PANNON EGYETEM

GAZDÁLKODÁSI KAR ZALAEGERSZEG

Kriptodevizák, mint felkapott befektetési eszközosztály

Témavezető: Dr. Joó István

Külső konzulens: Miszory Béla

Czene Mátyás Tamás

Alapképzés

Nappali tagozat

Gazdálkodási és menedzsment

Logisztika

2025

PANNON EGYETEM

GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI NYILATKOZAT A DOLGOZAT BENYÚJTÁSÁHOZ

Hallgató neve:	Czene Mátyás Tamás		
Képzési szint:	alapképzés		
Szak:	Gazdálkodási és menedzsment		
Szakirány (ha van):	Logisztika		
Neptun kód:	A6VNT9	Védés éve:	2025
Dolgozat címe:	Kriptodevizák, mint felkapott befektetési eszközosztály		
Egyetemi témavezető:	Dr. Joó István		
Gyakorlóhelyi konzulens:	Miszory Béla		
Öt kulcsszó a dolgozatról:	Blokklánc, Kriptovaluta, Bitcoin, Ethereum, árfolyammozgások		

Kérjük a szerzői döntésnek megfelelő opciót aláhúzni:

Hozzájárulok / nem járulok hozzá, hogy szakdolgozatomat / záródolgozatomat / diplomadolgozatomat 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, diplomaszerzés 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 rendelkezésemnek megfelelően biztosítható a kutatási célú hozzáférése,
- a dolgozat metaadatai és szerzői összefoglalója online nyilvánosak.

Zalaegerszeg, 2024.12.14.

Czene Mátyás

hallgató aláírása

Tartalom

BEVEZETÉS **5**

1. A KRIPTOPÉNZEK ÚTTÖRÉSÉNEK KEZDETE **6**

2. A BLOKKLÁNC TECHNOLÓGIA **6**

2.1. A BLOKKLÁNC TECHNOLÓGIA MŰKÖDÉSE 6
2.2. BÁNYÁSZAT 7
2.3. BÁNYÁSZATI POOL 9
2.4. KRIPTOGRÁFIA 10
2.4.1. Kriptográfia a digitális korszakban *11*
2.4.2. Hash-függvények *12*

3. MÁR HASZNÁLT TERÜLETEK BEMUTATÁSA, PÉLDÁK **14**

3.1. CHRONICLED 14
3.2. ETHEREUM 15

4. BITCOIN **16**

4.1. TRANZAKCIÓS STRUKTÚRA ÉS A DUPLA KÖLTÉS ELLENI VÉDELEM 16
4.2. IDŐBÉLYEGZŐ SZERVER ÉS A BLOKKLÁNC FELÉPÍTÉSE 16
4.3. MUNKABIZONYÍTÉK ÉS KONSZENZUSMECHANIZMUS 16
4.4. A HÁLÓZAT MŰKÖDÉSE ÉS BLOKKOK LÉTREHOZÁSA 17
4.5. ÖSZTÖNZÉS ÉS INFLÁCIÓ KEZELÉSE 17
4.6. ADATVÉDELEM ÉS DECENTRALIZÁLT BIZTONSÁG 17

5. ETHEREUM **18**

5.1. AZ ETHEREUM ALAPELEMEI ÉS TRANZAKCIÓS RENDSZERE 18
5.2. GÁZ ÉS TRANZAKCIÓK KÖLTSÉGSZABÁLYOZÁSA 18
5.3. ÁLLAPOTÁTMENET ÉS SZERZŐDÉSEK FUTTATÁSA 19
5.4. DECENTRALIZÁLT ALKALMAZÁSOK (DAPPS) ÉS SZOLGÁLTATÁSOK 19
5.5. A BÁNYÁSZAT SZEREPE AZ ETHEREUM HÁLÓZATBAN 19
5.6. KÜLÖNLEGES ADATTÁROLÁSI MÓDSZEREK ÉS BIZTONSÁG 19
5.7. OKOS SZERZŐDÉSEK ÉS DECENTRALIZÁLT AUTONÓM SZERVEZETEK (DAO-K) 20

6. BITCOIN ÉS ETHEREUM TÖRTÉNETE, FEJLŐDÉSE, MÉRFÖLDKÖVEI **20**

7. MI AZ ICO? **23**

8. GAZDASÁGI HATÁSOK, GLOBÁLIS GAZDASÁG HATÁSA A KRIPTOVILÁGRA **25**

9. A KRIPTOVALUTÁK ÁRFOLYAMÁT MEGHATÁROZÓ FŐ TÉNYEZŐK **26**

10. SZABÁLYOZÁSOK **27**

11. KRIPTOVALUTÁK KERESKEDELME **30**

11.1. ADÓZÁS MAGYARORSZÁGON 30
11.2. KRIPTOTŐZSDÉK 31
11.2.1. Binance *31*
11.2.2. Bybit *32*

12. KRIPTOVALUTÁK KERESKEDÉSÉNEK LEHETŐSÉGEI **33**

13. TECHNIKAI ELEMZÉS **34**

13.1. JAPÁN GYERTYA 36
13.2. FIBONACCI SZÁMOK 36
13.3. TŐZSDEI ALAKZATOK 37
13.4. RSI INDIKÁTOR 37
13.5. ELLENÁLLÁSI SZINTEK MEGÁLLAPÍTÁSA 40
13.6. FIBONACCI-SZINTEK ALKALMAZÁSA 40
13.7. MOZGÓÁTLAG 46
13.8. RSI INDIKÁTOR ALAPÚ STRATÉGIA 54

14. EREDMÉNY 56

SZAKIRODALOM FORRÁSOK: 2

INTERNETES FORRÁSOK 2

TÁBLÁZAT- ÉS ÁBRAJEGYZÉK 4

TÁBLÁZAT 4
ÁBRA 4

Bevezetés

Az utóbbi évtizedek egyik legnagyobb gazdasági és technológiai újítása kétségkívül a kriptovaluták megjelenése, amelyek mára nemcsak a pénzügyi piacok, hanem a szélesebb társadalmi és gazdasági diskurzus szerves részévé váltak. A választott szakdolgozati témám, "Kriptodevizák, mint felkapott befektetési eszközosztály", nemcsak az innovatív technológiák iránti érdeklődésemet tükrözi, hanem azt a törekvésemet is, hogy megértsem, hogyan formálhatják ezek a digitális eszközök a globális pénzügyi rendszereket és a befektetési gyakorlatokat. A kriptovaluták, mint például a Bitcoin vagy az Ethereum, a hagyományos pénzügyi rendszerektől eltérően egy teljesen új korszakot kínálnak. Decentralizált működésük, a blokklánc technológiára alapozott biztonságos tranzakciós mechanizmusuk, valamint a közvetítői szerep minimalizálása olyan innovációk, amelyek gyökeresen megváltoztathatják a pénzügyi világ struktúráját. Ugyanakkor ezek a digitális eszközök a befektetési piacokon is forradalmat indítottak el, és rövid idő alatt egy teljesen új eszközosztállyá váltak. Az elmúlt évek során a kriptovaluták szélsőséges árfolyam-ingadozásai, technológiai fejlesztéseik, valamint az ezekhez kapcsolódó szabályozási és etikai kérdések központi témává váltak a globális diskurzusban. Ez a dinamizmus tette őket vonzóvá a befektetők számára, miközben számos kérdést vetett fel, mint például a piac fenntarthatóságát, szabályozottságát és a technológiai fejlődés hatásait. A szakdolgozatom célja ezen kérdések mélyreható elemzése, különös tekintettel arra, hogy milyen szerepet játszanak a kriptovaluták a modern pénzügyi világban, és milyen befektetési lehetőségeket nyújtanak.

Személyes motivációm a témaválasztásban a digitális technológiák és a pénzügyek iránti érdeklődésemben gyökerezik. A koronavírus-járvány alatt lehetőségem nyílt alaposabban megismerkedni a kriptovalutákkal, és magam is befektetőként próbáltam ki ezt az új eszközosztályt. Ez az élmény nemcsak gyakorlati tapasztalatokkal gazdagított, hanem megerősítette bennem azt az igényt, hogy mélyebben megértsem e technológiai újítások működését és gazdasági hatásait. Ezért szakdolgozatom nem csupán a kriptovaluták gazdasági jelentőségét vizsgálja, hanem rávilágít arra is, hogy ezek a technológiák milyen módon alakítják át a befektetési szokásokat, és milyen hosszú távú hatásokat gyakorolhatnak a globális pénzügyi rendszerre. Úgy vélem, hogy a témakör aktualitása, valamint a technológia és gazdaság kapcsolatának mélyebb megértése nemcsak szakmai, hanem személyes fejlődésemet is elősegíti.

1. A kriptopénzek úttörésének kezdete

Több száz éve az emberiség pénzrendszerének alapjai szinte változatlanul működnek. A pénzhasználat mindig is a közvetítőkre épült, legyen az bankrendszer vagy kormányzati ellenőrzés. Az elektronikus fizetési módok felgyorsították a tranzakciókat, de a bankok továbbra is központi szerepet játszanak. A kriptopénzek rendszere ezzel szemben közvetítő nélkül működik, pusztán a technológián alapul. Ez olcsóbb, gyorsabb és biztonságosabb tranzakciókat tesz lehetővé, megnyitva az utat a pénztörténet új fejezete előtt. *(Györfi, 2019)*

2. A blokklánc technológia

A blokklánc technológia a digitális világ egyik legnagyobb és legjelentősebb innovációja, amely megváltoztatta a decentralizált rendszerek felépítését és a tranzakciók kezelését. A kriptovaluták, mint például a Bitcoin és az Ethereum -amire később részletesen is kitérek- mögött is a blokklánc technológia áll, de számos más területen is használják, mint az egészségügyben és az ellátási lánc menedzsmentben.

2.1. A blokklánc technológia működése

A blokklánc egy olyan elosztott főkönyvi technológia, amely lehetővé teszi a digitális tranzakciók biztonságos, átlátható és megváltoztathatatlan módon történő rögzítését. A blokkláncot leggyakrabban egy digitális adatbázisként szokták leírni, amelyben a tranzakciókat egymás után láncolva, blokkok formájában rögzítik. Minden blokk tartalmazza az előző blokk kriptográfiai lenyomatát, így összeláncolva az egyes blokkokat, és biztosítva, hogy a láncban visszamenőlegesen semmilyen adatot ne lehessen megváltoztatni anélkül, hogy az ne derülne ki. A blokkok az adatokat tartalmazó alapegységek, amelyek minden egyes tranzakcióról információt hordoznak. Egy blokk tartalmazhat több tranzakciót, és ezek digitálisan aláírtak, hogy biztosítsák az integritásukat. A digitális aláírás egy kód, amelyet egy üzenethez vagy dokumentumhoz kapcsolunk, és bizonyítja, hogy azt az elküldés után nem módosították. Úgyis vehetjük, mint egy kézzel készített aláírás, csak ennek a digitális formájában.

A blokklánc hálózat nem egyetlen központi szerveren tárolja az adatokat, hanem minden résztvevőnél egyidejűleg. Ez azt jelenti, hogy a rendszer nem függ egyetlen központi hatóságtól sem, és minden egyes felhasználó egyenlő jogokkal rendelkezik a hálózatban. Ezt peer-to-peer struktúrának is szokták nevezni, amiben nincsen harmadik fél és a tranzakciókat a szereplők

egymás között ellenőrzik és hagyják jóvá. Amint ez a lépés megtörtént a tranzakció kapcsolódhat a blokkhoz, ami a blokkláncra fonódik. A blokklánc hálózatokban a tranzakciókat több résztvevő ellenőrzi és hagyja jóvá. A konszenzus mechanizmusok biztosítják, hogy a hálózat összes csomópontja egyetértsen a tranzakciók érvényességében. A két legismertebb mechanizmus Proof of Work (PoW) és a Proof of Stake (PoS). A PoW mechanizmust használja például a Bitcoin. A bányászok bonyolult matematikai feladatokat oldanak meg, hogy új blokkokat adjanak a lánchoz, ami jelentős számítási kapacitást igényel. A másik ilyen a PoS konszenzus mechanizmus, amelyben a résztvevők az alapján kapják meg a jogot a blokkok validálására, hogy mennyi kriptovalutát birtokolnak a rendszerben. Nem mellesleg jelentős tulajdonsága a PoS rendszernek, hogy sokkal energiatakarékosabb, mint a PoW mechanizmus. *(Györfi, 2019)*

2.2. Bányászat

A kriptovaluták bányászata, különösen a Bitcoin esetében, egy olyan eljárás, amely során a bányászok számítógépes erőforrások (akár speciálisan erre a célra tervezett hardverek) segítségével versenyeznek egymással, hogy megoldjanak egy összetett matematikai problémát. Ezt a problémát egy kriptográfiai rejtvényeknek is nevezhetjük, amelynek megoldásával a bányászok létrehoznak egy új blokkot a blokkláncon. Az a bányász, aki elsőként oldja meg a rejtvényt, megkapja a „blokkjutalmat”, ami egy adott mennyiségű kriptopénz, például Bitcoin formájában realizálódik. A kriptovaluták bányászata két fő célt szolgál. Az egyik, hogy új kriptopénzeket bocsássanak ki. A bányászok munkája révén új egységek jönnek létre az adott kriptovalutából, amelyeket a bányászok megkapnak jutalomként. A Bitcoin esetében ez a jutalom jelenleg 3,125 BTC blokk bónuszként kerül kiosztásra minden alkalommal, amikor egy új blokkot sikeresen hozzáadnak a blokklánchoz. A másik a tranzakciók hitelesítése, ami az idő előrehaladtával egyre nagyobb jelentőséggel fog bírni a bányászok számára, mert a felezések hatására egyre nehezebb lesz új bitcoinok kibányászása, így a hitelesítésből kell megkeresni a jutalmukat. A bányászok erőforrásaikkal nemcsak új kriptopénzt generálnak, hanem hitelesítik a hálózaton történő tranzakciókat is. Minden tranzakciót ellenőrizni kell, mielőtt bekerül a blokkláncba, hogy biztosítva legyen annak érvényessége. Ezzel megakadályozzák az úgynevezett „dupla költést” vagy más visszaéléseket. Amikor egy felhasználó tranzakciót kezdeményez a hálózaton, például bitcoin küldését egy másik címre, a tranzakció először egyfajta várakozási sorba kerül. A bányászok ezután ezeket a tranzakciókat összegyűjtik, majd azokat egy blokkba helyezik, amit hozzáadnak a blokklánchoz, ha sikeresen megoldják a matematikai problémát. A matematikai feladat megoldása a bányászok számítási kapacitásán,

illetve a rendelkezésükre álló hardverek hatékonyságán múlik. A bányászok olyan számítógépes eszközöket használnak, mint az **ASIC**, amelyek kifejezetten erre a célra lettek optimalizálva, vagy **GPU**-kat, amelyek szintén rendkívül hatékonyak a számításigényes feladatok elvégzésében. A Bitcoin-hálózat a blokklánc technológián alapul, amely lényegében, ahogy már korábban is említettem egy elosztott főkönyv, amely tartalmazza az összes tranzakciót, amit valaha végrehajtottak. A bányászok feladata, hogy ezeket a tranzakciókat blokkokban rögzítsék, és biztosítsák, hogy minden új blokk pontosan illeszkedjen a lánchoz. A Bitcoin bányászati folyamata a **Proof of Work** konszenzusmechanizmuson alapul. A PoW rendszer garantálja, hogy a hálózat biztonságos maradjon, és hogy a bányászat költséges legyen, ezáltal megakadályozva, hogy egy rosszindulatú szereplő könnyedén átvehesse az irányítást a hálózat fölött. Ez a költség az elektromos energia és a bányászati hardverek költségeiből adódik, mivel a bányászok nagy mennyiségű energiát használnak fel a hash-algoritmusok futtatása közben. A bányászat nehézségi szintje folyamatosan változik, hogy biztosítsa a blokklánc stabil működését. A Bitcoin hálózata például úgy van tervezve, hogy nagyjából 10 percenként keletkezzen egy új blokk. Ha túl sok bányász vesz részt a folyamatban, és a blokkok gyorsabban jönnek létre, a hálózat automatikusan megemeli a nehézségi szintet, hogy fenntartsa ezt az időkeretet. Ezzel szemben, ha kevesebb bányász aktív, a nehézség csökken, hogy továbbra is megközelítőleg 10 percenként keletkezzen egy új blokk. *(Györfi: 2019)*

Tehát a bányászok kétféle jutalmat kapnak a munkájukért. Amikor egy bányász sikeresen hozzáad egy blokkot a blokklánchoz, blokkjutalmat kap. Ez a Bitcoin-hálózat esetében jelenleg 3,125 BTC (2024-as adat), és ez az összeg négyévente feleződik a Bitcoin protokollja szerint, ez a jelenség a "felezés" (halving). A Bitcoin bányászoknak járó jutalom 210 000 blokkonként megfeleződik, ami körülbelül négyévente történik. A kezdetekkor, 2009-ben a bányászok még 50 bitcoint kaptak minden egyes kibányászott blokkért, amely akkoriban nagyjából 1 dollárt ért. 2022 tavaszára azonban ez az összeg már több mint 2 millió dollárt ért blokkonként. A jutalom 2012-ben 25 BTC-re, 2016-ban 12,5 BTC-re, majd 2020-ban 6,25 BTC-re csökkent. A legutolsó felezés, amely 2024-ben teljesült, a blokkjutalmat tovább csökkentette, 6,25 BTC-ről 3,125 BTC-re. Minden tranzakció, amit a bányászok feldolgoznak, egy kis díjat is tartalmaz. Ahogy a blokkjutalom idővel csökken (a felezések miatt), a bányászok számára egyre fontosabbá válnak ezek a tranzakciós díjak, hogy továbbra is fenntarthassák bányászati tevékenységüket.

A Proof of Stake (PoS) modellben nincs szükség bányászatra, mint a Proof of Work (PoW) esetében. A PoS rendszerben a felhasználók a meglévő kriptopénzeiket "letétbe helyezik", ezzel segítve a tranzakciók hitelesítését. Ha jóváhagynak egy legitim tranzakciót, a rendszer jutalmazza őket további kriptopénzekkel. Ha viszont egy illegitim tranzakciót hagynak jóvá, a rendszer büntetésként levon egy részt a letétbe helyezett kriptopénzből. A PoS egyik fő hátránya, hogy sok rendszerben csak azokat választják ki validátorként, akiknek a legtöbb pénzük van. Ez azt jelenti, hogy sok esetben kevésbé demokratikus, mint a Bitcoin, ahol a Proof of Work rendszert használják. Egy másik probléma, hogy bár a PoS környezetbarátabb, mivel kevesebb energiát igényel, még nem bizonyította hatékonyságát olyan nagymértékben, mint a PoW alapú platformok. *(https://penzmuzeumpedia.hu/proof-of-stake-(pos/)*

A kriptovaluták bányászata egy rendkívül összetett folyamat, amely alapvető szerepet játszik a blokklánc hálózatok fenntartásában és biztonságában. Bár a Bitcoin és más PoW-alapú kriptopénzek bányászata egyre több számítási kapacitást és energiát igényel, ez a folyamat biztosítja a decentralizált rendszerek megfelelő működését, és megakadályozza a csalásokat. Az idő múlásával a bányászat tovább fejlődik, ahogy újabb technológiák jelennek meg, és a hálózati nehézség és a jutalmak rendszere is folyamatosan igazodik a résztvevők aktivitásához.

2.3. Bányászati pool

A modern bányászat verseny jellege miatt a legtöbb bányász már nem egyedül dolgozik, hanem úgynevezett **bányászati pool**-okhoz csatlakozik. Ezek a pool-ok több bányász erőforrásait összegyűjtik, hogy nagyobb eséllyel találják meg az új blokkot. Amint egy pool sikeresen kibányászik egy blokkot, a blokkjutalmat a pool tagjai között osztják szét az általuk nyújtott számítási teljesítmény arányában. Ez lehetővé teszi, hogy a kisebb bányászok is részt vehessenek a versenyben, és gyakrabban kapjanak jutalmat, mintha egyedül próbálnak szerencsét. 2011 óta működnek a világ első, kizárólag üzleti célú bányafarmjai. Azóta a helyzet odáig fejlődött, hogy ezek a létesítmények brutális befektetésekkel, több ezer speciális hardverrel, hűtéssel és folyamatos karbantartó személyzettel üzemelnek. A legnagyobb bányafarmok Kínában, Izlandon és az Egyesült Államokban találhatók, ahol az alacsony áramdíjak teszik lehetővé működésüket. A bányászat nemcsak gazdasági, hanem politikai kérdéssé is válik, mivel ezek az energiaigényes, ugyanakkor gyakran innovatív és munkahelyet teremtő létesítmények hamarosan kriptovaluták formájában adózási kötelezettséggel is szembesülhetnek. A legnagyobb bányafarmokat a kínai Bitmain üzemelteti, amely az AntPool, a legnagyobb Bitcoin bányász pool üzemeltetője is. A cég a Bitcoin árának emelkedése,

valamint saját hardverének gyártása és értékesítése révén a 2017-es évet több milliárd dolláros nyereséggel zárta, ezzel a legnagyobb hardvergyártók közé emelkedett. Ezek a bányafarmok több etikai kérdéseket is felvetnek, ezért a kriptovaluta közösség körében megoszlanak a vélemények a bányászóriásokról, mivel működésük ellentétes a decentralizáció eszméjével. Ugyanakkor az általuk biztosított óriási számítási kapacitás hozzájárult ahhoz, hogy a Bitcoin körülbelüli 15 éves története alatt nem történt hackelés vagy rendszerleállás. (*https://academy.binance.com/hu/articles/mining-pools-explained és https://kriptotarca.hu/mining-pool-kriptovaluta-banyaszati-pool-jelentese-es-mukodese-a-gyakorlatban/?utm)*

2.4. Kriptográfia

A kriptográfia a titkosítás és a rejtjelezés tudománya, amely biztosítja, hogy az információk csak az arra jogosultak számára legyenek hozzáférhetők. Célja az adatok védelme és a biztonságos kommunikáció lehetővé tétele. A kriptográfia (görög eredetű szó: „kripto” = rejtett, „gráfia” = írás) már az ókorban is jelen volt, például az egyiptomi hieroglifákban, és az emberek azóta is használják az információk biztonságos továbbítására. Az évszázadok során a kriptográfia jelentős fejlődésen ment keresztül. A középkortól kezdve a hadviselésben is fontos szerepet kapott, például a németek által használt Enigma gép révén, amelyet a második világháború során alkalmaztak. Noha a gép által kódolt üzeneteket eredetileg feltörhetetlennek tartották, később sikerült visszafejteni a titkosítását, ami döntő szerepet játszott a háború végkimenetelében. A 19. század elejéig a kriptográfiát a nyelvtudományokhoz sorolták, de később a módszerek fejlődésével átsorolták a matematika területére. Napjainkban azonban sokan külön tudományágként kezelik, hiszen a digitális világban új feladatokkal bővült, különösen a modern kriptovaluták és blokkláncok létrehozásában. Bár a kriptográfiát és a titkosítást gyakran egy kalap alá veszik, fontos megkülönböztetni őket: a kriptográfia a tudományágat jelöli, amely az adatok rejtésének módszereit kutatja és fejleszti, míg a titkosítás maga az a folyamat, amellyel ezeket az adatokat védjük. A kriptográfia, amely az információk biztonságos elrejtésének és visszafejtésének tudományával foglalkozik, szinte mindennapi életünk szerves része. Számos olyan terméket és szolgáltatást használunk naponta, ahol a háttérben kriptográfiai technológiák garantálják az adatok biztonságát. Böngészők, banki tranzakciók, mobilfizetések, chatprogramok, jelszavak, digitális aláírások és természetesen a kriptopénzek is kriptográfiai módszereket használnak. Az alábbiakban áttekintjük a kriptográfia fejlődését és modern alkalmazásait.

A kriptográfia története több ezer évre nyúlik vissza. Már az ókori Egyiptomban, a hieroglifákban is találunk olyan szimbólumcseréket, amelyeket a korabeli írnokok használtak az információk elrejtésére. Az első ismert eset, amikor egyiptomi írnok egy agyagtáblán rejtette el a kerámiamáz receptjét, jól mutatja, hogy a titkosítás kezdettől fogva praktikus célt szolgált. Az ókori görögök és rómaiak, különösen a spártaiak és Julius Caesar, szintén használtak titkosítási technikákat katonai kommunikáció védelmére. A Caesar-rejtjel, amely az ábécé betűinek eltolásán alapul, a mai napig az egyik legismertebb és legegyszerűbb helyettesítő rejtjel. *(Liptai Kálmán: Kriptográfia és* https://hu.wikipedia.org/wiki/Kriptogr%C3%A1fia)

2.4.1. Kriptográfia a digitális korszakban

A modern kriptográfia a számítógépes technológia megjelenésével új dimenziót kapott. A digitális világban a titkosítás nemcsak a kommunikáció védelmét szolgálja, hanem a tárolt adatok, a hitelesítési folyamatok és a digitális aláírások biztonságát is garantálja.

Az AES (Advanced Encryption Standard) bevezetése jelentős lépés volt a titkosítások világában, amikor a U.S. National Institute of Standards and Technology versenyt hirdetett, amelyet Vincent Rijmen és Joan Daemen nyert meg a Rijndael titkosítással. Az AES szimmetrikus kulcsú titkosítás, amely kiemelkedő sebességgel bír, ugyanakkor már voltak vele szemben sikeres támadások, amelyek módosításokat tettek szükségessé. A titkosítás mellett a kriptográfia egy másik fontos része a digitális aláírás, amely a kommunikáció hitelesítésére szolgál. Amikor egy üzenetet kapunk egy bizonyos X személytől, fontos biztosítanunk, hogy az valóban tőle származik-e, hogy elkerüljük a letagadás vagy a hamis állítás lehetőségét. E problémákra a digitális aláírás kínál megoldást, amely lehetővé teszi, hogy a privát kulcsunkkal aláírjuk a dokumentumokat, így egy digitális aláírás nevű bájtsorozatot kapunk, amelyet hozzáfűzhetünk az üzenethez. A címzett a publikus kulcsunk segítségével ellenőrizheti, hogy az aláírás valóban a mi privát kulcsunkkal készült, és hogy a tartalom azonos az aláírt üzenettel. Mivel csak nekünk van meg a privát kulcsunk, letagadni nem tudjuk az üzenet küldését, és ha valaki módosítaná az üzenetet, az aláírás érvénytelen lenne. (Liptai Kálmán: *Kriptográfia)*

Ez a megoldás azonban nagyobb üzenetek esetén komoly számítási teljesítményt igényel, így szükség volt egy alternatívára, ami Hash formájában született meg. A Hash gyorsan és hatékonyan kiszámítható, hossza általában 128-256 bit, és biztosítja, hogy ne lehessen visszafejteni az eredeti üzenetet, hogy szinte lehetetlen két különböző tartalmú üzenet azonos Hash értéket produkáljon, valamint hogy ugyanannak az üzenetnek mindig azonos Hash értéke

legyen. Ezáltal már nem szükséges az egész üzenetet aláírni, elegendő a Hash értékét aláírni, így a címzett is ellenőrizheti az üzenetet. Ezeket az eljárásokat a blokklánc is alkalmazza; a bányászat során a blokkokhoz hasheket számolunk, míg tranzakciók során a privát kulcsunkkal digitálisan aláírjuk a tranzakciókat. A privát kulcs tehát nem a tárcánkhoz való hozzáféréshez szükséges, hanem a pénzünk költéséhez. A tranzakciók csak akkor kerülnek elfogadásra és a blokkokba, ha azok digitális aláírása érvényes. *(https://hu.wikipedia.org/wiki/Advanced_Encryption_Standard)*

Ez biztosítja, hogy a tranzakciót küldő személy valóban az, akinek mondja magát, ám semmi sem akadályozza meg, hogy később módosítsa vagy törölje a tranzakciót. E problémára válaszol a blokklánc, amelyben minden blokk tartalmazza az előző blokk Hash értékét, lehetővé téve a blokkok érvényességének ellenőrzését. Egy blokk módosításához minden utána következő blokkot is át kellene írni, ami a szükséges számítási teljesítmény miatt rendkívül nehéz, mivel ezeket a műveleteket a hálózat 51%-ának számítási teljesítményével kellene végrehajtani. Ez a követelmény olyan magas, hogy ha lenne is rá lehetőség, pénzügyileg már nem érné meg a csalás. *(https://academy.binance.com/hu/articles/what-is-hashing)*

2.4.2. Hash-függvények

A kriptográfia harmadik fontos területe a hash-függvények használata, amelyek az adatok integritásának ellenőrzésére szolgálnak. Ezek a rövid, fix hosszúságú kódsorok biztosítják, hogy az adatokat nem módosították, és gyakran használják a fájlok letöltésekor az adatok épségének ellenőrzésére. A blokklánc rendszerében minden blokk nemcsak az általa tárolt adatokat tartalmazza, hanem két fontos Hash kódot is: az egyik a blokk saját Hash kódja, a másik pedig az előző blokk Hash kódja. A Hash kódok olyanok, mint a digitális ujjlenyomatok; egyediek, és pontosan azonosítják a blokkokat. Amikor egy blokk létrejön, az algoritmus meghatározza a hozzá tartozó Hash értéket, amely bármilyen adatváltozás esetén megváltozik. Ez a tulajdonság rendkívül hasznos, mivel lehetővé teszi az adatok manipulálásának észlelését. Például, ha egy kis-nagy betű eltérés vagy egy sor végén leütött Enter történik, az teljesen más Hash kódot eredményez. Szemléltetésül végezzük el a „Pannon” és „pannon” szavak SHA-256 hash-algoritmuson történő feldolgozását.

SHA-256	
Bevitel	Kivitel (256 bit)
Pannon	1e921128cb871aeb10ffa7fc0f633e9d29ee2e886245eb13d536cc68c0d01842
pannon	bba3234e123cdcc67c1cb7ac238f2941765026281c63d43cd7eb6d8251fb0fad

1. táblázat Saját szerkesztés, Az SHA-265 kódolás szemléltetése

Saját szerkesztés, Az SHA-265 kódolás szemléltetése

Az alábbi táblázat alapján is láthatjuk, hogy fix hosszúságú adatokból állnak a hashek, ezeknek a karakterszáma 64 darab, akkor is, ha bevitelként hosszabb szót adnánk meg. Mivel minden blokk az őt megelőző blokkra hivatkozik, ha valaki megpróbálja módosítani egy blokk adatait, az új Hash kód létrejötte miatt az átírt blokkban az előző blokkra hivatkozó kód érvénytelen lesz. Ezért a lánc összes további blokkja is érintetté válik, és az adatok értelmezhetetlenné válnak. Így a blokklánc rendszerében van egy jól működő mechanizmus a hamisítványok felfedezésére. Azonban a rendszer ezen védelmi mechanizmusai önmagukban nem elegendőek, mivel egy gyors számítógép képes lenne a blokkok módosítására és az új Hash kódok újraszámítására. Ezen problémák kiküszöbölésére került bevezetésre a Proof of Work (PoW) konszenzus, amely szabályozza az új blokkok létrehozásának idejét, például a bitcoin esetében körülbelül 10 percet. Ha a számítógépek ennél gyorsabban dolgoznának, az algoritmus nehezíti a folyamatot, míg ha lassabb a számítás, akkor felgyorsítja azt. Így, ha valaki megpróbálna átírni egy blokkot, legalább 10 percre lenne szüksége, ami csak egy blokk módosítását jelenti; a soron következő blokkok Hash értékeinek módosítására már nem lenne lehetősége. A rendszert tovább védi a decentralizált tárolás, amelyben a blokklánc másolatainak tízezrei léteznek a felhasználók személyi számítógépein. Ezek a résztvevők csomópontokat (node-okat) alkotnak, és feladatuk a blokkok hitelességének ellenőrzése. Amikor új blokk jön létre, a hálózat minden résztvevője kap egy másolatot. A résztvevők megállapodnak arról, hogy a blokk hiteles, és mindenki hozzáadja a saját másolatához. Ha valaki módosítani szeretné egy már hitelesített blokk adatait, akkor a változtatásokat a résztvevők legalább 51%-án kellene végrehajtania, mert addig a módosítást a rendszer visszautasítja. Tehát ahhoz, hogy valaki akár egy karaktert is megváltoztasson a blokkláncban, minden blokkot át kellene írnia, újra kellene számolnia a hash

kódokat, és több, mint felénél nagyobb kontrollt kellene szereznie a hálózat felett. Ezért a blokklánc egy rendkívül biztonságos és megbízható rendszer, amely a titkosításon alapul, és lehetővé teszi az értékek, például kriptopénzek biztonságos mozgatását, miközben mindkét fél védve van a tranzakció során. *(https://academy.binance.com/hu/articles/what-is-hashing)*

3. Már használt területek bemutatása, példák

Azonban a blokklánc technológiának a lehetséges alkalmazási köre jócskán túlmutat a kriptovalutákon. Alkalmazásának lehetősége egy sor esetben merült már fel, vagy bizonyos esetekben meg is valósították. Így például a közigazgatásban való használata nemcsak a mindennapi papíralapú munkát képes egyszerűsíteni vagy akár teljesen kiváltani, de akár a korrupció csökkenése is várható tőle, ahogy az emberi faktort kikapcsoljuk a folyamatból. Észtország a blokklánc felhasználásával építette ki igen széles körű digitális közigazgatását, de például Szöul önkormányzata is alkalmazza azt. Ezenkívül hasznosítása felmerül még például az elektronikus szavazás, az egészségügy, az adózás, az ingatlanpiac, az online szerencsejátékok, a biztosítások vagy az élelmiszerbiztonság és logisztika területein is. Elterjedésének korlátját jelentheti azonban az, hogy a rendszer általi validálás önmagában nem az információtartalom valóságát garantálja, hanem kizárólag csak azt, hogy valóban az eredetileg leírtakat rögzítik. *(DORNFELD László: A kriptovaluták és az e-bizalom kapcsolata)*

3.1. Chronicled

A Chronicled egy San Francisco-i székhelyű technológiai vállalat, amely 2014-ben alakult, és főleg a blockchain technológiára specializálódott. A cég célja, hogy megbízható és átlátható megoldásokat nyújtson különösen az ellátási lánc menedzsmentben, olyan iparágakban, mint a gyógyszeripar és az egészségügy. Fő platformja a MediLedger Network egy innovatív, blokklánc-alapú platform, amely kifejezetten az élettudományok iparágára lett tervezve. Küldetésük, hogy az adminisztrációkat biztosítsák és megoldásokat fejlesszenek ezen a hálózaton, hogy elősegítsék a bizalmat és lehetővé tegyék az automatizálást a kereskedelmi partnerek között. Az élettudományok szektora rendkívül összetett, különösen a gyógyszereknek az útja, a gyártóktól a betegekig való eljuttatása során. Ezt a bonyolultságot tovább növelik a szabályozási követelmények, az összetett árazási és szerződési kapcsolatok, valamint a számtalan kivétel az iparági normák alól. A blokklánc technológia átalakító lehetőséget kínál a cégek számára, hogy befolyást gyakoroljanak az adatokra és tranzakciókra, amelyeket partnereiktől kapnak, lehetővé téve ezzel az automatizálást, amely túlmutat a belső

rendszereken. A Chronicled egyedülálló módon ötvözi a blokklánc technológia és az élettudományok iparágában szerzett tapasztalatait, ami lehetővé teszi számukra, hogy olyan kihívásokat oldjanak meg, amelyeket más szervezetek nem tudnak. Hosszú távú víziójuk az, hogy létrehozzanak egy együttműködési platformot, ahol az élettudományokban tevékenykedő cégek és harmadik felek együtt dolgozhatnak olyan innovatív megoldások kifejlesztésén, amelyek olyan problémákat céloznak meg, amelyeket korábban el sem tudtak képzelni. Az együttműködéses fejlesztések ökoszisztémájának ösztönzésével felhatalmazzák a fejlesztőket és az ügyfeleket, hogy közösen hozzanak létre termékeket, amelyek megoldást nyújtanak a vállalatok közötti kihívásokra. A MediLedger Network ennek az együttműködési erőfeszítésnek az alapjaként szolgál, és olyan protokoll primitíveket kínál, amelyek lehetővé teszik bármilyen típusú információ vagy tranzakció megosztását a cégek között. Működésük alapját értékeik képezik, amelyek hangsúlyozzák a határozott, de rugalmas véleményeket, így olyan környezetet teremtenek, ahol a legjobb ötletek kibontakozhatnak, anélkül hogy az egó akadályozná őket. Hisznek a közös munkában és abban, hogy fontos egy sokszínű és fejlődésorientált környezetet létrehozni, ahol az egyéni kiválóság elismerésre kerül, de a csapatmunka a legfontosabb. Az integritás számukra kulcsfontosságú, és prioritásként kezelik, hogy a helyes döntéseket hozzák meg ügyfeleik és partnereik érdekében, miközben együttérző kapcsolatokat ápolnak az egész szervezetben. Bátorsággal ölelik fel az új innovációkat és céljuk, hogy, komplex problémákat oldjanak meg azzal a szándékkal, hogy olyan eredményeket érjenek el, amelyeket mások lehetetlennek tartanak. Az általuk kifejlesztett technológiák és rendszerek kiaknázásával céljuk, hogy felgyorsítsák az értékteremtést minden partnerük és azok ügyfelei számára, miközben hosszú távú célokat tartanak szem előtt. (*https://www.chronicled.com/*)

3.2. Ethereum

Az Ethereum számítógépek hálózata az egész világon, amelyek az Ethereum protokollnak nevezett szabályrendszert követik. Az Ethereum hálózat olyan közösségek, alkalmazások, szervezetek és digitális eszközök alapjaként működik, amelyeket bárki fel tud építeni és használni. Bárhol, bármikor létrehozhat Ethereum-fiókot, és felfedezheti az alkalmazások világát, vagy elkészítheti sajátját. Az alapvető újítás az, hogy mindezt megteheti anélkül, hogy megbízna egy központi hatóságban, amely megváltoztathatja a szabályokat vagy korlátozhatja a hozzáférést. Erre későbbiekben részletesen is kitérek és ismertetem az Ethereumot. (*https://ethereum.org/en/what-is-ethereum/*)

4. Bitcoin

A Bitcoin rendszer felépítése egy decentralizált, peer-to-peer hálózatot alkalmaz, amely lehetővé teszi a közvetlen tranzakciókat harmadik fél beavatkozása nélkül. Alapja egy digitális fizetési rendszer, amelyet kriptográfiai módszerek biztosítanak. A rendszer legfontosabb eleme a blokklánc, amely időrendi sorrendben rögzíti a tranzakciókat, és amelynek módosítása csak jelentős számítási erőfeszítéssel lehetséges. A Bitcoin rendszer minden tranzakcióját digitális aláírások igazolják, amelyek biztosítják a tulajdonosi lánc követhetőségét és a tranzakciók hitelességét.

4.1. Tranzakciós struktúra és a dupla költés elleni védelem

A Bitcoin rendszer minden tranzakcióját úgy tervezték, hogy egy „digitális érmét” alkosson, amely a tulajdonosi lánc aláírásaiból áll. Minden tulajdonos egy digitális aláírással adja át a jogot a következő tulajdonosnak, és így a tranzakciók hitelesíthetőek. Az egyik legnagyobb kihívás a „dupla költés” problémája volt, amelyet a rendszer egy decentralizált időbélyegző szerverrel oldott meg. Mivel minden tranzakció nyilvánosan bejelentésre kerül, a résztvevők egyetlen történelemben tudnak megegyezni a tranzakciók sorrendjéről.

4.2. Időbélyegző szerver és a blokklánc felépítése

A Bitcoin hálózat egy időbélyegző szerver segítségével biztosítja a tranzakciók kronológiai sorrendjét. A rendszer egy hash alapú proof-of-work (munkabizonyíték) algoritmust használ, amely összekapcsolja az egyes tranzakciókat egy blokkláncba, ahol minden blokk tartalmazza az előző blokk hash értékét. Ezzel egy olyan láncolt struktúra jön létre, amelynek visszamenőleges módosítása rendkívüli számítási kapacitást igényelne.

4.3. Munkabizonyíték és konszenzusmechanizmus

A Bitcoin rendszer munkabizonyíték alapú konszenzusmechanizmust használ, amely a Hashcash rendszerhez hasonlóan működik. A Hashcash egy proof-of-work (munkabizonyíték) rendszer, amelyet eredetileg e-mail spamek elleni védekezésre fejlesztette ki Adam Back 1997-ben. A rendszer lényege, hogy egy felhasználónak bizonyos számítási munkát kell elvégeznie, mielőtt elküldhetné az üzenetét. Ez a számítási feladat erőforrásigényes, így megnehezíti a nagy mennyiségű spam szétküldését, mivel minden egyes e-mailhez külön számítási munkát kell végezni *(https://en.wikipedia.org/wiki/Hashcash)*. A proof-of-work lényege, hogy minden

blokknak tartalmaznia kell egy bizonyos számú nullával kezdődő hash értéket, amihez szükséges számítási kapacitás exponenciálisan növekszik a nullák száma függvényében. Ez a folyamat megakadályozza, hogy egy támadó módosíthassa a láncot anélkül, hogy rendelkezne a szükséges számítási teljesítmény többségével. A rendszer alapelve, hogy a leghosszabb láncot tekinti érvényesnek, amely a legtöbb munkát igényelte, így, ha a becsületes csomópontok irányítják a hálózat számítási kapacitásának többségét, a támadó nem tudja meghamisítani a tranzakciókat.

4.4. A hálózat működése és blokkok létrehozása

A hálózat működése a következő lépésekből áll: új tranzakciókat a résztvevők megosztanak a hálózattal, amelyeket minden csomópont egy blokkba gyűjt. Ezt követően a csomópontok proof-of-work számításokat végeznek a blokkhoz, és ha egy csomópont megtalálja a megfelelő hash értéket, a blokkot elküldi a többi csomópontnak. A blokkokat a csomópontok elfogadják, amennyiben azok érvényes tranzakciókat tartalmaznak. A csomópontok ezután a következő blokk létrehozásával folytatják a láncot, az elfogadott blokk hash értékét használva.

4.5. Ösztönzés és infláció kezelése

A Bitcoin rendszerben minden blokk első tranzakciója egy új bitcoint hoz létre, amelyet a blokkot előállító csomópont kap meg. Ez az ösztönzőmechanizmus segít fenntartani a hálózat működését és kezdetben a bitcoinok elosztását is megoldja. Idővel, ahogy a bányászat nehezebbé válik és egyre kevesebb új bitcoin kerül forgalomba, a rendszer tranzakciós díjakra állhat át, ezzel biztosítva az infláció minimalizálását.

4.6. Adatvédelem és decentralizált biztonság

A Bitcoin hálózat nyilvános, ezért minden tranzakció látható, de az adatvédelem megőrzése érdekében a rendszer anonim nyilvános kulcsokat használ. Minden tranzakcióhoz egy új kulcspár generálható, ami nehezíti a tulajdonosi lánc követését. A hálózat biztonságát tovább növeli az, hogy a csomópontok nincsenek központilag összekötve; így a hálózat bármelyik résztvevője szabadon csatlakozhat vagy kiléphet, és a leghosszabb láncot tekinti a hálózat által elfogadott igaznak. *(https://bitcoin.org/bitcoin.pdf)*

Összességében a Bitcoin egy olyan rendszer, amely lehetővé teszi az elektronikus tranzakciókat anélkül, hogy bizalomra vagy harmadik félre lenne szükség. A proof-of-work alapú blokklánc garantálja, hogy a tranzakciók nyilvántartása visszamenőleg nem módosítható, ha a hálózat

többsége becsületesen működik. Az egyszerű, mégis robusztus felépítés biztosítja, hogy a résztvevők CPU teljesítményükkel szavaznak a tranzakciók érvényességéről, így egy megbízható és önállóan működő pénzügyi rendszert alkotnak.

5. Ethereum

Az Ethereum a legnagyobb piaci kapitalizációval rendelkező altcoin (altcoin: bitcoinon kívűl minden más) a piacon, ennek felépítése egy olyan decentralizált platformot hoz létre, amely támogatja az okos szerződéseket és a decentralizált alkalmazásokat (DApps), és amelyen a résztvevők saját szabályokat alakíthatnak ki, a tranzakciók formátumait és állapotát is módosíthatják. Az Ethereum blokklánc egy beépített Turing-complete programozási nyelvet kínál, amely lehetővé teszi bárkinek, hogy egyedi szerződéseket és alkalmazásokat hozzon létre. Mindez kódolási szempontból rugalmasságot nyújt, az Ethereum fejlesztői szabadon tervezhetnek új pénzügyi termékeket, tulajdonrendszereket vagy akár digitális szervezeteket.

A Turing-complete olyan gépet vagy rendszert jelöl, amely, ha elegendő idő és memória áll rendelkezésére, képes bármilyen számítási probléma megoldására, függetlenül annak összetettségétől. Ez a fogalom gyakran a modern programozási nyelvek jellemzésére szolgál, mivel a legtöbb ilyen nyelv (például C++, Python, JavaScript) Turing-complete tekinthető.

5.1. Az Ethereum alapelemei és tranzakciós rendszere

Az Ethereum rendszerében minden entitás "számlaként" létezik, amely rendelkezik egyedi címmel és bizonyos mezőkkel, például számlálóval, egyenleggel, tárolóval és ha van, szerződéses kóddal. A rendszer kétféle számlát különböztet meg: külső számlákat (ezek emberi felhasználók által ellenőrzöttek) és szerződéses számlákat, amelyek saját kóddal rendelkeznek, és amelyek automatikusan aktiválódnak, amikor üzenetet kapnak. A tranzakciók célja lehet értékátadás, vagy szerződések futtatása. Minden tranzakció tartalmaz egy korlátot (gázlimit) a végrehajtási lépésekhez és egy gázárat, amely a bányászoknak fizetendő díjat határozza meg.

5.2. Gáz és tranzakciók költségszabályozása

Az Ethereum rendszere a tranzakciókat gáz segítségével szabályozza, amely limitálja a végrehajtható műveletek számát, ezzel megakadályozva az elhúzódó vagy végtelen ciklusú műveleteket. Amikor egy tranzakció eléri a gázlimitet, az visszafordítja az állapotváltozásokat,

de a felhasznált gáz díja elvész. Ez a rendszer megvédi a hálózatot a túlterheléstől és biztosítja, hogy a bányászok csak hasznos műveleteket hajtsanak végre.

5.3. Állapotátmenet és szerződések futtatása

Az Ethereum állapotátmeneti funkciója egy tranzakciót új állapotra módosít, például egy tranzakció fogadásával és annak végrehajtásával. Ez magában foglalhat egy szerződés futtatását, amely során a kód olvas a tárolóból, írhat adatokat, üzenetet küldhet, vagy más szerződéseket hozhat létre. A gáz alapú rendszer elősegíti, hogy a futtatott kódok gyorsak és biztonságosak legyenek, míg a Turing-teljes nyelv lehetővé teszi bármilyen műveleti logika megvalósítását.

5.4. Decentralizált Alkalmazások (DApps) és Szolgáltatások

Az Ethereum lehetőséget biztosít többféle decentralizált alkalmazás létrehozására, amelyek pénzügyi, kereskedelmi, vagy akár kormányzati funkciókat látnak el. Ezek közé tartozhatnak például tokenrendszerek, származékos ügyletek, decentralizált szavazás vagy szervezetek. Az ilyen típusú alkalmazások, mint például a tokenrendszerek, könnyen implementálhatók és akár hagyományos pénzügyi eszközöket is helyettesíthetnek.

5.5. A bányászat szerepe az Ethereum hálózatban

Az Ethereum blokklánca a Bitcoinhoz hasonlóan bányászat alapú volt, bár bizonyos különbségekkel, minden blokk tartalmazza a tranzakciók listáját és a legutóbbi állapot másolatát, valamint a blokkszámot és a nehézségi szintet. Az érvényes blokkok megerősítik a tranzakciókat és frissítik a hálózat állapotát, miközben a blokkláncba építik a legutóbbi módosításokat. De az Ethereum 2.0-val a hálózat Proof of Stake (PoS) mechanizmusra áll át (2020), és nem lesz többé szükség az érmék bányászatára. A cél az Ethereum skálázhatóságának javítása, valamint további előnyök megteremtése a felhasználók számára.

5.6. Különleges adattárolási módszerek és biztonság

Az Ethereum blokkláncban alkalmazott Patricia fa (Merkle fa továbbfejlesztett változata) lehetővé teszi a tárolás hatékonyságát, mivel csak a változtatott adatelemek kerülnek módosításra az egyes blokkok között. Ezáltal az Ethereum rendszer egyre növekvő adatállományát kezelhetőbbé teszi. Az adattárolási rendszer biztosítja a megbízhatóságot, és a Patricia fa használata révén csökkenti a teljes blokklánc tárolási igényét.

5.7. Okos Szerződések és Decentralizált Autonóm Szervezetek (DAO-k)

A blokklánc technológia legérdekesebb hasznosítása mégiscsak az okosszerződések (smart contracts). Ezek alkalmazását először az 1990-es években Nick Szabo vetette fel. Szabo szerint az okosszerződés nem azt jelenti, hogy mesterséges intelligenciát alkalmaznak, csak azt, hogy a számítógépes programban tárolt szerződési feltételeket automatikusan végrehajtják, ha azoknak az előfeltételei meg- valósulnak. Ennek a gyakorlati megoldása lett, hogy a tranzakciót blokkláncokban tárolják, replikálják és frissítik, a szerződést pedig automatikusan végrehajtják. Ezzel szemben a hagyományos szerződéseket megbízható harmadik félnek kell centralizált módon teljesítenie, ami hosszú végrehajtási időt és többletköltséget eredményez. Ennek gyakorlati megvalósulása lehet például a biztosítások terén a síbiztosítás: amennyiben a biztosítás kedvezményezettje elutazik, de az időjárás- jelentések szerint az idő nem kedvez a szolgáltatás igénybevételére, az okosszerződés alapján automatikusan kiutalják neki a biztosító részéről a napidíjat, anélkül, hogy ehhez külön ügyintézésre szükség lenne. Fontos ugyanakkor azt is megjegyezni, hogy a tranzakciók visszafordíthatatlansága kétélű fegyver: ha ugyanis hibásan írják meg, abban az esetben súlyos pénzügyi veszteségekhez vezethet, amelyek visszakönyvelésére már nincs lehetőség (DORNFELD László: A kriptovaluták és az e-bizalom kapcsolata). Az Ethereum hálózaton futó már említett smart contractok vagy okosszerződések tehát olyan önállóan futtatható kódrészletek, amelyek automatikusan végrehajtódnak, ha a feltételek teljesülnek. A decentralizált autonóm szervezetek (DAO-k) további fejlesztést jelentenek, lehetővé téve olyan szervezetek létrehozását, ahol a döntéshozatal kriptográfia és blokklánc technológia révén történik. A DAO-kban a résztvevőknek lehetőségük van a szervezet eszközeinek irányítására és a szabályok módosítására, miközben a működés teljesen önálló és központosítás nélküli. *(https://ethereum.org/en/what-is-ethereum/)*

6. Bitcoin és Ethereum története, fejlődése, mérföldkövei

A kriptopénzek, köztük a Bitcoin, mint decentralizált elektronikus fizetési rendszerek ötlete már a múlt század 90-es éveiben megjelent. Wei Dai, egy Washingtoni Egyetemen végzett programozó, 1998-ban közzétette egy „b-pénz” nevű digitális valuta ötletét, amely névtelen felhasználók közötti lenyomozhatatlan fizetéseken alapult. Ez a koncepció már akkoriban is hasonlóságot mutatott a Bitcoin alapelveivel. A Bitcoin története azonban 2008-ban kezdődött, amikor a titokzatos Satoshi Nakamoto publikálta a „Bitcoin: A Peer-to-Peer Electronic Cash

System” című kiáltványát. Ebben a dokumentumban egy decentralizált hálózat felépítésének alapjait fektette le, amely a felhasználók proof-of-work algoritmusán alapult, és amely független a hagyományos pénzintézetektől.

A Bitcoin-hálózat 2009 januárjában indult el, amikor kibányászták az első blokkot, az úgynevezett genezis blokkot. Az első BTC-kliens lehetővé tette további felhasználók számára a csatlakozást, és ezzel a Bitcoin blokklánc fejlődését is elindította. A korai időszakban azonban nehézséget jelentett, hogy hogyan határozzák meg a valuta értékét. Az első, hivatalos árfolyamot csak 2009 októberében állapították meg, amely 1 dollár értéknek 1309 BTC-t felelt meg. Az első ismert kereskedelmi tranzakcióra 2010-ben került sor, amikor Hanyecz László 10000 BTC-t fizetett két pizzáért, amely a későbbi árfolyamokat tekintve milliárdos értéket képviselne.

Az első Bitcoin-kereskedési portál, a Bitcoin Market 2010-ben nyílt meg, ám a valódi áttörést az Mt. Gox platform jelentette, amely lehetővé tette a BTC vásárlását és eladását állandó árfolyam mellett. Az Mt. Gox sokáig a legnagyobb Bitcoin-tőzsdeként működött, és a kriptopénzpiac egyik meghatározó platformja lett. Az évek során a Bitcoin árfolyama jelentős emelkedést mutatott, ami felkeltette a befektetők és a média figyelmét. 2013-ra a Bitcoin kapitalizációja meghaladta az egymilliárd dollárt, és ezzel a mainstream figyelem középpontjába került. Számos nagy cég, mint a WikiLeaks, valamint különféle szervezetek és egyesületek is elkezdtek Bitcoint elfogadni adományként. 2011-ben, a Bitcoin sikere után, megjelentek az első alternatív kriptovaluták, az ún. altcoinok, amelyek célja, hogy különböző fejlesztéseket és extra funkciókat kínáljanak a Bitcoinhoz képest, például gyorsabb tranzakciókat vagy fokozott anonimitást. A Litecoin volt az egyik első altcoin, amelyet gyakran a Bitcoin "ezüstjének" neveztek. Az évek során az altcoinok száma robbanásszerűen megnőtt, mára több ezer különböző kriptovaluta létezik.

2013-ban a német hatóságok hivatalosan is elismerték a Bitcoint magánfizetési eszközként, ami újabb lökést adott az árfolyamának. Ez idő tájt azonban az FBI lecsapott a Silk Roadra, egy illegális kereskedelmet bonyolító weboldalra, amely Bitcoint használt a tranzakcióihoz. A Bitcoin árfolyama ezt követően 2017-ig stagnált, majd egy újabb bikapiac során megindult az árfolyam emelkedése. Ugyanakkor az Mt. Gox 2014-ben összeomlott egy hatalmas lopási botrány miatt, amely során több mint 744000 BTC veszett el.

A Bitcoin fejlődése nem állt meg, és 2017-ben újabb csúcsot ért el. Ebben az évben Japán is hivatalosan elismerte a Bitcoint, amely ezzel széles körben elfogadott alternatív fizetési

eszközzé vált. A szabályozások fejlődése és a kriptopénzpiac további növekedése új magasságokba emelte a Bitcoin árfolyamát, és egyre több intézményi befektető érdeklődését is felkeltette. Ugyanebben az évben az amerikai pénzügyi piacok bevezették a Bitcoin határidős szerződéseit, amelyek még inkább beemelték a mainstream pénzügyi világba.

A Bitcoin további elterjedése szorosan összefüggött a globális pénzügyi piacok változásaival, különösen a 2020-as COVID-19 járvány idején, amikor a hagyományos pénz iránti bizalom megingott. Az infláció növekedése és a hagyományos valuták értékcsökkenése miatt egyre többen tekintettek a Bitcoinra, mint értékőrző eszközre. 2021-ben El Salvador törvényes fizetőeszközként ismerte el a Bitcoint, ami egyedülálló kísérlet a kriptopénz társadalmi és gazdasági szerepének vizsgálatára.

A jövő azonban bizonytalan a Bitcoin számára. További technológiai adaptációk és a blokklánc alkalmazása újabb lendületet adhat az árfolyamának, különösen, ha a nagyvállalatok és a pénzügyi szabályozók is beépítik saját rendszereikbe. A szabályozások szigorítása viszont új kihívásokat jelenthet, ami befolyásolhatja milyen irányt vesz majd a Bitcoin piaca. A kriptopénz piaci szereplői mindenesetre folyamatosan figyelik a technológiai és szabályozási fejleményeket, miközben a Bitcoin továbbra is kiemelt szerepet tölt be, mint a fiat pénz digitális alternatívája. *(https://www.xtb.com/hu/oktatas/a-bitcoin-tortenete és https://kriptomat.io/hu/kriptovalutak/a-kriptovalutak-rovid-tortenete/)*

Az Ethereum története a blokklánc-technológia és a decentralizált alkalmazások fejlődésének egyik legizgalmasabb példája, amely számos fontos mérföldkővel és technikai újítással gazdagodott. Az Ethereum alapítója, Vitalik Buterin, 2013-ban tette közzé a Fehérkönyvet, amely bemutatta az Ethereum vízióját, mint egy programozható blokkláncot, amely lehetővé teszi a decentralizált alkalmazások (DApps) és okosszerződések létrehozását. Ezt követte 2014-ben a Sárgakönyv kiadása Dr. Gavin Wood részéről, amely technikai meghatározásokat adott az Ethereum protokollhoz, és ugyanebben az évben megkezdődött az Ether tokenek első értékesítése, amely 42 nap alatt zajlott le.

Az Ethereum hivatalos indulása 2015 júliusában a Frontier frissítéssel történt, amely egy kezdeti implementáció volt, lehetővé téve a bányászok és fejlesztők számára az első kísérletezéseket. Az első években számos elágazás segítette a hálózat fejlődését: a Homestead frissítés 2016-ban fontos hálózati változtatásokat vezetett be, előkészítve az utat a skálázhatóság és stabilitás felé. Az Ethereum korai sikerei azonban kihívásokkal is szembesültek; ugyanebben az évben a DAO-támadás során egy jelentős mennyiségű Ether veszett el egy hibás szerződés

miatt. Az Ethereum közössége válaszul egy „hard fork” mellett döntött, hogy visszaszerezzék az elvesztett értéket, így megszületett az Ethereum Classic, amely az eredeti lánc folytatása maradt a változtatás nélkül.

A következő nagy frissítések, mint a Byzantium és Constantinople, a hálózat hatékonyságát, biztonságát és a gázdíjak optimalizálását célozták meg. Az Istanbul elágazás 2019-ben tovább bővítette az Ethereum képességeit, például a skálázhatóságot és a különféle blokkláncok közötti kompatibilitást. Az egyik legfontosabb mérföldkő a 2020-as Beacon Chain elindítása volt, amely a proof-of-stake (PoS) rendszer alapját képezte, megnyitva az utat az energiahatékonyabb konszenzusmechanizmus felé.

A „Beolvadás” néven ismert Paris frissítés 2022 szeptemberében történt, amely a proof-of-work (PoW) helyett teljesen a PoS konszenzusra állította át az Ethereumot, és megszüntette a bányászok szerepét, helyette validátorok hálózata biztosítja a blokkok hitelességét. A következő években olyan frissítések érkeztek, mint a Shanghai-Capella, amely lehetővé tette a letétek egyszerű kivonását, és a Cancun-Deneb („Dencun”) frissítés, amely a Proto-Danksharding bevezetésével javította a hálózat skálázhatóságát és csökkentette a második blokkláncréteg költségeit.

Az Ethereum fejlődése máig tart, és az újabb technikai újítások révén folyamatosan javul a skálázhatóság, biztonság és felhasználói élmény. Az Ethereum víziója, hogy egy nyitott, globális platformot biztosítson decentralizált alkalmazások fejlesztésére, még mindig erősen formálja a digitális gazdaság jövőjét. *(https://ethereum.org/hu/history/#yellowpaper)*

7. Mi az ICO?

Az Ethereum 2015-ös megjelenése új lendületet adott a kriptopiacnak. Az Ethereum blokkllánca lehetővé tette az okos szerződések futtatását, amelyek által a blokklánc technológia alkalmazási köre jelentősen kibővült. Az Ethereum révén nemcsak pénzügyi tranzakciókat lehetett végrehajtani, hanem komplex, önállóan működő alkalmazásokat is létre lehetett hozni. Az Ethereum növekedésével megjelent az első érmekibocsátások (ICO-k) hulláma, amelyek segítségével különböző projektek crowdfunding révén szereztek tőkét, hasonlóan ahhoz, ahogy a tőzsdére lépésnél történik. A crowdfunding jelentése egy közösségi finanszírozás olyan innovatív, alternatív pénzügyi megoldása, amely egy vállalkozás tőkeemelését online kommunikációs kampányon keresztül, a közösség tőkéjének bevonásával valósítja meg. A közösségi kampányok piactere a közösségi finanszírozási portál.

A kriptopiac 2017-ben újabb óriási fellendülést élt át, amikor a Bitcoin árfolyama 20 000 dollár közelébe emelkedett, és az ICO-k száma robbanásszerűen növekedett. Ekkorra a kriptovaluták piaci kapitalizációja 800 milliárd dollár fölé nőtt. Azonban a piac növekedése fenntarthatatlan volt, és a „buborék" 2018-ban kipukkadt. A piac összeomlása után számos projekt elbukott, míg azok, amelyek megmaradtak, olyan megoldásokat kínáltak, amelyek valós problémákra adtak választ.

Az elmúlt évek során a kriptovaluták és a blokklánc technológia fejlődése stabilizálódott. Ma már sok projekt a valós világ problémáinak megoldására koncentrál, például a szerencsejáték, a sport, a személyazonosság kezelés és a pénzügy területén. A befektetők most már sokkal átgondoltabban vizsgálják meg a kriptovaluták üzleti modelljét és jövőbeli potenciálját. A világ digitális átalakulása révén a kriptovaluták olyan pénzügyi rendszert képviselnek, amely mindenki számára elérhető lehet. A Bitcoin és más kriptovaluták kulcsszerepet játszhatnak abban, hogy a bolygó minden lakójának pénzügyi autonómiát biztosítsanak, és a globális pénzügyi rendszer jövőjét alapjaiban változtathatják meg.

De még is mi az az ICO, vagyis az „Initial Coin Offering" (elsődleges érmekibocsátás) egy olyan forrásszerzési módszer, amelyet a blokklánc alapú projektek használnak pénzgyűjtésre. Az ICO során a projektcsapatok blokkláncalapú tokeneket hoznak létre és értékesítenek a korai támogatók számára, akik ezzel a projekt jövőbeli sikereiben reménykedve támogatják azt. Ez a közösségi finanszírozási modell lehetővé teszi a felhasználók számára, hogy tokeneket kapjanak, amelyeket később a projekten belül használhatnak, míg a projekt maga a befolyt összeget fejlesztési költségek fedezésére fordíthatja. Az ICO elindítása óta népszerűvé vált a kriptopiacon, különösen az Ethereum 2014-es sikeres finanszírozása óta, amely során az Ethereum fejlesztéseit ICO útján finanszírozták.

Bár az ICO hasonlít az IPO-hoz (elsődleges részvénykibocsátás), alapvető különbség köztük, hogy míg az IPO során a befektetők tulajdonrészt szereznek egy vállalatban, addig az ICO-k során megvásárolt tokenek nem jelentenek tulajdonjogot a cégben, hanem a projekt ökoszisztémájában használhatók fel. Az ICO tehát egy olyan alternatív finanszírozási módszert kínál a korai szakaszban lévő startupok számára, amely különösen előnyös lehet azok számára, akik működő termék nélkül szeretnének tőkét bevonni. Emellett egyes vállalatok a decentralizáció és a befektetők szélesebb körű bevonása érdekében választják az ICO-t, hogy finanszírozást gyűjtsenek egy új blokkláncalapú termékhez vagy szolgáltatáshoz.

Az ICO-k működéséhez gyakran okosszerződés-képes blokkláncokat, például az Ethereumot használják, ahol a tokenek ERC-20 szabványon alapulnak. A sikeres ICO-hoz a csapat meghatározza a kibocsátás időtartamát, a tokenek számát és más szabályokat, amelyeket a résztvevők követnek. A befektetők általában Bitcoint vagy Ethereumot utalnak egy meghatározott címre, a tokeneket pedig automatikusan vagy megadott címre küldi el a rendszer.

Fontos azonban, hogy az ICO-k körüli szabályozás joghatóságonként eltérő, és gyakran jogi kihívásokat jelentenek. Egyes országok kifejezetten tiltják az ICO-k indítását, míg más helyeken nincs egyértelmű iránymutatás. Ezért elengedhetetlen a jogi tanácsadás a közösségi finanszírozás ezen formájának alkalmazása előtt. Az ICO, bár izgalmas befektetési lehetőség lehet, magas kockázatokat is hordoz, mivel a befektetők számára nem garantált a hozam, és a projektek gyakran bizonytalanok lehetnek. *(https://academy.binance.com/hu/articles/what-is-an-ico)*

8. Gazdasági hatások, Globális gazdaság hatása a kriptovilágra

A kriptopénzek és a blokklánc-technológia egyik legjelentősebb újítása a decentralizáció, vagyis a központi szereplők kivonása az üzleti és pénzügyi folyamatokból. Ez lehetővé teszi, hogy a hagyományos közvetítőket, például a bankokat vagy a zenei iparban a stúdiókat, kiiktassuk, és a szereplők – például a zenészek és hallgatók – közvetlen kapcsolatba kerüljenek egymással. A decentralizált rendszerek nem támaszkodnak egyetlen, mindent ellenőrző központi entitásra, ami számos előnyt hordoz magában. A mai pénzügyi rendszerek, mint például a banki utalásokat támogató SWIFT-hálózat, központi szereplőkre épülnek. A SWIFT világszerte biztosítja a bankok közötti kommunikációt, azonban a rendszer használata magas költségekkel jár, és a nemzetközi tranzakciók teljesítése akár több napot is igénybe vehet. A kriptopénzek megjelenése ezt a modellt alapjaiban kérdőjelezi meg: segítségükkel a tranzakciók gyorsabbá és olcsóbbá válnak, mivel nincs szükség központi jóváhagyásra. Egy nemzetközi utalás például a blokkláncon keresztül percek alatt teljesülhet, miközben a költségek minimálisra csökkennek. Ezek az előnyök jelentős változásokat hozhatnak a globális pénzügyi rendszerekben. Az olcsóbb és gyorsabb pénzmozgások felgyorsíthatják a gazdasági folyamatokat, növelve a globális gazdaság hatékonyságát. Ugyanakkor a decentralizáció negatív hatásai is megjelenhetnek, például az anonimitás révén a pénzmosás és a terrorizmus finanszírozása is egyszerűbbé válhat. A kriptopénzek alacsony tranzakciós költségei gazdaságélénkítő hatással is bírhatnak. Mivel a vállalatok és a magánszemélyek kevesebbet költenek a pénzügyi műveletekre, több pénz marad náluk, amelyet fogyasztásra és

beruházásokra fordíthatnak. Ez a gazdasági növekedést, valamint az állami adóbevételek növekedését is elősegítheti, feltéve, hogy az állam képes kezelni az adózás kihívásait. Azonban a kriptopénzek tömeges elterjedése alapvetően átalakíthatja a pénzügyi rendszerek működését. A legtöbb kriptopénz maximális kibocsátása előre meghatározott, így az államok és központi bankok elveszíthetik azt a lehetőséget, hogy szabályozzák a gazdaságban mozgó pénz mennyiségét. Ez jelentősen csökkentheti az állam befolyását a gazdaságra, mivel a pénzkibocsátás a gazdaságpolitika egyik kulcsfontosságú eszköze. Emellett az államok a kriptopiacokra jelenleg szinte semmilyen kontrollt nem gyakorolhatnak, ami veszélyeztetheti a gazdasági stabilitást. A kriptopénzek véges készlete viszont további problémákat vethet fel. Például a bitcoinból legfeljebb 21 millió létezhet, ami az infláció elkerülését célozza. Azonban, ha a kriptopénzek tulajdonosai hosszú időre felhalmozzák vagyonukat, a gazdaság szempontjából káros lehet a tőke mozgásának hiánya. Továbbá a véges készlet lehetőséget teremthet arra, hogy egy-egy szereplő – legyen az egy állam vagy egy bűnszervezet – jelentős mennyiséget halmozzon fel, és ezzel akár a globális gazdaságot is zsarolni próbálja. A véges pénzkészlet deflációhoz is vezethet. Ha a gazdaságban elérhető pénzmennyiség nem növelhető, de a kereslet új termékek és szolgáltatások iránt folyamatosan bővül, a termelők kénytelenek lehetnek csökkenteni áraikat. Bár ez kedvező lehet a fogyasztók számára, a vállalatok számára nehézséget okozhat, hiszen csökkentheti a bevételeiket. Hosszabb távon ez a gazdasági növekedés lassulásához vezethet, mivel kevesebb új termék és szolgáltatás kerülhet a piacra. *(Györfi, 2019)*

9. A kriptovaluták árfolyamát meghatározó fő tényezők

A kriptovaluták árfolyamát számos tényező befolyásolja, amelyek a piac jövőjét és ezen digitális eszközök hasznosságát is alakítják. Az értéküket alapvetően az határozza meg, milyen gazdasági funkciókat töltenek be, és milyen problémákra nyújtanak megoldást. A hagyományos fiat valuták ötféle funkcióval rendelkeznek: csereeszközként, elszámolási és fizetési eszközként, értékőrzőként, valamint világpénzként is használhatók. Ezek a kritériumok a kriptovaluták megítélésében is iránymutatók. A csereeszköz szerepkörét tekintve, egyre több vállalat fogadja el a kriptovalutákat a világ számos országában. Az USA-ban például már több ezer vállalkozásnál érhető el kriptovaluta-ATM vagy biztosított a kriptofizetési lehetőség. A trendek különösen a bitcoin elfogadottságát erősítik, hiszen már két ország, El Salvador és a Közép-afrikai Köztársaság is hivatalos fizetőeszközként vezette be. Mivel a bitcoin kínálata korlátozott – legfeljebb 21 millió érme érhető el –, ezért a volatilitása ellenére bizonyos

értékőrző funkcióval is rendelkezhet, különösen az inflációval szemben. Ugyanakkor recessziós időszakokban még kevés tapasztalat áll rendelkezésre arra vonatkozóan, hogy ezek az eszközök mennyire képesek megőrizni értéküket. A kriptopénzek árfolyamának alakulását nagymértékben befolyásolja a hagyományos befektetési eszközökkel, mint az arany, az olaj és a részvénypiacokkal való kapcsolatuk. Az arany, mint klasszikus értékőrző eszköz, a menedékként ismert szerepét az évek során folyamatosan megőrizte. Az elemzők a bitcoint egyre gyakrabban emlegetik „digitális aranyként," mivel inflációval szembeni védelmet nyújthat. Ugyanakkor a kutatások vegyes eredményeket mutatnak, és több elemzés is azt igazolja, hogy a bitcoin nem rendelkezik az arany stabilitásával, különösen piaci sokkok idején, amikor a bitcoin árfolyama jelentős volatilitást mutat. A pandémia idején a kriptopénzek jelentősége inkább a portfóliódiverzifikációban (20-30 elemből álló **portfólió** tekinthető jól diverzifikáltnak) mutatkozott meg. A kriptopiacok és a devizapiac kapcsolata is meghatározó; egyes kutatások szerint a Covid–19-járvány idején a kriptopénzek piaca az amerikai dollár árfolyamának mozgatójává vált. A vezető kriptovaluták piacán belüli kapcsolatokat elemezve az is kiderült, hogy a kriptoeszközök szorosabban összekapcsolódnak egymással, bár a különböző eszközök nem feltétlenül reagálnak azonos módon a piaci változásokra.

A szabályozásoknak is jelentős hatásuk van a kriptovaluták árfolyamára. A kínai kormány szabályozási lépései például jelentős tovagyűrűző hatást gyakoroltak a kriptopiacra, és megnövelték a kriptoügyletek számát más valutákkal, mint a japán jen és a koreai won. Az ilyen korlátozó intézkedések hatására a közvetlen kriptokereskedés is egyre népszerűbb lett. Egy másik példa a 2021-es kínai kriptodeviza-tiltás, amely a helyi piacokról a nemzetközi kriptopiacra tolta át a kockázatot, és a keresztkorrelációs kapcsolatok átrendeződését is magával hozta. *(Czeczeli, Vilonya: 2022)*

Végső soron elmondható, hogy a kriptopiac dinamikája az évek során egyre érettebbé vált, amely pozitívan befolyásolja a kriptopénzek stabilitását és a piaci buborékok kialakulásának csökkenését. Az árfolyamok továbbra is ki vannak téve a nagy ármozgásoknak és a piaci bizonytalanságoknak, és míg egyes kriptopénzek, például a bitcoin, nagyobb stabilitást nyújtanak, a kisebb eszközök jelentős kockázatokat hordoznak.

10. Szabályozások

A kriptovaluták globális szabályozása még mindig nem egységes, és számos országban jogi bizonytalanságot okoz mind a szolgáltatók, mind a felhasználók számára. A szabályozások hiánya vagy folyamatos változása jogi kockázatokat rejt magában, azonban megfelelő törvényi keretek bevezetésével ezek a kockázatok minimalizálhatók. A szabályozás célja a csalások és illegális tevékenységek elleni küzdelem, a befektetők védelme, valamint a jogbiztonság megteremtése minden érintett fél számára. Bár egyes szolgáltatók és felhasználók a szabályozást szabad mozgásterük és anonimitásuk korlátozásának tekintik, összességében hozzájárul a kriptoszektor professzionalizációjához és hosszú távú stabilitásához.

A szabályozott kriptotőzsdék és szolgáltatók megbízhatóbbak a befektetők és ügyfelek számára, nagyobb biztonságot nyújtanak, és lehetővé teszik a kriptovaluták integrálását a hagyományos pénzügyi rendszerbe, elősegítve ezzel szélesebb körű elfogadásukat és használatukat. A szabályozás azonban közvetlen hatással van a piac működésére és szereplőire.

Világszerte eltérőek a kriptovalutákra vonatkozó szabályozások: míg Japán és Svájc fejlett, jól kidolgozott keretekkel rendelkezik, addig Kína és India szigorú korlátozásokat vezettek be, vagy részben be is tiltották a kriptovaluták kereskedelmét és használatát. Emiatt a nemzetközi együttműködés és szabályozási harmonizáció kulcsfontosságú a kriptovaluták jövője szempontjából. Az olyan megközelítések, mint a szabályozási „sandbox” rendszerek, például az Egyesült Királyságban és Szingapúrban, lehetőséget biztosítanak az induló kriptovállalkozásoknak arra, hogy ellenőrzött környezetben teszteljék termékeiket és szolgáltatásaikat, miközben védik a befektetőket. Az önszabályozó szervezetek, mint például a Virtual Commodity Association és a Crypto Valley Association, szintén segítik az eligazodást az ágazatban, irányelveket kidolgozva a magas szintű befektetővédelem érdekében.

A pénzügyi szabályozó hatóságok és a kriptotőzsdék közötti fokozott együttműködés szükséges a szabályok betartásának biztosítása érdekében. Az olyan nemzetközi szervezetek, mint a Pénzügyi Akció Munkacsoport (FATF), frissítették a pénzmosás és a terrorizmus finanszírozása elleni ajánlásaikat a kriptoeszközök kapcsán. A Pénzügyi Stabilitási Tanács és a G20-ak által folytatott párbeszéd fontos lépések a befektetővédelem globális minimumszabályainak megerősítése érdekében.

A kriptovaluták szabályozásában azonban még mindig számos kihívás és bizonytalanság áll fenn. A meglévő szabályozások lassan alkalmazkodnak a gyorsan fejlődő kriptopiachoz és új

technológiákhoz, mint például az intelligens szerződések, a decentralizált pénzügyi szolgáltatások (DeFi) és a stabil érmék. A nemzeti és nemzetközi szabályozások harmonizálására van szükség a befektetővédelem egységes szabványainak megteremtése és a szabályozási arbitrázs elkerülése érdekében. Továbbá a transzparencia növelése és az információ megosztásának gyorsítása is elengedhetetlen a bizalom erősítése és a kockázatok csökkentése érdekében.

Oktatási programok és tájékoztató kampányok segíthetnek a befektetők felvilágosításában a kriptoeszközök kockázatairól és lehetőségeiről, hogy megalapozott döntéseket hozhassanak. Az adóztatás országonként eltérő, és a nyereség típusától függően változhat. Például az Egyesült Államokban az adóhatóság (IRS) tulajdonként kezeli a kriptovalutákat, és nyereségadóval terheli őket. Rövid távú nyereség esetén a szokásos jövedelemadó-sávok, míg hosszú távú nyereség esetén kedvezményes adókulcsok vonatkoznak rájuk. Németországban a kriptovalutákból származó nyereség adómentes, ha az egyéves tartási időszak után realizálódik. Japánban a kriptovaluták kereskedelméből származó nyereség progresszív jövedelemadó alá esik.

A nemzetközi együttműködés és a globális szabályozási standardok kialakítása kulcsfontosságú a szabályozás széttagoltságának elkerülése és az átlátható, tisztességes környezet megteremtése érdekében. Ez hozzájárulhat a kriptovaluták szélesebb körű elfogadásához és hosszú távú sikeréhez. *(Varga, Birher, Knoll-Csetet: 2024)*

Az Európai Unió 2022 júniusában ideiglenes megállapodást kötött a kriptoeszközök új, egységes szabályozásáról, amely a piac szereplőit, fogyasztókat és környezeti kérdéseket egyaránt érinti. Az új szabályozási keretrendszer, amely a MiCA (Markets in Crypto-Assets) nevet viseli, a kriptoeszközök piacán kíván átláthatóságot, fogyasztóvédelmet és piaci stabilitást teremteni. Az új előírások kiterjednek a kriptoeszközök kibocsátásának és kereskedelmének átláthatóságára, közzétételére, engedélyezésére és felügyeletére, miközben szigorú előírásokat vezetnek be a pénzügyi bűncselekmények, például a pénzmosás és a terrorizmus finanszírozása ellen is.

A MiCA jogszabály a pénzügyi stabilitás és a fogyasztóvédelem erősítésére fókuszál. A szabályozás arra kötelezi a kriptoeszköz-szolgáltatókat (CASP-okat), hogy tájékoztassák ügyfeleiket a kockázatokról, költségekről és díjakról, valamint, hogy megfeleljenek a piac integritását és stabilitását támogató követelményeknek. A szabályok hatálya kiterjed minden olyan kriptoeszközre, amely nem esik a jelenlegi pénzügyi szabályozások alá. Az Európai Értékpapír-piaci Hatóság (ESMA) feladata lesz egy nyilvántartás létrehozása azoknak a

szolgáltatóknak a nyomon követésére, akik engedély nélkül nyújtanak kriptoeszköz-szolgáltatásokat az EU-ban. Kiemelt cél az is, hogy csökkentsék a kriptovaluták környezeti hatásait, különösen az energiaigényes bányászati és tranzakció-ellenőrzési folyamatokat. Az új szabályozás kötelezi a jelentős kriptoeszköz-szolgáltatókat, hogy nyilvánosan tegyék közzé energiafogyasztási adataikat, és az adatokat juttassák el a nemzeti hatóságokhoz, amelyek továbbítják azokat az ESMA-nak.

A szabályozás különbséget tesz a kriptoeszközök különböző típusai között: a kriptovaluták, például a Bitcoin, alternatív csereeszközként és befektetésként funkcionálnak, és a központi bankok által kibocsátott valuták alternatívái lehetnek. A tokenek, amelyeket gyakran vállalkozói projektekhez bocsátanak ki, befektetési lehetőséget nyújtanak, míg a stabil érmék értékét reáleszközök fedezik, ezáltal stabilabb és szélesebb körű felhasználási lehetőséget biztosítanak.

Az új EU-s szabályozás számos előnyt kínál a kriptoeszközök piacán: célja a jogbiztonság és az innováció támogatása, a fogyasztók és befektetők védelme, valamint a piac stabilitásának megőrzése. A kriptoeszközök körüli jogi bizonytalanság csökkentésével az EU szeretné elősegíteni, hogy e technológiák fenntartható módon fejlődjenek és szolgálják a gazdaságot, anélkül, hogy veszélyeztetnék a pénzügyi rendszert vagy környezeti problémákat okoznának. (*https://www.europarl.europa.eu/news/hu/press-room/20220613IPR32840/cryptocurrencies-in-the-eu-deal-struck-between-parliament-and-council* *és* *https://www.europarl.europa.eu/topics/hu/article/20220324STO26154/a-kriptovaluta-veszelyei-es-az-unios-jogszabalyok-elonyei*)

11. Kriptovaluták kereskedelme

11.1. Adózás Magyarországon

2022 január 1-től új szabályok vonatkoznak a kriptoeszközökből származó jövedelem adózására, amelyek már a 2021-es évre is alkalmazhatók. Magánszemélyeknek csak akkor kell adózniuk, ha a kriptoeszközt valós vagyoni értékre váltják, például pénzre, vagy abból ingóságot, ingatlant vásárolnak. Az ügyleti nyereség után 15% személyi jövedelemadót kell fizetni, amelyet a tárgyévi bevétel és a megszerzésre fordított igazolt kiadások különbözeteként kell kiszámítani. A veszteségeket is fel kell tüntetni az adóbevallásban, és azok későbbi adókiegyenlítésre felhasználhatók.

Nem kell adózni, ha a bevétel nem haladja meg a minimálbér 10%-át (20 000 forint), és az adóévben ezek összesen nem lépik túl a minimálbért (200 000 forint). Az adózott jövedelmet a 21SZJA-bevallás 164. sorában kell feltüntetni.

A 2021 előtti kriptoügyleteknél a bevételeket és kiadásokat összevontan, 2022-es ügyleti eredményként kell figyelembe venni, és az erre vonatkozó adót 2023. május 22-ig kell megfizetni. Az adókiegyenlítés a 2022-es bevallásban lesz először alkalmazható, a 2021-ben keletkezett veszteségek alapján. *(https://nav.gov.hu/ado/szja/a-kriptougyletek-jovedelmenek-adozasa#_ftn1)*

11.2. Kriptotőzsdék

#	Tőzsde	Trust Score	24 órás forgalom (normalizált)	24 órás forgalom	Havi látogatások	Utolsó 7 nap
1	Binance	10/10	24 673 290 193 USD	38 349 820 844 USD	50 M	
2	Bybit	10/10	8 168 153 400 USD	8 168 153 400 USD	20 M	
3	OKX	10/10	6 983 894 304 USD	6 983 894 304 USD	20 M	
4	Coinbase Exchange	10/10	6 267 038 719 USD	6 267 038 719 USD	30 M	
5	KuCoin	10/10	3 071 476 324 USD	3 346 466 448 USD	7 M	

1. ábra Az ábrán látható a megbízhatósági pontszám alapján legjobb 5 kriptovaluta-tőzsde.

Forrás: *https://www.coingecko.com/hu/exchanges*

11.2.1. Binance

A Binance a világ vezető blokklánc-ökoszisztémája, amely egy olyan termékcsomagot kínál, amelyben a legnagyobb digitális eszközökkel való kereskedési platform is helyet kap. A Binance célja, hogy a jövő kriptoalapú infrastruktúrájának alapkövévé váljon. A Binance egy globálisan elismert kriptovaluta-tőzsde, amely egyszerű, biztonságos és hatékony hozzáférést nyújt a digitális eszközökhöz. A platformot naponta több milliárd dollárnyi tranzakcióval használják, és ügyfelek milliói bíznak benne világszerte. A Binance arra törekszik, hogy mindenki számára szabadságot biztosítson pénzügyeik kezelésére – beleértve azokat, akik pénzt keresnek, tárolnak, költenek, megosztanak, vagy akár adományoznak is. Náluk a felhasználók állnak az első helyen. A platform a legmodernebb biztonsági intézkedéseket és szigorú adatvédelmi szabályokat alkalmazza, hogy védje ügyfeleit és eszközeiket. Az Binance elkötelezett a magas szintű szabályozói megfelelés mellett, hogy fenntartható és felelős

növekedést biztosítson a blokklánc iparágban. A Binance alapítói, Changpeng Zhao (CZ) és Yi He, kiemelkedő szerepet játszottak a vállalat globális sikerében. **CZ** a Binance társalapítója és korábbi vezérigazgatója, aki több sikeres startupot is létrehozott. 2017-ben indította el a Binance-t, amely mindössze 180 nap alatt a világ legnagyobb kriptotőzsdéjévé vált. CZ a blokklánc-technológia úttörője, aki jelentős szerepet vállalt a Binance Exchange, Labs, Launchpad, Trust Wallet és számos más szolgáltatás megalkotásában. **Yi He**, a Binance másik társalapítója, a vállalat üzleti stratégiáját, marketingjét és márkaépítését irányítja. Korábban az OKCoin társalapítójaként és a Yixia Technology alelnökeként tevékenykedett, ahol az innováció és az üzleti növekedés meghatározó alakja volt. Yi He az egyik legbefolyásosabb női vezető a blokklánc-iparban, és kiemelkedő szerepet játszik abban, hogy növelje a nők jelenlétét és szerepét a technológiai szektorban. Közösen a Binance alapítói nemcsak a vállalatot, hanem a globális blokklánc-ökoszisztémát is jelentősen formálták. A Binance a világ egyik legnagyobb kriptotőzsdéje, amely lenyűgöző számokat tudhat magáénak. A platformon a napi átlagos kereskedési volumen eléri a 65 milliárd dollárt, míg 2022-ben a spot piacon összesen 300 milliárd tranzakciót hajtottak végre. Ezek az adatok jól mutatják a Binance jelentőségét a globális kriptopénz-ökoszisztémában. *(https://www.binance.com/en/about)*

11.2.2. Bybit

A Bybit lenyűgöző fejlődést mutatott be 2018-as indulása óta, és ma már a világ egyik vezető kriptotőzsdéje. 2024-ben a Bybit átlépte a 40 millió felhasználót, ezzel a világ második legnagyobb kriptotőzsdéjévé vált. Az innováció jegyében elindította a Bybit Web3 platformot, amelyhez további 10 millió felhasználót csatlakoztatott a Bybit Wallet segítségével. Emellett megnyitotta első európai irodáját Hollandiában, és bővítette partneri kapcsolatait. 2023-ban a Bybit Dubai központjában helyezkedett el, megszerezve az MVP engedélyt. Felhasználói száma meghaladta a 20 milliót, és a CoinGecko a legmegbízhatóbb kriptotőzsdék között tartja számon. A Bybit rendszeresen a három legnagyobb volumenű tőzsde között szerepelt, valamint globális együttműködésbe kezdett a Mastercarddal, amelynek eredményeként elindította az exkluzív Bybit kártyát. 2022-ben a Bybit továbbra is fejlődött a kihívások közepette. Mindössze 39 nap alatt mutatta be az egységes kereskedési számlát, és bevezette a USDC-alapú opciós szerződéseket BTC és ETH számára. Az Oracle Red Bull Racing csapatával kötött partnersége rekordokat döntött, miközben valós idejű átláthatóságot biztosított vagyonkimutatásai révén a Proof-of-Reserves rendszerében. A korábbi évek is tele voltak sikerekkel. 2021-ben a Bybit elérte a napi 70 milliárd dolláros kereskedési volument, és teljes körű kriptotőzsdévé vált. 2020-ban már 4 milliárd dolláros napi volumennel megelőzte a BitMEX-et, míg 2019-ben lefektette

alapelveit: „Hallgatunk, törődünk, fejlődünk.” 2018-ban a Bybit két hónap alatt elindította első BTCUSD Inverse Perpetual Contractját, új korszakot nyitva a kriptokereskedelemben. *(https://www.bybit.com/en/promo/global/aboutus/)*

Ben Zhou, a Bybit társalapítója és vezérigazgatója, egy kriptoderivatív tőzsdét hozott létre, amelynek székhelye Szingapúrban található. Zhou Új-Zélandon nőtt fel, majd az Egyesült Államokban járt egyetemre. Később visszatért Kínába, ahol hét évig a Forex XM brókercég kínai régiójának ügyvezető igazgatójaként dolgozott. Zhou 2016-ban barátai révén ismerkedett meg a kriptovalutákkal, és gyorsan felfedezte a kriptokereskedelemben rejlő lehetőségeket. 2017-ben, amikor a kriptopiac fellendült, úgy érezte, hogy az általános közvélemény még kevéssé ismeri az ágazatot. Ennek hatására indított egy YouTube-csatornát, hogy oktatási tartalmakat nyújtson a kriptovilágról. Ezt a projektet közvetlenül a Bybit megalapítása előtt zárta le. A kriptók iránti érdeklődése és az XM-nél szerzett tapasztalatai révén Zhou felismerte a kriptokereskedelem egyes hatékonysági hiányosságait, mint például a rendszerleállásokat és a megfelelő ügyfélszolgálat hiányát. Ezek az élmények vezettek a Bybit 2018-as megalapításához, amelynek mottója: „Hallgatunk, törődünk, fejlődünk.” A Bybit célja a kriptoderivatív tőzsdék színvonalának emelése és a lehető legjobb kereskedési élmény biztosítása. A platform perpetuális szerződéseket kínál, és képes 100,000 tranzakciót kezelni másodpercenként, mindössze 10 mikroszekundumos feldolgozási idővel. A platform frissítéseit úgy hajtják végre, hogy nincs szükség szerverleállásra. A Bybit 24/7 élő ügyfélszolgálatot biztosít angol, kínai, japán és koreai nyelven. *(https://cryptoslate.com/people/ben-zhou/)*

12. Kriptovaluták kereskedésének lehetőségei

A kriptovalutákba való befektetésről sokan tévesen azt gondolják, hogy gyors és könnyű módja a meggazdagodásnak. Az igazság azonban az, hogy ez a piac rendkívül ingatag és kiszámíthatatlan, tele van kockázatokkal és spekulációval. A kriptovaluták körüli felhajtás és a spekuláció miatt sokan elveszítik megtakarításaikat, ami általában több kárt okoz, mint hasznot. Ezek az eszközök a hagyományos pénzekhez képest jóval nagyobb árfolyamingadozást mutatnak: egyes valuták értéke akár naponta 10 000%-kal is emelkedhet, majd órákon belül elveszíthetik ezt a nyereséget. Ez a szélsőséges volatilitás egy kétélű kard: bár lehetőséget ad gyors nyereség elérésére, ugyanilyen gyors veszteségeket is eredményezhet. Emellett a piac mérete és a befektetett tőke mennyisége is problémákat okoz, például a manipuláció lehetőségét, amit a nagyobb szereplők (ún. "bálnák") kihasználnak. A bálnák (whale) olyan

piaci szereplők, akik hatalmas mennyiségű kriptovalutát birtokolnak, akár több száz millió vagy milliárd dollár értékben. Bár kilétük anonim, tárcáik nyilvánosak, így tranzakcióik hatásai jól láthatók. Egyetlen nagyobb eladással például jelentős árfolyamesést idézhetnek elő. Ha egy bálna hatalmas mennyiségű valutát, például Dogecoint ad el, a piacot elárasztja a kínálat, és ha a kereslet nem tart lépést, az árfolyam zuhanásnak indul. A piaci pánik tovább fokozhatja az eladási hullámot. Hasonló folyamat zajlik le fordított helyzetben, amikor egy bálna nagy mennyiségben vásárol, felhajtva az árfolyamot. A bálnák tisztában vannak pozíciójukkal, és gyakran visszaélnek ezzel. Az egyik jellemző piaci manipulációs technika a "whale dump and buy back", amely során egy bálna nagy eladással leveri az árfolyamot, majd alacsonyabb áron visszavásárolja az eszközt, jelentős nyereséget termelve saját pénze mozgatásával. Ez az előny azonban kisebb befektetők vesztesége árán valósul meg. Az ilyen manipulációk nagyban hozzájárulnak a kriptovaluták árának kiszámíthatatlanságához. A volatilitást tovább növeli, hogy a kriptovaluták technológiája még viszonylag új, és kevés történelmi adat áll rendelkezésre az ármozgások vizsgálatára. Sok befektető technikai elemzést alkalmaz, amely a múltbeli mozgások elemzésével próbál jövőbeli trendeket meghatározni. Azonban az adatok hiánya miatt ezek az előrejelzések gyakran spekulatívak, és a tapasztalt kereskedők sikerességi aránya is mindössze 55%, ami alig jobb, mint a véletlenszerű találgatás. Mindezek alapján elmondható, hogy a kriptovaluták világa rendkívül kockázatos és bizonytalan terület a befektetők számára. *(https://nki.gov.hu/wp-content/uploads/2024/03/A-kriptovalutak-veszelyei.pdf)*

13. Technikai elemzés

A pénzügyi piacokon időről időre megjelenő árfolyambuborékok kérdése összetett és sokrétű jelenség, amely jelentős figyelmet kapott mind az elméleti közgazdaságtanban, mind a gyakorlati befektetési stratégiák elemzésekor. A buborékok olyan helyzeteket jelentenek, amikor egy eszköz árfolyama jelentősen eltávolodik a belső értékétől, vagyis attól az értéktől, amelyet az eszköz a jövőbeni jövedelemtermelő képessége alapján megérdemelne. Ha az ár magasabb, mint a belső érték, pozitív buborékról beszélünk, míg az alacsonyabb ár negatív buborékot jelez. Az ilyen árfolyammozgások jellemzően a piac pszichológiai dinamikájára vezethetők vissza, amelyek racionális közgazdasági modellekkel nem mindig magyarázhatók.

Egy árfolyam felfelé vagy lefelé történő elmozdulása azonban önmagában nem tekinthető buboréknak. Az árfolyam-ingadozások természetes következményei lehetnek a piacot érő új

információknak, amelyek megváltoztatják az eszköz értékelését. A buborékok lényege, hogy az árfolyam eltávolodása a belső értéktől nem fundamentális változásoknak, hanem pszichológiai vagy spekulatív tényezőknek köszönhető, és a piac szereplői továbbra is arra számítanak, hogy ez a tendencia folytatódik. E folyamat egyfajta öngerjesztő mechanizmust hoz létre: a folyamatos emelkedés újabb vásárlókat vonz, akik ár növekedést váltanak ki, amely ismét megerősíti a spekulatív magatartást.

A buborékok kialakulásának folyamata jól szemléltethető különböző befektetési stratégiák versengésével. Kezdetben a piacot a belső értékekre alapozó befektetők uralják, azonban a trendeket kihasználó stratégiák gyorsan népszerűvé válhatnak, különösen akkor, ha rövid távon sikeresnek bizonyulnak. Ahogy egyre több befektető kezd trendkövető stratégiát alkalmazni, az árfolyam elrugaszkodik a fundamentális értéktől, ami a buborék felfúvódásához vezet. E folyamatnak azonban határt szab az a tény, hogy az árak végtelen növekedése irracionális, és előbb-utóbb elkerülhetetlenül bekövetkezik a buborék kipukkadása, ami jelentős árfolyamcsökkenést eredményez.

A technikai elemzés a buborékok világában különösen releváns megközelítés, mivel a múltbéli árfolyamok és a piac szereplőinek viselkedése alapján próbálja megjósolni a jövőbeli trendeket. A technikai elemzők abból indulnak ki, hogy az emberi viselkedés, legyen az racionális vagy irracionális, gyakran sablonos mintázatokat követ. Az árfolyamgrafikonok tanulmányozása révén visszatérő viselkedési sémákat azonosítanak, amelyek alapot adhatnak a jövőbeli ármozgások előrejelzéséhez. E megközelítés előnye, hogy képes észlelni a buboréképítés vagy éppen a kipukkadás korai jeleit, különösen akkor, ha az információk lassan áramlanak a piacon. Az árfolyammozgások trendszerű viselkedése ilyen esetekben lehetőséget teremt arra, hogy a technikai elemzők profitáljanak a piaci dinamikákból.

A technikai elemzésnek azonban komoly korlátai vannak. Működése csak akkor válik relevánssá, ha egy adott árfolyammintázat már kialakult, így a lehetőségek egy részét lekésheti. Továbbá, a mintázatok felismerésére törekvő befektetők tömeges reakciói maguk is torzíthatják a piacot, ami a mintázatok megbízhatóságának csökkenéséhez vezethet. A gyors piaci mozgások szintén problémát jelentenek, hiszen a technikai elemzés feltételezi, hogy a mintázatok kirajzolódásához idő kell. Amikor azonban a piac szereplői az előrejelzésekre azonnal reagálnak, az árfolyamváltozások felgyorsulnak, és a „kicsit előbb” verseny kialakulásával az elemzések hatékonysága csökken. *(Andor, 2018)*

13.1. Japán gyertya

A japán gyertyák eredete a 18. század közepére nyúlik vissza, amikor Munehisa Homma, egy gazdag rizstermelő család sarja, új módszert dolgozott ki az oszakai rizstőzsdén. Homma a piaci hangulat és az ármozgások alapos elemzésével kialakította a gyertyaalapú kereskedési rendszert, amely annyira sikeresnek bizonyult, hogy samuráj rangot kapott. A japán gyertyák vizuálisan mutatják az adott kereskedési időszak fő ármozgásait. A gyertya teste a nyitó- és záróárat, a kanóc pedig az időszak maximum- és minimumárát jelöli. Hagyományosan az emelkedő napokat fehér, a csökkenőket fekete gyertyával jelölték. Manapság zöld és piros színekkel is ábrázolják őket. A módszer a nyugati világban a 20. század második felében vált ismertté, főként Steve Nison munkássága révén, aki népszerűsítette a japán gyertyák használatát a modern technikai elemzésben. *(https://elemzeskozpont.hu/japan-gyertya-29-alakzat-kereskedese-megbizhatosaga-elemzese)*

13.2. Fibonacci számok

Leonardo Fibonacci, más néven Leonardo di Pisa (1170 körül – 1250 körül), a középkor egyik legnagyobb matematikai tehetsége, akit a modern matematika egyik alapítójaként tartanak számon. Nevét a Fibonacci-sorozatról ismerjük, amely ma is számos tudományterület alapvető elemének számít. Nevét leginkább a róla elnevezett Fibonacci-sorozat őrzi, amelynek elemei úgy keletkeznek, hogy minden szám az előző két szám összege: **1, 1, 2, 3, 5, 8, 13, 21, 34, 55, stb.** Ennek a sorozatnak az eredete egy egyszerű problémához kapcsolódik: adott egy pár nyúl, amely havonta egy újabb pár nyulat hoz világra, és minden új nyúlpár két hónapos korától kezdve szintén szaporodik. A kérdés az, hogy hány nyúlpár lesz egy adott hónapban. A nyúlpárok száma pontosan a Fibonacci-sorozat elemei szerint növekszik. A Fibonacci-számok különlegessége az aranymetszéssel való kapcsolatukban rejlik. A sorozat két egymást követő elemének hányadosa egyre közelebb kerül az úgynevezett arany számhoz, amely körülbelül **1,618**. Az aranymetszés (phi) az univerzum egyik alapvető aránya, amely harmóniát teremt szimmetria és aszimmetria között. Ez az arány a természetben és a művészetben egyaránt megjelenik: például a napraforgómagok elhelyezkedése vagy a logaritmikus spirálok is ennek az aránynak engedelmeskednek. A Fibonacci-számok nemcsak a matematikában, hanem a pénzügyi piacokon is fontos szerepet játszanak. Számos kereskedési eszköz épül Fibonacci-alapú számításokra, például Fibonacci-ív, csatorna, ventilátor (fan), időzónák vagy a legismertebb Fibonacci visszatérés (retracement). Ez utóbbit főleg támasz- és ellenállási

szintek, illetve korrekciók meghatározására használják. A kereskedési platformokon elérhető arányok, mint például **23,6%, 38,2%, 50%, 61,8% és 100%**, a piaci mozgások elemzésében segítenek. *(https://traderklub.hu/forex-es-tozsde-leckek/fibonacci-szintek-es-aranyok/ és Simonyi, 2020)*

13.3. Tőzsdei alakzatok

A tőzsdei árfolyam-alakzatok, más néven tőzsdealakzatok, a technikai elemzés fontos eszközei közé tartoznak. Bár a technikai elemzés sok kereskedő által alkalmazott módszer, használata nem egyszerű, mivel felszínes ismeretekkel nem lehet megbízhatóan alkalmazni. Az elemzés objektivitásának hiánya is problémát jelent, ugyanis a technikai elemzés eszközei szubjektív értelmezést igényelnek, amely nagyban függ a kereskedő tapasztalatától. Emiatt a módszerek visszatesztelése és megbízhatóságuk vizsgálata gyakran nehézséget okoz.

Az árfolyam-alakzatok hasznosságát és hatékonyságát több kutatás is vizsgálta. Az első jelentős kutatásokat Robert A. Levy végezte, aki úgynevezett „ötpontos" árfolyam-alakzatokat vizsgált, például a **dupla csúcsot**, **dupla aljat**, **fej-váll alakzatot**, valamint az **emelkedő** és **csökkenő csatornákat**. Levy több mint 9000 kitörést és letörést elemzett, és arra jutott, hogy az árfolyam-alakzatok nem feltétlenül haszontalanok, de hatékonyságuk több tényezőtől függ. Az általa legjobbnak talált alakzatok a következők voltak:

- **Csökkenő csatorna** eladási jelzésre,
- **Fej-váll alakzat** eladási jelzésre,
- **Emelkedő csatorna** eladási jelzésre.

A legkevésbé hatékony alakzatok közé tartozott:

- A **fordított zászló** eladási jelzésre,
- A **csökkenő ék** vételi jelzésre,
- A **csökkenő csatorna** vételi jelzésre.

(https://elemzeskozpont.hu/tozsdei-arfolyam-alakzatok-17-tipus-jelzeseik-megbizhatosaguk)

13.4. RSI indikátor

Az RSI (Relative Strength Index) indikátort J. Welles Wilder fejlesztette ki, és a technikai elemzés egyik népszerű eszközévé vált. Wilder az RSI-t egy momentum alapú oszcillátornak szánta, amelynek segítségével fordulópontokat lehet azonosítani a különböző pénzügyi eszközök, például részvények, indexek és devizák grafikonjain. Az RSI mutató értéke 0 és 100 között mozog, középpontja az 50-es szint.

Az RSI értéke nő, ha az időszakon belül az árfolyam többször és nagyobb mértékben emelkedik, míg csökken, ha az árfolyam inkább esett. Ha az RSI értéke 50 fölött van, az azt jelzi, hogy az emelkedő árfolyammozgások átlagosan nagyobbak, mint a csökkenők. Ezzel szemben, ha az érték 50 alatt van, az átlagos csökkenések felülmúlják az emelkedéseket. Minél magasabb az RSI, annál erősebb az emelkedő trend, és minél alacsonyabb, annál erősebb a csökkenő trend.

Wilder az RSI indikátor használatakor két kulcsszintet emelt ki: a **30-as** és a **70-es** értéket.

- Ha az RSI 30 alá csökken, az adott eszköz **túladott állapotban** van, és fordulópont várható, ami vételi lehetőséget jelezhet. Vételi jelzés keletkezik, ha az RSI értéke visszaemelkedik a 30-as szint fölé.

- Ha az RSI 70 fölé emelkedik, az adott eszköz **túlvet állapotban** van, ami fordulatra és csökkenésre utalhat. Eladási jelzés akkor keletkezik, ha az RSI visszaesik a 70-es szint alá.

Volatilisebb termékeknél a 20-as és 80-as szinteket is használják a túladott és túlvet állapot jelzésére. *(https://elemzeskozpont.hu/rsi-indikator-jelzesei-mukodese-megbizhatosaga)*

Ez a technikai elemzés a Bitcoin árfolyamának vizsgálatára irányul, az egyszerűség kedvéért feltételezve, hogy a számítások során minden tranzakció pontosan 1 Bitcoin vásárlását vagy eladását jelenti. A jelenlegi vizsgálat során dollárban jelenítem meg az eredményt és a pillanatnyi árfolyama a dollárnak 394 Ft = 1 dollár. Az elemzés nem tartalmazza a tranzakciós költségeket, így a számított profit vagy veszteség tisztán az árfolyamváltozásokon alapul. Ez az egyszerűsítés lehetővé teszi, hogy az indikátorok és a kereskedési stratégia hatékonyságára összpontosítsunk anélkül, hogy a költségek torzítanák az eredményeket. A stratégia alapvetően három technikai indikátorra, a mozgóátlagokra, az RSI-re és a Fibonacci-szintekre épül, amelyek a kereskedési döntések meghozatalát támogatják.

Kutatási kérdésem:

Valóban lehetséges-e jelentős anyagi nyereséget elérni technikai elemzési módszerekkel (például RSI indikátorral vagy árfolyam-alakzatokkal vagy mozgóátlagok használatával) a Bitcoin és más kriptovaluták piacán, figyelembe véve a piacok magas volatilitását?

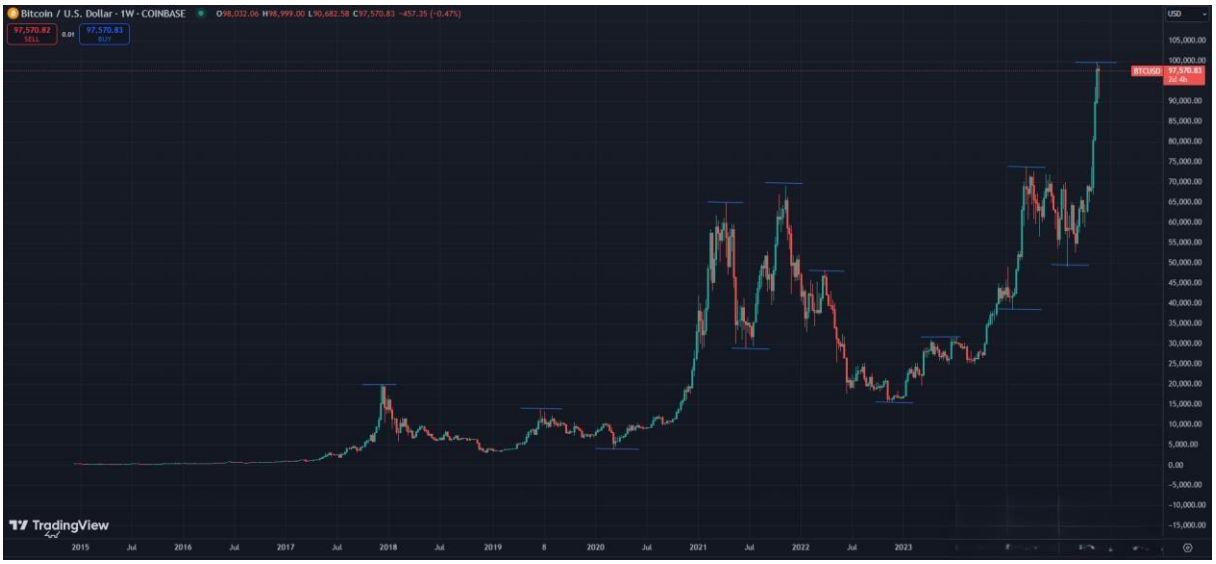
Milyen demográfiai tényezők és befektetési szokások befolyásolják a Bitcoin mint befektetési eszköz népszerűségét, valamint milyen célokkal és motivációkkal fordulnak az emberek ehhez az eszközhöz?

Hipotézis:

1. **Hipotézis:** az RSI indikátor hatékonysága a kriptovaluta piacokon túladott (30-) szintjéről történő fordulóknál a belépések magasabb profithozammal rendelkeznek, mint a mozgóátlagoknál való keresztezés utáni vásárlás.

2. **Hipotézis:** A rövid távú mozgóátlag (pl. 50 napos) és a hosszabb távú mozgóátlag (pl. 200 napos) keresztezései megbízható profitot biztosíthatnak, Fibonacci-szintek alkalmazásával.

13.5. Ellenállási szintek megállapítása



2. ábra Az ábrán látható az ellenállási szintek a Bitcoin árfolyamának. Az árfolyam napi bontásban jelenítettem meg 2015-től.

Forrás: Tradingview

13.6. Fibonacci-szintek alkalmazása

A Fibonacci-szintek a piaci korrekciók és trendfordulók előrejelzésére szolgálnak, a természetes számok arányait használva. Ezek a szintek kulcsfontosságú támasz- és ellenállási szinteket határoznak meg az árfolyammozgásokban. Támaszszintek, ha az árfolyam a Fibonacci-szintek egyikéhez közeledik (például 38,2%, 50% vagy 61,8%), a kereskedők gyakran számítanak arra, hogy az ár visszapattan, és emelkedni kezd. Ez vételi lehetőséget jelenthet. Ellenállásszintek, ha az árfolyam a Fibonacci-szintek egyikét éri el felfelé irányuló mozgásban, az ár gyakran visszafordulhat, ami eladási lehetőséget kínálhat. A Fibonacci-szintek segítenek a mozgóátlagokkal és az RSI-vel együttműködve pontosabban azonosítani a kereskedési belépési és kilépési pontokat, növelve a stratégia hatékonyságát.

3. ábra Fibonacci szintek 1. eset

Forrás: Tradingview

100%-os szint: 69919 $

78,6%-os szint: 65545 $

61,8%-os szint: 62095 $

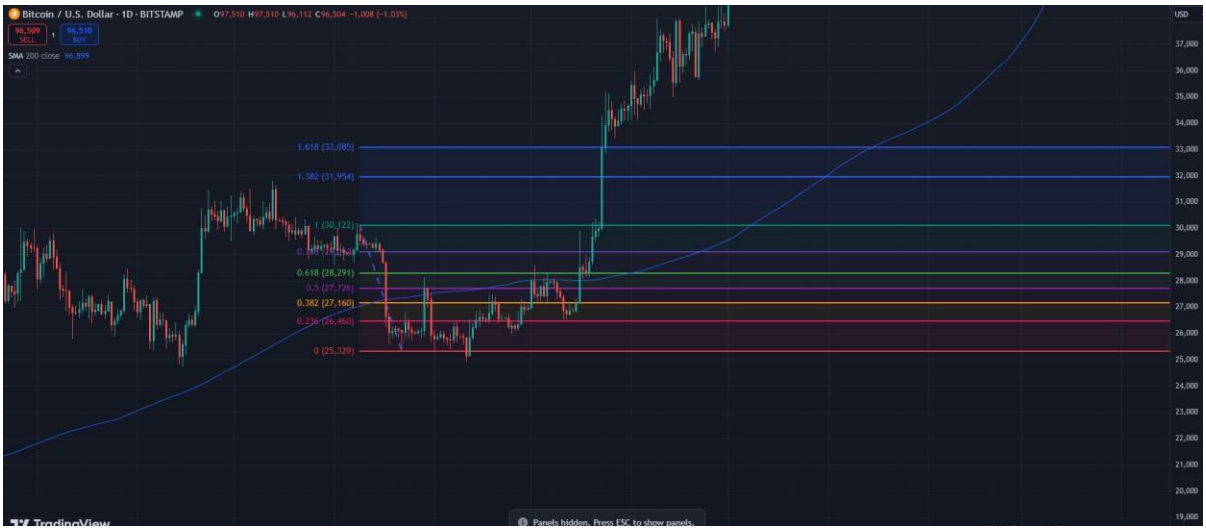
50,0%-os szint: 59678 $

38,2%-os szint: 57262 $

23,6%-os szint: 54272 $

0%-os szint: 49438 $

Az árfolyam a 69919 $-os csúcsot érte el (100%), majd innen kezdett lefelé korrigálni, a fontos ellenállásszintek 49438 $ (0%), 54272 $ (23,6%) voltak. Itt az ár mozgásának követésével lehetett dönteni az eladásról vagy vételről.



4. ábra Fibonacci szintek 2. eset

Forrás: Tradingview

100%-os szint: 30122 $

78,6%-os szint: 29393 $

61,8%-os szint: 28291 $

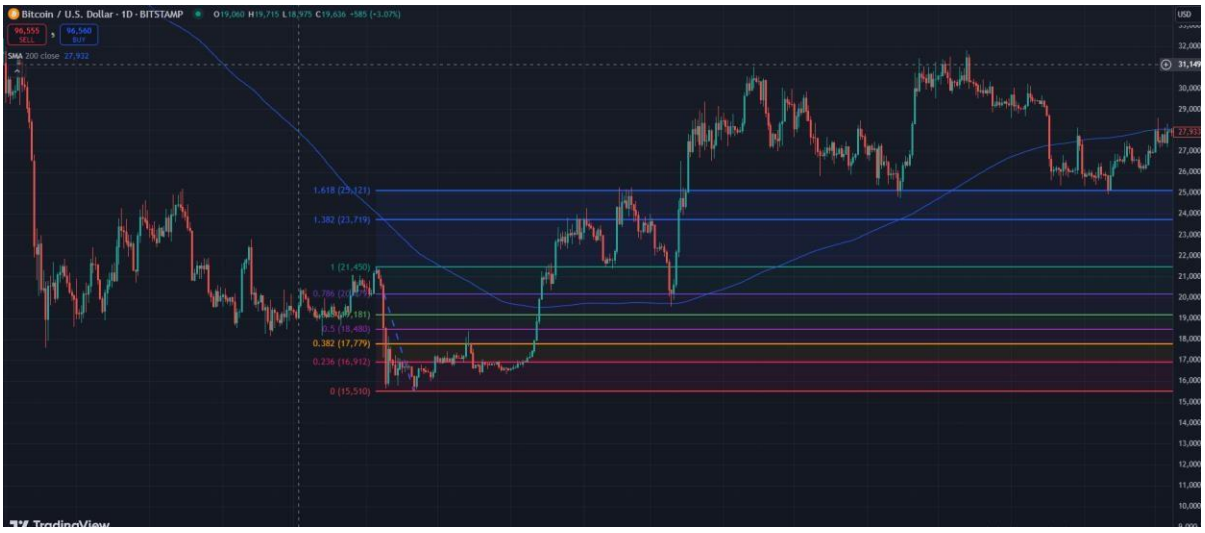
50,0%-os szint: 27726 $

38,2%-os szint: 27160 $

23,6%-os szint: 26460 $

0%-os szint: 25329 $

Az árfolyam elérte a 30122 $-os szintet (100%), majd csökkenés következett be. A kereskedők számára 25329 $-os (0%) szint támaszként és a 28291 $-os (61,8%) szint ellenállásként szolgálhattak a visszapattanásokra



5. ábra Fibonacci szintek 3. eset

Forrás: Tradingview

100%-os szint: 21450 $

78,6%-os szint: 20179 $

61,8%-os szint: 19181 $

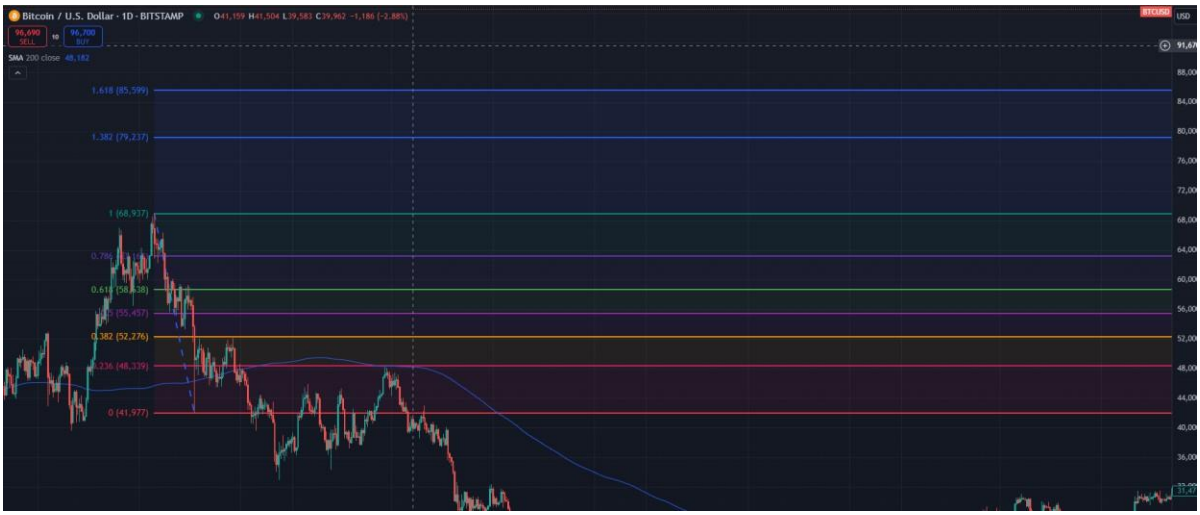
50,0%-os szint: 18480 $

38,2%-os szint: 17779 $

23,6%-os szint: 16912 $

0%-os szint: 15510 $

Az ár 21450 $-nál tetőzött, majd a korrekció során az alsó szintek, például a 15510 $ (0%) érték jelentett fontos fordulópontokat a kereskedési lehetőségek azonosítására.



6. ábra Fibonacci szintek 4. eset

Forrás: Tradingview

100%-os szint: 68937 $

78,6%-os szint: 63162 $

61,8%-os szint: 58638 $

50,0%-os szint: 55457 $

38,2%-os szint: 52276 $

23,6%-os szint: 48339 $

0%-os szint: 41977 $

Itt 68937 $-os csúcsot regisztráltak, amelyről lefelé indult az árfolyam. A szintek, mint például 55457 $ és 48339 $, ellenállási szinteknek bizonyultak, de végül ezeket is áttörve lefelé ment az árfolyam.

7. ábra Fibonacci szintek 5. eset

Forrás: Tradingview

100%-os szint: 59321 $

78,6%-os szint: 53039 $

61,8%-os szint: 48101 $

50,0%-os szint: 44636 $

38,2%-os szint: 41170 $

23,6%-os szint: 36882 $

0%-os szint: 29951 $

Az ár elérte az 59321 $-os szintet, majd a csökkenés során olyan támasz és ellenállásszintek jelentek meg, mint 29951 $ és 41170 $.

A Fibonacci-szintek használata fontos eszköz lehet a piaci ármozgások előrejelzésében, azonban az elemzett esetek alapján egyértelműen látszik, hogy ezek a szintek nem mindig váltják be az elvárt forgatókönyvet.

Például, bár gyakran számíthatunk az árfolyam visszapattanására egy támaszszintről (pl. 38,2% vagy 61,8%), vagy éppen visszafordulásra egy ellenállási szintről, a gyakorlatban előfordulhat, hogy az ár áttöri ezeket a szinteket és nem az elvárt irányba mozdul. Ez különösen akkor jelent kockázatot, ha egy befektető túlzottan támaszkodik a Fibonacci-szintek jelzéseire és nem veszi

figyelembe a piaci környezet egyéb tényezőit, például a hírek, trendek vagy indikátorok szerepét.

Az esetek többségében láthatjuk, hogy ha az árfolyam áttöri a Fibonacci 0,618-as szintjét, az gyakran fordulópontot jelez, amely különösen fontos jelzés lehet a kereskedők számára. A 0,618-as szintet a piaci szereplők az egyik legmegbízhatóbb Fibonacci szintként tartják számon, amely támaszként vagy ellenállásként működhet. Ennek áttörése általában jelentős piaci mozgást indít el, mivel utalhat a trend folytatódására vagy megfordulására. Amennyiben ezt a jelenséget a 200 napos mozgóátlag figyelembevételével elemezzük, az erőteljes vételi jelzésként értelmezhető, különösen akkor, ha az árfolyam a mozgóátlag fölé kerül vagy közelít hozzá. A 200 napos mozgóátlag ugyanis a hosszú távú trend meghatározásának egyik legfontosabb eszköze, amelyet sok piaci szereplő követ.

Azok a szituációk, ahol mind a Fibonacci szintek, mind a 200 napos mozgóátlag erős jelzést adnak, jelentős piaci konszenzust tükröznek. Ez a kombináció csökkenti a hamis jelek esélyét, mivel többszörös megerősítést biztosít a kereskedési döntésekhez. Az ilyen szituációk kihasználása nemcsak pontosabb belépési pontokat tesz lehetővé, hanem javítja a kockázatkezelést is, mivel a kereskedések kisebb eséllyel fordulnak a kereskedő ellen. Ennek eredményeként a Fibonacci szintek és a 200 napos mozgóátlag kombinált használata különösen nyereséges kereskedési stratégiát eredményezhet, mivel lehetővé teszi a legnagyobb valószínűséggel profitáló ügyletekbe való belépést.

13.7. Mozgóátlag

A mozgóátlagok, mint az 50 napos és a 200 napos mozgóátlag, a technikai elemzés népszerű eszközei, amelyek az árfolyamtrendek azonosítására és a kereskedési döntések támogatására szolgálnak. Ezek a mutatók az adott időszak átlagárát jelenítik meg, így kisimítják a rövid távú árfolyam-ingadozásokat, és a piaci trendek tisztább képét adják. A kereskedési stratégia az árfolyam és a mozgóátlag metszéspontjaira alapoz. Az alábbi elveken nyugszik: Vételi jelzés, amikor az árfolyam alulról metszi a mozgóátlagot, az egy potenciális vételi helyzet. Ez azt sugallja, hogy az árfolyam felfelé mozdulhat el, és az emelkedő trend kezdetét jelezheti. Az eladási jelzés, amikor az árfolyam felülről metszi a mozgóátlagot. Ez arra utal, hogy az árfolyam csökkenő pályára léphet, és érdemes lehet realizálni a nyereséget vagy minimalizálni a veszteséget.

50 napos

Dátum	Árfolyam		Realizát összeg
2017.04.03	$1 122	vétel	
2017.04.15	$1 155	eladás	$33
2017.07.20	$2 548	vétel	
2017.07.25	$2 530	eladás	-$18
2017.07.27	$2 550	vétel	
2017.09.13	$3 860	eladás	$1 310
2017.09.18	$4 050	vétel	
2017.09.19	$3 970	eladás	-$80
2017.09.27	$4 150	vétel	
2017.09.29	$4 100	eladás	-$50
2018.02.20	$11 724	vétel	
2018.02.21	$10 990	eladás	-$734
2018.02.28	$10 617	vétel	
2018.03.07	$9 993	eladás	-$624
2018.04.19	$8 460	vétel	
2018.05.17	$8 004	eladás	-$456
2018.07.17	$6 841	vétel	
2018.08.08	$6 812	eladás	-$29
2018.08.27	$7 032	vétel	
2018.09.05	$7 000	eladás	-$32
2019.01.07	$3 969	vétel	
2019.01.10	$3 663	eladás	-$306
2019.02.18	$3 688	vétel	
2019.07.16	$9 844	eladás	$6 156
2019.07.18	$10 090	vétel	
2019.07.23	$10 160	eladás	$70
2019.08.03	$10 690	vétel	
2019.08.13	$10 829	eladás	$139
2019.08.19	$10 900	vétel	

2019.08.20	$10 690	eladás	-$210
2019.09.03	$10 564	vétel	
2019.09.06	$10 299	eladás	-$265
2019.10.26	$8 974	vétel	
2019.11.15	$8 481	eladás	-$493
2020.01.07	$7 396	vétel	
2020.02.27	$9 201	eladás	$1 805
2020.04.21	$6 903	vétel	
2020.06.15	$9 201	eladás	$2 298
2020.07.21	$9 419	vétel	
2020.09.03	$11 022	eladás	$1 603
2020.10.08	$10 903	vétel	
2021.03.25	$50 326	eladás	$39 423
2021.04.30	$57 256	vétel	
2021.05.02	$56 009	eladás	-$1 247
2021.05.07	$56 960	vétel	
2021.05.10	$56 360	eladás	-$600
2021.07.25	$34 553	vétel	
2021.09.07	$43 079	eladás	$8 526
2021.09.14	$46 582	vétel	
2021.09.20	$46 186	eladás	-$396
2021.10.01	$46 979	vétel	
2021.11.18	$59 009	eladás	$12 030
2022.02.07	$43 013	vétel	
2022.02.17	$41 162	eladás	-$1 851
2022.02.28	$40 568	vétel	
2022.03.04	$39 973	eladás	-$595
2022.03.09	$40 237	vétel	
2022.03.10	$39 576	eladás	-$661
2022.03.16	$40 376	vétel	
2022.04.11	$41 674	eladás	$1 298
2022.04.21	$42 399	vétel	
2022.04.21	$41 748	eladás	-$651

2022.07.19	$23 519	vétel	
2022.07.25	$11 949	eladás	-$11 570
2022.07.27	$22 099	vétel	
2022.08.19	$22 029	eladás	-$70
2022.09.12	$22 300	vétel	
2022.09.13	$21 627	eladás	-$673
2022.10.25	$19 717	vétel	
2022.11.08	$19 563	eladás	-$154
2022.12.14	$18 173	vétel	
2022.12.15	$17 593	eladás	-$580
2023.01.04	$16 900	vétel	
2023.03.03	$22 774	eladás	$5 874
2023.03.13	$23 040	vétel	
2023.04.24	$26 973	eladás	$3 933
2023.05.28	$28 297	vétel	
2023.05.29	$28 087	eladás	-$210
2023.06.20	$27 124	vétel	
2023.07.24	$28 824	eladás	$1 700
2023.08.01	$29 673	vétel	
2023.08.02	$29 518	eladás	-$155
2023.08.08	$30 100	vétel	
2023.08.09	$29 885	eladás	-$215
2023.09.19	$27 200	vétel	
2023.09.21	$27 000	eladás	-$200
2023.09.28	$28 718	vétel	
2024.01.03	$40 644	eladás	$11 926
2024.01.16	$42 997	vétel	
2024.01.17	$42 703	eladás	-$294
2024.01.29	$43 055	vétel	
2024.01.31	$42 644	eladás	-$411
2024.02.06	$43 097	vétel	
2024.04.12	$65 864	eladás	$22 767
2024.05.15	$65 306	vétel	

2024.06.14	$65 703	eladás	$397
2024.06.16	$66 483	vétel	
2024.06.18	$66 081	eladás	-$402
2024.07.15	$64 158	vétel	
2024.07.18	$63 400	eladás	-$758
2024.08.08	$62 459	vétel	
2024.08.09	$61 583	eladás	-$876
2024.08.23	$61 822	vétel	
2024.08.27	$61 782	eladás	-$40
2024.09.13	$60 389	vétel	
2024.09.14	$59 592	eladás	-$797
2024.09.17	$59 513	vétel	
2024.10.02	$60 030	eladás	$517
2024.10.03	$60 906	vétel	
2024.10.09	$60 389	eladás	-$517
2024.10.11	$60 906	vétel	
2024.11.30	$96 000	eladás	$35 094
Összesen			$129 679

1. táblázat 50 napos mozgóátlag és az árfolyam keresztezések vétele és eladása.

Forrás: Saját szerkesztés Exelben

A táblázat alapján a technikai elemzés során a Bitcoin vételi és eladási tranzakciók időpontjait és azok eredményeit vizsgáltuk. Összesen 56 darab eladás történt. Az elemzés célja annak bemutatása, hogy a különböző kereskedési stratégiák milyen eredményt érhettek volna el egy 1 Bitcoin vásárlására vonatkozó egyszerű modell alkalmazása mellett. Az alábbiakban összefoglalom az elemzés legfontosabb megállapításait:

A Bitcoin kereskedés során 2017 és 2024 között több fontos tranzakció zajlott, amelyeket a mozgóátlag alapján határoztam meg. 2017 áprilisi és szeptemberi időszakában az árfolyam kisebb ingadozásokkal jellemezte a piacot, és több tranzakció veszteséggel zárult, kivéve a szeptember 13-i eladást, amely 1 310 dollár nyereséget hozott. 2018-ban február és szeptember között a piac csökkenő trendet mutatott, és az év végére a kereskedések veszteséggel zárultak, mivel az árfolyam tovább csökkent. 2019-ben január és november között az árfolyam fokozatos emelkedését figyelhettük meg, különösen a július 16-i eladás hozott jelentős, 6 156 dolláros

nyereséget, míg az év második felében kisebb veszteségek keletkeztek a volatilitás miatt. 2020 első három negyedévében a Bitcoin emelkedő trendet mutatott, kisebb korrekciókkal, és a február 27-i (1 805 dollár nyereség) és június 15-i (2 298 dollár nyereség) eladások kiemelkedtek a stratégiában. 2021 tavaszán és őszén a piac egyik legkiemelkedőbb emelkedési hulláma zajlott, különösen a március 25-i eladás 39 423 dolláros nyeresége volt jelentős, bár az év vége felé kisebb veszteségek is keletkeztek a volatilitás miatt. 2022-ben a piac csökkenő trendet mutatott, és az árfolyam többször áttörte a támaszszinteket, ami az év leginkább veszteséges időszakává tette ezt az évet. A július 25-i eladás jelentette a legnagyobb veszteséget, -11 570 dollárt. 2023-ban a piac stabilizálódni látszott, és kisebb nyereségeket hozott, különösen a március 3-i eladás 5 874 dolláros nyeresége. Az év második felében a volatilitás ismét visszatért, és több veszteséges tranzakcióval zárult a szeptemberi időszak. 2024-ben a piac ismét jelentős árfolyam-emelkedést mutatott, és az április 12-i eladás 22 767 dollár nyereséget hozott, míg november 30-án a Bitcoin árfolyama 96 000 dollárra emelkedett, és az eladás 35 094 dollár nyereséget eredményezett, amely a legnagyobb nyereség volt a teljes kereskedési időszak alatt. A teljes kereskedési időszakban összesen 129 679 dollár nyereség keletkezett. A szórása 8107 dollár volt.

200 napos

Dátum	Árfolyam		Realizát összeg
2018.02.08	8109	vétel	
2018.03.09	8888	eladás	$ 779
2018.03.11	9223	vétel	
2018.03.12	9004	eladás	-$ 219
2019.04.02	4672	vétel	
2019.09.24	8167	eladás	$ 3495
2019.10.26	8975	vétel	
2019.11.08	9144	eladás	$ 169
2020.01.19	9120	vétel	
2020.01.19	8944	eladás	-$ 176
2020.01.28	8950	vétel	
2020.02.26	8701	eladás	-$ 249
2020.03.02	8775	vétel	
2020.03.08	8617	eladás	-$ 158
2020.04.29	8022	vétel	
2021.05.19	39469	eladás	$ 31447
2021.08.09	45252	vétel	
2021.08.12	44770	eladás	-$ 482
2021.08.13	45735	vétel	
2021.08.17	45252	eladás	-$ 483
2021.08.19	46057	vétel	
2021.09.07	45735	eladás	-$ 322
2021.09.14	46298	vétel	
2021.09.20	45655	eladás	-$ 643
2021.10.01	45420	vétel	
2021.12.04	45977	eladás	$ 557
2021.12.14	47094	vétel	
2021.12.17	46805	eladás	-$ 289
2021.12.21	47383	vétel	

2021.12.28	47570	eladás	$ 187
2023.01.13	19648	vétel	
2023.08.17	27160	eladás	$ 7512
2023.10.16	28105	vétel	
2024.07.04	58379	eladás	$ 30274
2024.07.14	59375	vétel	
2024.08.03	61161	eladás	$ 1786
2024.08.08	62116	vétel	
2024.08.08	61701	eladás	-$ 415
2024.08.24	63321	vétel	
2024.08.26	63362	eladás	$ 41
2024.09.24	63985	vétel	
2024.09.25	63680	eladás	-$ 305
2024.09.26	63902	vétel	
2024.09.30	63570	eladás	-$ 332
2024.10.13	63445	vétel	
2024.11.30	96000	eladás	$ 32555
Összesen			104729

2. táblázat 200 napos mozgóátlag és az árfolyam kereszteződésének vétele és eladása.

Forrás: *Saját szerkesztés Excelben*

A kereskedése során az eladási tranzakciók 23 alkalommal történtek meg amik a következő eredményeket hozták:

Az első tranzakciók 2018 februárjában indultak, amikor a Bitcoin 8109 dolláron került vásárlásra. Az eladásokat a következő hónapban végeztem, melyek közül a március 9-i eladás 779 dollár nyereséget hozott, de a március 12-i eladás veszteséggel zárult (-219 USD). Ezt követően további vásárlások és eladások történtek, de az eredmény vegyes volt. 2019-ben az árfolyam emelkedett, és két fontos tranzakció zajlott, amelyek nyereséget hoztak. A szeptemberi eladás 3495 dollár profitot eredményezett. Az év végére a piac enyhe növekedést mutatott, és kisebb nyereségek voltak, mint például az 169 dolláros nyereség november 8-án. 2020 a kereskedési időszak során a Bitcoin árfolyama volatilis volt, kisebb korrekciókkal. A februári, márciusi és áprilisi tranzakciók viszonylag kis veszteségeket hoztak, de a januári és februári tranzakciók többsége veszteséggel zárult. 2021-ben jelentős emelkedést tapasztalt a

Bitcoin. A március 19-i eladás hatalmas nyereséget hozott, 31 447 dollárt realizálva. Az év további részében kisebb veszteségek is előfordultak, de a piacon erőteljes emelkedés volt jellemző. Az év vége felé volt néhány kisebb nyereség, például a december 4-i eladás, mely 557 dollár nyereséget hozott. 2022-ben jelentős visszaesés volt megfigyelhető, amely a kereskedési időszakot nehezítette. A legnagyobb veszteség július 25-én következett be, -11 570 dollárral, amikor az árfolyam drámaian esett. Ezen kívül több kisebb veszteséggel zárult tranzakció is történt. 2023-as év elején a Bitcoin stabilizálódott, és kisebb nyereségek születtek, például a március 3-i eladásnál, ami 5 874 dollár profitot eredményezett. Az év második felében, a volatilitás növekedése miatt, veszteséges tranzakciók is előfordultak, de az összegzés az augusztusi eladásnál már pozitív eredményeket mutatott. 2024-es év első felében ismét nagyobb árfolyam-emelkedés volt tapasztalható. Az áprilisi eladás 22 767 dollár nyereséget hozott, és november 30-án, amikor a Bitcoin árfolyama elérte a 96 000 dollárt, az eladás 35 094 dollár nyereséget eredményezett, amely a legnagyobb nyereség volt a teljes kereskedési időszak alatt. Ez időszak alatt 104729 dollár nyereséggel zárult a kereskedés, ha minden metszéspontnál 1 Bitcoint vásároltunk volna. A szórása 10793 dollár volt.

13.8. RSI indikátor alapú stratégia

Az RSI indikátor a piac momentumának mérésére szolgál, és segít a túlvett és túladott piaci helyzetek azonosításában. Akkor van vétel, ha az RSI értéke 30 alá esik, az túladott piacot jelez, így vételi lehetőséget kínál. Eladás viszont akkor, amikor az RSI eléri vagy meghaladja a 70-es szintet, az túlvett piacra utal, ezért az eladás válik indokolttá. Ez a stratégia az RSI extrém értékeit használja a potenciális árfolyamfordulók előrejelzésére, kihasználva a piaci túlhúzásokat és korrekciókat.

Dátum	**Árfolyam**		**Realizát összeg**
2017.07.16	1758	vétel	
2017.08.11	3433	eladás	$1 675
2017.09.14	3230	vétel	
2017.10.17	4809	eladás	$1 579
2018.02.05	6905	vétel	
2018.07.24	7695	eladás	$790

2018.11.14	5280	vétel	
2019.02.23	3911	eladás	-$1 369
2019.09.24	8159	vétel	
2020.02.08	9905	eladás	$1 746
2020.03.12	4644	vétel	
2020.04.29	7720	eladás	$3 076
2021.05.18	42300	vétel	
2021.07.28	38803	eladás	-$3 497
2022.01.21	35422	vétel	
2022.03.29	46589	eladás	$11 167
2022.05.09	30010	vétel	
2023.01.11	17315	eladás	-$12 695
2023.03.10	19568	vétel	
2023.03.17	24946	eladás	$5 378
2023.08.17	25234	vétel	
2023.10.21	29475	eladás	$4 241
2024.06.24	58414	vétel	
2024.11.08	75654	eladás	$17 240
Összesen			$29 331

1. táblázat RSI indikátor használata túladott állapotnál vétel és túlvett állapotban eladás.

Forrás: *Saját szerkesztés Excelben*

A Bitcoin kereskedés története alapján az alábbi tranzakciók történtek 2017 és 2024 között, vegyes eredményekkel:

2017-ben az első tranzakciók július 16-án kezdődtek, amikor Bitcoin vásárlás történt 1758 dolláros árfolyamon. Ezt követően 2017 augusztusában, augusztus 11-én a Bitcoin árfolyama 3433 dollárra emelkedett, és az eladás 1 675 dollár nyereséget eredményezett. Szeptember 14-én ismét vásárlás történt 3230 dolláron, majd október 17-én eladásra került sor 4809 dolláros árfolyamon, ami 1 579 dollár nyereséget hozott. 2018-ban a kereskedés február 5-én folytatódott, amikor 6905 dolláros árfolyamon történt vásárlás, majd július 24-én eladásra került sor 7695 dolláron, ami 790 dollár profitot jelentett. Az év végén, november 14-én ismét vásárlás történt 5280 dolláros árfolyamon, de 2019 február 23-án az árfolyam csökkenése miatt az eladás veszteséggel zárult, -1 369 dolláros veszteséggel. A következő vásárlás 2019

szeptember 24-én történt 8159 dolláros árfolyamon, majd 2020 február 8-án eladásra került sor 9905 dolláron, ami 1 746 dollár nyereséget hozott. Az árfolyam ismét csökkent, és 2020 március 12-én vásárlás történt 4644 dolláron, amelyet április 29-én követett egy 7720 dolláros eladás, ami 3 076 dollár nyereséget eredményezett. A következő jelentős vásárlás 2021 május 18-án történt 42 300 dolláros árfolyamon, majd 2021 július 28-án, amikor az árfolyam 38 803 dollárra csökkent, eladásra került sor, és a tranzakció veszteséggel zárult -3 497 dolláros veszteséggel. 2022-ben január 21-én vásárlás történt 35 422 dolláron, majd március 29-én eladás következett 46 589 dolláron, ami 11 167 dollár nyereséget hozott. Május 9-én ismét vásárlásra került sor 30 010 dolláros árfolyamon, de az év végére a tranzakciók eredménye negatív lett, mivel január 11-én egy nagyobb veszteség történt, -12 695 dollár. 2023-ben március 10-én vásárlás történt 19 568 dolláron, majd március 17-én eladásra került sor 24 946 dolláron, amely 5 378 dollár nyereséget eredményezett. Augusztus 17-én újabb vásárlás történt 25 234 dolláron, és október 21-én eladásra került sor 29 475 dolláron, ami 4 241 dollár nyereséget jelentett. A kereskedés folytatódott 2024 június 24-én, amikor 58 414 dolláros árfolyamon történt vásárlás, majd november 8-án eladásra került sor 75 654 dolláron, amely 17 240 dollár nyereséget hozott. Összesen a teljes kereskedési időszakban 29 331 dollár nyereség realizálódott, amely különböző tranzakciók során, ingadozó piaci körülmények között keletkezett. A szórása 7329 dollár volt.

14. Eredmény

Az első hipotézis, miszerint az RSI indikátor hatékonysága a kriptovaluta piacokon túladott (30-) szintjéről történő fordulóknál magasabb profithozammal jár, mint a mozgóátlagok keresztezésén alapuló stratégiák, az elemzés során nem nyert alátámasztást. Az eredmények azt mutatják, hogy az RSI indikátor által generált belépési jelek lényegesen alacsonyabb profitot biztosítottak, mint az 50 napos és a 200 napos mozgóátlag stratégiák. Konkrétan, az RSI indikátor alkalmazásával elért összesített profit 29,331 dollár volt, ami jelentősen alulmúlja az 50 napos mozgóátlag stratégiával elért 129,679 dollár, valamint a 200 napos mozgóátlag stratégiával elért 104,729 dollár eredményt. Ezek az adatok egyértelműen azt jelzik, hogy mind az 50 napos, mind a 200 napos mozgóátlag alapú stratégiák sokkal hatékonyabbak voltak a vizsgált időszakban. A túladott szinteknél történő fordulóknál az RSI indikátor által biztosított jelek valószínűleg nem elegendőek ahhoz, hogy hosszú távon versenyképes profitot biztosítsanak. Ez részben annak is betudható, hogy az RSI indikátor önmagában csak a piaci túladott és túlvett szintek meghatározására alkalmas, és nem veszi figyelembe a trend irányát

vagy a piaci momentumot, amelyek kulcsfontosságú tényezők lehetnek a hosszú távú sikeres stratégiák kialakításában. Ezzel szemben a mozgóátlag stratégiák, különösen az 50 napos és a 200 napos mozgóátlagok keresztezésére alapuló stratégiák, integráltabb képet adnak a piaci trendekről, és erőteljesebb iránymutatást nyújtanak a belépési és kilépési pontokra vonatkozóan.

Az eredmények tehát arra utalnak, hogy az RSI indikátor önálló használata nem elég hatékony ahhoz, hogy felülmúlja a mozgóátlag stratégiák által biztosított profitot. Ugyanakkor ez nem zárja ki az RSI indikátor alkalmazásának értékét, különösen más technikai elemzési eszközökkel kombinálva. Az RSI például hasznos lehet a piaci túladott és túlvett szintek azonosítására, de önmagában kevésbé hatékony, mint a trendek alapján működő stratégiák.

A második hipotézis, miszerint a rövid távú (50 napos) és a hosszabb távú (200 napos) mozgóátlag keresztezései megbízható profitot biztosíthatnak, különösen Fibonacci-szintek alkalmazásával, az elemzés során igazolást nyert. Az eredmények szerint mind az 50 napos, mind a 200 napos mozgóátlag stratégiák magas összesített profitot eredményeztek, ami azt mutatja, hogy ezek a technikai elemzési módszerek hatékonyan alkalmazhatók a kriptovaluta piacokon. Konkrétan az 50 napos mozgóátlag stratégiájával elért profit 129,679 dollár volt, amely felülmúlta a 200 napos mozgóátlag stratégiájával elért 104,729 dollárt. Ez arra utal, hogy a rövidebb távú mozgóátlag stratégiák potenciálisan nagyobb profitot kínálnak, mivel érzékenyebben reagálnak a piaci mozgásokra. Ezzel szemben a 200 napos mozgóátlag stratégia, bár valamivel alacsonyabb összesített profitot eredményezett, stabilabb és hosszabb távú trendeket követ, ami szintén megbízhatóságot mutat. A mozgóátlagok keresztezésén alapuló stratégiák lényege, hogy a rövidebb távú mozgóátlag keresztezése a hosszabb távú mozgóátlaggal erős piaci jelzésként szolgálhat. Ha a rövidebb távú mozgóátlag felülről keresztezi a hosszabb távút („golden cross”), az általában vételi jelzésként értelmezhető, míg az ellenkező irányú keresztezés („death cross”) eladási jelzést ad. Ezek a jelek segítenek a befektetőknek a piaci trendek felismerésében és a megfelelő döntések meghozatalában.

Összességében elmondható, hogy az 50 napos és 200 napos mozgóátlag stratégiák megbízható eszközként szolgálhatnak a kriptovaluta piacokon való befektetések során. Az első hipotézistől eltérően, amely az RSI indikátor önálló hatékonyságára alapozott, a második hipotézis megerősítést nyert, és azt mutatja, hogy a trendek alapján működő mozgóátlag stratégiák hatékonyabb eszközök a befektetők számára a profit maximalizálására. Ezek az eredmények

kiemelik a technikai elemzési eszközök integrált alkalmazásának fontosságát a dinamikus és gyakran volatilis kriptovaluta piacon.

Szakirodalom források:

- Andor György: Üzleti Gazdaságtan. Budapest: Akadémiai Kiadó, 2018. ISBN 978963454 0236
- Bugár Gyöngyi, Somogyvári Márta: Bitcoin: digitális szemfényvesztés, vagy a jövő valutája? 2020. ISSN 1588-6883
- Czeczeli Vivien, Vilonya Martin: A kriptovaluták árfolyamának alakulása eseményelemzés alapján. 2022. ISSN 0031-496X
- Dornfeld László: A kriptovaluták és az e-bizalom kapcsolata kapcsolata. 2022. ISSN 1586-2895
- Györfi András (szakmailag szerk.) (és mások): Kriptopénzek ABC. Budapest: HVG Könyvek, 2019. ISBN 978-963-304-713-2
- Jámbor Gellért: A kriptovaluták megjelenése, elterjedése és a jelenséggel szemben lehetséges jogi válaszlépések. 2023. ISSN 1586-2895
- Liptai Kálmán: Kriptográfia. Eger, 2011
- Simonyi Károly: A fizika kultúrtörténete a kezdetektől a huszadik század végéig. Budapest: Akadémiai Kiadó, 2020. ISBN 9789634544906
- Varga Norbert, Birher Nándor, Knoll-Csete Edit: A kriptovaluták szabályozása – Jogi kihívások és kockázatok. Humán Innovációs Szemle. 2024. ISSN2939-8614

Internetes források:

- https://www.password-depot.de/hu/know-how/blowfish-and-rijndael.htm [megtekintve: 2024.11.04.].
- https://tools.keycdn.com/sha256-online-generator [megtekintve: 2024.11.04.].
- https://hu.wikipedia.org/wiki/Advanced_Encryption_Standard [megtekintve: 2024.11.04.].
- https://ethereum.org/en/what-is-ethereum/ [megtekintve: 2024.11.04.].
- https://kriptomat.io/hu/blockchain/blockchain-tortenete/ [megtekintve: 2024.11.06.].
- https://www.xtb.com/hu/oktatas/a-bitcoin-tortenete [megtekintve: 2024.11.06.].
- https://www.chronicled.com/ [megtekintve: 2024.11.07].
- https://ethereum.org/hu/history/#yellowpaper [megtekintve: 2024.11.07.].

- https://academy.binance.com/hu/glossary/turing-complete [megtekintve: 2024.11.08.].
- https://en.wikipedia.org/wiki/Hashcash [megtekintve: 2024.11.08.].
- *https://nki.gov.hu/wp-content/uploads/2024/03/A-kriptovalutak-veszelyei.pdf* [megtekintve: 2024.11.10.].
- https://tokeportal.com/kozossegi-finanszirozas/ [megtekintve: 2024.11.11.].
- https://academy.binance.com/hu/articles/what-is-an-ico [megtekintve: 2024.11.11.].
- https://www.europarl.europa.eu/news/hu/press-room/20220613IPR32840/cryptocurrencies-in-the-eu-deal-struck-between-parliament-and-council [megtekintve: 2024.11.11.].
- https://www.europarl.europa.eu/topics/hu/article/20220324STO26154/a-kriptovaluta-veszelyei-es-az-unios-jogszabalyok-elonyei [megtekintve: 2024.11.11.].
- *https://www.binance.com/en/about* [megtekintve: 2024.11.15.].
- https://cryptoslate.com/people/ben-zhou/ [megtekintve: 2024.11.15.].
- https://www.bybit.com/en/promo/global/aboutus/ [megtekintve: 2024.11.15.].
- *https://www.coingecko.com/hu/exchanges* [megtekintve: 2024.11.15.].
- https://nav.gov.hu/ado/szja/a-kriptougyletek-jovedelmenek-adozasa#_ftn1 [megtekintve: 2024.11.18.].
- https://kriptomat.io/hu/kriptovalutak/a-kriptovalutak-rovid-tortenete/ [megtekintve: 2024.11.20.].
- https://academy.binance.com/hu/articles/mining-pools-explained [megtekintve: 2024.11.20.].
- https://academy.binance.com/en/articles/proof-of-work-explained [megtekintve: 2024.11.22.].
- https://kriptotarca.hu/proof-of-work-jelentese-hogyan-mukodik-a-pow-konszenzus-mechanizmus/ [megtekintve: 2024.11.23.].
- https://penzmuzeumpedia.hu/proof-of-stake-(pos [megtekintve: 2024.11.23.].
- https://kriptotarca.hu/mining-pool-kriptovaluta-banyaszati-pool-jelentese-es-mukodese-a-gyakorlatban/?utm_ [megtekintve: 2024.11.23.].
- *https://traderklub.hu/forex-es-tozsde-leckek/fibonacci-szintek-es-aranyok/* [megtekintve: 2024.11.28.].
- https://www.tradingview.com/chart/?symbol=BITSTAMP%3ABTCUSD [megtekintve: 2024.11.28.].

Táblázat- és ábrajegyzék:

Táblázatok

1. táblázat Saját szerkesztés, Az SHA-265 kódolás szemléltetése 13
2. táblázat 50 napos mozgóátlag és az árfolyam keresztezések vétele és eladása. 50
3. táblázat 200 napos mozgóátlag és az árfolyam kereszteződésének vétele és eladása. 53
4. táblázat RSI indikátor használata túladott állapotnál vétel és túlvett állapotban eladás 55

Ábrák

1. ábra Az ábrán látható a megbízhatósági pontszám alapján legjobb 5 kriptovaluta-tőzsde. 31
2. ábra Az ábrán látható az ellenállási szintek a Bitcoin árfolyamának. Az árfolyam napi bontásban jelenítettem meg 2015-től 40
3. ábra Fibonacci szintek 1. eset 41
4. ábra Fibonacci szintek 2. eset 42
5. ábra Fibonacci szintek 3. eset 43
6. ábra Fibonacci szintek 4. eset 44
7. ábra Fibonacci szintek 5. eset 45

PANNON EGYETEM

GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI ÖSSZEFOGLALÁS

A dolgozat címe: Kriptodevizák, mint felkapott befektetési eszközosztály	
Hallgató neve: Czene Mátyás Tamás	NEPTUN kód: A6VNT9
Képzési szint: alapképzés	
Szak: Gazdálkodási és menedzsment	Szakirány: Logisztika
Témavezető neve: Dr. Joó István	Beosztása: oktatási dékánhelyettes
Tanszék: Pénzügy és Gazdálkodás	

A szakdolgozat célja a kriptovaluták és a mögöttük álló blokklánc technológia részletes vizsgálata, különös tekintettel azok technikai működésére, befektetési lehetőségeire és gazdasági szerepére. A kriptovaluták az elmúlt évtized egyik legnagyobb innovációját képviselik, amelyek nemcsak a pénzügyi rendszereket formálták át, hanem új lehetőségeket teremtettek a decentralizált adatkezelés és a digitális értékmegőrzés terén is. A dolgozat középpontjában a Bitcoin és más jelentős kriptovaluták állnak, amelyek technológiai fejlődése és befektetési potenciálja globális érdeklődést váltott ki, miközben számos kihívást is felvetett.

A dolgozat első részében részletes bemutatásra kerül a blokklánc technológia, amely a kriptovaluták alapját képezi. A decentralizált hálózatok működésének megértése érdekében a munka tárgyalja a blokklánc adatstruktúráját, a tranzakciók hitelesítésének mechanizmusát, valamint a konszenzus algoritmusokat, különösen a **Proof of Work (PoW)** és a **Proof of Stake (PoS)** mechanizmusokat. Ezek a rendszerek biztosítják a hálózat biztonságát, átláthatóságát és a központi irányítás nélküli működését. A PoW mechanizmus például a bányászat révén teszi lehetővé a blokklánc fenntartását, azonban ennek jelentős energiaigénye környezeti és gazdasági vitákat is generál. A PoS mechanizmus ezzel szemben energiahatékonyabb alternatívát kínál, amely új irányokat nyithat a blokklánc technológia fejlődésében.

A munka kitér a **bányászat** gazdasági szerepére is, különös tekintettel a bányászati pool-ok működésére. A bányászati pool-ok lehetővé teszik, hogy kisebb bányászok egyesítsék erőforrásaikat, így növelve esélyeiket a blokkjutalmak megszerzésére. A központosított pool-ok növekvő dominanciája azonban felveti a hálózat decentralizációjának csökkenését és ezzel összefüggésben a biztonság kérdését is. A dolgozat rávilágít arra, hogy a bányászati infrastruktúra fejlődése és a verseny éleződése hogyan formálja a kriptovaluták gazdasági ökoszisztémáját.

A kutatás második részében a **technikai elemzés** eszközeinek hatékonyságát vizsgáltam a kriptovaluta piacokon. Két fő hipotézis került felállításra és elemzésre:

1. Az RSI indikátor hatékonysága túladott (30-) szintekről történő fordulóknál magasabb profithozamot eredményez, mint a mozgóátlagok keresztezésén alapuló stratégiák.
2. A rövid (50 napos) és hosszú távú (200 napos) mozgóátlagok keresztezései stabil és megbízható profitot biztosíthatnak, különösen Fibonacci-szintek alkalmazásával.

Az eredmények alapján az **RSI indikátor** stratégiájával elért összesített profit (29,331 egység) jelentősen elmaradt mind az 50 napos mozgóátlag (129,679 egység), mind a 200 napos mozgóátlag (104,729 egység) által biztosított profittól. Ez azt mutatja, hogy az RSI indikátor önálló használata kevésbé hatékony a piaci fordulók jelzésében, mivel nem veszi kellőképpen figyelembe a trendek irányát és a piaci momentumot. A mozgóátlag stratégiák, különösen az 50 napos és a 200 napos mozgóátlagok keresztezései, megbízhatóbb és stabilabb profitpotenciált kínáltak a vizsgált időszakban. Ezek a stratégiák hatékonyan alkalmazhatók a trendkövető befektetési döntések meghozatalában, míg a **Fibonacci-szintek** kombinált használata tovább javíthatja a belépési és kilépési pontok pontosságát.

A kutatás eredményei rávilágítanak arra, hogy a technikai elemzési eszközök hatékonysága jelentősen függ a piaci környezettől és az alkalmazott módszerek kombinációjától. A trendkövető stratégiák, mint például a mozgóátlag keresztezések, kiemelkedően hatékonyak a kriptovaluta piacok dinamikájában, míg az RSI indikátor inkább kiegészítő szerepet tölthet be más elemzési eszközökkel együtt. Az eredmények összességében értékes betekintést nyújtanak a kriptovaluták gazdasági és technikai vonatkozásaiba. Egy szélesebb körű adatgyűjtés lehetővé tenné a következtetések pontosítását, és részletesebb képet nyújtana a befektetői magatartásokról, attitűdökről és a technikai stratégiák hosszú távú hatékonyságáról. A szakdolgozat így nemcsak a jelenlegi kriptovaluta piaci trendekre és stratégiákra világít rá, hanem hozzájárul a téma tudományos megértéséhez és gyakorlati alkalmazásához egyaránt.