

PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

A kriptovaluta világa

Témavezető: Hegedűs Géza József

Külső konzulens: Kuffej Attila

Nyirádi Ferenc Bálint

Felsőoktatási szakképzés

Nappali tagozat

Gazdaságinformatika

2022

**PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG**

SZERZŐI NYILATKOZAT A DOLGOZAT BENYÚJTÁSÁHOZ*

Hallgató neve:	Nyirádi Ferenc Bálint		
Képzési szint:	felsőoktatási szakképzés		
Szak:	Gazdaságinformatika		
Szakirány (ha van):			
Neptun kód:	V36YP2	Védés éve:	2022
Dolgozat címe:	A kriptovaluta világa		
Egyetemi témavezető:	Hegedűs Géza József		
Gyakorlóhelyi konzulens:	Kutfej Attila		
Öt kulcsszó a dolgozatról:	Kriptovaluta, Bitcoin, Digitalizáció, Blokklánc, Okosszerződés		

Kérjük a szerzői döntésnek megfelelő opciót aláhúzni:

Hozzájárulok / nem járulok hozzá, hogy szakdolgozatom/záródolgozatomat az Egyetem az interneten a nyilvánosság számára repozitóriumában közzétegye.

A hozzájárulás szerzői feltételei:

- a dolgozat magáncélra letölthető, a forrás megjelölésével szabadon idézhető, de az idézés szokásos terjedelmét meghaladó felhasználás (átvétel) tilos,
 - hozzájárulásom időtartamra nem korlátozott és bármikor visszavonható.
- (Hozzájárulás hiányában a dolgozat csak az Egyetem arra kijelölt számítógépein, képernyős megtekintéssel kutatható. Egyéb hozzáférés, többszörözés nem engedélyezett.)

Büntetőjogi felelősségem tudatában nyilatkozom az alábbiakról:

- dolgozatom mindenben eleget tesz a vonatkozó és hatályos intézményi előírásoknak,
- a dolgozatban foglalt tények és adatok a valóságnak megfelelnek, a leírtak saját, önálló munkám eredményei,
- a dolgozatban felhasznált adatokat, forrásokat a szerzői jog figyelembevételével alkalmaztam,
- a dolgozat nem került felhasználásra korábban oktatási intézmény más képzésén felsőoktatási szakképzés, diplomaszerezés vagy szakirányú továbbképzés során.

Tudomásul veszem az alábbiakat:

- a dolgozat szerzői jogtisztaságának ellenőrzésére az Egyetem szoftveres ellenőrzést (plágiumszűrést) végezhet és eredményét a dolgozat értékelésében felhasználhatja,
- a dolgozat elektronikus formában, az Egyetem repozitóriumában kerül elhelyezésre és a hatályos jogszabályok, intézményi szabályzatok szerint, valamint fentebbi szerzői rendelkezéseimnek megfelelően biztosítható a kutatási célú hozzáférése,
- a dolgozat metaadatai és szerzői összefoglalója online nyilvánosak.

Zalaegerszeg, 2022.05.20.


hallgató aláírása

PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

Beszámoló a szakmai gyakorlatról

2022

TARTALOM

1. VÁLLALAT BEMUTATÁSA	1
1.2. DECKMAN, MINT SAJÁTMÁRKA.....	1
2. A SZAKMAI GYAKORLAT SORÁN ELVÉGZENDŐ FELADATOK	3
2.1. MEGBESZÉLÉSEKEN VALÓ RÉSZVÉTEL ÉS ANNAK JEGYZETELÉSE.....	3
2.2. OKOS-ÜGYVITEL KEZELÉSE	3
2.3. PROFIT CENTRUM MEGALKOTÁSA.....	4
3. SZAKMAI GYAKORLATI NAPLÓ	5
4. ÖSSZEGZÉS	6
5. FORRÁSOK.....	6

1. VÁLLALAT BEMUTATÁSA

Szakmai gyakorlatomat a C-Belt Szállítószalag Kereskedelmi Kft.-nél tölthettem Lentiben, amelynek időtartama 14 hét volt.

A cég 2017 végén alakult meg. Először csak szállítószalagokkal foglalkoztak, majd később elkezdtek állványrendszerekkel és zsalurendszerekkel is foglalkozni. Fontos megemlíteni, hogy Magyarországon kizárólagos forgalmazói a C-Belt Kft. a szállítószalagoknak. Ezeken kívül még a cég foglalkozik hőszigeteléssel, akciókeverőkkel, emelőgépekkel és még sok mással is. A termékeket lehet vásárolni is és bérelni is. Az évek során a fő profilja a cégnek az állványrendszer lett, amiből 2 fajtát forgalmazunk: Ringer, Deckman. A cégnél összesen 8 fő dolgozik.



Deckman állványrendszer
Forrás: <https://deckman.hu/allvany/>

1.2. DECKMAN, MINT SAJÁTMÁRKA

A cég vezetői létrehoztak egy sajátmárkát, ami a Deckman. Az állványrendszeren kívül a zsalurendszerek is Deckman márkájúak. Az alkatrészeket nem Magyarországon, hanem Törökországban gyártják le és ott is lesznek lematricázva Deckman felirattal.

Állványalkatrészek esetében bele is vésik a márkanévet. Ezeket az állványokat kizárólag Magyarországon, Lentiben forgalmazzuk.

A legnagyobb különbség a Deckman- és a Ringerállványok között az, hogy a Ringernél fapadló van, míg a Deckmannál horganyzott acél, ezáltal a fapadlót cserélni kell, míg a horganyzott acélpalló évekig kitűnő állapotban marad. Ezen kívül még, ami észrevehető, hogy a Ringer festett fém. A Ringert Ausztriában gyárják Regau-ban.

2. A SZAKMAI GYAKORLAT SORÁN ELVÉGZENDŐ

FELADATOK

Szakmai gyakorlatom során számos feladatot végeztem, amiből hármát szeretnék kiemelni: szakmai beszélgetéseken való részvétel és jegyzetelés, okos-ügyvitel kezelése, profit centrum kialakítása. Ezen kívül természetesen segítettem a beérkezett zsalurendszeres matricázásában, valamint fontos volt, hogy ellenőrizzem az elkészített szettek, áruk kontrollálását. Nagyon fontos volt, hogy minden össze legyen készítve a vevőnek és semmi ne maradjon le, ezért én feleltem.

2.1. MEGBESZÉLÉSEKEN VALÓ RÉSZVÉTEL ÉS ANNAK JEGYZETELÉSE

Számos szakmai megbeszélésen, értekezleten vettem részt, amiről jegyzeteket készítettem. Az ukrán-orosz háború, a vas és az euró áremelkedése miatt szükség volt megbeszéléseket tartani. A folyamatos euróingadozás miatt, úgy döntöttük, hogy megemeljük 385 forintra az euró értékét. A folyamatos ingadozás miatt még azt a döntést is meghoztuk, hogy a díjbekérőre 8 nap helyett, 3 napos határidő legyen megszabva. Az áremelkedés miatt igyekeztünk ajándékot is csatolni a megrendelt termékekhez. Ajándékok közé tartozott egy ajándék Krauser létra, vagy a kiszállítás árának felét álltuk.

Következő megbeszélésen a hírlevél volt a fő téma. Szerettünk volna hírlevelet létrehozni. Ha egy vásárló az oldalunkra kattint, akkor egy kis ablak ugorjon fel. Ha a vásárló megadja az e-mail címét, 10% kedvezményhez jut.

2.2. OKOS-ÜGYVITEL KEZELÉSE

Munkáim nagy részét az Okos-Ügyvitelen keresztül végeztem. Az Okos-Ügyvitel egy több modulból álló program. Számlázó, CRM, készletnyilvántartási- és pénztári program. Az én feladatomban a készletnyilvántartás volt. A beérkezett árukat, alkatrészeket fel kellett vinnem a rendszerbe. Ahhoz, hogy ténylegesen meggyőződjek, mennyi darab alkatrész jött egy adott termékből, meg kellett számolnom, mert előfordult, hogy eggyel kevesebb vagy több érkezett.

Minden termékekhez, alkatrészhez egy kódszám tartozott, például a Ringer, kétsínes keret (0,65x2 m) kódszáma 111 0007. Ha új áru érkezett, akkor a „Készletek” menüpontra belül a Raktári bevét opciót kell kiválasztani, majd kódszám, darabszám, egységár alapján felrögzíteni. A Raktári kivét lehetőségére a fent említett ajándékba adott termékeknel volt szükség.



Okos-Ügyvitel: Készletek

Forrás: <https://www.youtube.com/watch?v=Cntmxf4l8wQ>

2.3. PROFIT CENTRUM MEGALKOTÁSA

Külső konzulenssel egy profit centrumot építettünk fel. A profit centrum arra szolgál, hogy megmutatja, egyes termékek negyedévente mekkora profitot termeltek. Röviden a beszerzési ár és az eladási ár különbsége. Tudni szeretnénk volna, hogy milyen szolgáltatásokat használunk fel egyes termékek eladásához. Például, ha a szállítószalagot nézzük, a targoncakezelőnek a szállítószalagot a vevő autójára fel kell helyeznie. Ez azt jelenti, hogy az elfogyasztott üzemanyagot, le kell vonni az eladási árból.

3. SZAKMAI GYAKORLATI NAPLÓ

Hetek (2022.02.14-2022.05.20.)	Feladatok
1. hét (február 14-18.)	Gyakorlati hely megismerése Dolgozók munkakörének megismerése
2. hét (február 21-25.)	Adminisztratív feladatok elvégzése
3. hét (február 28 – március 4.)	Leltár készítés
4. hét (március 7-11.)	Raktári feladatok elvégzése, adminisztrációja
5. hét (március 14-18.)	Adminisztratív feladatok elvégzése
6. hét (március 21-25.)	Beérkezett áruk felvitele a rendszerbe
7. hét (március 28 – április 1.)	Profit centrum felépítésének kidolgozása
8. hét (április 4-8.)	Számítógépes problémák helyreállítása
9. hét (április 11-15.)	Raktári feladatok elvégzése
10. hét (április 18-22.)	Adminisztrációs feladatok elvégzése
11. hét (április 25-29.)	Elkészített áruk ellenőrzése
12. hét (május 2-6.)	Beérkezett áruk felvitele a rendszerbe
13. hét (május 9-13.)	Beérkezett áruk matricázása
14. hét (május 16-20.)	Záródolgozattal való foglalkozás, konzultációk

4. ÖSSZEGZÉS

A 14 hetes szakmai gyakorlatom során a C-Belt Kft. munkatársainak segítségével beletanulhattam a készletnyilvántartás kezeléseibe. Az Okos-Ügyvitel segítségével könnyen és gyorsan tudtam feladataimat elvégezni.

5. FORRÁSOK

<https://deckman.hu/>

<https://ringerallvany.hu/allvanyzatok/homlokzati-allvanyok/>

PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

A kriptovaluta világa

2022

TARTALOMJEGYZÉK

1. VÁLLALAT BEMUTATÁSA	1
1.2. DECKMAN, MINT SAJÁTMÁRKA	1
2. A SZAKMAI GYAKORLAT SORÁN ELVÉGZENDŐ FELADATOK	3
2.1. MEGBESZÉLÉSEKEN VALÓ RÉSZVÉTEL ÉS ANNAK JEGYZETELÉSE	3
2.2. OKOS-ÜGYVITEL KEZELÉSE	3
2.3. PROFIT CENTRUM MEGALKOTÁSA	4
3. SZAKMAI GYAKORLATI NAPLÓ	5
4. ÖSSZEGZÉS	6
5. FORRÁSOK	6
1. BEVEZETÉS	1
2. ELŐZMÉNYEK	3
3. KRIPTOVALUTÁK	4
3.1. MI IS AZ A KRIPTOVALUTA?	4
3.2. KRIPTOBÁNYÁSZAT	5
3.3. BITCOIN	7
3.4. ETHEREUM	9
3.5. HATÁSUK A GAZDASÁGRA	11
4. BLOKKLÁNC	13
4.1. MŰKÖDÉSE	14
4.2. A HASH ALGORITMUS	15
5. AZ OKOSSZERZŐDÉSEK	16
5.1. MŰKÖDÉSŰK	17
5.2. FELHASZNÁLÁSUK	18
5.3. BLOKKLÁNC ORÁKULUMOK	19
6. ÖSSZEGZÉS	21
7. IRODALOMJEGYZÉK	24
8. ÁBRA- ÉS TÁBLÁZATJEGYZÉK	29

1. BEVEZETÉS

Egyetemi tanulmányaim során informatikai, gazdasági és pénzügyi területekkel is megismerkedtem. A pénzügyi területen belül nagyon érdekesnek találok a digitális fizetőeszközöket, azaz a kriptovalutákat, ezért záródolgozatom témájául ezek bemutatását választottam. Úgy gondolom, hogy a kriptovaluták az utóbbi évtizedben nagyon népszerű fizetőeszközökké váltak, köszönhető a digitalizált világnak. Ma már több száz kriptovaluta létezik. Záródolgozatomban ismertetem a digitális fizetőeszközöket röviden, a bányászatukra és a gazdasági hatásukra is rátérek, illetve bemutatom a két leghíresebb kriptovalutát, a Bitcoinot és az Ethereumot. Bemutatom a blokkláncot és annak algoritmusát, majd ezután az okosszerződések működését, felhasználását és pár blokklánc orákulum fajtát. A dolgozatom egy részénél a Számítástechnika alapjai tárgyánál tanult ismereteimet is tudom hasznosítani.

Dolgozatomhoz többnyire internetes forrásokból tájékozódtam: weboldalakból, blogokból. Ezen kívül a Kriptopénz ABC nevezetű könyvből is szereztem információkat. Ehhez a könyvhöz e-könyv formájában jutottam hozzá. Weboldalak közül szeretném kiemelni a <https://cryptofalka.hu/> oldalt, amely segítségével bővebb, részletes információkhoz juthattam hozzá. Emellett a <https://kriptoakademia.com/> oldal is megemlíteném, ahol mindig a legfrissebb hírekről olvashatunk.

Dolgozatomba igyekeztem saját tevékenységet is hozzáadni, ezért a Bitcoin és az Ethereum értékének változását figyelem meg a dolgozatom kezdetén és a végén, valamint 2 fajta altcoin is vásároltam, hogy megnézzük azoknak is az értékváltozását. Ezeket az altcoinok 2022.05.10-én vásároltam. Az egyik a Wrapped Luna (továbbiakban: WLUNA) és a másik a Cardano (továbbiakban: ADA) volt. Mindkét kriptopénzbe 1500 forintot fektettem be, ez pontosan 0,13525238 WLUNA és 6,025559 ADA. Amikor vásároltam a WLUNA-t, aznap már az értékéből veszített 27,81%-ot, míg az ADA értéke 5,31%-kal nőtt.



ábra 1: Wrapped Luna grafikonja (2022.05.10)
Forrás: saját szerkesztés



ábra 2: Cardano grafikonja (2022.05.10.)
Forrás: saját szerkesztés

2. ELŐZMÉNYEK

A kriptovaluták előzményei egészen az 1980-as évekig nyúl vissza, amikor is a kamionsofőrök készpénz helyett újmódi okoskártyával fizették a tankolást, így a tankolás biztonságosabban, egyszerűbben és gyorsabban valósult meg. 1993-ban David Chaum, amerikai informatikus és kriptográfus feltalálta az e-cash nevű digitális fizetési rendszert. Ez a fajta digitális fizetési rendszer tökéletesen működött. Az emberek tudtak elektronikusan pennyket, ötcenteseket és tízcenteseket küldeni az interneten keresztül. Sikeres működésének ellenére a cég 5 év múlva csődbe ment. 1996-ban Douglas Jackson és Barry Downey aranyat helyeztek egy trezorba, majd létrehoztak egy weboldalt, amely segítségével az emberek az aranynak egy-egy részét tudták vásárolni. Ezt nevezték az úgynevezett e-goldnak. Ez lett az első, olyan digitális fizetőeszköz, amelyet már több millió ember használt. Később ez is csődöt mondott, mert az e-gold rendszere nem volt elég biztonságos és hackerek sikeresen fel tudták törni. 1998-ban megalakult egy olyan nemzetközi digitális rendszer, amely lehetővé tette online pénzáttalások lebonyolítását. Ez volt a PayPal. A Paypal segítségével lehetségessé vált a pénzügyi műveletek interneten való lebonyolítása. Ezt a fizetőeszközt mai napig sokan használják az interneten keresztül.

Az első tényleges kriptovaluta 2009-ben jelent meg. Ez volt a Bitcoin, amit Satoshi Nakamoto álnévű „valaki” mutatott be. A Bitcoin protokoll alapjait híres fehér könyvében, az "Egy peer-to-peer elektronikus készpénzrendszer" című tanulmányában fektette le. Néhány év elteltével szélesebb körben is ismert lett a Bitcoin.¹ [1,2]

¹ Györfi András: Kriptopénz ABC [35-36. oldal]

3. KRIPTOVALUTÁK

3.1. MI IS AZ A KRIPTOVALUTA?

A kriptovaluta olyan digitális eszköz, mely csereeszközként vagy manapság fizetőeszközként is funkcionál. Kriptográfiát² használ a tranzakciók biztonságossága érdekében. A kriptovaluták a digitális valuták egy részhalmozát képviselik, de besorolhatók az alternatív valuták vagy a virtuális valuták csoportjába is. A legtöbb kriptovaluta közös jellemzője a decentralizáció³, azaz a központi felügyelet nélküli működés, amelynek köszönhetően országhatárokon keresztül fizetőeszközként lehet használni. Az első kriptovaluta a már említett Bitcoin, amiről bővebb információt később tudhatunk meg.

A Bitcoin népszerűségének hála, ma már több száz kriptopénz jelent meg. A Bitcoinon kívül az összes kriptovalutát, amik blokkláncon futnak altcoinnak hívjuk. Jelenleg a Bitcoinon kívül több ezer (~5000) kriptovaluta létezik, de csak talán száz olyan van, aminek komolyabb értéke van technológia szinten is. A Bitcoin és alternatívái a hagyományos, centralizált bankrendszerrel szemben decentralizáltak. Kriptopénzt online tőzsdéken tudunk vásárolni, vagy ha valamit eladunk és a vevő kriptopénzzel szeretne fizetni. A kriptopénzünket árukra, szolgáltatásokra, pénznemekre (pl. euró, dollár) lehet váltani.

Felmerülhet a kérdés, hogy akkor az altcoinok átverések, úgynevezett scam⁴? Vannak olyan altcoinok (pl. Ethereum, Binance Coin), amelyek meg tudják haladni a Bitcoin értékét. Általában ezek a ténylegesen értékes projektek tartalmaznak valamilyen megoldást egy valós problémára vagy egy olyan innovációt, amelyet pozitívan áraz be a piac. A többi altcoin, amely nem tud hasonló megoldást biztosítani, azokat nevezhetjük scamnak. Ezeknél minden előfordulhat a hatalmas ígéretektől, a tőzsdei manipuláción át a szintiszta csalásokig.

Bitcoint jelenleg már csak ASIC gépekkel lehet bányászni, míg az altcoinokat főként videokártya segítségével. Néhány ismertebb altcoin: Tether, Binance Coin, Dogecoin, Shiba Inu, XRP, Dash. Az altcoinok próbálnak azokon a pontokon javítani, amelyekben a Bitcoin nem éppen a legjobb. Például az XRP rendkívül gyors tranzakciókat biztosít a felhasználó számára, a DASH pedig az anonimitásra fókuszál.

² A matematika azon ága, amely lehetővé teszi számunkra, hogy olyan matematikai bizonyításokat hozzunk létre, amelyek magas szintű biztonságot teremtenek.

³ Központosítás csökkentése, megszüntetése

⁴ Csalás, átverés

A kriptovaluta a kriptográfia eszközét használja a tranzakciók hitelesítésére. Így az elsődleges funkciója, hogy a csere eszközeként működjön egy peer-to-peer (P2P) rendszerben, ami a kriptográfia segítségével előzi meg a visszaéléseket és hamisításokat. A peer-to-peer vagy P2P paradigma lényege, hogy az informatikai hálózat végpontjai közvetlenül egymással kommunikálnak, központi kitüntetett csomópont nélkül.

A kriptovaluta és a hagyományos valuta között számos különbség van. A hagyományos fizetőeszközök bankjegyek vagy érmék, a kriptopénzeknél nincs semmilyen fizikai forma. A kereslet és a kínálat törvénye határozza meg egy kriptopénz értékét, a háttérüket a számítógépek hálózata biztosítja, amelyek minden egyes tranzakciót ellenőriznek. Hagyományos valutáknál a valutát kibocsátó kormányzatba vetett bizalom alapján tartja meg az értékét a pénz és a háttérüket a bankok vagy kormányok biztosítják. Ami közös bennük, hogy mind a kettővel lehet fizetni, de még a kriptovaluta annyira új, hogy csak ott lehet vele fizetni, ahol a kereskedők elfogadják. [2,3,4,5,6]

3.2. KRIPTOBÁNYÁSZAT

A kriptobányászat nem tartozik a legkönnyebb feladatok közé. Többfajta nehézséggel kell szembenézni, ha részt akar valaki venni egy blokklánc⁵ (4. fejezetben bővebb információ) fenntartásában. A bányászat az a folyamat, amely során a felhasználók közötti tranzakciókat ellenőrzik és hozzáadják a blokklánc nyilvános főkönyvéhez. A bányászati folyamat feladata az új érmék bevezetése a meglévő forgalomban lévő készletbe. Valamint, hogy lehetővé tegye, hogy a kriptovaluták peer-to-peer decentralizált hálózatként működjenek egy harmadik fél központi hatósága nélkül. A kriptovaluta bányászat során ezek a gépek bonyolult matematikai műveleteket oldanak meg. A bányászathoz a gépeknek nagyon erős hardverekkel kell rendelkeznie. A legtöbb kriptovaluta ún. Proof of Work mechanizmust használja a bányászáshoz. A Proof of Work (PoW) mechanizmus egy elosztott hálózatban működő kriptovaluta validációjához⁶ a tagok bármelyike bányásként algoritmusokat futtat annak érdekében, hogy hitelesítse a rendszer felhasználóinak tranzakcióit. A bányászgépek nagy számítási kapacitási igénye miatt a PoW konszenzusmechanizmus helyett egyre inkább a Proof of Stake (PoS) konszenzusmechanizmus kerül előtérbe. A PoS algoritmus a PoW alternatívájaként jött létre, hogy annak a hátrányait kiküszöbölje. A PoS algoritmussal a digitális valutát nem bonyolult matematikai feladatok megoldásával bányásszák, hanem azáltal,

⁵ A blokklánc a Bitcoin-tranzakciók nyilvános jegyzéke

⁶ Visszaigazolás; elismerésre irányuló cselekedet

hogy az adott digitális valuta előre meghatározott részét a pénztárcákban lekötve tárolják. A PoS továbbra is kriptográfiai algoritmusokat használ az érvényesítéshez, de a tranzakciókat egy kiválasztott érvényesítő hitelesíti, attól függően, hogy hány érmét birtokolnak, vagy más néven tétjüket. Már vannak olyan kriptovaluták, amelyek ezen a protokollon alapulnak: PivX, Zcoin.⁷

Korábban említettem, hogy a Bitcoint csak ASIC gépekkel lehet bányászni. Na de mik is azok az ASIC gépek? Nagy energiaigénnyel, hatalmas zajjal és hővel rendelkező gépek. Kínában konténerekben szokták elhelyezni az eszközöket, amelyeket az egész világ területén szállítani lehet. Érdekesség, hogy Monzun ideje alatt Kínában működtetik a gépeket, az alacsony áram díja miatt, míg egy szárazabb évszakban akár Norvégiáig is elviszik a konténereket. A nagy energiaigény miatt érdemesebb napelemmel üzemeltetni ezeket a gépeket. A Bitcoinbányászat évente körülbelül 80 terrawattóra (TWH) áramot fogyaszt, ami nagyjából 50 millió magyar háztartás éves energiaigényének felel meg, vagyis közel 12 Magyarországnyi háztartást lenne



ábra 3: ASIC gépek

Forrás: <https://kriptoakademia.com/2018/05/23/mi-az-a-kriptobanyaszat>

képes ellátni árammal. Ez nagyon sok áramot jelent. Mivel a bányászat egyre bonyolultabbá válik, ezért egyre komolyabb gépekre lesz szükség a jövőben. Videokártyákból általánosságban véve hiány érzékelhető. [23]

⁷ Léderer András: Kriptopénz ABC [94. oldal]

Kriptovalutát akár otthon, a saját lakásunkban is lehet bányászni. Több száz YouTube videó van arról, hogyan kell egy bányász riget⁸ megépíteni. Az egyik legfontosabb, hogy nagyon erős videokártyára lesz szükség hozzá. Minél erősebb a videokártya, annál nagyobb teljesítmény értéket tud az adott kártya elérni. Általában az otthon összebarkácsolható rigeknél, egy alaplaphoz 6-12 db videokártyát szoktak hozzákötni. Fontos az is, hogy milyen tápról működik a gép, hiszen ki kell bírnia a 24 órás terhelést több hónapon, vagy akár több éven keresztül. Az ilyen bányászgépek több millió forintba kerülnek. [7, 8, 11]

3.3. BITCOIN

Először is azt meg kell említenem, hogy a „Bitcoin” szót láthatjuk nagy- és kisbetűvel is. Ez azért van, mert ha nagybetűvel írjuk, akkor magára a technológiára utalunk. Például: „Ma a Bitcoinról tanultam.” Ha a kisbetűvel írjuk, akkor a kriptovalutáról van szó, vagy magára a mértékegységről. Például: „Ma vásároltam 5 bitcoint.” [42]

A Bitcoin (későbbiekben: BTC) egy nyílt forráskódú digitális fizetőeszköz, amelyet 2009. január 3-án egy Satoshi Nakamoto álnevű férfi, nő vagy szervezet bocsátott ki, a 2008-as amerikai bankválság kirobbanása után. Az elnevezés vonatkozik továbbá a fizetőeszközt kezelő nyílt forráskódú szoftverre, és az azzal létrehozott elosztott hálózatra is. Jelenleg (2022.03.04.) 1 BTC értéke 14.532.975 Ft.



ábra 4: Bitcoin logója
Forrás:

<https://photodune.net/item/bit-coin-physical-bit-coin-digital-currency-cryptocurrency-golden-coin-with-bitcoin-symbol/21888358>

Satoshi Nakamoto saját bevallása szerint 2007-ben kezdte a munkát a BTC protokollon⁹. 2008 októberében közzétette az elektronikus készpénzrendszer működését bemutató fehér könyvet, majd 2009-ben elindította a BTC első verzióját, majd egy levelezőlistán együtt dolgozott egy fejlesztőcsapattal a tökéletesítésén. Figyelt arra, hogy semmi olyan dolog ne derüljön ki róla, ami által beazonosítható lenne a személye. A mai napig nem tudjuk, hogy kicsoda Satoshi Nakamoto. A satoshi japánul bölcset jelent, a nakamoto pedig egy gyakori családnév, amelynek egyik jelentése eredet. Azonban nincsenek róla információk, hogy nő, férfi vagy esetleg egy szervezet lenne. Joshua Davis, a The New Yorker újságírója szerint Nakamoto valódi neve Michael Clear, kriptográfiát hallgató diák a dublini Trinity College-ben. Mások véleménye szerint Satoshi Nakamoto valójában Martti Malmi, aki a

⁸ Asztali számítógép. Különösen az egyedi építésű számítógépet értjük alatta

⁹ Olyan alapvető szabályrendszerek, amelyek lehetővé teszik az adatok megosztását a számítógépek között.

kezdetektől a felhasználói felület programozásában vett részt. Ezen kívül még sok feltételezés van, de amit biztosan tudunk róla, hogy nagy alaposággal építette fel a BTC rendszerét és nem hajtott végre kockázatos teszteléseket. Utolsó információ róla egy 2011-es email, amit egy fejlesztőnek küldött: “Továbbléptem. Jó kezekben lesz Gavinnél és a többiekénél.” Valószínűsíthető, hogy titokban szerette volna tartani a személyét, ezzel azt sugallni, hogy amit létrehozott az a fontos, és nem, aki létrehozta. [10, 12]

A BTC-nak számos előnye van:

- A hálózat decentralizálásának köszönhetően már nincs szükség közvetítőkre, mint például bankokra
- A nemzetközi pénzáttalások gyorsabbak és olcsóbbak, mint a hagyományos banki szolgáltatások
- A többi kriptovalutához képest a BTC rendelkezik a legmagasabb likviditással

Azonban van hátránya is:

- Kevés helyen lehet BTC-nal fizetni
- Deflációs jellegű pénznem
- Az árfolyama nagyon ingadozó [16,17]

Satoshi Nakamoto kikötötte, hogy a BTC-ből maximum 21 millió érme létezzen. Körülbelül 10 percenként mindig egy újabb BTC-t bocsátanak ki. Ha a kereslet nő az autók iránt, akkor a gyártó növelheti a termelést, hogy megfeleljen a keresletnek. A BTC-ban a kínálat ilyen formán nem növelhető, és nem változhat, ezért a kereslet és az ár szorosabban kötődik, mint bármely más iparág vagy eszközosztály. A 21 millió BTC-nak azonban a 90 százalékát már kitermelték a kriptobányászok. A szakértők úgy vélik, hogy az utolsó BTC-t 2140 körül fogják kitermelni. Innentől kezdve a forgalomban lévő BTC-ok száma már nem fog változni. Jelenleg (2022.03.07.) a forgalomban levő BTC-ok száma: 18.977.000 BTC. Vélhetően a 21 milliós szám korábban lesz elérve, mint 2140. Az elemzők úgy látják, ehhez a BTC-os gazdaságnak is muszáj lesz változnia, például azzal, hogy a 21 milliós limitet kibővítik. Ez azonban csökkentheti a már kibányászott BTC-ok értékét. [14]

Az első tranzakció már 2009-ben megtörtént, amikor egy finn fejlesztő 5.050 BTC-t vásárolt 5 dollárért. Ez az 5.050 BTC 2022-ben már több, mint 140 millió dollárnak felel meg. Egy évvel

később, 2010-ben pedig sor került az első termékvásárlásra BTC-nal. Egy magyar származású, floridai férfi, úgynevezett Laszlo Hanyecz 2 darab pizzát vásárolt 10.000 BTC értékért. [22]

Több városban, vagy országban már törvényes fizetőeszköz a BTC. A városok, országok lakói így a különböző adókat tudják BTC-nal fizetni. 2021 júniusában El Salvador, Közép -Amerika országa lett az első ország, amely elfogadta a Bitcoint törvényes fizetőeszközként. Ezen kívül több száz légitársaságnál és Mol kutaknál is elfogadják a BTC-t, mint fizetőeszközt. Egyre több helyen létezik már BTC automata. Ez ugyanúgy néz ki, mint a hagyományos ATM-ek, annyi különbséggel, hogy itt csak BTC-t vásárolni és eladni tudunk. Ilyen típusú valutaváltókból Magyarországon 28 helyen található, ebből 16 Budapesten, 12 pedig vidéki városokban. [9, 13, 15, 38, 40]

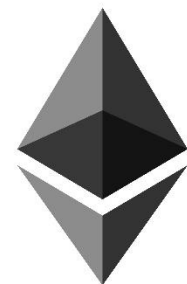


ábra 5: Bitcoin automata Budapesten
Forrás:

<https://www.hungarybudapestguide.com/can-i-pay-with-bitcoin-in-budapest/>

3.4. ETHEREUM

2013-ban jelent meg az Ethereumról (későbbiekben: ETH) szóló fehér könyv, amelyet az egyik alapító, az orosz származású Vitalik Buterin készített. Ebben bemutatta egy nyílt forráskódú, blokklánc alapú számítógépes platform ötletét, amely képes okosszerződések futtatására. Ez olyan alkalmazások futtatását jelentené a gyakorlatban, amely decentralizált módon bármilyen egyéb közvetítő harmadik fél jelenléte nélkül valósulna meg, kiküszöbölve visszaélések, rendszerhibák és egyéb problémák létrejöttét. Az ETH tehát nem csak egy kriptopénz, hanem egy olyan platform is, aminek segítségével különböző alkalmazások készülhetnek a blokkláncra. Jelenleg (2022.03.04.) 1 ETH értéke 963.976,83 Ft.



ábra 6: Ethereum logója
Forrás:

<https://ethereum.org/en/assets/>

Az ETH előnyei:

- **Turing képes:** Játékokat és sok másféle programot is beágyazhatunk a hálózatba
- **Okosszerződések:** Az okosszerződéseknek hála képesek vagyunk automatizált utalásokra, feltételes utalásokra, protokollok kiépítésére is.

- **Közösségi finanszírozás:** Ha például küldünk egy ICO-nak¹⁰ pénzt és cserébe akarják adni az ERC-20¹¹ tokeneket, akkor automatikusan meg fogjuk kapni visszautalásként az adott tokeneket.

Az Ether (ETH) az Ethereum blokkláncon használatos digitális fizetőeszköz. Második generációs kriptovalutaként emlegetik, mivel a BTC-hoz hasonlóan Proof of Work algoritmuson futó bányászgépek decentralizált hálózata bonyolítja a tranzakciókat közvetlenül az ETH címek között.

Az ETH lehetővé teszi a fejlesztők számára, hogy létrehozzanak okoszerződéseket, vagy kibocsátanak saját kriptovalutát az ETH blokkláncát használva, anélkül, hogy saját blokkláncot hoznának létre. Az ETH blokkláncán elkészült okoszerződések az ETH Virtual Machine (EVM) elnevezésű virtuális gépre épülnek. EVM a protokollnak az a része, amelyik ténylegesen végrehajtja ezeket a szerződéseket, mindezt az önkéntesen üzemelő, public node-ok¹² nemzetközi hálózatának köszönhetően. A szkriptek vagy okoszerződések egy új programozási nyelvben, a Solidity-ben készülnek.

2016-ban elkészült az első tervezet a „The DAO” projektre és el is kezdődött a közösségi finanszírozás az ETH hálózatán. A DAO lényege egy olyan szervezet lett volna, ami képes szavazások útján az önfejlesztésre, költség allokálásra és egyéb projektek közösségi finanszírozására. A The DAO-t magát a résztvevők irányították volna centrális behatás nélkül minden országtól függetlenül. Végül elkészült a The DAO okoszerződés és a közösségi finanszírozás globális rekordokat döntött, mivel sikeresen összegyűjtött 150 millió dollárt ETH-ban. 2016 júniusában aztán a The DAO-ban tárolt Etherek 1/3-át sikerült egy hackernek ellopnia (ez volt a *Dao Hack*) egy, a projektre írt okoszerződés biztonsági rését kihasználva. Végül 2017 júliusában úgy döntöttek az ETH fejlesztők, hogy elindítanak egy hard forkot, aminek a lényege az, hogy semmissé teszik magát a The DAO okoszerződését és visszarakják a pénzt a felhasználók számlájára. Miután az ETH blockchain hard forkolt és átírta a láncot, létrejött az **Ethereum Classic** egy független fejlesztői brigáddal, akik tovább vitték az eredeti láncot és hagyták a hackernek, hogy elvigye azt, ami “járt neki” az okoszerződés szerint. Az

¹⁰ Initial Coin Offering

¹¹ Ethereum Request for Comments 20

¹² Nonprofit, nyílt tagsággal rendelkező szervezet

Ethereum Classic, mint a hard fork eredménye a mai napig létezik és más az ETH-tól eltérő fejlesztési logikával közelít a különféle problémák felé. [18]

Az ETH rendelkezik a legnagyobb fejlesztő gárdával világszerte, piaci kapitalizációt tekintve pedig a második legnagyobb kriptovaluta 2016 óta a BTC mögött.

ETH alkalmazási lehetőségei:

- **Digitális azonosítás:** a blokkláncon létrehozott adat megváltoztathatatlan, így nem hamisítható kívülállók által (pl. jogosítvány, internetes szavazás eredménye)
- **Tokenizálás¹³:** A digitális tokeneket sokkal egyszerűbb, olcsóbb és gyorsabb átruházni másra, mint bármi mást, mert fizikailag nem kell szállítani, nem kell az ügyletbe bevonni (és kifizetni) lebonyolító harmadik felet és nem vonatkoznak rá hatósági szabályozások
- **Adattárolás:** a blokklánc fizikailag megosztott jellegéből fakadóan az adatokat a bányászgépek hálózatán tárolja. A technológiára jellemző programozhatóság miatt a titkosítás és egyetlen privát kulccsal való visszafejtés csökkenti az adatvesztés és illetéktelen hozzáférés lehetőségét
- **Egyéb területek:** választások, egészségügyi applikációk, szerencsejáték

A legfrissebb hírek szerint az ETH bányászata hónapokon belül megszűnhet. Pár hónapon belül sor kerülhet a kriptopénzek történelmének egyik legfontosabb eseményére, az ETH 2.0 indulására. A Merge, vagyis összeolvadás során az ETH bányagépekkel történő proof-of-work bányászata örökre véget ér. A hálózat biztonságát ezt követően a Proof-of-Stake konszenzus fogja biztosítani. [19, 20, 21, 22, 39]

3.5. HATÁSUK A GAZDASÁGRA

A BTC számos jó tulajdonsága mellett a gazdaságra is gyakorol hatásokat. A kriptopénzek egyre nagyobb törést okozhatnak a globális pénzrendszerekben, olcsóbbá és gyorsabbá teszik a pénzmozgásokat, ezzel pedig segítik és javítják az egész globális gazdaság működését. Negatív hatásuk, hogy az anonimitáson keresztül segítik a pénzmosást, könnyebbé tehetik a terrorizmus finanszírozását és a legkülönfélébb illegális tevékenységeket. A kriptopénzek tömeges

¹³ A tokenizáció az a folyamat, amelynek során az érzékeny adatainkat kicseréljük egy algoritmus által generált számra, vagyis tokenre.

elterjedése után a központi bank többé nem tud arról dönteni, hogy mennyi pénz mozog a gazdaságban, mert egy-egy kriptopénz maximális mennyisége előre meghatározott. Ennél többet nem lehet előállítani. Ha a kriptopénzek teljesen kiszorítják a hagyományos pénzeket, akkor az állam elveszítheti a beleszólását egy alapvető gazdasági kérdésbe. Tulajdonképpen az állam semmilyen kontrollal nem rendelkezhet a kriptopénzek felett, ezzel a hatalom az egyik kulcseszközét veszíti el.¹⁴

A Bitcoinbányászok nagy teljesítményű számítógépeket használnak a blokkláncon történő tranzakciók feldolgozása és a hálózat biztonsága érdekében, cserébe megkapják a hően áhított BTC-t. Ez nagyon energiaigényes folyamat, így az elmúlt években a BTC árának emelkedésével és népszerűségének növekedésével még tovább nőtt a környezetre gyakorolt hatása. A Greenpeace és a Környezetvédelmi Munkacsoport amerikai aktivistacsoport által vezetett kampány arra kérte meg a BTC-os közösséget, hogy térjen el az eddig használatos úgynevezett proof-of-worknek nevezett munkabizonyításról, úgynevezett proof-of-stake-re, azaz tétbizonyításra. A proof-of-stake lehetővé teszi, hogy a hálózatok lényegesen alacsonyabb erőforrás-fogyasztással működjenek. Ettől függetlenül mindkét konszenzusmechanizmusnak vannak olyan gazdasági következményei, amelyek büntetik a hálózati zavarokat és megghiúsítják a rosszindulatú szereplőket.

Nem csak a BTC okozhat hatásokat, hanem fordítva is előfordul. Különböző események folyásolhatják be a BTC árfolyamát. A kínai holdújév negatív hatással van a BTC-ra. Kína legnagyobb ünnepén készpénzzel szokták az emberek egymást ajándékozni, amit BTC eladásokból szoktak finanszírozni. [25, 35]

¹⁴ Györfi András: Kriptopénz ABC [162. oldal]

4. BLOKKLÁNC

Az első blokklánc-szerű protokollt David Chaum kriptográfus javasolta 1982-ben. Később, 1991-ben Stuart Haber és W. Scott Stornetta írt a konzorciumokkal kapcsolatos munkájukról. Satoshi Nakamoto volt az, aki feltalálta és megvalósította az első blokklánc-hálózatot a világ első digitális valutájának, a BTC-nak.

Úgy kell elképzelni ezt a blokkláncot, hogy bank nélkül tudunk pénzt küldeni másnak. Így az elküldött összeget pár másodpercen megkapja a másik fél. A blokklánc (angolul: blockchain) egy olyan adatbázis, amelyben adatokat tárolhatunk, és amelyen keresztül mozgathatjuk őket. A benne történő tranzakciók minden csomópont részére elérhetőek, láthatóak. Eredetileg a kriptovaluták használatához lett kitalálva, és a BTC-nal kezdődött meg a használata. Több nagyvállalatnál már alkalmazzák a blokkláncot: Visa, Pfizer, Ford, Shell. A blokklánc-hálózattal kapcsolatos hibalehetőség rendkívül alacsony. Mivel az emberek nem vesznek részt az egyes tranzakciókban, kisebb az esély a hibákra. A blokklánc technológia átláthatóságot biztosít, mivel minden tranzakciót a számítógépek hálózatán dokumentálnak. Azonban a BTC tranzakciók feldolgozása sokkal lassabb, mint a szokásos hitelkártya-társaság. Míg a BTC másodpercenként hét egyedi tranzakciót tud feldolgozni, a Visa 24 000-et. Nagy potenciállal rendelkező befektetési lehetőségnek tekintik a blokkláncot, ami más alkalmazások előtt is kaput nyit: ingatlan értékesítés, jogi szerződések.

A Blokkláncoknak négy típusa van:

- **Nyilvános blokkláncok:** A nyilvános blokkláncok a számítógépek nyílt, decentralizált hálózatai, amelyekhez bárki hozzáférhet, aki tranzakciót kérni vagy érvényesíteni szeretne
- **Privát blokkláncok:** A privát blokkláncok nem nyitottak, hozzáférési korlátozásokkal rendelkeznek. Azok, akik csatlakozni szeretnének, engedélyt kérnek a rendszergazdától.
- **Hibrid blokkláncok:** Nyilvános és privát blokkláncok kombinációi, amelyek központosított és decentralizált funkciókat tartalmaznak
- **Oldalláncok:** Az oldallánc a főlánccal párhuzamosan futó blokklánc. Lehetővé teszi a felhasználók számára a digitális eszközök mozgását két különböző blokklánc között, és javítja a méretezhetőséget és a hatékonyságot.

A blokklánc a BTC legfőbb technológiai újítása, amely nyilvános főkönyvként működik, ugyanis tartalmazza a mindenkori összes BTC-tranzakciót.

A BTC elosztott főkönyvének blokkjai minden esetben tartalmazza az előző blokk kriptográfia segítségével titkosított hash-ét, egy timestamp-et (időbélyeg), és a tranzakciós adatokat.[29]

4.1. MŰKÖDÉSE

A hálózat több ezer csomópontot tartalmaz a világon, amelyek minden műveletet ellenőriznek és megerősítenek. A csomópontok ezt egy sor számítógépes algoritmuson keresztül teszik meg, amelyeket BTC bányászatnak is neveznek. A tranzakció blokklánc-kriptográfiájának ellenőrzése után az eladás új blokkként kerül az elosztott főkönyvbe. Az eladás hivatalosan akkor fejeződik be, amikor a blokk hozzákapcsolódik az előző BTC-tranzakcióblokkhoz. [36]

A BTC és az ETH hálózatok nyilvános, decentralizált peer-to-peer hálózatok saját tokenekkel: BTC-okkal és éterrel. Mindkettő kriptográfiára támaszkodik, és mindkettő digitális főkönyvi technológiát használ. De jelentősen különböznek a céljuktól és a képességeiktől. A BTC egy decentralizált fizetési rendszer és értéktároló. A blokklánc az összes BTC tranzakció adatbázisa, és nyomon követi azok tulajdonjogát. Az ETH több mint egy fizetési rendszer, és lehetővé teszi, hogy intelligens szerződéseket és alkalmazásokat építsenek rá, így ez egy esztétikusabb blokklánc. [26, 29, 30, 41]

A blokkláncot úgy szoktuk elképzelni, mint az egymás tetejére pakolt építőköveket. Minden egyes kocka, egy blokkot szimbolizál, amiben a tranzakciók vannak. Most egy BTC átutalást nézünk meg, hogy megy végbe az egyik pénztárcáról a másikba. A BTC blokklánc jelenleg (2022.05.02.) 734.551 blokk magas, ezt egész pontosan 2022. május másodikán, 10:42-kor bányászták ki. Az elosztott hálózatok csomópontjaiban lévő számítógépek mindegyike leellenőrizte a blokkot, majd csatolta a saját nyilvántartásában vezetett blokklánc 734.550-ik blokkjához. Ezzel a művelettel mindenkinél egy blokkal magasabb lett a blokklánc, és természetesen mindenkinél ugyanakkora magas lett. A bányászgépek között azonnal megindul a verseny a következő 734552-ik blokk kibányászásáért. Ez úgy történik, hogy mindegyik számítógép elkészíti a saját blokkját, amibe összegyűjtik az elmúlt 10 perc tranzakcióit. Az első tranzakció, amit a blokkba kell foglalniuk, mindig a coinbase tranzakció, ami az újonnan generált coinokat jelenti. A tranzakciókat körbe küldik a hálózaton, ahol a full node-ok (csomópontok, számítógépek) leellenőrzik őket különböző szempontok alapján, majd, amik megfeleltek, tovább küldik a többi full node-nak ellenőrzésre. [36]

4.2. A HASH¹⁵ ALGORITMUS

A hash függvények olyan informatikában használt eljárások, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Ezek az algoritmusok az 1980-as évek legvégén az elektronikus aláírás megjelenésével váltak szükségessé. A hash függvények, elsősorban a tároló technikában már az 1950-es évek elején megjelentek. Amennyiben a bemeneti oldalon megváltoztatunk akár egyetlen karaktert is, a kimeneti oldalon a hash értéke teljesen megváltozik. Ezt a változást az alábbi táblázatban szemléltetem egy online hash generátor (SHA256 Hash Generator - <https://passwordsgenerator.net/sha256-hash-generator/>) segítségével: [27]

Bemeneti oldal	Kimeneti oldal
Vettem 3 bitcoin	4CDD26EDB1DA4DCA549515733E19392FDFE88372722B1B3A287BEAE8ED7D38CD
Vettem 4 bitcoin	ED49C3D6EB47E988EED68DAA41DF771510C6B7B80DD4E86E36FCE94928213253
Vett 3 bitcoin	EEF6CFC7C6DB95A45298035CCA56CC116B587B74FD5A1BA2D631CE0571D24B03
Vett 3 bitcoin.	BB77E866B391E1E5BDE854E28A6BF25F93614B1C77DF56984ABCDD05E2D273DF

*táblázat 1: Hash-függvény
Forrás: Saját szerkesztés*

Látható, hogy egyetlen karakter megváltoztatásával az egész kimenet megváltozik. Ez egyébként egy plusz szóköz lenyomására is igaz. Ezt a fajta hash generátort használja a BTC is. A hash függvény egy stringet ad eredményül minden esetben. A string számok és betűk, különböző egyszerű objektumok, leggyakrabban karakterek sorozata.

Tegyük fel, hogy egy blokk tartalmazza a fent említett példában az első tranzakciót. 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 hashnek egy bizonyos része hogyan kell, hogy kinézzen. Mivel a hash kimenetele nagyon bonyolult, ezért a bányásznak próbálkozni kell, hogy mi az a szám, 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. Ha valaki az egyik blokkban egy tranzakciót módosítani szeretne, akkor az összes többi blokk hash-ét is meg kellene változtatnia, így biztosítva van a felülírhatatlanság.

¹⁵ A hash-függvény által generált string

5. AZ OKOSSZERZŐDÉSEK

Az ETH egyik legfontosabb újítása az okosszerződések voltak. Az okosszerződés (smart contract) egy olyan blokkláncon futó program, amelyeknél a szerződéskötéshez szükséges feltételek teljesülésekor az ügylet automatikusan létrejön, így például az eladó azonnal megkapja a pénzt, a vevő pedig a szolgáltatást. Az okosszerződést úgy kell elképzelni, mint egy szoftveres kóddá alakított szerződést, ahol a szerződésben szereplő feltételek teljesülése esetén a program automatikusan érvényesíti, vagy lefuttatja a meghatározott forgatókönyvet. Előre



ábra 7: Okosszerződés

Forrás: <https://www.pwdconsulting.hu/hu/publikaciok/az-okosszerzodesek-jogi-kerdesei/>

kódolt utasításoknak köszönhetően az adott esemény bekövetkezésekor automatikusan végrehajtásra kerülnek. Külön sajátossága, hogy a szerződésben foglalt kikötéseket nem lehet utólag átírni, vagy módosítani. Lehetővé teszik, hogy gyakorlatilag bármilyen érték gazdát cseréljen, legyen az pénz, részvény, ingatlan, autó. Legnagyobb előnye, hogy nem szükséges köztes, harmadik fél ahhoz, hogy megkössünk egy szerződést. Nincsen szükség ügyvédekre, sem a szerződés megkötésekor, sem az utólagos bírálatokkor. Röviden tehát olyan szerződések, amelyek előre programozva vannak, ezáltal a szerződések automatikusan megtörténnek.

Az okosszerződések két típusát különböztetjük meg: determinisztikus és nondeterminisztikus.

Előnyei:

- **Biztonság:** A rendszer mögött álló nyilvántartás védett az utólagos beavatkozások ellen. A megtörtént tranzakciót nem lehet módosítani
- **Gyorsaság:** A legtöbb folyamat automatizált és nincs szükség közvetítőkre (pl. ügyvéd, bank)
- **Átláthatóság:** A szerződésben rögzítettek minden fél által láthatók, előre rögzítettek és jóváhagyottak

Hátrányai:

- **Emberi tényező:** A kódot az emberek írják, és hibákat követhetnek el
- **Jogállás:** Az okosszerződéseket egyetlen kormány sem szabályozza [38, 41]

Szükség van az okosszerződéseknél az aláírókra, akik között a megállapodás történik. Az okosszerződéseknél kell lennie tárgynak, mint minden hagyományos, papír alapú szerződésnél, például: Autóvásárlás. Továbbá szükség lesz a megállapodás pontos, számszerűsített részletei: ezeket az okosszerződések programnyelvén kell meghatározni, valamint minden érintett félre vonatkozóan tartalmazniuk kell a pontos jutalmakat és büntetéseket is.

5.1. MŰKÖDÉSÜK

Az okosszerződések leegyszerűsítve olyanok, mint az automaták. Bedobjuk a szükséges kriptopénz mennyiséget és az escrowba¹⁶ helyezendő letétet, majd megkapjuk például egy ingatlan tulajdonjogát. Egy okosszerződés működhet önállóan, vagy akár más okosszerződésekkel összefüggésben is, például úgy, hogy az egyik okosszerződés teljesülése automatikusan elindítja a következőt. [40]

Egy okosszerződés létrehozásához öt dologra lesz szükségünk. Először is egy decentralizált blokkláncra, mint például az ETH. Szükség lesz egy programnyelvre, amivel az adatokat tudjuk rögzíteni, például: Solidity. Szerződés tárgyára. Meg kell határoznunk és a programban hozzáférést kell biztosítanunk a szerződésben rögzített eszközhöz, hogy azokat egy előre meghatározott időpontban automatikusan feloldja, vagy lezárja. Szerződési feltételekre. Rögzítenünk kell a szükséges adatokat, a szerződési feltételeket, illetve a műveletek és

¹⁶ Harmadik személynél letett okirat

események pontos sorrendjét. Digitális aláírásokra. A saját titkos kulcsával a szerződés összes szereplőjének alá kell írnia az okosszerződést.

Az elektronikus aláírásnak köszönhetően ma már papír és toll használata nélkül is lehet bizonyító erejű dokumentumokat létrehozni. Volt szerencsém már szerződést digitálisan aláírni. Véleményem szerint nagyon gyors és egyszerű folyamat. A digitális aláírás helyszíntől és időponttól független, akár mobiltelefonon is megvalósítható. Az aláírás 100% hiteles és megfelel a magyar és az EU jogszabályoknak. Megszünteti a nehézkes papíralapú folyamatokat és csökkenti a költségeket. A hagyományos aláírásokat könnyen lehet hamisítani, ezért célszerűbb a digitális aláírás. A digitális aláírás tartalmaz egy ellenőrző összeget, ezáltal biztosítva van az, hogy az aláírás nem vihető át egy másik dokumentumra.

Egyelőre még távol vagyunk attól, hogy okosszerződésekkel teljesen kiváltunk egy ügyvéd munkáját, de néhány év múlva bekövetkezhet. Nagyon új technológiáról van szó, így, ha előfordulna véletlenül egy szoftveres hiba, akkor a hackerek könnyen és gyorsan kihasználnák azt. Így egy ingatlan adásvételét vagy egy cégek közötti megállapodást akár teljesen tönkre tehet egy hackertámadás. Az USA-ban már van néhány olyan állam, ami elismeri az okosszerződéseket, azonban nem egyszerű az általános elfogadásukhoz vezető út.

5.2. FELHASZNÁLÁSUK

Az okosszerződések felhasználási területei közé tartozik az ingatlan adás-vétel. Egy ingatlan eladási folyamat rengeteg papírmunkával jár és több féllel való kommunikációt igényel. Az ingatlan-nyilvántartás például Svédországban hamarosan a blokklánc technológiára épül. Így a hagyományos szerződéskötési folyamat helyett egyszerűbb megítélésű esetekben elegendő lehet egy megfelelően elkészített okosszerződés, amely kizárólag abban az esetben rendelkezik a vevő tulajdonjogának bejegyzéséről, amennyiben az eladó az előzetesen meghatározott vételárat megfizette az okosszerződésen keresztül. Az ingatlanközvetítő, az ügyvéd, a közjegyző, a földhivatal stb. által végrehajtott összes tevékenység kódolható az okosszerződésbe, így jelentős mennyiségű pénz takarítható meg mind a vevő, mind az eladó részéről.

Az okosszerződések a káresemények ellenőrzését és kárkifizetések teljesítését is meggyorsíthatják: egy repülőjárat késése esetén közvetlen, a biztosító automatizált kárrendezést nyújt a biztosított személynek. Például, ha egy járat több órát késne, a biztosító igénybejelentése nélkül, azonnal teljesítve lesz a kártérítés. Ha összetörünk egy autót, a

biztosító a blokklánc technológia segítségével azonnali értesül a káreseményről. Ha a járművet a biztosító által kijelölt és ellenőrzött műhelyben megszerelték annak költségét azonnal kifizeti a biztosítottnak.

Munkaszerződéseknél is fontos lehet az okoszerződések használata. Ha bármelyik fél nem felel meg a szerződésben foglalt feltételeknek, akkor valamelyik fél részéről bizalomvesztés következik be. Egy megfelelően kódolt okoszerződés ezt képes megoldani. Ez akár javítja a munkavállalói-munkaadói kapcsolatot. Ezen túlmenően az okoszerződésben a bérkifizetések is rögzítésre kerülhetnek, annak érdekében, hogy az alkalmazott meghatározott időszakonként automatikusan megkapja a bérét. Egy Japán szállítmányozási cég már egy ideje dolgozik saját tokenjén, amelyben kifizetné az alkalmazottjait, akiket világszerte foglalkoztatnak.

5.3. BLOKKLÁNC ORÁKULUMOK

Az okoszerződések végrehajtásához szükség van külső adatokra. Ezeket az ún. blokklánc orákulumok biztosítják az okoszerződések számára.

Az orákulumoknak több típusai vannak, különféle felhasználásra. Ezek közül három fajtát szeretnék kiemelni. Az első a **szoftveres orákulum**, amely online információkat szolgáltat, az adatokat online forrásból szerez. Ilyenek például a kereskedési oldalak, céges oldalak, híroldalak. Az interneten sok szolgáltatás megtalálható, ezért rengeteg cég használja már fő működési eszközeként. A következő a **hardveres orákulum**. Ha tudni szeretnénk, hogy egy adott jármű mikor éri el a célpontot, akkor az adatokat ez a típusú orákulum szolgáltatja. Emellett előfordulnak az ellátási láncok követésénél is, mivel az ilyen orákulumok tudják megerősíteni azokat az adatokat, melyek arra vonatkoznak, hogy adott időpontban, helyen, távolságban, hőmérsékleten mi történt. A harmadik orákulum a **konszenzus alapú orákulum**. Egyszerre több forrásból szerez adatokat, és azokat összeveti, adott esetben átlagolja.

Ez az orákulum két összetevőből áll. A láncon belüli orákulum (intelligens szerződés) és a láncon kívüli orákulum szolgáltatás (node.js szerver). A láncon belüli orákulum egy intelligens szerződés, amelynek nyilvános funkciója van (createRequest), amely megkapja a lekérdezendő URL-t és a lekérni kívánt attribútumot. Ezután elindít egy eseményt, hogy figyelmeztesse a láncon kívüli jóslatot egy új kérésre. A láncon kívüli orákulum több, különböző felek által telepített node.js szolgáltatásból áll, amelyek lekérdezik az API-t, és visszaküldik a szerződéshez a választ.

Az Oracle szerződést a megállapodás szerinti feltételekkel határozzuk meg: Minimum Quorum és Total Oracles. [28]

Felmerülhet az a kérdés, hogy mennyire lehet megbízni az orákulumokban. Egy centralizált, külső blokklánc orákulum egészen más megbízhatósági szintet kínál, mint egy decentralizált változat. A bizalom szempontjából az úgynevezett konszenzus-alapú orákulumok teljesítenek a legjobban. Mivel ahelyett, hogy egyetlen adatforrásra építkeznének, vagy egyetlen orákulumtól várnánk a pontos adatokat folyamatos jelleggel (miközben a valóságban előfordulhatnak pontatlanságok, hibák, kiesések), ezek decentralizált módon sok adatforrást használnak. Szerencsére most már több ilyen decentralizált orákulum megoldás is működik.

Az előrejelzési piacok, mint például az Augur, decentralizált orákulumokat használ ahhoz, hogy adatokat szerezzen a hálózatba. Az Augur esetében a felhasználó létrehoz egy előrejelzési piacot egy kérdéssel, például egy focimeccs eredményével kapcsolatban. Más Augur felhasználók piaci részesedést szereznek ebből. A piac létrehozója kiválaszt egy orákulumot ahhoz, hogy adatot szerezzen az általa feltett kérdés eldöntéséhez. [31, 32, 33, 34, 37]

6. ÖSSZEGZÉS

Érdekességképpen a mai napon is (2022.05.10.) utánanézttem összehasonlítás miatt a BTC és az ETH értékét. 2022. március 4-én, 1 BTC 14.532.975 forint volt. Jelenleg (2022.05.10.) 1 BTC 11.377.737,15 forint. Ez idén a BTC mélypontja és az eddigi legnagyobb zuhanása. Tavaly július óta nem volt ilyen olcsó. Most fele annyit ér, mint hat hónappal ezelőtt, amikor csúcson volt. 2022. március 4-én 1 ETH 963.976,83 forint volt. Mai napon (2022.05.10.) 1 ETH 865.051,35 forint. BTC-hoz hasonlóan, itt is csökkent az értéke az ETH-nak. Az alábbi két képen látható a BTC-t és az ETH áringadozása forintban az elmúlt fél évben: [24]



ábra 8: Bitcoin grafikonja (2022.05.10)

Forrás: https://www.google.com/finance/quote/BTC-HUF?sa=X&ved=2ahUKEwjXl8r5q_33AhWkiv0HHXvzCjEQ-fUHegQIChAX



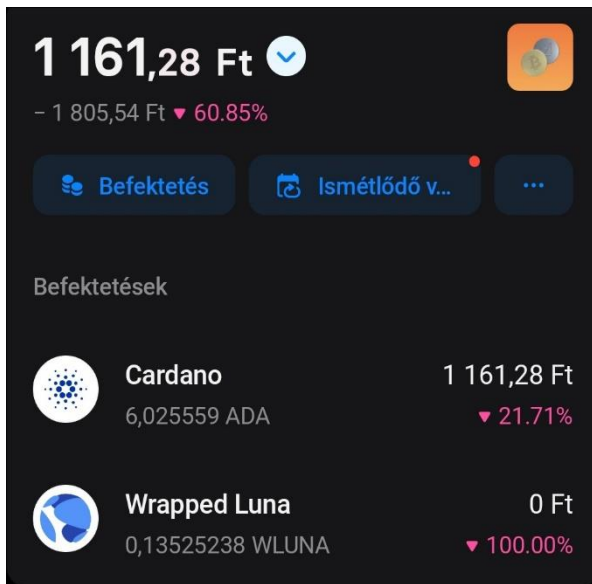
ábra 9: Ethereum grafikonja (2022.05.10.)

Forrás: https://www.google.com/finance/quote/ETH-HUF?sa=X&ved=2ahUKEwjJ9ZzKr_33AhVnhP0HHT8QCKoQ-fUHegQIBRAX

Az olvasható le az ábrákról mindkét esetben, hogy jelentősen csökkent az értékük mind a kettő coinnak. Hat hónappal ezelőtti értékhez nézve a BTC 44,67%-kal lett olcsóbb, az ETH pedig 40,99%-kal. A két ábrán is nagyon jól látható, az említett ingadozó árfolyamuk. Amit még észrevehetünk a grafikonon, hogy nagyjából az áringadozásuk hasonlónak mondható. Ez egyébként elmondható minden altcoinról is, hogy nagyon hasonló mértékben csökken vagy éppen növekszik az értékük.

A dolgozatom elején említett WLUNA és ADA értéke jelentősen értékét veszítette. A WLUNA elvesztette értéke 100%-át, ami annyit jelent, hogy az általam vásárolt 0,13525238 WLUNA értéke 0 forint. A ADA 21,71%-ot veszített az értékéből. Itt nem annyira tragikus az eredmény. A megvásárolt 6,025559 ADA, jelenleg 1161,28 forintot jelent. Ez azt jelenti, hogy közel két hét alatt nem sikerült profitálnom. A befektetett 3.000 forint 60,85%-a elveszett. Egy olyan alkalom volt mikor profitom volt, ez az alábbi grafikonon is látható lesz. Ez aznap volt mikor megvásároltam a kriptopénzeket, de pár órán belül már veszítettek az értékükből és vesztséges lett. Összességében az tudom mondani, hogy nem érdemes, olyan kriptopénzeket venni, amelyek pár száz forintba kerülnek, mert előfordulhat, hogy csak scam. Nem gondolom, hogy mind a kettő altcoin scam lenne, egyszerűen csak nem volt szerencsém, nem sikerült ennyi idő alatt profitálnom, de úgy gondolom, hogy nagyobb profit eléréséhez nem is két hét kell, hanem több hónapok. Lehetséges, hogy az ADA értéke még akár mikor megemelkedhet, ezt nem tudni

előre. Ami mindenképp érdekes volt ettől függetlenül, hogy a WLUNA vásárlása után pár órán belül, szépen, lassan elvesztette a teljes értékét.



ábra 10: A WLUNA és az ADA 10 nap utáni eredménye (2022.05.20.)
Forrás: saját szerkesztés



ábra 11: WLUNA és az ADA nyereség/veszteség grafikonja (2022.05.20.)
Forrás: saját szerkesztés

7. IRODALOMJEGYZÉK

Szakkönyvek:

Kriptopénz ABC (Györfi András - Léderer András - Paluska Ferenc - Pataki Gábor - Trinh Anh Tuan)

Internetes források:

[1] Napkelepce: A kriptovaluta története [online]. – Megjelent: <http://napkelepce.hu/>

[Megtekintés dátuma: 2022.03.03.]. – Hozzáférés: <http://napkelepce.hu/capricoin/a-kriptovaluta-tortenete/>

[2] Wikipédia: Kriptovaluta [online]. – Megjelent: <https://hu.wikipedia.org/> [Megtekintés dátuma: 2022.03.03.]. – Hozzáférés: <https://hu.wikipedia.org/wiki/Kriptovaluta>

[3] Cryptofalka: MI AZ AZ ALTCOIN? [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.03.]. – Hozzáférés: https://cryptofalka.hu/mi_az_az_altcoin/

[4] Kriptomat: Mi az a kriptovaluta és hogyan működik? [online]. – Megjelent: <https://kriptomat.io/> [Megtekintés dátuma: 2022.03.03.] Hozzáférés: <https://kriptomat.io/hu/kriptovalutak/mi-az-a-kriptovaluta/>

[5] Árpási Zoltán: KRIPTOVALUTA, A JÖVŐ PÉNZE VAGY EGY MEGFOGHATATLAN VAGYONTÁRGY? [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.03.] Hozzáférés: <https://cryptofalka.hu/kriptovaluta-a-jovo-penze/>

[6] Wikipédia: Peer-to-peer [online]. – Megjelent: <https://hu.wikipedia.org/> [Megtekintés dátuma: 2022.03.03.]. – Hozzáférés: <https://hu.wikipedia.org/wiki/Peer-to-peer>

[7] RSM: Proof of Work (PoW) [online]. – Megjelent: <https://www.rsm.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://www.rsm.hu/kisokos/proof-of-work-pow>

[8] Marci: MI IS AZ A KRIPTOVALUTA BÁNYÁSZAT? (1/2 RÉSZ) [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: https://cryptofalka.hu/kriptovaluta_banyaszat/

- [9] Yoair: Kriptoaluta: Technológiai forradalom története és alkalmazása [online]. – Megjelent: <https://www.yoair.com/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://www.yoair.com/hu/blog/cryptocurrency-history-and-application-of-a-technology-revolution/>
- [10] Árpási Zoltán: SATOSHI NAKAMOTO, A TITOKZATOS PROGRAMOZÓ A BITCOIN MÖGÖTT! [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: https://cryptofalka.hu/satoshi_nakamoto_a_bitcoin_atyja/
- [11] Péter German: MI IS AZ A PROOF OF STAKE ÉS A PROOF OF WORK? [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://cryptofalka.hu/proof-of-work-proof-of-stake/>
- [12] BitcoinBázis: Kicsoda Satoshi Nakamoto? [online]. – Megjelent: <https://www.bitcoinbazis.hu/> [Megtekintés dátuma: 2022.03.04.] Hozzáférés: <https://www.bitcoinbazis.hu/utmutato/kicsoda-satoshi-nakamoto/>
- [13] Portfolio: Igaz a hír, a Mol egyes kútjain már bitcoinnal is lehet fizetni [online]. – Megjelent: <https://www.portfolio.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://www.portfolio.hu/uzlet/20210328/igaz-a-hir-a-mol-egyes-kutjain-mar-bitcoinnal-is-lehet-fizetni-475780>
- [14] hvg: Már kibányászták a bitcoin közel 90 százalékát, de új kriptopénz csak 2140-ben jöhet [online]. – Megjelent: <https://hvg.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: https://hvg.hu/tudomany/20211011_bitcoin_kriptoaluta_kriptopenz_banyaszat
- [15] Andrea: 650 légitársaság járataira lehet kriptoalutákkal jegyet venni [online]. – Megjelent: <https://www.bitcoinbazis.hu/> [Megtekintés: 2022.03.04.]. – Hozzáférés: <https://www.bitcoinbazis.hu/650-legitarsasag-jarataira-lehet-kriptoalutakkal-jegyet-venni/>
- [16] Dora: Mi a Bitcoin? Előnyei és hátrányai [online]. – Megjelent: <http://digitalisnomadok.com/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <http://digitalisnomadok.com/2017/12/13/mi-a-bitcoin-elnyei-s-htrnyai/>
- [17] PortalCripto: Mik a Bitcoin előnyei és hátrányai? [online]. – Megjelent: <https://portalcripto.com.br> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://portalcripto.com.br/hu/mik-a-bitcoin-el%C5%91nyei-%C3%A9s-h%C3%A1tr%C3%A1nyai/>

- [18] Coinmixed: Az Ethereum Története [online]. – Megjelent: <https://coinmixed.eu/>
[Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://coinmixed.eu/az-ethereum-tortenete/>
- [19] Árpási Zoltán: ETHEREUM (ETH), PROGRAMOK ÉS PROJEKTEK EGY BLOKKLÁNCON [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://cryptofalka.hu/ethereum-programok-a-blokklancon/>
- [20] Cryptofalka: MI AZ ETHEREUM? RÉSZLETES KRIPTOVALUTA PROJEKT ISMERTETŐ [online]. – Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://cryptofalka.hu/mi-az-ethereum-projekt-ismerteto/>
- [21] Moonbaby: Merge: hónapokon belül megszűnhet az Ethereum bányászat [online]. – Megjelent: <https://kriptoakademia.com/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://kriptoakademia.com/2022/03/29/merge-nyarra-megszunhet-az-ethereum-banyaszat>
- [22] Coinmixed: A Bitcoin Sztori – Kezdetek [online]. – Megjelent: <https://coinmixed.eu/>
[Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://coinmixed.eu/a-bitcoin-sztori-kezdetek/>
- [23] Dén Mátyás András: A kriptovaluták meleg helyzetet teremthetnek [online]. – Megjelent: <https://index.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: [https://index.hu/gazdasag/2021/08/03/a-kriptovalutak-a-klimavaltozas-okai-/](https://index.hu/gazdasag/2021/08/03/a-kriptovalutak-a-klimavaltozas-okai/)
- [24] Világi Máté: Feleannyit ér a bitcoin, mint fél évvel ezelőtt, pár nap alatt 300 milliárd dollár tűnt el a kriptopiacról [online]. – Megjelent: <https://telex.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://telex.hu/tech/2022/05/09/bitcoin-kriptovaluta-ethereum-ar-zuhanas>
- [25] Singer Zoltán: Fordulat jöhet a bitcoin környezetkárosító hatása miatt [online]. – Megjelent: <https://index.hu/> [Megtekintés dátuma: 2022.03.04.]. – Hozzáférés: <https://index.hu/gazdasag/2022/03/30/bitcoin-ethereum-kriptodevizak-proof-of-work-proof-of-stake/>
- [26] Wikipédia: Blokklánc [online]. – Megjelent: <https://hu.wikipedia.org/> [Megtekintés dátuma: 2022.03.11.]. – Hozzáférés: <https://hu.wikipedia.org/wiki/Blokk%20l%C3%A1nc>

[27] Wikipédia: Kriptográfiai hash függvény [online]. – Megjelent: <https://hu.wikipedia.org/>
[Megtekintés dátuma: 2022.03.19.]. – Hozzáférés:

https://hu.wikipedia.org/wiki/Kriptogr%C3%A1fiai_hash_f%C3%BCggv%C3%A9ny

[28] Pedro Costa: Implementing a Blockchain Oracle on Ethereum [online]. – Megjelent:

<https://medium.com/> [Megtekintés dátuma: 2022.03.19.]. – Hozzáférés:

<https://medium.com/@pedrodc/implementing-a-blockchain-oracle-on-ethereum-cedc7e26b49e>

[29] Nick Darlington: Blockchain For Beginners: What Is Blockchain Technology? A Step-by-Step Guide [online]. – Megjelent: <https://blockgeeks.com/> [Megtekintés dátuma:

2022.03.20.]. – Hozzáférés: <https://blockgeeks.com/guides/what-is-blockchain-technology/>

[30] Matthew Baggetta: What is Blockchain Technology and How Does it Work? [online]. –

Megjelent: <https://blockgeeks.com/> [Megtekintés dátuma: 2022.03.20.]. – Hozzáférés:

<https://blockgeeks.com/guides/how-does-blockchain-work/>

[31] Wikipédia: Okos szerződés [online]. – Megjelent: <https://hu.wikipedia.org/> [Megtekintés dátuma: 2022.03.28.]. – Hozzáférés:

https://hu.wikipedia.org/wiki/Okos_szerz%C5%91d%C3%A9s

[32] Marci: MI IS AZ AZ OKOS SZERZŐDÉS AVAGY SMART CONTRACT? [online]. –

Megjelent: <https://cryptofalka.hu/> [Megtekintés dátuma: 2022.03.28.]. – Hozzáférés:

<https://cryptofalka.hu/mi-is-az-az-okos-szerzodes-avagy-smart-contract/>

[33] Györfi András: Mi az az okos szerződés (Smart Contract) és mire használható? [online]. –

Megjelent: <https://hu.coincash.eu/> [Megtekintés dátuma: 2022.03.28.]. – Hozzáférés:

<https://hu.coincash.eu/blog/mi-az-az-okos-szerzodes-smart-contract-es-mire-hasznalható>

[34] Virtualis Cash: Mi az az okos szerződés? [online]. – Megjelent:

<https://www.virtualis.cash/> [Megtekintés dátuma: 2022.03.28.]. – Hozzáférés:

<https://www.virtualis.cash/mi-az-az-okos-szerzodes/>

[35] Moonbaby: A kínai holdújév hatása a bitcoin árfolyamára [online]. – Megjelent:

<https://kriptoakademia.com/> [Megtekintés dátuma: 2022.04.05.]. – Hozzáférés:

<https://kriptoakademia.com/2021/01/31/a-kinai-holdujev-hatasa-a-bitcoin-arfolyamara>

- [36] Blockchain: Block 734551 [online]. – Megjelent: <https://www.blockchain.com/>
[Megtekintés dátuma: 2022.05.02.]. – Hozzáférés:
<https://www.blockchain.com/btc/block/000000000000000000000008a4e20c4dd87fcd60e7c33eb5c2b700d500e3ec9e8ce>
- [37] E-szigno: Teljes bizonyító erő papír és toll nélkül [online]. – Megjelent: <https://e-szigno.hu/> [Megtekintés dátuma: 2022.05.02.]. – Hozzáférés: <https://e-szigno.hu/elektronikus-alairas>
- [38] Wikipédia: Bitcoin [online]. – Megjelent: <https://hu.wikipedia.org/> [Megtekintés dátuma: 2022.05.02.]. – Hozzáférés: <https://hu.wikipedia.org/wiki/Bitcoin>
- [39] Cryptofalka: Ethereum fundamentális elemzés a Cryptofalka jóvoltából Megjelent: <https://hu.coincash.eu/> [Megtekintés dátuma: 2022.05.02.]. – Hozzáférés: <https://hu.coincash.eu/blog/ethereum-fundamentalis-elemzes>
- [40] CoinCash: CoinCash Bitcoin ATM [online]. – Megjelent: <https://hu.coincash.eu/>
[Megtekintés dátuma: 2022.05.20.]. – Hozzáférés: <https://hu.coincash.eu/atm/>
- [41] Kelemen Péter Bálint: NFT – művészet és szerzői jog [online]. – Megjelent: <https://arsboni.hu/> [Megtekintés dátuma: 2022.05.20.]. – Hozzáférés: <https://arsboni.hu/nft-muveszet-es-szerzoi-jog/>

Szótár:

- [42] <https://bitcoin.org/hu/szotar#bitcoin>

8. ÁBRA- ÉS TÁBLÁZATJEGYZÉK

ábra 1: Wrapped Luna grafikonja (2022.05.10)	2
ábra 2: Cardano grafikonja (2022.05.10.)	2
ábra 3: Asic gépek	6
ábra 4: Bitcoin logója	7
ábra 5: Bitcoin automata Budapesten	9
ábra 6: Ethereum logója	9
ábra 7: Okosszerződés	16
ábra 8: Bitcoin grafikonja (2022.05.10)	21
ábra 9: Ethereum grafikonja (2022.05.10.)	22
ábra 10: A WLUNA és az ADA 10 nap utáni eredménye (2022.05.20.)	23
ábra 11: WLUNA és az ADA nyereség/veszteség grafikonja (2022.05.20.)	23
táblázat 1: Hash-függvény	15

PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI ÖSSZEFOGLALÁS

A dolgozat címe: A kriptovaluta világa	
Hallgató neve: Nyirádi Ferenc Bálint	NEPTUN kód: V36YP2
Képzési szint: felsőoktatási szakképzés	
Szak: Gazdaságinformatika	Szakirány:
Témavezető neve: Hegedűs Géza József	Beosztása: mesteroktató
Tanszék: Informatikai Rendszerek és Alkalmazásai Tanszék	

Véleményem szerint egy új korszaka következik az internetnek. Már most is nagyon népszerűek a digitális fizetőeszközök, úgy gondolom még ennél is népszerűbbek lesznek. Akár olyan gyorsan beleolvadhat a technológia a hétköznapi életbe, mint az internet. Dolgozatom célja, hogy átfogó, érthető képet kapjunk magáról a kriptovalutáról, blokkláncról és az okosszerződésekről. Dolgozatom elején ismertettem a kriptovaluta előzményeit, milyen technológia újítások jöttek létre az 1980-as, 1990-es években, majd ezután, majd szót ejtettem az első tényleges kriptovalutáról, a Bitcoinról. Ezután tisztáztam, hogy mik is azok a kriptovaluták és mit értünk altcoin alatt. Ugyanebben a részben választ adtam, hogy megbízható-e a kriptovaluták és emellett különbséget tettem a kriptovaluta és a hagyományos valuta között. Mielőtt még a két nagy kriptopénzt mutattam volna be, előtte tisztázni szerettem volna, hogy hogyan működik a kriptobányászat, egy kriptobányász milyen feladatok elé néz. Majd ezután következett a legismertebb kriptovaluta, a Bitcoin. Próbáltam a legegyszerűbben bemutatni és előnyeit és hátrányait is ismertetni. Megemlítettem az első tranzakciót is vele, valamint, hogy hol lehet fizetni vele. A Bitcoinnál kitértem Satoshi Nakamotora is, az ismeretlen személyre, aki létrehozta a Bitcoinot. Ezután következett az Ethereum, a másik híres kriptopénz, valamint szemléltettem a „The DAO” projektet. Ez a rész utolsó pontja a gazdasági hatása volt a kriptovalutáknak. Következő részben prezentáltam a blokklánc működését,

típusait és a hash algoritmust. Az utolsó résznél, az okoszerződéseket mutattam be. Igyekeztem példákat hozni, hogy milyen területen érdemes használni a szerződéseket, valamint a digitális aláírást is ismertettem. Dolgozatom során igyekeztem érthetően, egyszerűen bemutatni a blokklánc és az okoszerződések működését és folyamatát. Igyekeztem gyakorlati példákkal egyszerűbben és érdekesebben leírni különböző részeket. Elemzést készítettem a Bitcoinról és az Ethereumról, hogy láthassuk miként változott a dolgozatírásom kezdetétől a befejezésig. Emellett két véletlenszerűen kiválasztott kriptovalutát vásároltam, hogy megfigyeljük az értékváltozásukat.