogok egy példát mutatni a későbbiek során az Ethereummal kapcsolatosan.
- Egyelőre egyetlen kormány sem szabályozza ezeket a szerződéseket, és nem tudni mi fog történni akkor, ha elkezdenek ezzel a kérdéssel foglalkozni.

- Továbbá ott vannak még a szerződések költségei. Amennyiben teljesen új szerződéseket szeretnénk létrehozni és nem vagyunk profi fejlesztők, akkor alkalmaznunk kell valakit, aki megírja számunkra a szerződéseket.

5.2. Digitális aláírás

A digitális aláírás lényegében egy hitelesítés az adott dokumentum hamisítatlanságáról, másolhatatlanságáról. 2016. július 1.-jétől Magyarországon is törvényileg engedélyezett, a használata a hagyományos aláírás helyett. Sok helyen olvashatunk róla úgy, mint elektronikus aláírás. Több előnye is van a hagyományos aláírással szemben:

- A hagyományos aláírást, ha gyakorolja az ember, akkor könnyen lemásolható, így könnyen hitelesíthető egy dokumentum egy másik ember aláírásával. Mivel a digitális aláírás tartalmaz egy ellenőrző összeget, ezáltal biztosítva van az, hogy az aláírás nem vihető át egy másik dokumentumra. Ebből kifolyólag a digitális aláírások dokumentumonként eltérők.
- Egy hagyományos dokumentum az aláírás után is szerkeszthető. Nem szabályos ugyan, de megtehető és adott esetben nem szerez róla tudomást senki, hogy később módosították a dokumentumot. Mivel a digitális aláírás a dokumentum tartalmától is függ, így nagyon könnyen kiderül, hogy valaki módosította-e a dokumentumot az aláírás után vagy sem.
- Mivel a digitális aláírás nem hamisítható, így nem is lehet letagadni.

A digitális aláírás nagyjából úgy tevődik össze, hogy tartalmaz egy ellenőrző összeget. Ez az ellenőrző összeg általában a dokumentum tartalmából, az aláíró nevéből vagy azonosítójából, az aláírás időpontjából illetve az ellenőrző összeget előállító algoritmus nevéből tevődik össze. Az ellenőrző összeget a már korábban a blokkok hitelesítésnél említett hash-függvénnyel állítják elő.

5.3. Ethereum

Az Ethereumot hibásan gyakran egy lapon emlegetik a Bitcoinnal, mint a második legnagyobb kriptovaluta. Ha a mélyére nézünk a dolgoknak, akkor láthatjuk, hogy az Ethereum sokkal több, mint egy kriptovaluta, sokkal több lehetősége rejlik benne. Annyiban indokolt a két fogalom együttes használata, hogy mindkettő mögött ugyanaz a technológia működik, a blokklánc.

Az Ethereumról először Vitalik Buterin, programozó írt, majd három társával fejlesztette ki 2013 végén. Az Ethereum felhasználását két nagyobb részre tagolhatjuk. Az egyik a dAppok fejlesztése, a másik pedig cégek létrehozása a kibertérben. A dApp a decentralizált applikáció rövidítése, ami azt jelenti, hogy ezzel a technológiával megvalósíthatóak például szálláskiadó vagy szállítmányozási applikációk központi közvetítő szervezet nélkül, ezzel csökkentve a költségeket. [9,10]

A másik lehetőség a DAO-k (decentralized autonomous organization) létrehozása, amelyek teljesen önállóan működő szervezetek. Nincsenek vezetői egy ilyen cégnek, akik döntenének a fontos kérdésekben, kiválasztanák a legjobb projektet, ami megvalósításra kerüljön és a többi vezetői döntést. Egy ilyen cégnek a működéséért egy okos szerződés felel. Minden döntést, amit egy hagyományos cég esetében a vezetők, dolgozók hoznak meg az okos szerződés szerint meghatározott szavazással hoznak meg a tagok. [9,10]

The DAO

Az Ethereum fejlesztőcsapatából kiszálltak páran, olyan szándékkal, hogy létrehozzanak egy a fentiekben említett decentralizált céget. Nem túl kreatívan, de lényegre törően a neve The DAO lett. A cég érdekessége az, hogy az Ethereumban rejlő két ágat kettő az egyben módon próbálták megvalósítani, ugyanis a cég fő profilja a dAppok fejlesztése lett. Az elindításhoz szükséges tőkét közösségi finanszírozással igyekeztek összegyűjteni. [9,10]

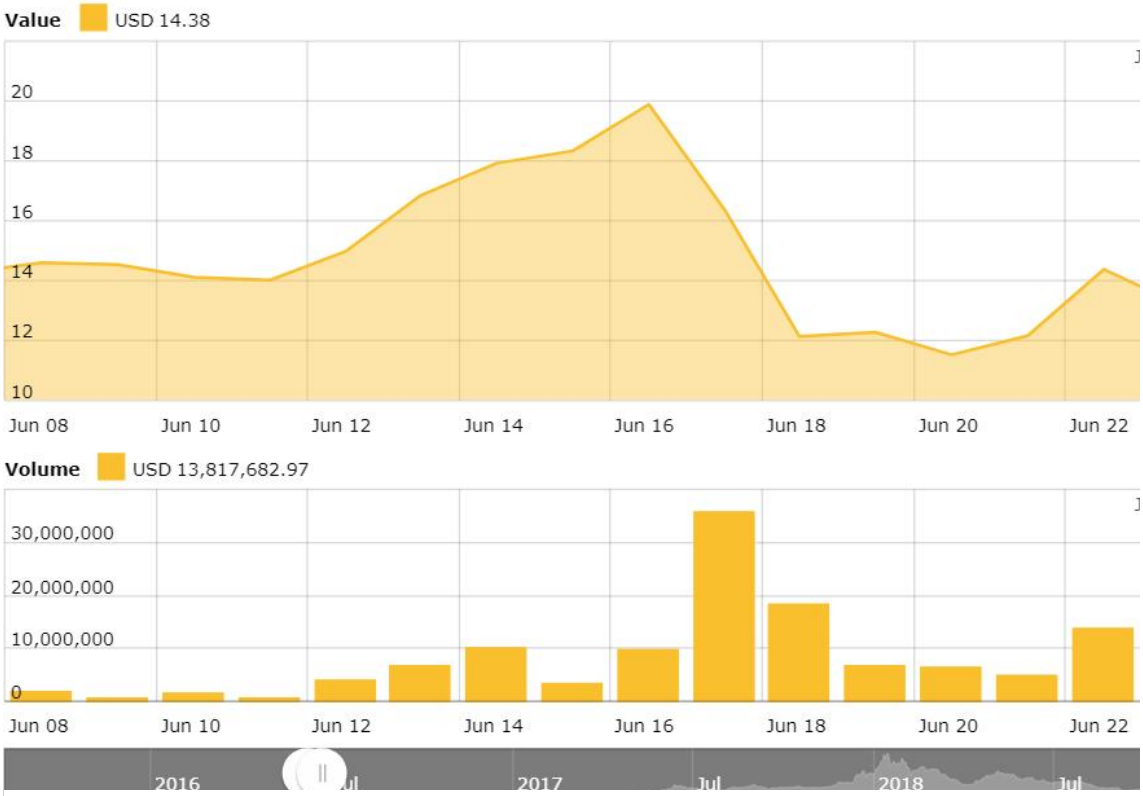
Ez le is zajlott 2013 májusában, ahol 12 millió ether-t (az Ethereum kriptovalutája) sikerült összegyűjteniük, ami az akkor forgalomban lévő ethereknek közel az ötöde volt. Az akkori árfolyamok szerint ez 150 millió amerikai dollárnak felelt meg illetve ez lett a legnagyobb összegű közösségi finanszírozású cég. 2018-ra mindössze a hetedik helyet foglalja el ugyanezen a listán. A tagoknak vagy nevezzük őket részvényeseknek a támogatásért cserébe tokeneket adtak, amik a cég részvényeinek feleltek meg. [9,10]

A cég okos szerződése magába foglalja azt, hogy bárki indítványozhatja, hogy milyen projektet valósítsanak meg, és ezután egy szavazással döntenek róla. Értelemszerűen többségi alapon dől el a szavazás. Amennyiben egy projektet megszavaznak, azok a tagok, akik nem szeretnék a projekt megvalósulását, lehetőségük van a kilépésre.

Ekkor ők egy másik cégbe kerülnek, ami ugyanazokon az elveken alapszik, mint az előző, és ide átkerül az ő ether vagyonuk is, amit még nem kötöttek le korábban projektekre. [9,10]

Amelyik projektekbe korábban beléptek, az onnan származó hasznuk ugyanúgy átkerül majd ebbe az új cégbe. A kiválásnak a menete, szigorúan le van írva a céget működtető okos szerződésben. Ez a folyamat több hetet is igénybe vehet, főleg az az időszak, amikor a kivált tagok az átemelt etherjeikhez hozzá tudnak nyúlni.

Az emberek elkezdtek bízni a cégben, és ezáltal az ether értéke is elindult felfelé ezekben a napokban, 2016 júniusában. Az addigi márciusi közel 15 dolláros tetőpont megdőlni látszott. [9,10]



18. ábra: ETH árfolyam és volumen [képernyőkép]. Letöltés időpontja: 2018.09.27. Hozzáférés (URL): https://cointelegraph.com/ethereum-price-index

Ahogy a diagramon is látszik, június 16.-ára közel 20 dollárra emelkedett az értéke az Ethereum kriptovalutájának. Ezután, eddig nem látott hatalmas csökkenésnek indult az ether. Ennek az oka pedig a cég okos szerződésében lévő hiba volt, amit egy hacker vagy hackercsoport észrevett és elkezdte kivenni a cégből az ethereket. Az emberek bizalma nem alaptalanul ingott meg az Ethereumban, hiszen az etherek nagy része, közel ötöde a cégben volt. [9,10]

Mivel egy nyilvános peer-to-peer alapú blokkláncról beszélünk, ezért minden tag, minden egyes résztvevő a blokkláncban élőben követhette, ahogy a hacker „kilopja” az ethereket a cégből. Erre úgy volt lehetősége, hogy a cégből való kiválás mellett döntött, ahogy korábban is írtam ezáltal átkerül egy új cégbe, ahova az összes addigi etherjét, ami nem volt lekötve, viszi magával. A hiba olyan mértékű volt, hogy mindenféle erőfeszítés nélkül végre tudta hajtani a lopást a hacker. [9,10]

Amikor kivált a cégből, egy olyan metódust hívott meg, ami kiemelte az ő vagyonának megfelelő ether mennyiséget és áthelyezte az új cégbe, viszont az onnan történő kiemelés, és az ott történő etherjeinek a törlése nem egy időben történt. Így a hackernek nem volt más feladata, minthogy abban a rövid időtartamban, amikor a pénze megtalálható mindkét cégben újra meghívja ezt a metódust. Ennek a részletnek az érdekessége az, hogy vajon hogy maradhatott benn az okos szerződésben egy ekkora hiba, annak ellenére, hogy mielőtt elindították a céget több szakértő is átnézte a szerződést. [11,12]

A hiba tehát nem az Ethereum működésében volt, az hibátlanul működött ugyanúgy tovább, hanem az okos szerződésben. A hacker tehát folyamatosan emelte ki az ethert a cégből, és ezt meg is tehette volna a cég egész vagyonával, ám saját akaratából megállt 3,6 millió ethernél. Valószínűleg ennek az oka az lehetett, hogy ha mindet kiemeli magának, akkor az embereknek még jobban lecsökken a bizalmuk az Ethereum iránt, és ezáltal az árfolyama is elindul a lejtőn megállíthatatlanul. Így tehát megelégedett ennyivel és várta a fejleményeket, ugyanúgy ahogy a többi tag, hiszen ahogy korábban is írtam, ez a folyamat több hétig is eltarthat, így nem tudta rögtön értékesíteni az általa kilopott ethert. [11]

A fejlesztőcsapatnak sürgősen ki kellett találnia valamit, hiszen ha egy ember észrevette a hibát, valószínűleg más is észre fogja. Így tehát megalapították a fejlesztőkből álló Robin Hood Group-ot és kilopták a saját cégükből a bennmaradt összeget és biztonságba helyeztek. [11]

Úgy tervezték, hogy majd később visszajuttatják ezeket az ethereket a jogos tulajdonosaikhoz. Ekkor ott volt az egész cég teljesen üresen, egy teljesen összezavarodott és felháborodott közösséggel karöltve. [11]

Adott volt a kérdés, hogy most merre tovább, mi lesz ezután, hogyan oldják meg ezt a problémát a fejlesztők, illetve, hogy kell-e egyáltalán tenniük bármit is? A közösség nagyjából két részre szakadt. A tömeg egyik része a hard forkot javasolta megoldásként.

Ez azt jelentette volna, hogy átírják a szabályrendszerét a blokkláncnak. Szembe ment volna a blokklánc alapelveivel, olyan esemény lett volna ez, ami azelőtt sosem történt meg. [11]

Gyakorlatilag, ha valakinek van a tulajdonában egy blokklánc alapú kriptovaluta, az csak azért van így, mert a bányászok többsége ezt elfogadta, hitelesítette. De amennyiben a többség úgy dönt, hogy ezt átírja, egy másik számlára akkor a birtokosa nem tehet az ellen semmit, hogy ez megtörténjen. Azonban a közösség másik fele, ellenezte ezt a döntést, azzal indokolva, hogy ezzel átírnák a szabályokat, ami sértené az alapelveket, egy szóval csalás lenne. [11]

Továbbá az érveik között szerepelt, hogy a múltban is történtek hasonló lopások és a jövőben is fognak, és ha minden egyes alkalommal így reagálnak, az emberek bizalma teljesen elszáll az Ethereum iránt, hiszen hogyha egyszer átírják a szabályrendszert, miért is ne írhatnák át bármikor máskor? [11]

A fejlesztőcsapatnak viszont muszáj volt valamit lépni, úgy nézett ki, hogy három lehetséges megoldás van a folytatásra:

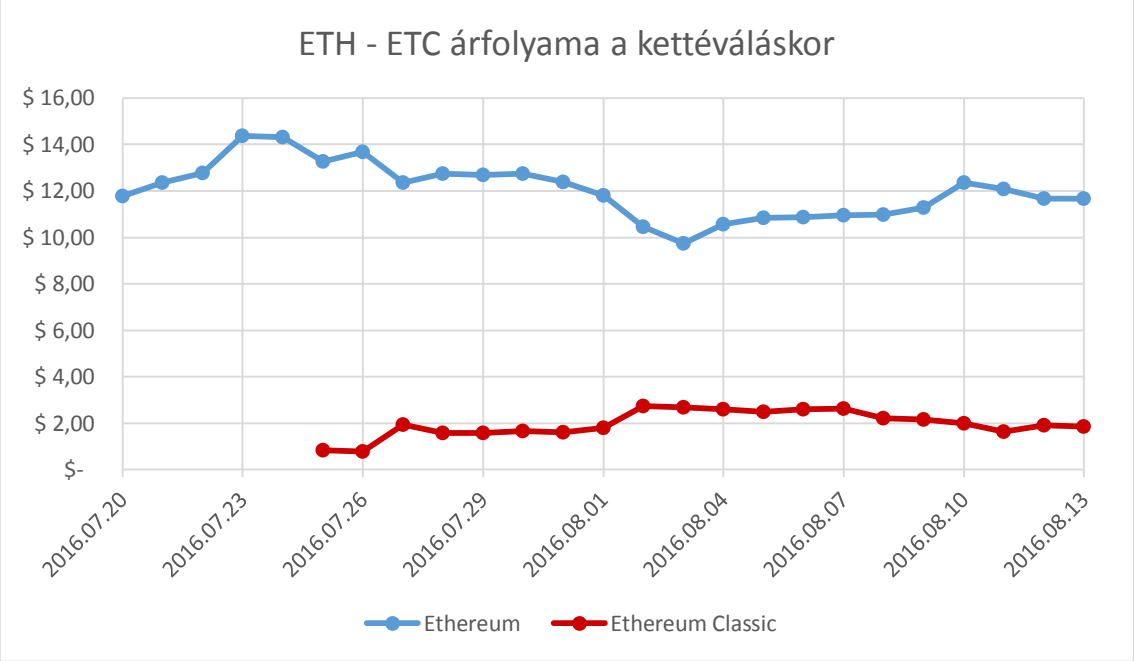
- Az első, hogy nem tesznek semmit, mivel az Ethereum jól működik, nem volt benne hiba, ezért nincs teendő.
- A második a soft fork, ez azt jelentené, hogy valamilyen szinten átírnák ugyan a szabályrendszert, de csak azt jelentené, hogy a hacker által ellopott ethereket lezárolnák, és nem lehetne velük kereskedni a továbbiak során. Ezzel a megoldással nem kapnák vissza azt a pénzt az emberek, viszont nem használhatná a hacker sem.
- A harmadik lehetőség, amit a tömeg egy része korábban is említett, ez pedig a hard fork. [11]

A soft fork lehetőségét a fejlesztők meg nem határozott okok miatt kizárták. Ezáltal maradt két lehetőség. Az hogy melyik mellett döntenek, teljesen mindegy volt a The DAO szempontjából, ugyanis a cég mindkét esetben halálra volt ítélve. Ha az első opciót választják, vagyis nem tesznek semmi, akkor a cég teljesen üresen marad. Amennyiben a másik lehetőséget részesítik előnyben, akkor sem a cégbe töltötték volna vissza a kilopott pénzt, hanem közvetlenül a részvényeseknek. [11]

Úgy gondolták, hogy döntse el a többség egy valós szavazással. Az 1 920 000. blokk lesz a döntő az ügyben, ugyanis a következő verzióba a fejlesztők beleírták mindkét lehetőséget. Azt várták ettől a fejlesztők, hogy ahogy a többség dönt, az a lánc fog tovább menni, azt fogják ezután Ethereumnak nevezni. Várakozásaik szerint a másik ágat, úgyis ott fogják hagyni a bányászok, hiszen az ott bányászott pénz értéktelen lesz, és előbb utóbb átállnak a másik ágra ők is.

Az elágazást jelentő blokk létrehozása 2016. július 20.-ára volt várható. Az elágazás lezajlott, minden rendben ment mindkét ágon. A nagy többség a hard fork mellett tette le a voksát, így várható volt, hogy a másik ág hamarosan el fog halni. Az ether értéke elkezdett emelkedni, tartott vissza a korábbi árfolyamához. A másik ágon azonban az a furcsaság esett meg, hogy nem hagyták abba a bányászást azok a tagok, akik amellett szavaztak. [11]

Nem akartak engedni az ő igazukból. Pár nappal később az egyik tőzsde elkezdte listázni az általuk bányászott pénzt Ethereum Classic néven. Ugyan a számítási kapacitás jóval kisebb volt ezen az ágon, és az értéke is elmaradt jóval az ether értékétől (még 2018 szeptemberében is), de már nem volt értéktelen, mint ahogy korábban jósolták, így nyilvánvalóvá vált, hogy nem fog elhalni az a szál sem, ezért az Ethereum megduplázódott és egymással párhuzamosan mindkét szál élt tovább. [12]



19. ábra: Saját szerkesztés a https://www.cryptocurrencychart.com adatai alapján. Letöltés dátuma: 2018.10.02.

Kissé zavaró lehet ugyan, hogy pont annak a blokkláncnak kellett megváltoztatni a nevét, amelyiken nem történt semmilyen változtatás, vagyis ugyanúgy haladt tovább, mint korábban. Ennek az ágnak a pénzét Ether Classic (ETC) néven ismerjük ma, a másik ágnak pedig maradt az ether (ETH). [12]

Ennek a duplázódásnak az érdekessége, hogy akinek az eredeti blokkláncon volt egy bizonyos számú etherje (kivéve azokat, amik a The DAO cégben voltak), annak ezután mindkét blokkláncon megvolt ugyanaz a mennyiségű pénze ETH és ETC formájában. Ezek a pénzek nyilvánvalóan mivel külön blokkláncon szerepelnek, ezért külön is költhetőek el mindkét világban másra. Ugyanakkor a szétválás előtt megkötött szerződések, ugyanúgy mindkét világban kötelezik a közösség embereit. [12]

A szétválás miatt, a The DAO cégnek is úgymond kétféle vége lett. A hard forkos ágon egy könnyű lezárása lett a történetnek, hiszen a korábban a céghez tartozó ethereket átrakták egy olyan számlára, ahonnan a tagok egy okos szerződés segítségével át tudták írni a saját számlájukra az azelőtt magukhoz tartozó összegeket. [12]

A másik ágon viszont pár héttel a szétválás után (2016. szeptember 5-én) a hacker számára elérhetővé vált az általa kilopott összeg. Mivel, ahogy korábban írtam egy publikus blokkláncról beszélünk, ezért a mai napig nyomon tudjuk követni, hogy ezek a kriptovaluták hol tartózkodnak, kinek a birtokában vannak. Érdekesség, hogy a hacker számláján található szinte az egész összeg még 2018 szeptemberében is. [12]

A cég számláján lévő maradék összeget viszont a fejlesztőcsapat tagjaiból álló csoport lopta ki azért, hogy később visszaadják a részvényeseknek. Ezen az ágon is egy számlára utalták át az általuk kilopott kriptovalutákat. A korábbi összeg közel háromnegyedét tudták visszafizetni a fejlesztők. Itt is egy okos szerződés segítségével tudták felvenni a tagok a számukra meghatározott összegeket, viszont a szerződésben meghatározhatták, hogy ennek az összegnek mekkora részét szeretnék felajánlani, meghagyni a fejlesztőcsapat tagjaiból álló csoportnak, azért cserébe, hogy megmentették a maradék pénzüket a támadás után. Az adományozás személyre szabottan állítható volt, a tagok úgy is dönthettek, hogy nem ajánlanak fel semmit a csoport számára. [12]

Ezzel a másik ágon is lezárult a történet, és így teljes mértékben véget ért a The DAO cég életútja. Tanulságos volt az Ethereum első decentralizált, a kibertérben teljesen autonóm módon működő cége mind a fejlesztők számára, mind pedig a tagok/részvényesek számára. Az Ethereum blokklánca és rendszere végig hiba nélkül működött, ugyanakkor láthatóvá vált, hogy ezekben a bonyolult okos szerződésekben egy-egy apró hiba, milyen végzetes lehet egy cég vagy akár egy részvényes pénztárcája szempontjából. [12]

6. UX[8] design

„A design nem csak a kinézetről szól. A design arról szól, hogyan működik a termék.”

Az idézet Steve Jobs-tól származik, aki a haláláig az Apple vezérigazgatója volt. Bárhol találkozunk a UX szemlélettel, szinte biztos, hogy ez az idézet visszaköszön ránk, hiszen ez talán az egyik legjobb idézet amivel le lehet írni mit is jelent a UX. [22]

A legtöbb ember, ha meghallja azt a szót, hogy design, akkor valaminek a kinézetére, a látszatra, a külső tényezőkre asszociál. Egy designer feladata azonban sokkal többet jelent, minthogy csak megtervezze, hogy hogyan nézzenek ki a felületek egy rendszerben. Egy designernek át kell látnia az egész rendszer működését, és ami a legfontosabb, tudnia kell, hogy mit szeretne a felhasználó. [22]

Ez nem egyszerű feladat, hiszen sok esetben a felhasználó nem tudja megfogalmazni, hogy mit is szeretne látni a képernyőn, vagy ami még fontosabb, hogy hogyan is működjenek az egyes felületek, az egyes funkciók mit foglaljanak magukba.

Egy rendszer megtervezésénél nem mindig az a legfontosabb, hogy hogyan is néz ki. Itt arra gondolok, hogy nem attól lesz jó egy applikáció, hogy a legszebb képeket válogatjuk ki háttérképeknek vagy „össze-vissza” színezzük a képernyőt, hogy úgymond „dizájnos” legyen. [22]

Persze lehetnek esetek, amikor ezek a tényezők is nagyon fontosak tudnak lenni egy rendszerben, de alapvetően a felhasználó-barátság illetve az, hogy könnyen, egyértelműen kezelhető legyen a rendszer, sokkal fontosabb elem. [22]

Gondoljuk például egy kriptovaluta váltó alkalmazásra. Tegyük fel, hogy az alkalmazásban bárki bárkivel cserélhet kriptovalutát (tehát nem egy tőzsdei alkalmazásról van szó). Ebben az esetben nem az lesz a legfontosabb, hogy az egyes felhasználóknak a profilja milyen módon jelenik meg, vagy adott esetben a fényképeit milyen minőségben tudja feltölteni (ha egyáltalán része ez egy ilyen alkalmazásnak). Sokkal fontosabb ebben az esetben az, hogy könnyen, egyértelműen megtaláljuk azokat a funkciókat, amikkel a kriptovalutáinkat el tudjuk cserélni, vagy éppen az, hogy könnyen megtaláljuk az éppen aktuális kriptovaluta árfolyamokat.

[8] A „User experience” rövidítése. Magyarul felhasználói élményt jelent. A UX design a felhasználói élmény tervezését jelenti.

Ugyanakkor, ha egy social media alkalmazásra gondolunk, akkor nyilvánvalóan nem mindegy, hogy a fotóinkat vagy videóinkat milyen minőségben tudjuk felöltetni. Ez csak egy példa volt a sok közül, de jól szemlélteti, hogy fontos tudnia azt egy designernek, hogy kinek is történik a fejlesztés, ki a célcsoport és mire fogja használni az alkalmazást.

Az első feladata egy designernek, hogy felmérje, ki a célcsoport, illetve az, hogy hányféle célcsoport létezik. Az egyes célcsoportokat perszónának nevezi a szaknyelv. Perszónákat sok féle szempont szerint lehet készíteni, nyilván az alkalmazástól függően. Ezek lehetnek például:

- Nem
- Lakóhely
- Kor
- Milyen végzettsége van?
- Milyen az érdeklődési köre?
- Milyen a családi állapota?
- Milyen az anyagi helyzete?
- Milyen informatikai eszközöket használ?
- stb. [22]

A perszónák alkotásánál négy nagyon fontos kérdésre kell választ adnia egy designernek:

- Milyen előzetes tudással rendelkezik a perszónáról?
- Milyen kontextusban, milyen helyzetben használja az alkalmazást?
- Milyen problémái vannak, miket szeretne megvalósítani az alkalmazásban?
- Milyen motivációja van az alkalmazással kapcsolatban?

Arra, hogy egy perszónát egy designer feltérképezzen, sokféle megoldás létezik, ilyen lehet például az interjúztatás vagy a terepkutatás. [22]

A következő lépésben egy jó designer továbbra sem a képernyők megtervezésének lát neki, hanem megtervezi a folyamatokat. Ehhez két lehetőség, eszköz áll rendelkezésére. Két eszköz együttes használata a célra vezető. Az egyik a user journey (felhasználói útvonal), a másik a customer journey vagy gyakran találkozhatunk vele úgy is mint experience map (élmény térkép). Az előbbi csak azt vizsgálja, ami az alkalmazáson belül történik, a másik a teljes folyamatot érzelmekkel, gondolatokkal egybevéve. [22]

Amint ezekkel a feladatokkal elkészül egy designer, nekiláthat az onboardingnak. Az onboarding az a folyamat, amikor a felhasználó először használja az alkalmazást. Ebben az időszakban lehetőleg a legrövidebben és a legérthetőbben kell elmagyaráznia az alkalmazásnak azt, hogy miért is használja a felhasználó, milyen haszna származik belőle, illetve az alapvető funkciókat az applikáción belül. [22]

Talán ennek a folyamatnak a megtervezése a legnehezebb feladat, hiszen itt dől el az, hogy valaki használni fogja-e az alkalmazást. Az onboarding folyamatára rengeteg rossz példa létezik kezdve a tutorialoktól, az ablak elsötétítésén keresztül egészen a videókig. [22]

A következő nagyon fontos lépés a Hooked-modell. Ennek az a lényege, hogy meggyőzze a felhasználót az alkalmazás a felhasználót rendszeres használatról. Itt általában valamiféle jutalmazást szokás alkalmazni a rendszerben, ha a felhasználó valamit jól csinál, vagy teljesít egy feladatot. Egy kriptavaluta váltó alkalmazásban, például ha jó áron hozzá tudtuk jutni egy kriptovalutához, akkor az alkalmazás gratulálhat, hogy mennyit spórolt azon a felhasználó, hogy egy másik személytől vette meg nem a napi árfolyamon. [22]

A következő lépésnél érkezik el a designer a felületek, képernyők megtervezéséhez. Itt sok mindenre érdemes figyelni, többek között arra, hogy a szöveg is része a designnak. Szem előtt kell tartani az oldalak színezését, a menürendszer átláthatóságát és még sok más dolgot is. Ügyelni kell arra is, hogy a mai világban nem csak számítógépes felületre, hanem mobilra is terveznie kell egy designernek. [22]

Egy alkalmazás design-ja nem jöhet lére kutatás nélkül, legalábbis egy jó design alapja a kutatás. Ez a kutatás gyakran időigényes és annál hatásosabb minél többféle módszert alkalmazunk, de mindennek az eredménye nagyon sokat tud segíteni egy sikeres applikáció kifejlesztésében. A UX design alapvető kutatási módszere a megfigyelés. Sokszor úgy kezd el egy ilyen kutatást egy designer, hogy elkészít egy prototípust, és megfigyeli mindenféle segítség nélkül, hogy hogyan fogja használni a rendszert a felhasználó. [22]

A prototípus lényege, hogy a megtervezett képernyőket, funkciót egy „kattintható” verzióban elkészítjük. Ez azt jelenti, hogy nem lesz mögötte adatbázis vagy programkód, de az alapvető funkcióit a rendszernek szemléltetni tudja, és a rendszer hiányossága, vagy hibái könnyen ki tudnak derülni. [22]

A prototípus készítés az agilis fejlesztés egyik alapköve. Az agilis fejlesztés lényege, hogy a lehető leghamarabb eredményt tudjon felmutatni a fejlesztőcsapat. Erre akkor van lehetőség, hogyha a projektek le vannak bontva kisebb, tervezhető részekre. Ezeknek a kisebb részeknek az a lényege, hogy ne csak a fejlesztőcsapat számára mutassanak eredményt, hanem a konkrét felhasználó is lásson belőle valamit, önmagukban is használhatóak tudjanak lenni. [22]

Agilis fejlesztésre az egyik legelterjedtebb módszer a scrum. Ennek bemutatását a későbbiek során teszem meg, hiszen ezt a módszert alkalmazza a Zalaszám Informatika Kft. egyik fejlesztőcsapata is.

6.1. A Zalaszám, az agilis fejlesztés és a UX

A Zalaszám Informatika Kft. kivételes tudásbázissal és 4 évtizedes tapasztalattal rendelkező, dinamikusan fejlődő zalaegerszegi székhelyű vállalkozás. A Zalaszám célja, hogy az informatikai termék-előállítás és szolgáltatások piacán és az információbiztonság területén minden partnere számára folyamatosan kiemelkedő és egyenletes minőséget, magas megbízhatóságot biztosítson. A cég mottója: "A mai szolgáltatásokkal a holnapit kell megalapozni."

2015 szeptembere óta dolgozom a Zalaszám Informatika Kft.-nél duális képzés keretein belül. Mint duális hallgató, egy tanévben szeptembertől szeptemberig 110 napot dolgoztam minden évben. Ez idő alatt jól megismerkedtem a rendszerszervezői munka feladataival. Eleinte kisebb feladatokat kaptam a cégnél, aztán az idő előrehaladtával, egyre nagyobb volumenűek feladatok elvégzésére volt lehetőségem. Körülbelül másfél évvel ezelőtt bekerültem egy konkrét projekt agilis fejlesztőcsapatába. Jelenleg a cégnél egy szemléletváltás van folyamatban, ennek lehet az egyik iránymutatója ez a csapat.

A cég ezen a csapaton keresztül próbálja az agilis fejlesztés egyik ágát behozni a fejlesztésbe. Ezt a fejlesztőtechnikát a szaknyelv scrum-nak nevezi. A scrum részletes bemutatásától most eltekintenék, szeretném inkább azt bemutatni, hogy a Zalaszám Informatika Kft-nél hogyan működik, hogyan használjuk/használtuk a módszert az elmúlt másfél évben.

A scrum során „disznókról” és „csirkékről” beszélünk. A disznók azok a személyek, akik közvetlenül részt vesznek a fejlesztésben ilyen a Scrum Master, a fejlesztőcsapat, illetve a Zalaszám esetében a projektvezető. A scrum célja, hogy a disznók együtt dolgozzanak, bevonják a munkába a csirkéket, vagyis a felhasználókat, megrendelőket. Ez azt jelenti, hogy bizonyos időközönként találkozókat kell létrehozni az ügyfelek és a fejlesztők között. A scrum szerint ez az időintervallum két hét, de lehet több és kevesebb is. A Zalaszámnál, amióta ezt a módszert alkalmazza az említett fejlesztőcsapat, két hetes ciklusokban folyik a munka.

Egy ilyen ciklust hív a szaknyelv sprintnek. Egy sprintnek van egy indító megbeszélése (Sprint planning), illetve egy sprint záró megbeszélése (Sprint review). A sprint zárók tartalmazhatnak vagy járhat velük egy visszatekintő megbeszélés (Retrospective) is.

A cégnél ez úgy zajlik, hogy egy két hetes sprint lezárását megtartjuk délelőtt, illetve ugyanazon a napon délután az új sprint indítását. Bizonyos időközönként a sprintzáráshoz kapcsolódik egy retrospective, de jelenleg nem minden sprint végén.

A sprint célja, hogy olyan feladatokat végezzünk el, amelyek a sprint után bemutatható termékként szolgálnak. Olyan termékek, amelyeket be lehet mutatni a felhasználóknak, megrendelőknek.

A Zalaszám Informatika Kft. a projektjeit a Jira Software-ben kezeli. A szoftver webes felületen fut, lehetőség van az alkalmazásban az adott projekten belül feladatokat, illetve részfeladatokat létrehozni, ezeket ütemezni, valamint felelősökhöz rendelni.

Az adott fejlesztéshez kapcsolódik a cégnél egy product backlog amit a Jira Software-ben vezet a csapat. Ez a product backlog tartalmazza mindazokat a feladatokat, amiket az adott projekt kapcsán el kell végezni. Ez a feladatlista a fejlesztés előrehaladtával, illetve a növekvő vevőigénnyel folyamatosan tovább bővül.

A product backlog nagyobb feladatokat tartalmaz, ezeket kisebb feladatokra kell bontani. Mikor egy sprintet elindítunk a Zalaszámnál, össze kell rakni az úgynevezett sprint backlogot. Ez úgy zajlik, hogy a product backlogból az egyes feladatok részfeladatait pontozzuk egy ötös skálán. Ezek után a rendszerszervezők és a fejlesztők is feladatokat választanak maguknak. Ezek a feladatok bekerülnek a sprint backlogba. Egy sprint backlogját a scrum szabályai szerint feladattal utólag nem lehet bővíteni, csak részfeladattal.

A cégnél a rendszerszervezőknek kell egy kis előkészületet végezniük a sprint indító megbeszélésekre. A feladatok egyszerűbb pontozása érdekében, az egyes feladatokhoz prototípust készítenek. Ezek a prototípusok nem csak a vevőknek, felhasználóknak segítik megérteni a folyamatokat (ezzel segítve a fejlesztést), hanem a fejlesztőknek is segítenek a probléma átlátásban, a fejlesztés nehézségének megértésében.

Miután összeállt a sprint backlog, kapunk egy összesített pontszámot a nehézségi értékekből. Ezt nevezzük a sprint sebességének (Velocity). Egy kezdő scrum csapatnál ez a szám sprintenként eltérő lehet, hiszen kell idő, amíg egy csapat megtapasztalja, mennyi feladatot tudnak bevállalni egy adott sprintre. Egy több éve együttműködő csapatnál ez a szám állandó, vagy legalábbis nagyon hasonló minden sprintnél.

Miután a sprint indító megbeszélés lezajlott, kezdődhet maga a sprint. A fejlesztőcsapat elkezdi csinálni a feladatait. Tartani kell, ahogy a nevében is benne van, minden nap egy daily standup-ot. Ezt a Zalaszámnál minden reggel fél kilenckor tartjuk. Szerencsére ez könnyen megoldható, hiszen pár hónappal a fejlesztőcsapat összeállítása után sikerült egy irodába kerülnie a fejlesztőknek és a rendszerszervezőknek is.

A daily standupot lehet különböző pózokban tartani, extrémebb esetekben mérlegállásban is tarthatják. A Zalaszámnál a megszokott, hagyományos standup-ot tartjuk, vagyis álló pozícióban. Ilyenkor sorban végighaladva az embereken, mindenkinek három kérdésre kell válaszolnia:

- Min dolgozott tegnap?
- Mit fog csinálni a mai napon?
- Van-e valamilyen problémája/fennakadása a munkával kapcsolatban?

Ennek a megbeszélésnek körülbelül 5 percesnek kell lennie. Törekedni kell arra, hogy minél hamarabb vége legyen (ezért is állómegbeszélés), itt tényleg csak a lényeges információkat kell megosztani a többiekkel. A cégnél a csapat egyik tagja egy dokumentumban, egy emlékeztető formájában mindig rögzíti a standupon elhangzottakat.

Miután a sprint befejeződött, megtartjuk a sprint záró megbeszélést (sprint review). Ezen a megbeszélésen a csapattagok megbeszélik, hogy mely fejlesztések készültek el, illetve melyek nem. A cél az, hogy egy sprintbe annyi feladatot tervezzünk, amennyit el is tudunk végezni az adott idő alatt. Ezeken a sprintzárókon kell bemutatni a fejlesztőcsapatnak azokat a „termékeket” amelyek elkészültek a sprint alatt. A Zalaszámnál jelenleg ez nem esik egybe a felhasználói/megrendelői termékbemutatókkal.

Ezután bizonyos időközönként az adott sprint review után tartani szoktunk egy retrospective-et is, amin megbeszéljük, hogy az elmúlt sprintek hogyan alakultak, mik a tapasztalatok, benyomások az elmúlt időszakot követően.

Itt alapvetően kettő kérdésre kell választ adnunk, az egyik az, hogy mi az, ami jól működött az előző sprintekben (ezeket a dolgokat meg kell tartani és ugyanígy folytatni tovább), illetve, hogy mik azok a dolgok, amiket a következő sprint/sprintek során jobban lehetne csinálni, ami a korábbi sprintek során nem igazán működött jól.

Ezek mellett a Zalaszám igyekszik behozni a fejlesztésébe a UX szemléletet. Ehhez először külső oktatást igényelt a cég, majd belső képzések során folytatódott/folytatódik a rendszerszervezők továbbképzése. Ennek az oktatásnak az egyik részét a későbbiek során jelen állás szerint én fogom tartani. Egy ilyen oktatáson/képzésen az elméleti előadások mellett különböző gyakorlati/interaktív feladatokkal próbáljuk a dolgozókat megismertetni a UX szemlélettel.

20. ábra: UX oktatás. Letöltés időpontja: 2018.12.13.
Hozzáférés (URL): Zalaszám UX oktatás (céges dokumentumok)

Jelenleg a UX design gyerekcipőben jár a cégnél, de az elmúlt időszakban a cég, illetve a dolgozók sokat tesznek azért, hogy ez a folyamat minél jobban beépíthető legyen a Zalaszám fejlesztési folyamataiba.

6.2. Blokklánc és az okos szerződések UX design problémái és megoldásai

A blokkláncos alkalmazások, környezetek UX designolása nehezebb feladat, és több kihívást jelent, mint bármely más szoftveré. Egy UX designernek a legnagyobb feladata, hogy megteremtse, felépítse a bizalmat a felhasználókban, azért, hogy használják az alkalmazást. A hétköznapi emberek számára jelenleg a blokklánc vagy egy ismeretlen fogalom, vagy úgy gondolják, hogy egy nagyon kockázatos befektetés, technológia.

Az emberek ránéznek a bitcoin árfolyamára és gyakran elpártolnak a blokklánc technológia mellől. Egy UX designernek nehéz ma megmutatnia azt, hogy a blokklánc technológia egy hibátlanul működő újítás és nem függ a bitcoin árfolyamától.

Sok-sok tesztelés szükséges ahhoz, hogy feltérképezzük azt, mi is a konkrét kiváltó oka annak, hogy ebben a bizalom nélküli technológiában bízzanak az emberek.

„ Steve used to say, technology can either be beautiful or technology should be invisible…" – John Sculley

Az idézet értelmezése nagyjából úgy hangzik, hogy: A technológia lehet gyönyörű vagy a technológia lehet láthatatlan. Úgy vélem, a blokklánc szempontjából ez egy nagyon fontos idézet lehet. Hiszen véleményem szerint a blokklánc nem egyik napról a másikra fog betörni a hétköznapokba, ezt a feladatot lehetetlen is lenne megoldani a designereknek. A hosszú távú feladata a designereknek az, hogy eltüntessék a technológiát, a háttérbe szorítsák, hiszen a felhasználók számára nem az a fontos hogy milyen technológiai megvalósítása van egy adott terméknek, szolgáltatásnak, valutának.

Számukra az a fontos, hogy megbízható legyen, könnyen használható és a lehető legkevesebb bizalmi kérdés merüljön fel vásárlások, szolgáltatások igénybevétele esetén. Ahogy korábban is említettem, elég csak az internetre gondolnunk. Hányan tudjuk valójában, hogy hogyan is működik igazából az internet? Hányan látják át azt a folyamatot, ahogyan kialakult, és ahogyan a mai nap használjuk? Nagyon kevés az ilyen felhasználó manapság, ugyanakkor, akinek lehetősége van rá, az használja, hiszen megkönnyítette a hétköznapokat rengeteg téren, mind személyes, mind vállalati, kormányzati, politikai szempontból.

A következőkben szeretnék bemutatni négy UX problémát az okos szerződésekkel kapcsolatban.

1. Az okos szerződések és a walletok közötti kapcsolat

Egy okos szerződés megkötésekor ügyelnünk kell arra, hogy ezek a szerződések megkövetelik, hogy a teljesítés kriptovalutában történjen. Viszont manapság nincs olyan pénztárca, amely tudná kezelni az összes kriptovalutát, még olyan sincs, ami legalább a top 30-at tudná. [23]

Egy példán szemléltetve, képzeljük csak el, hogy minden weboldal megnyitásakor egy másik böngészőt kellene használnunk, vagy ahhoz, hogy a TV-n csatornát váltsunk, minden adóhoz külön távirányítót kellene használnunk. [23]

Az okos szerződések és a kriptovaluták mindennapi használatával kapcsolatosan ez egy nagyon nagy probléma lehet a jövőben, ami megoldásra vár. [23]

A felhasználói interfészek, illetve az alkalmazások teljesen különbözően, eltérően működhetnek egymástól, így minden egyes változatot külön meg kell tanulnia a felhasználónak ahhoz, hogy tudja használni őket. [23]

Gondoljunk csak bele, milyen furcsa lenne, ha például megnyitunk mindig egy új böngészőt egy új weboldalhoz, és az URL címet mindig máshol kéne megadnunk.

2. Jelenleg az okos szerződések használata megköveteli a kriptovaluták ismeretét.

Ahhoz hogy a hagyományos pénzeket használjuk, nem kell, hogy tudjunk pénzt verni, illetve különösebb információra sincs szükségünk róluk. Ismerjük a keresetünket, látjuk mennyibe kerülnek a szolgáltatások, termékek, ez bőven elég ahhoz, hogy használni tudjuk őket.

Viszont ahhoz, hogy az okos szerződéseknél használatos kriptovalutákat használni tudjuk, szükségünk van kriptográfiai ismeretekre, értenünk kell a blokklánc technológia lényegét, tudnunk kell a tranzakciók megerősítésének a folyamatát, idejét illetve költségeit. Ezek mind kriptovalutánként eltérőek lehetnek. [23]

A designerek, fejlesztők nagy feladata, hogy ezeket a tényezőket kiszűrjék a rendszerből, persze amennyiben ez lehetséges.

3. Lassú tranzakciók magas tranzakciós díjak

Jelenleg a blokkláncok növekedése és a megnövekedett adattartalmak miatt az utalások lassabban működnek, mint amire a technológia képes lehetne. [23]

A kriptovaluta utalásának a tranzakciós díjai manapság magasabbak, mint bármelyik állam által használt valutáé. [23]

4. A szabályozások hiánya

Jelenleg a kormányzati szervek és a bankok sem szabályozzák, korlátozzák a blokklánc alapú alkalmazások kriptovaluta használatait. Mivel mindig is lesznek a világban olyan emberek, akik át akarnak verni másokat, és jogtalanul szeretnének pénzhez jutni, így ez is egy megoldandó probléma. [23]

A kriptovaluták jelenleg ilyen szempontból megmutatják azt, hogy milyen volt a helyzet a bankok megjelenése előtt. Jelenleg, ha a bankban elutalok egy összeget egy rossz számlára, akkor bemegyek a bankba és kijavítják a hibámat, hiszen több pontos a biztonság ilyen szempontból, hiszen a számlaszám mellett meg kell adnom például az fogadó fél nevét. [23]

Jelenleg, ha egy rossz címre utalok kriptovalutát, az a folyamat visszafordíthatatlan. Ezt pedig nagyon sokan ki tudják, és ki is fogják használni. Főleg, a technológiát kevésbé ismerő embereket könnyen át lehet verni ilyen téren. Ebből kifolyólag a UX designereknek ki kell találniuk valamit erre a problémára, különben gyakran megtörténhetnek olyan utalások, amelyek rossz címre érkeznek meg. [23]

Mit tehetnek a UX designerek, tervezők a problémák megoldása, megelőzése szempontjából?

Korábban a designerek feladata az volt, hogy megtervezzék a kinézetet, hogy jól nézzenek ki a weboldalak, alkalmazások. Manapság a designerek feladata sokkal tágabb és főleg arra összpontosít, hogy funkcionálisan a lehető legjobban és könnyen kezelhetőek legyen ezek a rendszerek, amellett, hogy meggyőzzék a felhasználókat a használatról, illetve a rendszeres használatról. [23]

A UX designerek fő feladata az lenne, hogy a kriptovalutákkal kapcsolatban elkerüljék ezt a hibát. Ebben komoly szerepe van az alkalmazásokat, rendszereket fejlesztő csapatoknak, hiszen a képzett UX designerek tisztában vannak ezekkel a problémákkal, nekik csak annyi lenne a feladatuk, hogy a fejlesztőcsapataikba felvegyenek UX designereket is. [23]

A designolás folyamatában, nagy hangsúlyt kell fektetni a felhasználók oktatására, például onboarding szempontból is. Célszerű lehet a Hooked-modell használata apróbb segítségekkel, jutalmazásokkal, annak érdekében, hogy a felhasználók valóban megértsék mire is használhatóak az adott alkalmazások, kriptovaluták, okos szerződések. [23]

7. Összefoglalás

Véleményem szerint, egy új technológiai korszak előtt állunk. Ahogy a 2000-es évek elején az internet meghódította a világot, úgy a következő években, évtizedekben az internet új korszaka átformálhatja a világ gazdaságának alapjait. Ez a technológia a blokklánc. Dolgozatom elsődleges célja, hogy bárki, aki elolvassa, kapjon egy átfogó képet erről a technológiáról, függetlenül attól, hogy jártas-e ebben a témában, a számítógépek világában, illetve, hogy rendelkezik-e bármiféle előzetes informatikai tudással. Igyekeztem úgy felépíteni, hogy minden egyes témához kapcsolódjon egy gyakorlati példa a könnyebb megértés és a jobb szemléltetés érdekében.

Ahelyett, hogy a különböző technikai részleteket mélységében bemutatnám, előtérbe helyeztem azt, hogy különféle adatokkal, érdekességekkel tűzdelve ismertessem a blokklánc technológiát. Értem ez alatt Satoshi Nakamoto legendás alakját, az első elköltött bitcoinokat a magyar származású Laszlo Hanyecztől vagy például egy nagyon érdekes cég, a The DAO hirtelen népszerűségét, felemelkedését majd összeomlását.

Az én álláspontom ezzel a technológiával kapcsolatban az, hogy az internethez hasonló módon fog beszivárogni a hétköznapjainkba. Használni fogunk különféle alkalmazásokat, rendszereket anélkül, hogy a legtöbb ember tudná, hogy milyen technológia működik valójában a háttérben.

Nyitott kérdés a jövőre nézve, hogy átveszik-e a kriptovaluták a hagyományos fizetőeszközök helyét. Amennyiben igen, akkor egyszerre több fog-e belépni a hétköznapokba, vagy akár a bitcoin, akár másik kriptovaluta ki tudja-e sajátítani ezt a pozíciót.

Dolgozatom elején röviden ismertettem a blokklánc technológia kialakulásának előzményeit. Néhány gondolatot ejtettem Nick Szabo munkásságáról, illetve Satoshi Nakamoto ötletéről.

Ezek után áttértem a blokklánc ismertetésére, először általános szinten. Megfogalmaztam több fontos fogalmat a témával kapcsolatban, illetve írtam a blokklánc technológia hátteréről, a működési folyamatáról, amit példákkal szemléltettem.

A következő részben igyekeztem minél több gyakorlati példát hozni a mindennapok különböző területeiről, ahol használható ez a technológia.

Ezután a kriptovaluták ismertetésével folytattam, ahol lényegre törően ismertettem néhány általános dolgot a kriptovalutákról, majd a bányászatról, illetve a kriptovalutákhoz kapcsolódó tárolási módszerekről. A Bitcoinról – mint konkrét technológiáról – is írtam.

A következő fejezetben az okos szerződésekhez kapcsolódó technológiát és a hozzá kötődő digitális aláírást részleteztem. Majd az Ethereumról ejtettem néhány szót, illetve részletesen bemutattam egy, az Ethereumhoz kapcsolódó, a digitális világban létrejött és működtetett céget, a The DAO-t.

Az utolsó fejezetben, saját ismereteimet is használva mutattam be a UX szemléletet, a Zalaszám Informatika Kft-t, illetve az ott működő fejlesztési folyamatokat, a scrum-ot – mint agilis fejlesztést – továbbá a UX szemlélet beépülését a cég életébe.

Ennek a fejezetnek a végén a blokklánc technológia valamint az okos szerződések UX szemlélet szerinti problémáit tártam fel. Ezekre próbáltam megoldást, iránymutatást adni a fejlődés érdekében.

Összegzésem után, szükségesnek tartottam a témával kapcsolatban egy fogalomtár beillesztését is. Ez véleményem szerint azért fontos, mert ugyan az egyes fogalmakat kifejtem a dolgozatom során, mégis úgy gondolom, hogy rengeteg új fogalommal találkozhatunk ezzel a témával kapcsolatban, amelyeket jó, ha kigyűjtve megtalálunk. Adott esetben nem kell visszakeresnünk a szövegben, hogy melyik fogalom pontosan mit is jelentett, hanem a dolgozat végén, egy helyen megtalálható mindaz, ami szükséges lehet ilyen szempontból.

Kriptovaluta/Dátum	2018.09.20.	2018.12.17.
Bitcoin (BTC)	$6396,18	$3284,55
Ripple (XRP)	$0,3232	$0,2899
Ethereum (ETH)	$209,73	$86,97

2. táblázat: A TOP3 kriptovaluta árfolyama a dolgozatom kezdete, illetve befejezése időpontjában. Saját szerkesztés https://coinmarketcap.com/ adatai alapján. Letöltés időpontja: 2018.12.17.

8. Fogalomtár

51% Attack: Amikor egy blokkláncon a felhasználók 51%-a (a fele +1) összeáll, azért hogy valamiféle „csalást” hajtsanak végre.

Altcoin: A bitcointól eltérő összes kriptovalutát altcoinnak nevezzük.

Bányász farm: Több tucat eszköz üzemeltetése bitcoin vagy valamilyen kriptovaluta bányászása céljából.

Bitcoin: Nagy betűvel írva a technológiára utal, amit Satoshi Nakamoto talált és fejlesztett ki.

bitcoin: Kis betűvel írva, magára a kriptovalutára utal. A tőzsdén úgy találkozhatunk vele, mint BTC.

Blokklánc: Decentralizált, elosztott, nyilvános adatbázis. Részletesebben lásd a Blokklánc pontnál.

Blokk: A blokk a blokklánc egy része. Tranzakciókat tartalmaz, illetve az előző blokk hash-ét. Részletesebben lásd a Blokklánc pontnál.

Customer journey: A UX folyamat tervezésének egyik lépése. Magába foglalja a teljes felhasználói folyamatot érzelmekkel, gondolatokkal egybevéve. Gyakran találkozhatunk vele úgy is, mint Experience map, magyarul élménytérkép.

Crowdfunding: Magyarul közösségi finanszírozás. A közösségi finanszírozás lényegében azt jelenti, hogy az emberek tőkét fektetnek be bizonyos cégek megalapításába, termékek vagy szolgáltatások megvalósításába.

Daily standup: A scrum – mint agilis fejlesztési forma- egyik eszköze. Napi szintű megbeszélés, ahol a fejlesztőcsapat tagjai elmondják mit csináltak tegnap, mivel foglalkoznak a mai nap, illetve, hogy van-e valamilyen problémájuk a fejlesztéssel kapcsolatban.

DAO: Az angol decentralized autonomous organization rövidítése. Teljesen önállóan, okos szerződések által vezérelt szervezetek. Amennyiben úgy találkozunk vele, hogy The DAO, akkor egy konkrét az Ethereum blokkláncán létrehozott cégről beszélünk.

dApp: Decentralized applications, magyarul Decentralizált alkalmazás.

Ethereum: Vitalik Buterin által alapított cég. Fő tevékenysége az okos szerződések létrehozása.

ether: Az Ethereum kriptovalutája. A tőzsdén úgy találkozhatunk vele, mint ETH.

Fiat pénz: A hagyományos „kézzel fogható" pénzeket nevezzük fiat pénzeknek. Ilyenek például a forint, a dollár vagy az euró.

Fork: Lehet soft vagy hard. Mindkettő esetben a programkód átírását jelenti a blokkláncon. A soft egy finomabb verziója, a hard egy drasztikusabb változata. Mindkét eset szigorúan szembemegy a blokklánc szabályrendszerével.

Hash-függvény: Ez a függvény változó számú karakter befogadására képes, de meghatározott számú karaktert (string) ad eredményül. Amennyiben a bemeneti oldalon megváltoztatunk akár csak egyetlen karaktert is, a kimeneti oldalon a hash értéke teljesen más lesz.

Hash: A hash-függvény által generált string.

Hooked-modell: Lényege, hogy meggyőzze a felhasználót egy applikáció rendszeres használatáról.

Kriptográfia: Informatikai tudomány, amely titkosírással, titkosítással, kódolással foglakozik.

Kriptovaluta: Digitális pénz, amely kriptográfiai módszereket használ titkosítás szempontjából. Kizárja a köztes harmadik szereplőt a tranzakciókból, az utalások teljesen közvetlenül zajlanak egy blokkláncon.

Middleman: Utalásoknál, szerződéseknél bármilyen ügyletnél a köztes szereplőt jelenti. Lehet ez egy utalás esetén például egy bank, egy szerződés esetén pedig egy ügyvéd.

Middleware: A blokkláncos keretrendszerek és az applikációk közötti harmadik, köztes réteg. Ezek a szolgáltatások általában integrációt biztosítanak. Ugyanakkor ide soroljuk a különböző kriptovaluta váltó alkalmazásokat is.

Mining: Magyarul bányászást jelent. A bányászat lényege, hogy a blokkláncban résztvevő csomópontok matematikai feladványokat oldjanak meg a blokklánchoz csatlakozott eszközükkel, amiért jutalmul kriptovalutát kapnak. Részletesebben lásd a Bányászat pontnál.

Node: A blokklánc decentralizált hálózatának egyes csomópontjain lévő számítógépeket, eszközöket node-oknak nevezzük.

Nonce: Mikor egy hash-függvénnyel egy előre meghatározott hasht, vagy egy olyan hasht, aminek egy része előre meghatározott (Bitcoin esetén például valahány 0-val kell kezdődnie) akarunk előállítani, akkor hozzá kell raknunk egy számot a tranzakciók listájához, hogy a hash kimenetelét megváltoztassuk. Ezt a számot nevezzük nonce-nak. Részletesebben lásd a Hash-ek, megváltoztathatatlanság, biztonság pontnál.

Onboarding: A UX designnal kapcsolatban az onboarding azt jelenti, amikor egy felhasználó először találkozik a rendszerrel. Ekkor kell megismertetni a felhasználóval a rendszert, illetve bemutatni neki, hogy miért jó az alkalmazás és számára miért lehet hasznos.

Peer-to-peer: A peer-to-peer hálózat lényege, hogy nincs egy központi számítógép, szerver vagy kliens, hanem az eszközök közvetlenül egymással kommunikálnak.

Prediction market: Magyarul előrejelzési piacok. Ezeken a blokkláncon működő alkalmazásokon bármire fogadhatunk, továbbá saját magunk is hozhatunk létre fogadási tételeket.

Product backlog: Egy product backlog tartalmazza mindazokat a feladatokat, amiket az adott projekt kapcsán el kell végezni.

Proof of work: Magyarul a munka bizonyítéka. Ez jelenti a blokkok hashelés által végzett hitelesítését.

Prototípus: A prototípus lényege, hogy egy rendszer fejlesztésekor a megtervezett képernyőket, funkciót egy „kattintható” verzióban elkészítjük. Ez azt jelenti, hogy nem lesz mögötte adatbázis vagy programkód, de az alapvető funkcióit a rendszernek szemléltetni tudja, és a rendszer hiányossága, vagy hibái könnyen ki tudnak derülni.

Retrospective: A scrum – mint agilis fejlesztés – egyik eszköze. A korábbi sprint/sprintek visszatekintése, elemzése, tapasztalatok, vélemények megosztása.

Scrum: A scrum egy agilis fejlesztési forma. Részletesebben lásd az A Zalaszám, az agilis fejlesztés és a UX pontnál.

Smart contract: Magyarul okos szerződést jelent. Blokkláncon működő kriptográfiai titkosítást, digitális aláírást használó technológia. Részletesebben lásd az Okos szerződések pontnál.

Sprint: Általában kettő vagy négy hetes folyamat, amely idő alatt a fejlesztőcsapat bemutatható eredményt állít elő.

Sprint backlog: A product backlog azon elemeit tartalmazza, amelyeket a fejlesztőcsapat beválasztott egy sprint feladatai közé.

Sprint planning: Magyarul sprint indító megbeszélés. Itt a fejlesztőcsapat tagja nehézség szerint pontozzák az egyes feladatokat, majd mindenki feladatot/feladatokat választ magának a következő sprintre.

Sprint review: Magyarul sprint záró megbeszélés. Itt a fejlesztő csapat értékeli az elmúlt sprintben megvalósított feladatokat. Két fő kérdése van a megbeszélésnek. Az egyik, hogy mi az, amit jól csináltak, a másik pedig, hogy mi az, amit jobban csinálhattak volna.

String: Karakterek sorozata. Hash esetén számok és betűk meghatározott, fix hosszúságú láncolata.

TEU: Twenty-foot equivalent unit rövidítése, magyarul húsz láb – megközelítőleg 6 méter - hosszú konténert jelent.

Token: A token egyfajta részesedést jelent egy decentralizált cégben vagy egy használati jogot egy ilyen applikációhoz. Egy tokennek van egy kezdeti értéke, illetve a későbbiek során el lehet adni, üzletelni lehet vele.

Trigger: Az okos szerződés feltételeit nevezzük triggereknek.

User journey: Magyarul felhasználói útvonalat jelent. Hasolnó a customer journey-hez, viszont itt csak azt a folyamatot figyeljük meg, amikor a felhasználó az alkalmazást közvetlenül használja, az alkalmazáson belüli történéseket.

UX: User experience rövidítése, magyarul felhasználói élményt jelent. A UX design a felhasználói élmény tervezését jelenti.

Velocity: Magyarul sebességet, gyorsaságot jelent. Miután a fejlesztőcsapat a sprint planning-en összeállította a sprint backlogot kapunk egy összesített pontszámot a nehézségi értékekből. Ezt nevezzük a sprint sebességének.

Wallet: Magyarul digitális pénztárcaként értelmezzük az adott környezetben. Ezen tudjuk tárolni a kriptovalutáinkat. A wallet lehet online vagy offline.

White paper: Magyarul fehér könyvet jelent. Ez egy olyan dokumentum, amely egy ötletnek/tervezetnek a részletes leírását jelenti.

9. Irodalomjegyzék

[1] Varsányi Károly: Nick Szabo és a kriptovilág születése [online]. Letöltés időpontja: 2018.09.20. Hozzáférés (URL): https://fintechzone.hu/nick-szabo-es-a-kriptovilag-szuletese/

[2] Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electonic Cash System [fájl]. Letöltés időpontja: 2018.09.20. Hozzáférés (URL): https://bitcoin.org/bitcoin.pdf

[3] Ismeretlen szerző: Kicsoda Satoshi Nakamoto? [online]. Letöltés időpontja: 2018.09.20. Hozzáférés (URL): https://www.bitcoinbazis.hu/utmutato/kicsoda-satoshi-nakamoto/

[4] Adam L. Penenberg: Újabb fejezet a Satoshi-aktában [online]. Letöltés időpontja: 2018.09.20. Hozzáférés (URL): https://bitcoin.hu/ujabb-fejezet-a-satoshi-aktaban/

[5] Ismeretlen szerző: What is Blockchain Technology? A Step-by-Step Guide For Beginners [online]. Letöltés időpontja: 2018.09.25. Hozzáférés (URL): https://blockgeeks.com/guides/what-is-blockchain-technology/

[6] Don Tapscott: Hogy alakítja át a blokklánc a pénz és az üzleti világot (TED előadás) [online]. Letöltés időpontja: 2018.09.25. Hozzáférés (URL): https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=hu

[7] Bettina Warburg: How to blockchain will radically transform the economy (TED előadás) [online]. Letöltés időpontja: 2018.09.25. Hozzáférés (URL):

https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy/transcript

[8] Ismeretlen szerző: How Blockchain Technology Works. Guide for Beginners [online]. Letöltés időpontja: 2018.09.27. Hozzáférés (URL): https://cointelegraph.com/bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners#hash-function

[9] kriptosuli.eu: Mi az az Ethereum Classic és a DAO támadás? [online]. Letöltés időpontja: 2018.09.27. Hozzáférés (URL): https://kriptosuli.eu/etc.html

[10] Szabó Dávid: Egy virtuális cég felemelkedése – The DAO, 1. rész [online]. Letöltés időpontja: 2018.09.27. Hozzáférés (URL): http://www.superposition.hu/hu/blog/egy-virtualis-ceg-felemelkedese-dao-1-resz

[11] Szabó Dávid: Egy virtuális cég bukása – The DAO, 2. rész [online]. Letöltés időpontja: 2018.09.27. Hozzáférés (URL): http://superposition.hu/hu/blog/egy-virtualis-ceg-bukasa-dao-2-resz

[12] Szabó Dávid: Párhuzamos univerzumok – The DAO, 3. rész [online]. Letöltés időpontja: 2018.09.27. Hozzáférés (URL): http://superposition.hu/hu/blog/parhuzamos-univerzumok-dao-3-resz

[13] Szegő Dániel, Tuan Anh Trinh: Bitcoin és blokchain technológián alapuló lehetőségek [online]. Letöltés időpontja: 2018.09.28. Hozzáférés (URL): http://www.logsysteam.com/hungary/bitcoin-es-blockchain-technologian-alapulo-lehetosegek/

[14] Johnny Sessa: What is ETHLEND? | Beginner's Guide [online]. Letöltés időpontja: 2018.10.30. Hozzáférés (URL): https://coincentral.com/ethlend-beginner-guide/

[15] Dr. Varsányi Károly: Néhány mondatban az ERC20 tokenekről és az ún. Howey tesztről [online]. Letöltés időpontja: 2018.11.08. Hozzáférés (URL): http://digitalcash.hu/2018/01/23/nehany-mondatban-az-erc20-tokenekrol-es-az-un-howey-tesztrol/

[16] Ismeretlen szerző: What is Blockchain Technology? A Step-by-Step Guide For Beginners [online]. Letöltés időpontja: 2018.11.13. Hozzáférés (URL): https://blockgeeks.com/guides/what-is-blockchain-technology/

[17] BoardRoom honlap [online]. Letöltés időpontja: 2018.11.14. Hozzáférés (URL): http://boardroom.to/#About

[18] Szedlák Ádám: Az adat az új adat. In: Forbes 2018.10., p. 64.

[19] Moonbaby (a kriptoakademia.com egyik szerkesztője): Jósold meg a jövőt! – Elindult az Augur mainnet [online]. Letöltés időpontja: 2018.11.22. Hozzáférés (URL): https://kriptoakademia.com/2018/07/10/elindult-az-augur

[20] Németh Mónika: A bitcoin után itt az adrenalin-függők új játéka: ICO [online]. Letöltés időpontja: 2018.11.22. Hozzáférés (URL): https://fintechzone.hu/mi-az-ico-bitcoin-utani-kripto-vilag/

[21] BLNT (a kriptoakademia.com egyik szerkesztője): „Halott az Augur" és más gyászjelentések [online]. Letöltés időpontja: 2018.11.22. Hozzáférés (URL): https://kriptoakademia.com/2018/08/22/halott-az-augur

[22] Pásztor Dávid: UX Design – Hogyan tervezz felhasználóbarát és szerethető alkalmazásokat? Budapest: UX studio Zrt., 2016.
ISBN 978-963-12-5259-0

[23] Yuval Keshtcher: The 4 UX problems when designing blockchain-based smart contracts [online]. Letöltés időpontja: 2018.12.14. Hozzáférés (URL): https://blog.prototypr.io/the-4-ux-problems-when-designing-blockchain-based-smart-contract-d37ee4c8c64b

10. Ábra- és táblázatjegyzék

18 57 BUDAPESTI GAZDASÁGI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME

BGE GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI NYILATKOZAT

Alulírott, Budai Gergő büntetőjogi felelősségem tudatában nyilatkozom, hogy a szakdolgozatomban foglalt tények és adatok a valóságnak megfelelnek, és az abban leírtak a saját, önálló munkám eredményei.
A szakdolgozatban felhasznált adatokat a szerzői jogvédelem figyelembevételével alkalmaztam.
Ezen szakdolgozat semmilyen része nem került felhasználásra korábban oktatási intézmény más képzésén diplomaszerzés során.

Zalaegerszeg, 2018.december hó 20. nap

Budai Gergő

hallgató aláírása

BUDAPESTI GAZDASÁGI EGYETEM
ALKALMAZOTT TUDOMÁNYOK EGYETEME
GAZDÁLKODÁSI KAR ZALAEGERSZEG

ÖSSZEFOGLALÁS

Blockchain

A kriptovaluták és az okos szerződések világa

Budai Gergő
Nappali tagozat / Gazdaságinformatikus / Logisztikai informatikus

A világunk gazdasága egy új technológiai korszak küszöbén áll. Napjainkban rengetegen dolgoznak azon, hogy ne úgy essünk be ezen a képzeletbeli küszöbön, hanem stílusosan sok-sok területet felölelve szivárogjon be a hétköznapokba. Ez a technológia a blockchain. Blokkok láncolata.

A Satoshi Nakamoto által elképzelt, majd megvalósított technológia alapvető felhasználási területe a Bitcoinra összpontosult. A 2008-as világválság alatt kitalált, majd elindított kriptovaluta jelenleg – 2019 januárjában – is történelmünk eddigi legnagyobb volumenű, legismertebb, illetve a legelfogadottabb digitális pénze.

Ahogy a Bitcoin szép lassan elkezdett ismertté válni, úgy kezdték el a mögötte rejlő technológiát is újra felhasználni más-más területeken. A kriptovaluták világa után a blockchain második legfontosabb felhasználási területe jelenleg az okos szerződéseknél található.

Az 1990-es években a magyar felmenőkkel rendelkező Nick Szabo már megfogalmazott gondolatokat okos szerződésekkel, illetve digitális pénzekkel kapcsolatban. Érdekes, hogy az első elköltött bitcoinok is egy magyar felmenőkkel rendelkező, de az Egyesült Államokban élő személyhez, Laszlo Hanyeczhez kapcsolódik.

A dolgozat felépítésében és tartalmilag is úgy készült, hogy laikusok számára is értelmezhető legyen. Mindenekelőtt fontos ismertetni, hogy milyen előzményekkel rendelkezik a technológia, kialakulásának helyzetét, illetve azokat a személyeket, akik szerepet játszottak a megvalósulásában.

Ezután ismertetésre kerül maga a technológia, melynek végén a jelenleg még kevésbé ismert felhasználási területei kerülnek bemutatásra. Két külön fejezetben történik a kriptovaluták, illetve az okos szerződések ismertetése.

A dolgozat végén UX design szempontjából kerülnek vizsgálásra a korábban említett témák, melyekhez személyes tapasztalataim alapján önálló véleményt formáltam.

A technológia – ugyan 2019-ben már 10 éve működik – még gyerekcipőben jár és valószínűleg még sokáig abban is fog. A mindennapi életbe való beillesztése egy nagyon hosszú folyamat, melyet sok-sok nagyvállalat, intézmény, a világ gazdaságát közvetlenül befolyásoló szervezetek igyekeznek a saját területükön felhasználni a lehető legjobban.

A blockchain technológia egy lehetőség, amelynek még rengeteg kiaknázatlan területe van és amennyiben a megfelelő szervezetek a megfelelő energiabefektetéssel fejlesztik és támogatják a gazdasági – de akár politikai vagy bármilyen más – területen való felhasználását, akkor éveken belül a hétköznapi ember keze közé kerülhet, akár anélkül, hogy azt a laikusok észrevennék.